دورة أساسيات الأمن السيبراني

الوحدة الأولى: الأمن السيبراني

الوحدة الثانية: دراسات تحليلية لأشهر الهجمات السيبرانية

الوحدة الثالثة : فيروسات الفدية

الوحدة الرابعة : الجهود الدولية والوطنية لحماية الأمن السيبراني

الوحدة الخامسة : قواعد الأمن السيبراني في المؤسسات

الوحدة الأولي: الأمن السيبراني

الأهداف التفصيلية للوحدة الأولي:

أن يكون المتدرب في نهاية الوحدة قادرا على:

1- **يوضح العناصر الأساسية للأمن السيبراني**

2- **يُعرِّف الأمن السيبراني**

3- **يذكر الجوانب القانونية لحماية الأمن السيبراني**

4- **يبين عناصر أمن المعلومات**

5- **يعرف أهمية الأمن السيبراني**

6- **يوضح أهداف الأمن السيبراني**

7- **يبين الفرق بين أمن المعلومات والأمن السيبراني**

تشمل الوحدة على المواضيع الفرعية التالية "

1- **الدرس الأول / مفهوم الأمن السيبراني**

2- **الدرس الثاني / التعريف بالأمن السيبراني ومحاوره والحماية القانونية له**

3- **الدرس الثالث / العناصر الأساسية للأمن السيبراني**

4- **الدرس الرابع / الجوانب القانونية لحماية الأمن السيبراني**

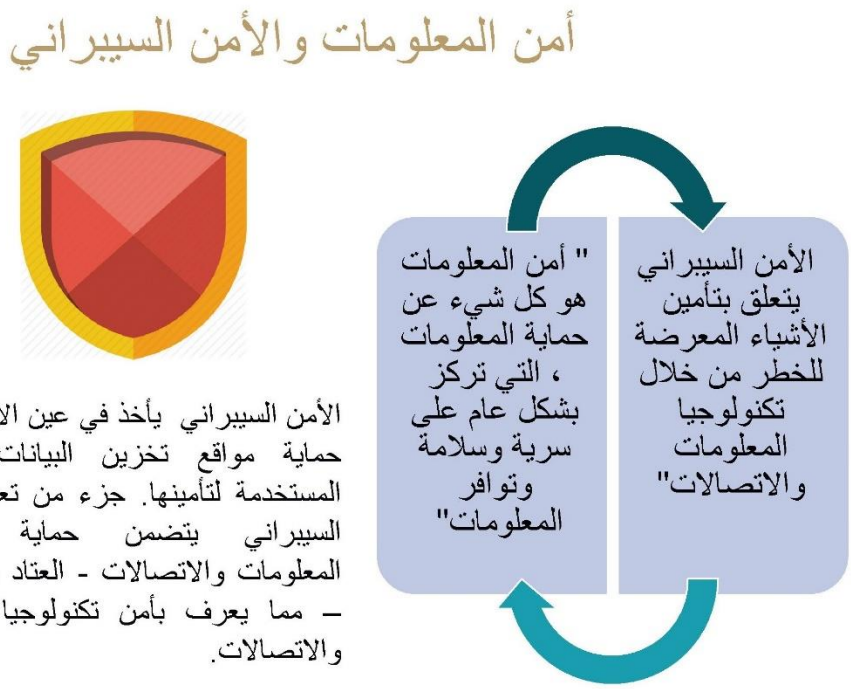
الدرس الأول / مفهوم الأمن السيبراني

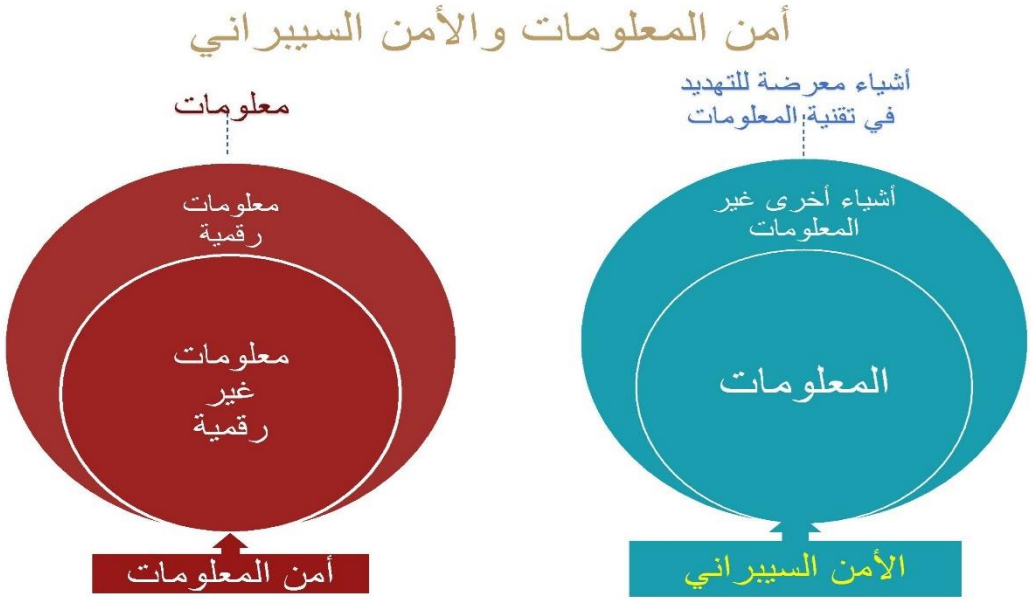
الأمن الإلكتروني

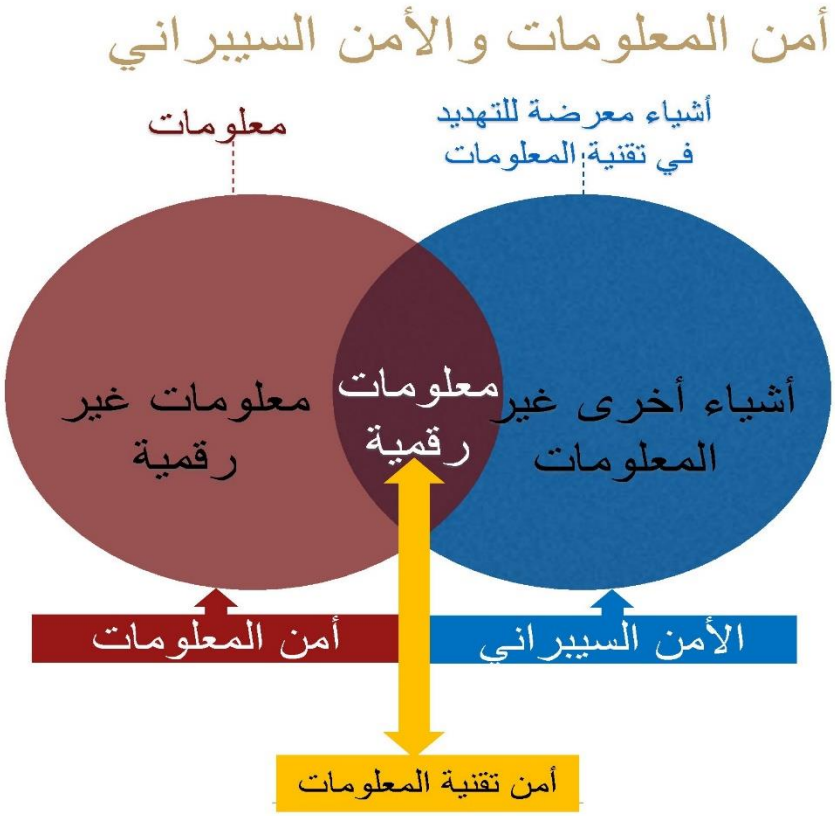
هو ممارسة حماية الشبكات والأجهزة والتطبيقات والأنظمة والبيانات من التهديدات الإلكترونية. الهدف العام هو صد الهجمات التي تحاول الوصول إلى البيانات أو تدميرها، أو ابتزاز الأموال، أو تعطيل العمليات التجارية العادية - سواء كانت تلك الهجمات تأتي من داخل المنظمة أو خارجها.

ما المقصود بالأمن السيبراني؟

الأمن السيبراني هو ممارسة حماية أجهزة الكمبيوتر والشبكات وتطبيقات البرامج والأنظمة الهامة والبيانات من التهديدات الرقمية المحتملة. تتحمل المؤسسات مسؤولية تأمين البيانات للحفاظ على ثقة العملاء والامتثال للمتطلبات التنظيمية. فهي تعتمد تدابير وأدوات الأمن السيبراني من أجل حماية البيانات الحساسة من الوصول غير المصرّح به، وكذلك منع أي انقطاع للعمليات التجارية بسبب نشاط الشبكة غير المرغوب فيه. تطبّق المؤسسات الأمن السيبراني من خلال تبسيط الدفاع الرقمي بين الأفراد والعمليات والتقنيات .



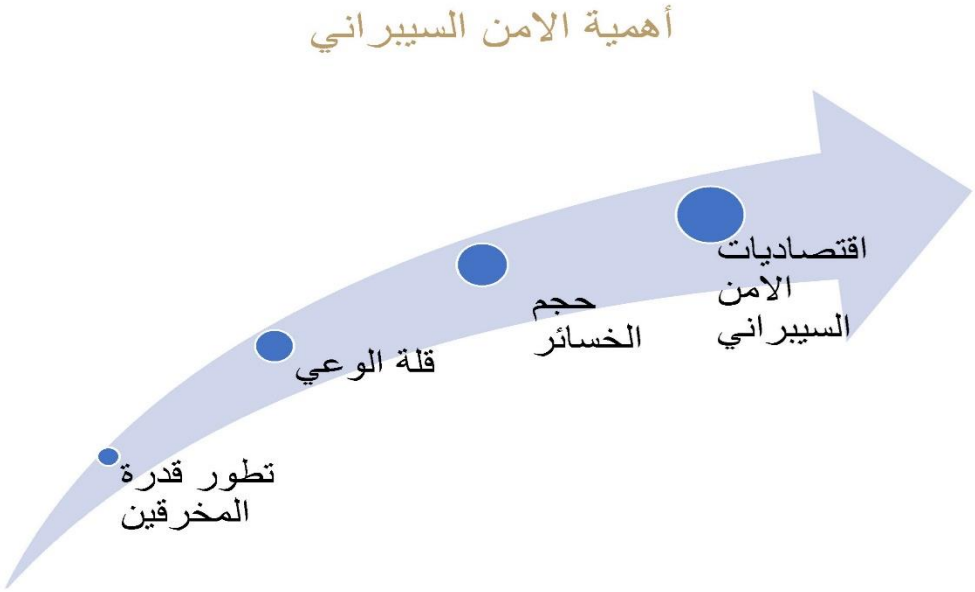

أمن المعلومات والأمن السيبراني
معلومات
معلومات رقمية
معلومات غير رقمية
أمن المعلومات
أشياء معرضة للتهديد في تقنية المعلومات
أشياء أخرى غير المعلومات
المعلومات
الأمن السيبراني


أمن المعلومات والأمن السيبراني
معلومات
أشياء معرضة للتهديد في تقنية المعلومات
معلومات غير رقمية
معلومات رقمية
أشياء أخرى غير المعلومات
أمن المعلومات
الأمن السيبراني
أمن تقنية المعلومات

الدرس الثاني / التعريف بالأمن السيبراني ومحاورة والحماية القانونية له

أهمية الأمن السيبراني

تستخدم الشركات في مختلف القطاعات، مثل الطاقة والنقل وتجارة التجزئة والتصنيع، الأنظمة الرقمية والاتصال عالي السرعة لتوفير خدمة عملاء فعّالة وإجراء عمليات تجارية ميسورة التكلفة. مثلما تؤمّن هذه المؤسسات أصولها المادية، عليها أيضًا تأمين أصولها الرقمية وحماية أنظمتها من أي وصول غير مقصود. إنّ حدث الاختراق والحصول على وصول غير مصرّح به إلى نظام كمبيوتر أو شبكة أو منشآت متصلة يُسمّى "هجومًا سيبرانيًا" إن كان متعمّدًا. يؤدي الهجوم السيبراني الناجح إلى الكشف عن البيانات السرية أو سرقتها أو حذفها أو تغييرها.



تدافع تدابير الأمن السيبراني ضد الهجمات السيبرانية وتوفّر الفوائد التالية:

منع الانتهاكات أو تقليل تكلفة عواقبها

تقلّل المؤسسات التي تطبق استراتيجيات الأمن السيبراني من العواقب غير المرغوب فيها للهجمات السيبرانية التي قد تؤثر في سمعة الشركات، ووضعها المالي، والعمليات التجارية، وثقة العملاء. على سبيل المثال، تفعّل الشركات خطط التعافي من الكوارث لاحتواء التدخلات المحتملة وتقليل مدة تعطيل العمليات التجارية .

ضمان الامتثال للوائح التنظيمية

على الشركات في مجالات ومناطق محددة الامتثال للمتطلبات التنظيمية من أجل حماية البيانات الحساسة من المخاطر السيبرانية المحتملة. على سبيل المثال، على الشركات التي تعمل في أوروبا الامتثال للائحة العامة لحماية البيانات(GDPR) ، التي تتوقع من المؤسسات اتخاذ تدابير الأمن السيبراني المناسبة لضمان خصوصية البيانات .

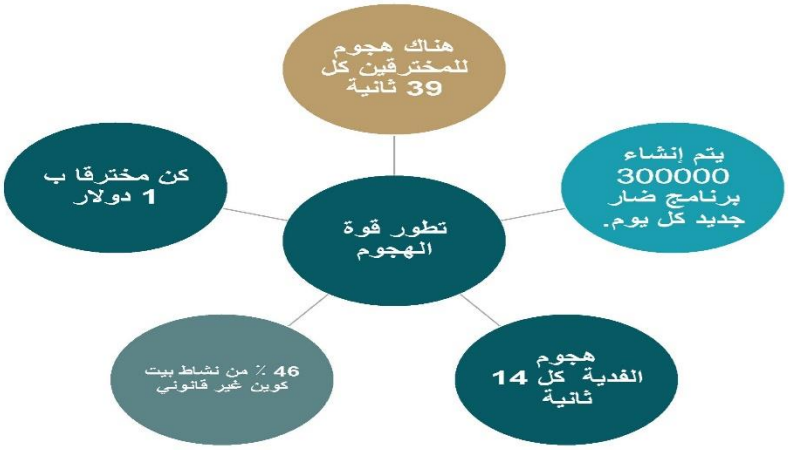
الحدّ من التهديدات السيبرانية المتطوّرة

مع تغيّر التقنيات، تنشأ أشكال جديدة من الهجمات السيبرانية. يستخدم المجرمون أدوات جديدة ويبتكرون استراتيجيات جديدة للوصول إلى النظام بدون إذن. تتبنّى المؤسسات تدابير الأمن السيبراني وتحدّثها لمواكبة تقنيات وأدوات الهجوم الرقمي الجديدة والمتطورة .

وفي العام الماضي، ارتفعت الهجمات الإلكترونية للمؤسسات ارتفاعا كبيرا في الحجم والتعقيد على حد سواء. المجرمون الإلكترونيون مستعدون دائما للاستفادة من الفرص الجديدة. وفقا لمكتب التحقيقات الفيدرالي، قفزت حالات الجرائم الإلكترونية بنسبة تصل إلى 300٪ في وقت مبكر من الوباء في عام 2020. ويرجع هذا الارتفاع جزئيا إلى قيام قراصنة يستهدفون الشركات بالتحول إلى القوى العاملة النائية والمكاتب المنزلية من دون وجود بنية تحتية قوية للأمن السيبراني. كما كان ذلك بسبب الفرص المتاحة لاستغلال الوباء نفسه، بما في ذلك العروض المزيفة للقاحات وحملات التصيد المرتبطة بكوفيد-19.

الهجمات الإلكترونية

هي دائما تقريبا حول الوصول إلى البيانات لتحقيق مكاسب. ويتم تخزين غالبية تلك البيانات في السحابة، ولكن بشكل متزايد يتم تخزينها أيضًا على الأجهزة الشخصية، وأجهزة إنترنت الأشياء(IoT) ، والشبكات والخوادم الخاصة. ويتسارع نمو البيانات بمعدل هائل، ومن المتوقع أن يخزن العالم 200 زيتابايت من البيانات بحلول عام 2025 .ولا يمكن المبالغة في أهمية الأمن السيبراني ووضع نظم قوية لحماية البيانات على رأس أولويات الشركات والحكومات في جميع أنحاء العالم.



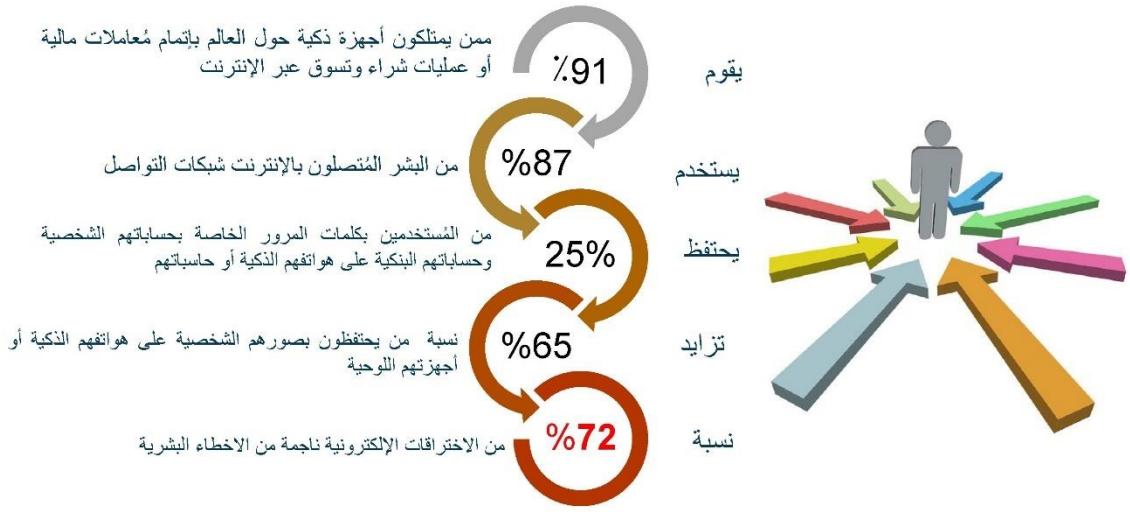
أنواع الهجمات الإلكترونية

وبينما يصبح العالم أكثر اتصالاً واعتماداً على التكنولوجيا، ومع تزايد قيامنا بأعمالنا وحياتنا عبر الإنترنت، فإننا نخلق المزيد من الفرص – وسطح هجوم دائم الاتساع – لمجرمي الإنترنت الذين أصبحت أساليبهم أكثر تطوراً.

وتشمل الأنواع الشائعة من تهديدات الأمن السيبراني ما يلي :

- **هجمات الهندسة الاجتماعية: الهندسة الاجتماعية هي ممارسة التلاعب بالأشخاص في الكشف عن المعلومات الحساسة والسرية لتحقيق مكاسب نقدية أو الوصول إلى البيانات. ويشمل التصيد والتصيد بالرمح ويمكن دمجه مع تهديدات أخرى لإغراء المستخدمين بالنقر على الروابط أو تنزيل البرامج الضارة أو الثقة بمصدر ضار .**
في عام 2020، ما يقرب من ثلث الاختراقات شملت تقنيات الهندسة الاجتماعية، منها 90٪ التصيد .
- **هجمات البرمجيات الخبيثة: البرمجيات الخبيثة تعني البرامج الضارة. وهي تتضمّن مجموعة من البرامج التي تم إنشاؤها من أجل منح أطراف ثالثة إمكانية الوصول غير المصرّح به إلى المعلومات الحساسة أو السماح لها بتعطيل سير العمل العادي للبنية الأساسية بالغة الأهمية. تشمل الأمثلة الشائعة للبرمجيات الخبيثة أحصنة طروادة وبرامج التجسس والفيروسات**
- **البرمجيات الخبيثة: هي برمجيات خبيثة مثل الفيروسات والديدان وبرامج التجسس وبرامج adware التي يمكن أن تصيب أجهزة الكمبيوتر Ransomware .هي البرامج الخبيثة المعروفة التي تصل وتحجب الملفات أو أنظمة لابتزاز دفع الفدية .ومن المتوقع أن تصل تكاليف أضرار الفدية العالمي ة إلى 20 مليار دولار أمريكي بحلول نهاية العام، بعد أن كانت 325 مليون دولار في عام 2015.**
- **برامج الفدية: تشير برامج الفدية إلى نموذج عمل ومجموعة واسعة من التقنيات ذات الصلة التي تستخدمها الجهات المسيئة لابتزاز الأموال من الكيانات. سواء كنت قد بدأت للتو باستخدام AWS أو سبق أن بدأت بالتطوير، فلدينا موارد مخصصة لمساعدتك على حماية أنظمتك الهامة وبياناتك الحساسة من برامج الفدية.**
- **هجوم الوسيط: في هجوم الوسيط، يحاول طرف خارجي الوصول بشكل غير مصرّح به إلى الاتصالات في شبكة أثناء تبادل البيانات. تزيد مثل هذه الهجمات من المخاطر الأمنية للمعلومات الحساسة، مثل البيانات المالية .**
- **التصيد الاحتيالي: هو تهديد سيبراني يستخدم تقنيات الهندسة الاجتماعية من أجل خداع المستخدمين للكشف عن معلومات التعريف الشخصية. على سبيل المثال، يرسل المهاجمون السيبرانيون رسائل إلكترونية تستدرج المستخدمين للنقر عليها وإدخال بيانات بطاقة الائتمان في صفحة ويب وهمية لإتمام الدفع. يمكن أن تؤدي هجمات التصيد الاحتيالي أيضًا إلى تنزيل مرفقات ضارة تثبّت برامج ضارة على أجهزة الشركة.**
- **التهديد الداخلي: هو خطر أمني يسبّبه الأفراد ذوي النوايا السيئة داخل مؤسسة. يمتلك الموظفون وصولاً عالي المستوى إلى أنظمة الكمبيوتر ويمكن أن يزعزعوا استقرار أمن البنية الأساسية من الداخل .**

- **هجمات إنترنت الأشياء: (IoT) هناك الآن أجهزة إنترنت الأشياء أكثر من الناس في العالم، وهي توفر فرصًا متعددة للقراصنة حيث أن هذه الأجهزة عرضة للهجمات من خلال الوسط، وهجمات الحرمان من الخدمة (DoS)، والبرامج الضارة، وهجمات الحرمان من الخدمة الدائمة(PDoS) ، والهجمات الصفري اليوم . ومن المقرر أن يصل سوق إنترنت الأشياء إلى 31 مليار جهاز متصل في عام 2020، وبحلول عام 2025 سيكون هناك حوالي 75 مليار جهاز إنترنت الأشياء.**
- **التهديدات المستمرة المتقدمة (APTs): (APTs) هي هجمات متعددة المراحل حيث يتسلل القراصنة إلى شبكة غير مكتشفة ويبقوا داخلها لفترة طويلة من الوقت للوصول إلى البيانات الحساسة أو تعطيل الخدمات الحرجة. وغالبا ما تهدف إلى الصناعات ذات المعلومات عالية القيمة مثل الدفاع الوطني، والتصنيع، والتمويل .**
- **هجمات(Denial-of-service (DoS: هجمات DoS ، أو هجمات الحرمان من الخدمة الموزعة(DDoS) ، تحدث عندما يغمر المهاجم الخادم أو الشبكة لجعله مؤقتًا أو إلى أجل غير مسمى غير متوفر، عادة عن طريق غمره بحركة المرور حتى لا يتمكن المستخدمون الآخرون من الوصول إليه. ويمكن أن يؤدي هذا التدخل إلى تعطل كامل للأنظمة المتصلة، مما يسبب انقطاعات واسعة النطاق وعواقب مالية كبيرة بسبب وقت التوقف. شهد النصف الأول من عام 2020 زيادة بنسبة 15٪ في هجمات .DDoS تم تسجيل ما يقرب من 4.83 مليون هجوم، مع زيادة 126٪ في هجمات ناقلات 15.**



الاستراتيجية الوطنية للأمن السيبراني

مقدمة

إن وجود بنية فضاء سيبراني وطنية متكاملة وآمنة يعد أحد أهم العوامل الممكنة للنمو والازدهار؛ إلا أن التوسع في استخدام التقنية يفتح آفاقًا جديدة للمخاطر والتهديدات السيبرانية؛ مما يستوجب تعزيز الأمن السيبراني لحماية الشبكات، وأنظمة تقنية المعلومات وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات وحماية ما تقدمه من خدمات وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال وكذلك لتعزيز الربط التقني الآمن بين الخدمات الحكومية ودعم الاقتصاد الرقمي.
وتسعى الهيئة إلى قيادة وتنسيق الجهود الوطنية كجهة تشريعية من خلال تفاعل ومشاركة الجهات الوطنية وتكاملها لتحقيق طموحها ومستهدفاتها.

رؤية الاستراتيجية الوطنية للأمن السيبراني

تم وضع رؤية للاستراتيجية الوطنية للأمن السيبراني تعكس الطموح الاستراتيجي للمملكة وبأسلوب متوازن بين الأمان والثقة والنمو،

وتتضمن الرؤية التي تسعى الهيئة إلى الوصول لها:

فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار

بحيث تكون هذه الرؤية شاملة للفضاء السيبراني بأكمله؛ تلبي أولويات المملكة وتطلعاتها، وتؤكد على تعزيز حماية الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة والقدرة على الصمود والتصدي للحوادث السيبرانية وامتصاص الأضرار والتعافي منها في الوقت المناسب، بالإضافة إلى تعزيز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي، وكذلك المساهمة في النمو الاقتصادي والاجتماعي للمملكة.

وهذه الرؤية تتضمن مصطلحات تم دراستها بعناية:

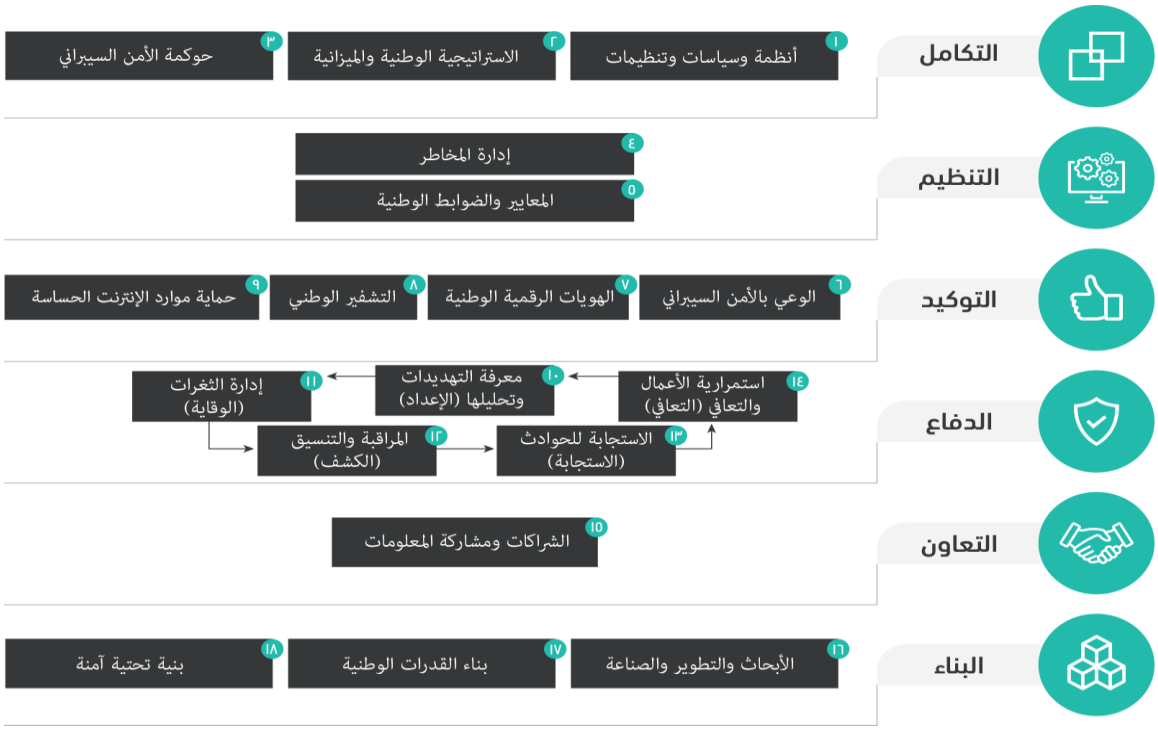
فضاء سيبراني: يشمل الفضاء السيبراني السعودي بأكمله

- **سعودي: لتلبية أولويات المملكة وتطلعاتها**
- **آمن: التأكيد على حماية وصمود الأنظمة التقنية والتشغيلية والبنى التحتية الحساسة**
- **موثوق: يعزز ثقة الجهات الوطنية والمستثمرين والأفراد في الفضاء السيبراني السعودي**
- **يمكّن النمو والازدهار: إسهام حماية الفضاء السيبراني في النمو الاقتصادي والاجتماعي للمملكة**

الإطار المرجعي:

من أجل وضع مرجع عملي للجوانب المختلفة في الأمن السيبراني على المستوى الوطني، حرصت الهيئة على تصميم إطار مرجعي للأمن السيبراني خاص بالمملكة مبني على أفضل الممارسات المحلية والعالمية وأهم المستجدات والتحديات التي تواجه الأمن السيبراني، بحيث يعد نموذجًا متقدمًا يشمل الجوانب المختلفة للأمن السيبراني على مستوى الدول. ويحتوي هذا الإطار على ستة محاور تتضمن ثمانية عشر عنصرًا رئيسيًا من عناصر الأمن السيبراني، ويساعد هذا الإطار على تعميق الفهم لفضاء المملكة السيبراني.

وتم استخدام هذا الإطار لتصميم الاستراتيجية على المستوى الوطني. ويوضح الشكل أدناه الإطار المرجعي:



وتعرف المحاور الستة الرئيسية لهذا الإطار كما يلي:

1- محور "التكامل":

يعنى هذا المحور بتكامل جميع مكونات منظومة الأمن السيبراني، ويحتوي على ثلاثة عناصر هي:

- **أنظمة وسياسات وتنظيمات:** الأطر والآليات اللازمة لإدارة التوجهات الاستراتيجية بالشكل المطلوب، وذلك من خلال الصلاحيات والسياسات والأنظمة والتشريعات اللازمة.
- **الاستراتيجية الوطنية والميزانية:** تطوير ومراجعة التوجهات الاستراتيجية الوطنية للأمن السيبراني، من خلال العمل على إعداد ومراجعة النطاق والأهداف والمبادرات والميزانيات المتوقعة ومؤشرات الأداء لقياس مدى الالتزام بالخطة التنفيذية.

- **حوكمة وإدارة الأمن السيبراني:** إعداد إطار حوكمة يوضح الأدوار والمسؤوليات والصلاحيات للجهات والأفراد المعنين.

2- محور "التنظيم":

يعنى هذا المحور بتحديد البنى التحتية الحساسة وإدارة المخاطر السيبرانية، ويحتوي على عنصرين:

- **إدارة المخاطر السيبرانية:** تقليل المخاطر من التهديدات والثغرات، عن طريق تنفيذ عمليات إدارة المخاطر التي تبدأ بتحديد البنى التحتية الحساسة، وتعريف المخاطر وتقييمها والعمل على تقليلها، انتهاءً بمراقبة المخاطر ورصدها للمساهمة بتعزيز الصمود السيبراني.
- **المعايير والضوابط الوطنية:** توفير نموذج مرجعي للمعايير الوطنية والضوابط السيبرانية، بحيث تعمل على تحديد نطاق الضوابط الأساسية والفرعية، ونوعيتها ومدى شموليتها وكيفية العمل على تنفيذها مع مختلف القطاعات والجهات ذات العلاقة، ووضع الآليات اللازمة للتأكد من التزام الجهات بهذه الضوابط.

3- محور "التوكيد":

يعنى هذا المحور بالتأكد من حماية الفضاء السيبراني، ويحتوي على أربعة عناصر هي:

- **الوعي بالأمن السيبراني:** التوعية في المجال السيبراني على المستوى الوطني عن طريق حملات التوعية والتدريب؛ مما يساهم في تحسين السلوك وتبني أفضل الممارسات وتطبيقها.
- **الهويّات الرقمية الوطنية:** تعزيز جوانب الأمن السيبراني في الهويات الرقمية على المستوى الوطني، مما يساهم في رفع مستوى موثوقية الهويات الرقمية في الفضاء السيبراني للتجارة وتوفير الخدمات الحكومية وغيرها.
- **التشفير الوطني:** الآلية الوطنية لتشفير البيانات وتشمل تطوير وتقييم أنظمة وخوارزميات ومعايير التشفير الوطنية.
- **حماية موارد الإنترنت الحساسة:** عن طريق تعزيز جوانب الأمن السيبراني لحماية موارد الإنترنت الحساسة وتعزيز اعتمادية الإنترنت من جوانب الأمن السيبراني.

4- محور "الدفاع:"

يعنى هذا المحور بمواكبة آليات الدفاع الوطنية السيبرانية للمخاطر والتهديدات المتسارعة، ويحتوي على خمسة عناصر هي:

- **معرفة التهديدات وتحليلها:** رصد التهديدات السيبرانية ومشاركتها مع الجهات ذات العلاقة من القطاعين العام والخاص.
- **إدارة الثغرات:** تشمل العمل بشكل مشترك مع الأفراد والجهات ذات العلاقة؛ للبحث عن أي ثغرات يمكن استغلالها ومشاركة التوصيات مع الجهات المتأثرة لاتخاذ الإجراءات المناسبة.
- **المراقبة والتنسيق:** تعزيز مستوى الدراية الأمنية وتصنيف التهديدات واختبار خطط الاستجابة للحوادث على هجمات محددة ومن ثم احتواءها في حال حدوثها قبل أن تتسبب بأضرار كبيرة.
- **الاستجابة للحوادث:** آليات الاستجابة للحوادث واختبار خططها على هجمات محددة لخلق تحسينات مستمرة للتكيف مع التهديدات والمخاطر السيبرانية، ويتم تنسيق الأنشطة على المستوى الوطني لاحتواء الهجمات السيبرانية وتقليل أضرارها والحد من تكرارها.
- **استمرارية الأعمال والتعافي:** يشمل هذا العنصر التأكد من وجود خطط للطوارئ واختبار البنى التحتية الحساسة والخدمات الإلكترونية الهامة، وكذلك إجراءات محددة لاستعادة عملها بعد الحوادث السيبرانية، والعمل باستمرار على إجراء هذه الاختبارات للتحقق من سلامة البنى التحتية الحساسة والخدمات الهامة، وجاهزيتها مستقبلًا.

5- محور "التعاون:"

يعنى هذا المحور بوضع الآليات المناسبة لبناء الشراكات ومشاركة المعلومات، ويحتوي على:

- **الشراكات ومشاركة المعلومات:** يمكّن من وضع السياسات والآليات وأفضل الممارسات التي تتيح مشاركة المعلومات المتعلقة بالتهديدات السيبرانية مع الجهات الوطنية والدولية، وكذلك المساعدة في التنسيق والتعاون مما يسهم في رفع الجاهزية والاستعداد والوقاية وسرعة الاستجابة في حالة وقوع حادث سيبراني.

6- محور "البناء:"

يعنى هذا المحور بالتأكد من وجود قاعدة وطنية متينة وآمنة، ويحتوي على ثلاثة عناصر كالتالي:

- **الأبحاث والتطوير والصناعة:** تشجيع الأبحاث في مجال الأمن السيبراني وفقًا لأولويات مشتركة على المستوى الوطني، ودعم الابتكار والاستثمار في مجال الأمن السيبراني لتحويل مخرجات الأبحاث والتطوير إلى منتجات وخدمات. كما يشمل تحفيز صناعة الأمن السيبراني لضمان بناء قدرات كافية.

- **بناء القدرات الوطنية:** يشمل هذا العنصر إعداد وتأهيل كوادر وطنية متخصصة في الأمن السيبراني وتطوير تلك الكوادر بالمحافظة عليها؛ وذلك لسد الاحتياج الوطني في هذا المجال من خلال برامج تعليم وتدريب عالية الجودة.
- **بنية تحتية آمنة:** العمل على تبني نهج استباقي لضمان أمن الأنظمة والأجهزة والخدمات عبر سلسلة التوريد بأكملها، بدءًا من التصميم حتى الإنتاج ومن ثم التشغيل وانتهاءً بالإتلاف، وتطوير آليات ومعايير للتقييم والاختبار والفسح لمعدات وبرامج وخدمات الأمن السيبراني؛ للتأكد من سلامتها واستعدادها.

الأهداف الاستراتيجية:

للوصول إلى فضاء سيبراني سعودي آمن وموثوق يمكّن النمو والازدهار، سوف تحقق الاستراتيجية الوطنية للأمن السيبراني ستة أهداف رئيسية كما يلي:

1. حوكمة متكاملة للأمن السيبراني على المستوى الوطني

من أجل ضمان تحقيق درجات عالية من التنسيق والمواءمة، من المهم تبني توجه وطني شامل للأمن السيبراني، وذلك من خلال تكامل وتحديد أدوار ومسؤوليات الجهات ذات العلاقة بالأمن السيبراني على المستوى الوطني لأجل تطوير التنظيمات والسياسات وتنفيذها، ومتابعة الالتزام بالمعايير الوطنية في جميع جوانب الأمن السيبراني. بالإضافة إلى وجود آليات موحدة للتخطيط والميزانية، وترتيب الأولويات في مجال الأمن السيبراني بفعالية مما يعزز رفع كفاءة الإنفاق.

2. إدارة فعّالة للمخاطر السيبرانية على المستوى الوطني

إدارة المخاطر السيبرانية على مستوى الجهات والقطاعات وعلى المستوى الوطني، وتحديد العناصر المتضررة في الفضاء السيبراني ومدى حدّة الضرر، واختيار أفضل الطرق لمعالجتها أو الحد من آثارها. بالإضافة إلى تحديد إجراءات الحماية والدفاع حسب درجة المخاطر.

3. حماية الفضاء السيبراني

إن وجود ضوابط شاملة ومعايير وطنية ونظام لمتابعة الالتزام يحقق حماية منظومة الأمن السيبراني، بالإضافة إلى رفع مستوى وعي المجتمع بالأمن السيبراني واستمرار وتعزيز التواصل معه من خلال حملات توعوية إعلامية عامة للأفراد والجهات، مما يحقق النضج والتطبيق لضوابط الأمن السيبراني على مستوى الافراد والقطاعات والجهات الوطنية.

4. تعزيز القدرات الفنية الوطنية في الدفاع ضد التهديدات السيبرانية

التعزيز والتطوير المستمر للقدرات الوطنية في الدفاع ضد التهديدات السيبرانية، وذلك لكشف الهجمات والتهديدات السيبرانية، والتعامل معها، والاستجابة والتعافي منها في حال الإصابة بها – لا قدر الله-.

5. تعزيز الشراكات والتعاون في الأمن السيبراني

يتطلب الأمن السيبراني وجود شراكات محلية ودولية فعالة، ومعززة بآليات متطورة لمشاركة المعلومات؛ إذ تمكّن من التطوير والتحسين المستمر ومشاركة أفضل الممارسات والمعلومات الاستقصائية والتدابير اللازمة، بالإضافة إلى أهميتها العالية لمواكبة التهديدات، والحد من المخاطر. وللوصول للدرجة المرجوة من التعاون، ويساهم تعزيز الشراكات وبناء قنوات لمشاركة المعلومات داخل المملكة وخارجها، في مشاركة المعلومات المتعلقة بالأمن السيبراني.

6. بناء القدرات البشرية الوطنية وتطوير صناعة الأمن السيبراني في المملكة

حماية الفضاء السيبراني للمملكة تتطلب وجود قاعدة قوية من الكوادر الوطنية المؤهلة في هذا المجال بالإضافة لصناعة أمن سيبراني وطنية مزدهرة، ومن التوجهات الرئيسية بناء القدرات الوطنية في الأمن السيبراني من خلال برامج تعليم وتدريب عالية الجودة، بالإضافة لبرامج تحفز وتدعم الصناعة والبحث والتطوير والابتكار والاستثمار في الأمن السيبراني لتمكين النمو والازدهار.

الخطة التنفيذية

تهدف إلى تحقيق أثر وطني ملموس على المدى البعيد ومكاسب سريعة على المدى القصير من خلال العمل على ثلاث مسارات متوازية، وقد تم تحديد ثلاث مساراتٍ رئيسية، تشمل عددًا من المبادرات والمشاريع الوطنية.

مسارات تنفيذ الاستراتيجية

المسار الأول	المسار الثاني	المسار الثالث
مشاريع العائدات المرتفعة	برنامج دعم الجهات الوطنية	المـبادرات الوطنـية

الدرس الثالث / العناصر الأساسية للأمن السيبراني

كيف يعمل الأمن السيبراني؟

ولا يوجد حل واحد يناسب جميع المؤسسات في مجال الأمن السيبراني .وبدلاً من ذلك، تعمل طبقات متعددة من الحماية معًا للحماية من تعطيل العمليات والوصول إلى المعلومات أو تغييرها أو تدميرها أو الاحتفاظ بها للحصول على فدية. ويجب أن تتطور تلك الحماية باستمرار لمواجهة التهديدات السيبرانية الناشئة بصورة استباقية. يمكن دمج حلول متعددة لخلق دفاع موحد ضد الهجمات الإلكترونية المحتملة.

أمان التطبيق

يركز أمان التطبيق على تحسين الأمان عندما تكون التطبيقات في مرحلة التطوير وبمجرد نشرها. وتشمل أنواع أمن التطبيقات برامج مكافحة الفيروسات والجدران النارية وبرامج التشفير .

أمان السحابة

إن الترحيل المستمر إلى السحب الخاصة والعامة والهجينة يعني أنه يجب على موفري الخدمات السحابية الاستمرار في تحديد أولويات تطبيق أمان سحابي قوي ومحدث لحماية الأنظمة والبيانات والتوفر. يتضمن الأمان السحابي تصنيف البيانات ومنع فقدان البيانات والتشفير والمزيد.

أمان إنترنت الأشياء

ومع انتشار إنترنت الأشياء، هناك أيضا انتشار للمخاطر. في حين أن أمن إنترنت الأشياء يختلف باختلاف الجهاز وتطبيقه، فإن بناء الأمن في الأجهزة، وضمان الترقيات الآمنة والتكامل الآمن، والحماية من البرامج الخبيثة هي بعض أفضل الممارسات المتعلقة بأمن إنترنت الأشياء.

أمان البنية الأساسية الحيوية

إن الأنظمة الحيوية السيبرانية المادية التي تعتمد عليها مجتمعاتنا – بما في ذلك شبكات الكهرباء وأنظمة المياه وخدمات الصحة العامة – معرضة لمخاطر مختلفة. يتم نشر أمن البنية التحتية الحرجة لحماية هذه الأنظمة من الكوارث الطبيعية والهجمات المادية والهجمات الإلكترونية .

أمان الشبكة

أمن الشبكة هو مزيج من حلول الأجهزة والبرمجيات التي تحمي من الوصول غير المصرح به إلى الشبكة، والتي يمكن أن تؤدي إلى اعتراض المعلومات أو تغييرها أو سرقتها. تتضمن أنواع أمان الشبكة عمليات تسجيل الدخول وكلمات المرور وأمان التطبيق.

أمان نقطة النهاية

نقاط النهاية أو أجهزة المستخدم النهائي - بما في ذلك أجهزة الكمبيوتر المكتبية والحواسيب المحمولة والأنظمة اللاسلكية والأجهزة المحمولة - كلها نقاط دخول للتهديدات. ويشمل أمان نقطة النهاية حماية مكافحة الفيروسات والبرامج الضارة، وأمن إنترنت الأشياء، وأمن السحابة .

أمن المعلومات

أمن المعلومات، أوInfoSec ، يركز على الحفاظ على سرية وسلامة وتوافر جميع البيانات الرقمية والتناظرية للمؤسسة. هناك العديد من أنواع أمن المعلومات، بما في ذلك أمن التطبيقات، والتشفير، والتعافي من الكوارث. الأمن السيبراني يمكن أن ينظر إليه على أنه مجموعة فرعية من أمن المعلومات؛ وكلاهما يركز على أمن البيانات، ولكن InfoSecلها نطاق أوسع.

منع فقدان البيانات

تركز الوقاية من فقدان البيانات، أوDLP ، على إيقاف البيانات الحساسة من مغادرة المنظمة - سواء تم تسريبها عن قصد أو مشاركتها عن غير قصد. وتشمل تقنيات DLP التي تتبع، وتحديد، ومنع تدفق المعلومات غير المصرح به التصنيف، والتشفير، والمراقبة، وإنفاذ السياسة .

إدارة الهوية والوصول(IAM)

تساعد أنظمة إدارة الهوية والوصول - بما فى ذلك المصادقة ثنائية العوامل والمصادقة متعددة العوامل وإدارة الوصول المتميزة والقياسات الحيوية - المؤسسات على التحكم في وصول المستخدمين إلى المعلومات والأنظمة المهمة في مكان العمل وفي السحابة.

إدارة معلومات الأمان والأحداث(SIEM)

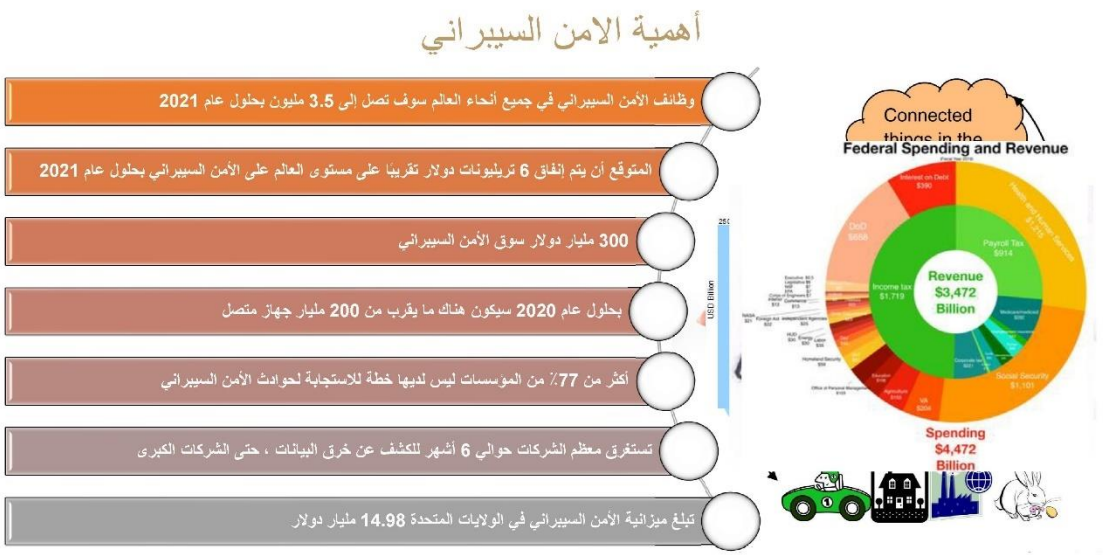
وتقوم حلول SIEM الحديثة بمراقبة وتحليل البيانات والأحداث الأمنية في الوقت الحقيقي، مما يساعد المؤسسات على اكتشاف التهديدات الإلكترونية والاستجابة لها قبل أن تتاح لها فرصة لتعطيل العمليات التجارية. باستخدام الذكاء الاصطناعي (AI) وتدريب الآلة، تقدم SIEM تحليلات سلوك المستخدمين والكيانات المتقدمة (UEBA) للبقاء على قمة التهديدات دائمة التطور .

التدريب على التوعية بالأمن السيبراني

يعتبر المستخدمون النهائيون خط الدفاع الأول ضد الهجمات الإلكترونية وأضعف حلقة في سلسلة الأمن السيبراني، وهذا هو سبب بقاء التصيد مثل هذا التهديد السيبراني السائد. تشير التقديرات إلى أن السلوك البشري يسبب ما يصل إلى 90٪ من الهجمات الإلكترونية، لذلك فإن تثقيف المستخدمين النهائيين باستمرار بشأن مبادرات الأمن السيبراني لدعمهم في اتخاذ خيارات ذكية للدفاع الإلكتروني أمر بالغ الأهمية. وما دام الناس يسقطون لسكات التصيد، واستخدام كلمات مرور ضعيفة، والعمل على شبكات غير مؤمنة، فإنهم منفتحون على الاستغلال. ومع استمرار العمل عن بعد خلال الجائحة وتبدو القوى العاملة المختلطة هي القاعدة في المستقبل، فإن العاملين عن بعد سيظلون مستهدفين من قبل الجهات الفاعلة السيئة.

إطار عمل الأمن السيبراني للمؤسسة

يتضمن إطار الأمن السيبراني الخاص بالمعهد الوطني للمعايير والتكنولوجيا (NIST) خمس ركائز تقدم لمنظمات القطاع الخاص إرشادات حول أفضل الممارسات لإدارة المخاطر الإلكترونية وبناء إطار قوي للأمن السيبراني. ويمكن للمنظمات أن تضع نهجاً استباقياً للأمن السيبراني من خلال وضع هذه الركائز لتلعب بشكل مستمر ومتزامن.



الأركان هي :

الركائز الخمس لإطار أمن الفضاء الحاسوبي

1. **تحديد** : هذه الركيزة التأسيسية تتعلق بتطوير فهم كامل لأصولك والمخاطر التي تتعرض لها حتى تتمكن من وضع السياسات والإجراءات اللازمة لإدارة تلك المخاطر.
2. **الحماية** : يركز هذا الركيزة الثانية على وضع الضمانات المناسبة لحماية منظمتك من حدث الأمن السيبراني.
3. **الكشف** : يقع تنفيذ تدابير لتحديد أحداث الأمن السيبراني، بما في ذلك الرصد المستمر، في صميم ركيزة الكشف .
4. **الاستجابة** : بمجرد اكتشاف حدث ما، فإن وجود خطة للاستجابة السريعة والمناسبة واحتواء التأثير هو دعامة أساسية لإطار عمل المعهد الوطني لتكنولوجيا المعلومات والاتصالات.
5. **الاستعادة** : إن القدرة على استعادة القدرات والخدمات بعد هجوم الأمن السيبراني هو جزء مما يجعل من مرونة الأعمال وهو أمر بالغ الأهمية مثل الاستجابة السريعة للهجمات .

مستقبل الأمن السيبراني

ويتطور كل عنصر من عناصر الأمن السيبراني. وتبرز أهداف جديدة جنبا إلى جنب مع التكنولوجيات الجديدة. المجرمون الإلكترونيون يبتكرون باستمرار نوع وشدة هجماتهم – ويتصاعد تأثير هذه الهجمات. الأدوات التي يمكن أن تساعد في تحسين الأمن السيبراني - مثل شبكات الذكاء الاصطناعي و 5 - G هي نعمة لخبراء الأمن السيبراني والمجرمين الإلكترونيين على حد سواء. في حين أن طبيعة التهديدات المستقبلية يصعب تثبيتها، إلا أنه من الواضح أن مستقبل الأمن السيبراني يحتاج إلى أن يكون استباقيًا حتى يتمكن من التكيف والتكيف مع التهديدات المتطورة والناشئة .

الذكاء الاصطناعي والأمن السيبراني

الذكاء الاصطناعي (AI) هو جزء لا يتجزأ من مستقبل الأمن السيبراني سواء كسلاح للقراصنة أو كأداة للخبراء لمعالجة نقاط الضعف والكشف عن القضايا وصد الهجمات. إن قدرة الذكاء الاصطناعي على مراجعة البيانات الضخمة بسرعة واستخدام تعلم الآلة لتحليل أنماط المستخدم وتحديثها وتعلمها يجعلها أداة ممتازة للتنبؤ بهجمات جديدة والكشف عن السلوك الخبيث المحتمل في الوقت الفعلي. في حين أن أساليب الأمن السيبراني التقليدية تركز على حماية الدفاعات الخارجية لصد الهجوم، يمكن لبرامج الأمن السيبراني الذكاء الاصطناعي المضمنة تعزيز الدفاعات الداخلية .

5G والأمن السيبراني

5G ، الجيل الخامس من التكنولوجيا اللاسلكية، يعد بمزيد من السرعة، والمزيد من الاتصال، وأكثر موثوقية، ودعم تدابير الأمن السيبراني القوية بشكل متزايد. ومع ذلك، مع زيادة عرض النطاق الترددي يأتي المزيد من طرق الهجوم، بما في ذلك نقاط النهاية الأكثر ضعفا. وللتقليل إلى أدنى حد من المخاطر التي تشكلها مجموعة 5 جي، سيحتاج مجتمع الأمن السيبراني إلى تحديد مواطن الضعف والضعف ومن ثم وضع التدابير المضادة للأجهزة والبرمجيات موضع التنفيذ.

برامج ضارة بدون ملفات

تتزايد هجمات البرمجيات الخبيثة بلا ملفات - وهي واحدة من أكبر التهديدات الرقمية للشركات اليوم، ويرجع ذلك جزئيًا إلى صعوبة اكتشافها. تستخدم البرمجيات الخبيثة الخالية من الملفات البرامج والأدوات الخاصة بالشركة لتنفيذ الأنشطة الخبيثة، بدلاً من استخدام أطر هجومها الخاصة أو تثبيت البرامج الضارة على محركات الأقراص الصلبة. هذا النمط من الهجوم "المعيشة خارج الأرض (LotL) "لا يولد ملفات جديدة، لذلك يتهرب من الكشف عن طريق حلول الأمن السيبراني التي تبحث عن مرفقات الملفات الخبيثة أو تتبع إنشاء الملفات.

الأعماق

إن التعقيم هو تهديد ناشئ مقنع يمكن أن يغذي الأخبار المزيفة والتضليل بشكل كبير بالإضافة إلى هجمات الهندسة الاجتماعية. على كل حال، إذا رأيت أو سمعت مديرك يخبرك بالقيام بشيء ما، فمن المرجح أن تتبع أوامرهم، مهما بدت غير عادية. ويمكن لتثقيف المستخدم النهائي المستمر حول مصادر الثقة أن يساعد في مكافحة التضاريس العميقة، وستكون حلول الأمن السيبراني بخوارزميات الذكاء الاصطناعي المصممة للكشف عن عمليات التعقيم العميقة دفاعًا حاسمًا ضدها .

ما هي مكونات استراتيجية الأمن السيبراني؟

تتطلب استراتيجية الأمن السيبراني القوية اتباع نهج مُنسّق يشمل أفراد المؤسسة وعملياتها وتقنياتها.

الأفراد

معظم الموظفين غير مدركين لأحدث التهديدات وأفضل ممارسات الأمان التي تساعد على حماية أجهزتهم وشبكاتهم وخادمهم. إن تدريب الموظفين وإعلامهم بمبادئ الأمن السيبراني يقلل من مخاطر الرقابة التي قد تؤدي إلى حوادث غير مرغوب فيها.

العملية

يطوّر فريق أمن تكنولوجيا المعلومات إطار عمل أمني قوي لضمان المراقبة المستمرة والإبلاغ عن نقاط الضعف المعروفة في البنية الأساسية الحاسوبية للمؤسسة. إطار العمل هو خطة تكتيكية تضمن استجابة المؤسسة وتعافيها فوريًا من الحوادث الأمنية المحتملة .

التكنولوجيا

تستخدم المؤسسات تقنيات الأمن السيبراني لحماية الأجهزة والخوادم والشبكات والبيانات المتصلة من التهديدات المحتملة. على سبيل المثال، تستخدم الشركات جدران الحماية وبرامج مكافحة الفيروسات وبرامج الكشف عن البرامج الضارة وفلترة نظام أسماء النطاقات (DNS) من أجل اكتشاف الوصول غير المصرّح به إلى النظام الداخلي تلقائيًا، ومنعه. تستخدم بعض المؤسسات التقنيات التي تعمل على أمان انعدام الثقة لتعزيز الأمن السيبراني بشكل أكبر .

ما هي تقنيات الأمن السيبراني الحديثة؟

هذه هي تقنيات الأمن السيبراني الحديثة التي تساعد المؤسسات على تأمين بياناتها .

انعدام الثقة

انعدام الثقة هي أحد مبادئ الأمن السيبراني الذي يَفترض عدم الوثوق بأي تطبيقات أو مستخدمين تلقائيًا، حتى في حالة استضافتهم داخل المؤسسة. بدلاً من ذلك، يفترض نموذج انعدام الثقة أنّ عنصر التحكم في الوصول هو الأقل امتيازًا، ما يتطلب مصادقة صارمة من السلطات المعنية ومراقبة مستمرة للتطبيقات .تستخدم AWS مبادئ انعدام الثقة لمصادقة كل طلب فردي لواجهة برمجة التطبيقات (API) والتحقق منه .

تحليلات السلوك

تراقب تحليلات السلوك عملية نقل البيانات من الأجهزة والشبكات لاكتشاف الأنشطة المشبوهة والأنماط غير المعتادة. على سبيل المثال، يتم تنبيه فريق أمن تكنولوجيا المعلومات بحدوث ارتفاع مفاجئ في نقل البيانات أو بتنزيل ملفات مشبوهة إلى أجهزة معينة.

نظام كشف التسلل

تستخدم المؤسسات أنظمة كشف التسلل لتحديد الهجوم السيبراني والاستجابة له بسرعة. تستخدم حلول الأمان الحديثة تقنية تعلّم الآلة وتحليلات البيانات بهدف الكشف عن التهديدات الخاملة في البنية الأساسية الحاسوبية للمؤسسة. تحدّد آلية الدفاع ضد التسلل أيضًا مسارًا للبيانات في حالة وقوع حادث، ما يساعد فريق الأمن على اكتشاف مصدر الحادث .

التشفير السحابي

يعمل التشفير السحابي على تشفير البيانات قبل تخزينها في قواعد البيانات السحابية. هذا يمنع الأطراف غير المصرّح لها من إساءة استخدام البيانات في انتهاكات محتملة. تستخدم المؤسسات خدمة إدارة مفاتيح التشفير من AWS (AWS KMS)للتحكم في تشفير البيانات في أعباء عمل.AWS

خصائص الأمن السيبراني:

للأمن السيبراني مجموعة من الخصائص التي تميزه عن غيره من المجالات، أهمها هم:

1- الثقة وعدم الثقة:

يمتلك جدار الحماية الخاص بنظام الأمن السيبراني بما يشبه مرشح إلكتروني لنوع وطبيعة البرامج والتقنيات المسموح بتفعيلها، بحيث يسمح بمرور البرامج التي بالفعل تمتلك الثقة من المستخدم وكذلك المتجر الإلكتروني وتم التأكد من أمان استخدامها، ومنع البرامج الخبيثة. من التطفل أو استغلال الثغرات

يمكن ترجمة فلسفة أمن المعلومات في هذه النقطة كون الأمن السيبراني يتعامل مع كافة البرامج كونها برامج غير جديرة بالثقة، حتى يتم السماح لها من قبل المستخدم والتأكد من أمانها من خلال مصداقيتها في المتاجر الإلكتروني، فيسمح بمرور ما تم التأكد من سلامته، ويمنع المصادر المجهولة من اختراق النظام.

2- الحماية من التهديدات الداخلية:

واحدة من أهم خصائص الأمن السيبراني هو حماية الجهاز من التهديدات الداخلية والتي قد تتم بناء على قلة ثقافة المستخدم أو جهله بمجال أمن المعلومات وفيه قد يقوم بالسماح ببرامج مجهولة المصدر أن يتم تفعيلها أو أن يقوم باستخدام أدوات تمس أمنه الشخصي أو حساسية مشاركة ما يملكه من معلومات، أو تحتوي إحدى الأدوات التي يقوم باستخدامها بفيروس خبيث لا يجب أن يحتوي نظامه عليه، حينها يقوم الأمن السيبراني بسرعة تنبيه الفرد أو المؤسسة بالخطر التي تواجهه ويقوم بمنع حدوث هذا الإجراء في أسرع وقت.

3- الحماية من التهديدات الخارجية:

تمثل خاصية الحماية من التهديدات الخارجية أهم صفات الأمن السيبراني، حيث يتم فيها بناء جدار الحماية قادر على تصفية المخاطر الخارجية التي يسفر عنها التعامل مع العالم الرقمي، بداية من مخاطر الرسائل الإلكترونية الخطرة أو الروابط الخبيثة أو الفيروسات أو معالجة الضعف في النظام أو الثغرات التي قد يستغلها طرف ثالث في السيطرة والتحكم.

4- رؤية شاملة:

تقوم الادوات الخاصة بالأمن السيبراني على منح مستخدميها-أفراد كان أو شركات-رؤية شاملة على ما يحتويه أنظمتهم من نقاط قوة وضعف، بحيث يمكنهم معرفة الثغرات التكنولوجية والعمل على حلها بأسرع وقت، مع منحهم اقتراحات تخص الطريقة المثالية لمنع تكراره مرة أخرى.

5- مراقبة مستمرة:

يقوم الأمن السيبراني على خاصية المراقبة المستمرة، حيث لا تقوم جدار الحماية الخاص به بالعمل لمرة واحدة أو في ساعات معينة، بل النظام يعمل طوال الوقت بهدف اكتشاف أي خلل بمجرد وجوده والعمل على سرعة إصلاحه ومنعه من إحداث أي ضرر والحفاظ على أمن المعلومات والأمن الخاص بالمستخدم لأطول فترة ممكنة.

6- الامتثال للسياسات والقوانين:

الهدف من الأمن السيبراني في المقام الأول هو الحفاظ على سرية وخصوصية البيانات والمعلومات، بالإضافة إلى مكافحة الفيروسات الضارة بجميع أنواعه، ولكي يتم تحقيق هذا الهدف بفعالية لا يجب أن يتم استغلال الصلاحيات التي تمنح لمحترفيه في سبيل اختراق القاعدة التي من أساسها تم إنشائه.

لذلك تعد خاصية الامتثال للقوانين والسياسات التشريعية الخاصة بأمن المعلومات واحدة من أهم خصائص الأمن السيبراني، حيث لا يتاح لمصادر خارجية الاطلاع عما يتم مشاركته من معلومات وبيانات حساسة، أو إساءة استغلالها بأي صورة ممكنة، وتتنوع هذه القوانين طبقًا لنوع وطبيعة المجال الذي يتم فيه تطبيق الحماية السيبرانية.

7- التنوع:

يجب أن يمتلك النظام الخاص بالأمن السيبراني حلول مجمعة تتعلق بالتعامل مع التهديدات السيبرانية، بحيث لا يكون النظام مفعل للحماية من نوع معين من التهديدات والسماح بأخر، بل عليه أن يحلل ويكتشف ويتعامل ويمنع كل أنواع الهجمات الممكنة والتي تشكل تهديدًا على سلامة وأمن المعلومات.

مكونات وهيكلية الضوابط الأساسية للأمن السيبراني

المكونات الأساسية

يوضح الشكل ١ أدناه المكونات الأساسية للضوابط.

شكل ١: المكونات الأساسية للضوابط

نموذج لتهديد سيبراني أدى إلى الوفاة

في خريف 2020، تمكن فيروس الفدية الشهير من السيطرة على النظام التكنولوجي المتحكم في عيادة جامعية في ألمانيا، وعندما عان الدكاترة والأطباء من التواصل مع بعضهم البعض أو معرفة تاريخ سجلات المرضى يتعاملوا معهم بالطريقة الصحيحة، لاقت امرأة ما حتفها.

هذه الحادثة تمت بسبب اضطرار الممرضين بنقلها إلى مكان آخر جراء عدم توافر دكاترة كافية لتغطية التعامل مع هذه الأزمة. وهو ما أدى بدوره إلى تدهور الحالة ووفاتها، وكل هذا بسبب إهمال في أساليب الحماية الرقمية الخاصة بأنظمة العيادة، بالإضافة إلى جهل الضحايا بالثقافة التكنولوجية المطلوبة.

إذن عندما يخبرك خبير تقني أن البيانات التي تمتلكها يجب حمايتها بكل الصور، وتهز أنت رأسك دون اكتراث معللًا إنك لست برئيس وزراء أو شخصية هامة لكل هذا التحفظ، فلا تستعجب أن تكون أنت طرفًا وسيطًا لعملية قتل إلكترونية أخرى أو وسيلة سهلة لابتزاز شخصًا ما أو السيطرة على امواله او السيطرة على حياتك أنت شخصيًا.

في النهاية، عالم الأمن السيبراني كبير ومليء بالتهديدات المختلفة، ومهما نجح مختصو الحماية من تجديد الدفاعات وعلاج الثغرات التقنية، إلا إن أكبر نقاط الضعف تتمثل في الاعتماد على الثغرة البشرية، وهي نقطة لن يتم حلها إلا بالتثقيف التكنولوجي المستمر المتمثل في ثقافة حماية المعلومات، فإذا كنت تخشى أن تكون ضحية جديدة من ضحايا اختراق الأمن السيبراني، فيجب عليك البدء في تثقيف نفسك من الآن، وإذا لم تعرف الطريقة الصحيحة لذلك، فإليك كورس الأمن السيبراني المتخصص والمقدم على أكاديمية اعمل بيزنس المحترفة.

الدرس الرابع / الجوانب القانونية لحماية الأمن السيبراني

أنظمة وتشريعات البيانات والأمن السيبراني

ركَّزت المملكة العربية السعودية منذ عام 2020 على أهمية سنّ تشريعات متخصّصة لحماية البيانات وإنفاذها، وأدى تزايد الوعي بحماية بيانات الأفراد وحقوق الوصول للبيانات وملكيتها إلى نشوء تحديات جديدة تؤثر على الشركات داخل المملكة وخارجها. وتماشيًا مع العديد من الأنظمة القانونية في المنطقة، تنص الأحكام العامة للنظام السعودي على حماية خصوصية الأفراد وبياناتهم الشخصية عوضًا عن سنّ تشريعات مخصّصة لمسألة "خصوصية البيانات" أو "حماية البيانات". وتفرض هذه الأنظمة التزامات صارمة على القطاع الخاص تخص كيفية وسبب وتوقيت جمع البيانات الشخصية واستخدامها وتخزينها.

نظام الخصوصية وحماية البيانات

اعتمدت المملكة العربية السعودية أنظمة وسياسات حماية البيانات الشخصية الصارمة من أجل ضمان حماية خصوصية المستخدمين، وتتضمن هذه الأنظمة واللوائح نظام حماية البيانات الشخصية (المرسوم الملكي رقم (م/19) بتاريخ 1443/2/9 هـ)، والمبادئ الأساسية لنظام حماية المعلومات الشخصية والمبادئ الأساسية والأحكام العامة لنظام مشاركة البيانات الصادرة عن الهيئة السعودية للبيانات والذكاء الاصطناعي و مكتب إدارة البيانات الوطنية.

نظام حماية البيانات الشخصية

تعد البيانات التي تنتجها الجهات الحكومية والخاصة أو تتلقاها أو تتعامل معها أحد أهم الأصول الوطنية التي تساهم في تحسين الأداء والإنتاجية وسهولة تقديم الخدمات العامة؛ لذا تسعى المملكة إلى تطبيق أفضل الممارسات العالمية لسياسات وضوابط إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية وتعزيز القيمة المستفادة منها في اتخاذ القرارات الاستراتيجية واستشراف المستقبل وتحقيق مستويات عالية من المسؤولية والشفافية

تسعى الدول في جميع أنحاء العالم إلى الاستفادة من قيمة البيانات باعتبارها مورداً اقتصادياً يساعد على الابتكار ويساهم في دعم التحولات الاقتصادية وتعزيز المقومات التنافسية للدول. وعلى المستوى الوطني تقوم الجهات الحكومية بجمع ومعالجة كميات هائلة من البيانات التي يمكن الاستفادة منها للمساهمة في النمو الاقتصادي والارتقاء بالمملكة إلى الريادة ضمن الاقتصادات القائمة على البيانات، وفي ظل رؤية 2030 تسعى المملكة إلى عصر جديد يعزز أداء الجهات الحكومية ويرفع مستوى شفافيتها ومسؤوليتها، ويشجع على تنويع الاقتصاد والاستفادة من الخدمات المعتمدة على البيانات، مما سيكون له دور فعال في الاقتصاد العالمي الذي يقوم على الثقة والشراكات الدولية.

تمّ اعتماد نظام حماية البيانات الشخصية بموجب المرسوم الملكي الصادر بتاريخ 16سبتمبر 2021، وذلك إنفاذًا للقرار رقم (98) بتاريخ 4 سبتمبر 2021. وتُعدّ الهيئة السعودية للبيانات والذكاء الاصطناعي الجهة المختصّة بتطبيق أحكام نظام حماية البيانات الشخصية الجديد ولوائحه التنفيذية وذلك لمدة سنتين، في ضوء نقل مهمة الإشراف على تطبيق أحكام النظام ولوائحه التنفيذية إلى مكتب إدارة البيانات الوطنية الذي يمثّل الذراع التنظيمي للهيئة السعودية للبيانات والذكاء الاصطناعي.

حدّد نظام حماية البيانات الشخصية ولوائحه التنفيذية الأساس القانوني لحماية الحقوق المرتبطة بمعالجة البيانات الشخصية لدى جميع الجهات بالمملكة، إلى جانب جميع الجهات القائمة خارج المملكة التي تضطلع بمعالجة البيانات الشخصية الخاصة بالأفراد المقيمين في المملكة باستخدام أي وسيلة، بما يشمل معالجة البيانات الشخصية عبر مواقع الإنترنت.

تشمل المبادئ الأساسية لسياسة حماية البيانات ما يلي:

- مساءلة رئيس الجهة (أو من ينوب عنه) عن سياسات وإجراءات الخصوصية المتبّعة لدى جهة مراقبة البيانات.
- الشفافية من خلال إشعار الخصوصية الذي يشير إلى الأغراض التي تجمع البيانات الشخصية من أجلها.
- الاختيار والموافقة المعتمدة من خلال الموافقة الضمنية أو الصريحة فيما يتعلق بجمع البيانات الشخصية واستخدامها والإفصاح عنها قبل جمعها.
- اقتصار جمع البيانات على الحد الأدنى من البيانات التي تمكّن من تحقيق الأغراض.
- الاستخدام والاحتفاظ والإتلاف بشكل صارم للغرض المقصود، والاحتفاظ بالبيانات طالما كان ذلك ضروريًا لتحقيق الأغراض المقصودة أو كما هو مطلوب بموجب الأنظمة واللوائح وإتلافها بأمان، ومنع التسرب، أو الفقدان، أو السرقة، أو سوء الاستخدام أو الوصول غير المصرح به.

- الوصول إلى البيانات الذي يمكّن أي جهة مالكة للبيانات من خلالها استعراض بياناتها الشخصية وتحديثها وتصحيحها.

- قيود الإفصاح عن البيانات المعتمدة من قبل الجهة المالكة للبيانات تُقيّد الجهات الخارجية بالأغراض المنصوص عليها في إشعار الخصوصية.

- أمن البيانات من خلال حماية البيانات الشخصية من التسرب، أو التلف، أو الفقدان، أو السرقة، أو سوء الاستخدام، أو التعديل أو الوصول غير المصرح به؛ وفقًا للضوابط الصادرة عن الهيئة الوطنية للأمن السيبراني والسلطات الأخرى ذات الصلة.

- جودة البيانات بعد التحقّق من دقتها واكتمالها وتوقيتها.

- مراقبة سياسات وإجراءات خصوصية جهة التحكم بالبيانات والامتثال لها، وأي استفسارات وشكاوى ونزاعات متعلقة بالخصوصية.

تغطي ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية 15 مجالًا ذي صلة. وتنطبق المعايير على جميع البيانات الحكومية بغض النظر عن الشكل أو النوع، بما يشمل السجلات الورقية، أو رسائل البريد الإلكتروني، أو البيانات المخزنة في شكل إلكتروني، أو التسجيلات الصوتية، أو مقاطع الفيديو، أو الخرائط، أو الصور، أو البرامج النصية أو المستندات المكتوبة بخط اليد أو البيانات المسجلة الأخرى. ولا يخل تطبيق أحكام نظام حماية البيانات الشخصية ولائحته التنفيذية باختصاصات ومهام الهيئة الوطنية للأمن السيبراني باعتبارها هيئة أمنية مختصة بالأمن السيبراني وشؤونه في المملكة.

أنظمة وتشريعات الأمن السيبراني

يهدف نظام مكافحة جرائم المعلوماتية إلى الحد من الجرائم المعلوماتية بهدف تحديد الجرائم والعقوبات المترتبة عليها، وذلك للمساعدة في تحقيق أمن المعلومات، وحماية المصلحة العامة والأخلاق، وحفظ الحقوق المترتبة على الاستخدام المشروع للحواسيب الآلية والشبكات المعلوماتية وحماية الاقتصاد الوطني.

أصدرت الهيئة الوطنية للأمن السيبراني مجموعة من الضوابط والأطر التنظيمية والمبادئ التوجيهية المرتبطة بالأمن السيبراني على المستوى الوطني لرفع مستوى الأمن السيبراني في المملكة سعيًا إلى حماية مصالحها الحيوية وأمنها الوطني وبنيتها التحتية الأساسية وخدماتها الحكومية. وتشمل الضوابط والأطر التنظيمية والمبادئ التوجيهية الصادرة عن الهيئة الوطنية للأمن السيبراني ما يلي:

- ضوابط الأمن السيبراني لحسابات التواصل الاجتماعي للجهات

- الضوابط الأساسية للأمن السيبراني

- ضوابط الأمن السيبراني للحوسبة السحابية

- ضوابط الأمن السيبراني للعمل عن بعد

- ضوابط الأمن السيبراني للأنظمة الحساسة
- ضوابط الأمن السيبراني للأنظمة التشغيلية
- ضوابط الأمن السيبراني للبيانات
- الإطار السعودي لكوادر الأمن السيبراني (سيوف)
- المعايير الوطنية للتشفير
- الإطار السعودي للتعليم العالي في الأمن السيبراني (سايبر-التعليم)
- إرشادات الأمن السيبراني لمستهلكي التجارة الإلكترونية

للحصول على مزيد من المعلومات، يُرجى زيارة الموقع الإلكتروني للهيئة الوطنية للأمن السيبراني.

تشريعات حرية المعلومات

يُعد حق الحصول على المعلومات في المملكة العربية السعودية عنصرًا أساسيًا في السياسات المعلوماتية، والتي تؤكد على سياسة حق الحصول على المعلومات ذات الصلة بالمعلومات العامة السرية. ووُضِعت التشريعات بُغية تحديد شروط الأهلية المعنية بالحصول على المعلومات وحق الأفراد في الحصول على المعلومات وفقًا لخمسة شروط، إلى جانب تحديد نوع المعلومات التي يُمكن طلبها والمعلومات المستثناة من ذلك. وهناك خطوات وإجراءات رسمية لطلب الحصول على المعلومات وتحديد المنصات التي يُمكن للمواطنين تقديم الطلب عبرها، إلى جانب توفير معلومات التواصل للجهات ذات العلاقة في حال وجود أي استفسارات تتعلق بسياسة حق الحصول على المعلومات.

تتصل سياسة حرية المعلومات بالمعلومات العامة غير المحمية أو السرية التي تقوم المنصّة بمعالجتها مهما كان مصدرها أو شكلها أو طبيعتها، وتندرج البيانات المفتوحة ضمن فئة المعلومات العامة. ويطلق على عملية توفير البيانات العامة للأفراد بمقابل مادي "حرية المعلومات" أو كما تُعرف باسم "سياسة حق الحصول على المعلومات".

تحدّد اللوائح المؤقتة لحرية المعلومات الأساس القانوني لحقوق الأفراد في الوصول إلى معلومات القطاع العام والحصول عليها، والتزامات الجهات العامة بجميع طلبات الوصول إلى المعلومات العامة -غير المحمية- التي تنتجها أو تحتفظ بها، بغض النظر عن المصدر أو الشكل أو الطبيعة. ويشمل ذلك: السجلات الورقية، رسائل البريد الإلكتروني أو المعلومات المخزنة على أجهزة الحاسب، أو التسجيلات الصوتية، أو الفيديو، أو الميكروفيش، أو الخرائط، أو الصور الفوتوغرافية، أو الملاحظات المكتوبة بخط اليد أو أي شكل آخر من أشكال المعلومات المسجلة. كما تحدّد اللائحة أدوار ومسؤوليات الهيئة السعودية للبيانات والذكاء الاصطناعي والجهات التابعة لها، بالإضافة إلى التزامات مكتب إدارة البيانات الوطنية، ومركز المعلومات الوطني.

كل فرد يملك الحق في تقديم طلب ومعرفة المعلومات المتعلقة بأنشطة المنصّة، وأيضًا يملك الحق في الاطلاع على المعلومات العامة –غير المحمية– مقابل رسوم مالية. وليس بالضرورة أن يتمتّع مقدّم الطلب بحيثية معينة أو باهتمام معين بهذه المعلومات ليتمكن من الحصول عليها، كما أنه لن يتعرض لأي مساءلة قانونية متعلقة بهذا الحق، ويأتي ذلك تعزيزًا لمنظومة النزاهة والشفافية والمساءلة.

وتشمل حقوق الفرد في الحصول على المعلومات ما يلي:

- **الحق في تقديم طلب للحصول على أو الوصول إلى المعلومات غير محمية لدى الجهات العامة.**
- **الحق في معرفة سبب رفض طلب الوصول أو الاطلاع على المعلومات المطلوبة.**
- **الحق في التظلم من قرار رفض طلب الحصول على المعلومات المطلوبة أو الوصول إليها.**
- **أن يتم التعامل مع جميع طلبات الوصول إلى المعلومات العامة أو الحصول عليها على أساس المساواة وعدم التمييز بين الأفراد.**
- **أن تكون أي قيود على طلب الاطلاع أو الحصول على المعلومات المحمية التى تتلقاها أو تنتجها أو تتعامل معها المنصّة مبررة بطريقة واضحة وصريحة.**

تنطبق السياسة على جميع طلبات الوصول إلى المعلومات "غير المحمية والبيانات المفتوحة" مهما كان مصدرها أو شكلها أو طبيعتها بغرض تحسين أداء وكفاءة العمل والاستفادة من البيانات.

أما المعلومات المستثناة التي لا تنطبق أحكام هذه السياسة عليها هي "المعلومات المحمية" مثل:

- **المعلومات التي يؤدي إفشاؤها إلى الإضرار بالأمن القومي للدولة أو سياستها أو مصالحها أو حقوقها.**
- **المعلومات التي تتضمن توصيات أو اقتراحات أو استشارات من أجل إصدار تشريع أو قرار حكومي لم يصدر بعد.**
- **المعلومات ذات الطبيعة التجارية أو الصناعية أو المالية أو الاقتصادية التى يؤدي الإفصاح عنها إلى تحقيق ربح أو تلاقي خسارة بطريقة غير مشروعة.**
- **الأبحاث العلمية أو التقنية، أو الحقوق المشتملة على حق من حقوق الملكية الفكرية التي يؤدي الكشف عنها إلى المساس بحق معنوي.**
- **المعلومات المتعلقة بالمناقصات والعطاءات والمزايدات التى يؤدي الإفصاح عنها إلى الإخلال بعدالة المنافسة.**
- **المعلومات التي تكون سرية أو شخصية بموجب نظام آخر، أو تتطلب إجراءات نظامية معينة للوصول إليها أو الحصول عليها.**
- **المعلومات العسكرية والأمنية.**
- **المعلومات والوثائق التي يتم الحصول عليها بمقتضى اتفاق مع دولة أخرى وتصنف على أنها محمية.**
- **التحريات والتحقيقات وأعمال الضبط وعمليات التفتيش والمراقبة المتعلقة بجريمة أو مخالفة أو تهديد.**

لمزيد من المعلومات حول التزامات الجهات العامة والأحكام العامة، يُرجى زيارة هذا الرابط.

سياسات ولوائح البيانات المفتوحة

البيانات الحكومية المفتوحة هى البيانات التى يمكن لأي شخص استخدامها دون أي قيود تقنية أو مالية أو قانونية. كما يُمكن إعادة استخدام البيانات المفتوحة وإعادة توزيعها، شريطة مراعاة متطلبات ترخيص البيانات المفتوحة التي بموجبها يتم توزيع هذه البيانات، فضلًا عن كونها تساعد على سد الفجوة بين الحكومات والمواطنين.

تحقيقًا لمبدأ الشفافية وتمكينًا للمواطنين القائمين في المملكة من الوصول إلى قاعدة كبيرة من البيانات الحكومية، أطلقت المملكة السياسات واللوائح الإرشادية ذات الصلة.

تُعد الهيئة السعودية للبيانات والذكاء الاصطناعي الجهة الوطنية المنظّمة للبيانات في المملكة العربية السعودية، حيث طوّرت سدايا إطار عمل حوكمة البيانات الوطنية لوضع السياسات واللوائح المطلوبة لتصنيف البيانات، ومشاركتها، وخصوصيتها، وحرية المعلومات، والبيانات المفتوحة، وغيرها تحسبًا للتشريعات اللازمة.

اللوائح المؤقتة للبيانات المفتوحة

تحدّد اللوائح المؤقتة للبيانات المفتوحة الأساس القانوني والالتزامات لجميع البيانات والمعلومات العامة التي تنتجها الجهات العامة بغض النظر عن المصدر أو الشكل أو الطبيعة. كما تعين الأسس القانونية والحد الأدنى من المعايير للوكالات الحكومية لنشر مجموعات البيانات الخاصة بها. وتبيّن اللائحة المؤقتة للبيانات المفتوحة أدوار ومسؤوليات الهيئة السعودية للبيانات والذكاء الاصطناعي وجهاتها الفرعية، ومكتب إدارة البيانات الوطنية ومركز المعلومات الوطني. وجميع الجهات الحكومية الأخرى التى لديها التزامات فيما يتعلق بوضع خطط البيانات المفتوحة وتحديدها ونشرها وصيانتها وتتبع الأداء والامتثال.

لوائح وسياسات التشغيل البيني للبيانات

استجابت الحكومة إلى ضرورة وضع إطار التشغيل البينى رسميًا منذ عام 2006، كجزء من الاستراتيجية الرقمية الوطنية الأولى للحكومة السعودية.

جرى العمل على تطوير إطار التشغيل البيني واعتماده، حيث يتضمن تعريفًا للبيانات المشتركة والمعايير التقنية، وإطار يسّر للتشغيل البيني، ويهدف إلى دعم الوزارات والجهات الحكومية لتبادل البيانات وتقديم الخدمات عن طريق البنية التحتية المشتركة للتكامل. وأدت جهود تيسير تقديم الخدمات الإلكترونية، وتوفير المزايا الفنية المنسّقة إلى تمكين قابلية التشغيل لخطط التحوّل الرقمي ذات الأولوية.

تركّز الخطط الحالية للتشغيل البيني على ما يلي:

- تحديد معايير البيانات المشتركة البيانات على المستويين التشغيلي والمنطقي، ووصف مخططات البيانات الهياكل المستخدمة في الربط بين الأنظمة.
- تحديد معايير البيانات الوصفية الخصائص والقواميس المستخدمة لتصنيف وفهرسة المحتوى الإلكتروني.
- ضمان المعايير والسياسات التقنية لفاعلية التشغيل البينى على المستوى التقنى، وشمولية معايير الاتصال والربط ومعايير التكامل والمعايير الأمنية.

لا تشكّل عملية تطوير إطار التشغيل البينى نشاطًا لمرة واحدة، ولكنها مبادرة مستمرة تستدعي بذل جهود متواصلة. ويتضمن التحوّل الرقمي مواصفات مُفصّلة، مثل: المواصفات المتعلقة بالبيانات والبيانات الوصفية والمعايير التقنية. يُعرّف الإطار هياكل البيانات المشتركة وعناصر البيانات بكونها ضرورية لضمان التكامل السلس بين الأنظمة ومشاركة

البيانات على مستوى جميع الجهات الحكومية. وتُعد وثيقة معايير قابلية التشغيل البيني الوطنية في غاية الأهمية لأنها توفّر الإرشادات وتعريفات هياكل البيانات اللازمة لضمان التشغيل البيني، والتكامل، وقابلية النقل للأنظمة، وإمكانية إعادة استخدامها. كما وتوضّح المعايير واللوائح التنظيمية التي تمكّن الجهات من مشاركة الخدمات والاستفادة منها من خلال البنية التحتية التقنية الحكومية، وتزيل أوجه الغموض وعدم الاتساق في استخدام البيانات من خلال تفويض مجموعة من عناصر البيانات وهياكل البيانات للتكامل.

تُولي وزارة الصحة اهتمامًا بالغًا بقابلية التشغيل البيني نظرًا لحساسية مشاركة البيانات بين مواقع وجهات مختلفة. ووُضعت مجموعة من الوثائق المرتبطة بالتشغيل البيني لتحديد الإرشادات واللوائح الأساسية الرامية إلى ضمان مشاركة البيانات القابلة للتشغيل البيني بأمان. وتُطبّق المواصفات الأساسية للتشغيل البيني على أنظمة المعلومات الحالية والجديدة التي سيجري من خلالها تبادل المعلومات الصحية. وتُطبَق هذه المواصفات بوجه خاص على تشغيل منصات تبادل المعلومات لمجال الصحة الإلكترونية.

ويُمكن الاطّلاع على أمثلة في المركز الوطني للمعلومات الصحية، مثل:

- تفعيل قابلية التشغيل البيني في السجلات الصحية الإلكترونية IS0010 القائمة على المعايير للمواصفات الأساسية السعودية للتشغيل البيني في مجال الصحة الإلكترونية للمناعة، النسخة الأولى بتاريخ 21 أبريل 2016

- تفعيل قابلية التشغيل البيني في السجلات الصحية الإلكترونية IS0003 القائمة على المعايير للمواصفات الأساسية السعودية المعنية بالتشغيل البيني للصحة الإلكترونية لمشاركة نتائج الفحوص المختبرية المشفرة، بتاريخ 21 أبريل 2016

سياسات البيانات المعنية بتبادل البيانات

ينطوي تخزين البيانات على محتواها وهيكل التخزين وغيرها من المعلومات التي يجب أن تُلحق بها ولا يُمكن أن تُخزن دونها. وتشمل تلك المعلومات إرشادات حول القضايا الإلزامية لضمان صلاحية البيانات واستخداماتها، على سبيل المثال: يجب تحديد مدة التخزين لجميع البيانات المُخزنة أو مدى صلاحيتها، حيث يجب أن تحدّد المدة متى أصبحت البيانات قديمة أو غير قابلة للمشاركة، وهو ما يُعرف بمدة الاحتفاظ بالبيانات. وتشمل القضايا الأخرى ما يلي:

- المعلومات المعنية بهوية الفرد وماهية البيانات التي يجب أن يحتفظ بها، والمدة الزمنية، ومتى وإذا كانت مدة الاحتفاظ هي القصوى أو الدنيا.

- المراجع القانونية والروابط الناقلة إلى المصدر القانوني الرسمي.

- البيانات المحدّثة وجدول بمواعيد تحديثها بوتيرة متكررة.

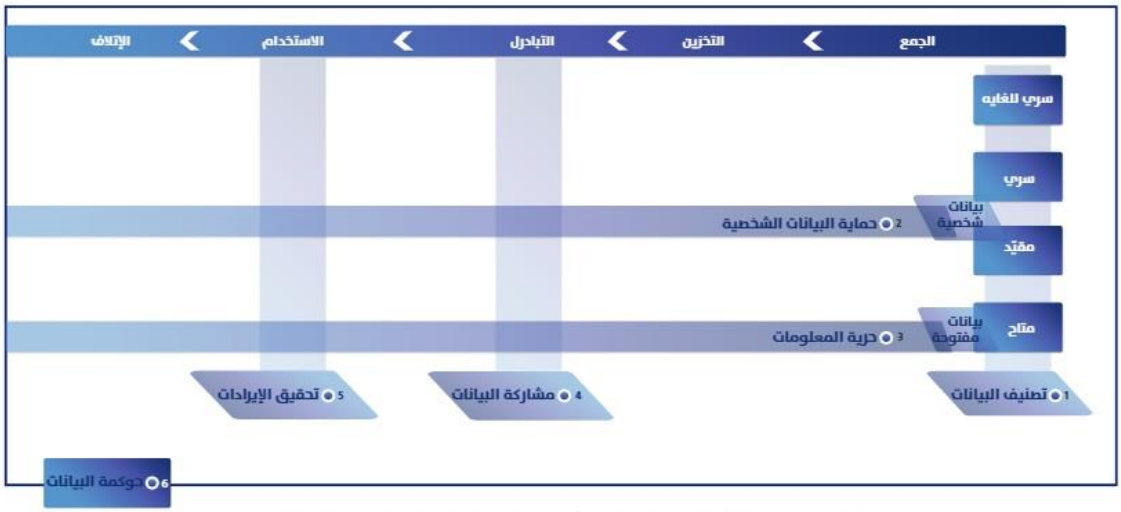
- الوصول المحمي والخاضع للرقابة.

- يجب أن تكون البيانات التي جرت مشاركتها مرنة من حيث الاستخدام، ويُقصد بذلك أن تكون قابلة للتحويل أو الجمع للتحليلات الفردية أو إصدار التقارير.

يرتبط الغرض من جمع البيانات الشخصية ارتباطًا مباشرًا بأغراض الحكومة الرقمية (GOV.SA) ولا يتعارض مع أي من الأحكام المحدّدة. وتكون طرق ووسائل جمع المعلومات الشخصية مناسبة لظروف المالك، ومباشرة وواضحة وآمنة، وخالية من الخداع أو المعلومات المُضلّلة أو الابتزاز. وفي حال اتضّح أن البيانات الشخصية المجمّعة لم تُعد ضرورية

لتحقيق الغرض من جمعها، فستتوقف الحكومة الرقمية (GOV.SA) عن اكتنازها وستتلف البيانات التى جُمعت آنفًا على الفور.

اعتُمدت الاتفاقية بخصوص هذه المعايير مسبقًا ويجري استخدامها في الوقت الحالي، حيث تحدّد ضوابط ومواصفات إدارة البيانات الوطنية وحوكمتها وحماية البيانات الشخصية (منذ يناير 2021) هذه المعايير.



العلاقة بين الأنظمة والتشريعات والسياسات الخاصة بالبيانات

سياسات إدارة واستخدام البيانات

يجب أن يوافق جميع المستخدمين المُخوّلين على السياسات واللوائح التنظيمية للخصوصية وحماية البيانات المعمول بها فى المملكة العربية السعودية. ويجب أن توفّر جميع منصات البيانات إمكانيات وميزات التحكم فى البيانات من خلال المنصّة وتطبيقاتها. وتُعد هذه الاتفاقية سارية فور استخدام المنصّة أو الوصول إليها لأول مرة.

يرتبط الغرض من جمع البيانات الشخصية ارتباطًا مباشرًا بأغراض الحكومة الرقمية بهدف تقديم خدمات إلكترونية أسهل وأكثر كفاءة ولا يتعارض مع أي حكم محدّد في أنظمة وسياسات أمن وخصوصية البيانات. وتكون الطرق والوسائل المختلفة لجمع المعلومات الشخصية مناسبة لظروف المالك، ومباشرة وواضحة وآمنة، وخالية من الخداع أو المعلومات المُضلّلة أو الابتزاز. وفي حال اتضّح أن البيانات الشخصية المجمّعة لم تُعد ضرورية لتحقيق الغرض من جمعها، فستتوقف الجهة ذات العلاقة عن اكتنازها وستتلف البيانات التي جُمعت آنفًا على الفور.

وستضمن الحكومة الرقمية (GOV.SA) استيفاء المعايير التالية قبل جمع البيانات الشخصية وفق ما يلي:

- المبرر المنطقي لجمع البيانات الشخصية.
- الغرض من جمع البيانات الشخصية، سواءً كان جميعها أو جزء منها، سواءً بصورة إلزامية أو اختيارية، مع توفير المزيد من المعلومات حول معالجة البيانات التي لا تتعارض مع الغرض من جمعها أو التي ينص عليها النظام بطريقة أخرى.
- الهوية والعنوان المرجعي لجامع البيانات الشخصية عند الاقتضاء، ما لم يكن ذلك لأغراض أمنية.

- **الجهات التى ستحظى بإمكانية الاطلاع على البيانات الشخصية ووصفها، وفى حال ستنُقل البيانات الشخصية أو يُفصح عنها أو ستُعالج خارج المملكة.**

- **العناصر الأخرى التي تحدّدها اللوائح اعتمادًا على طبيعة النشاط الذي تمارسه هذه الجهة.**

المراجع:

- **مقدمة في الأمن السيبراني، د. أيمن الحربي، معهد البحوث والدراسات الاستشارية بجامعة أم القري،**
- **المنصة الوطنية الموحدة .gov.sa، أنظمة وتشريعات البيانات والأمن السيبراني (my.gov.sa)**
- **الهيئة السعودية للبيانات والذكاء الاصطناعى، حماية البيانات(sdaia.gov.sa)**
- **الهيئة الوطنية للأمن السيبراني، الهيئة الوطنية للأمن السيبراني(nca.gov.sa)**

الوحدة الثانية: دراسات تحليلية لأشهر الهجمات السيبرانية

الأهداف التفصيلية للوحدة :

أن يكون المتدرب في نهاية الوحدة قادرا على:

1. يوضح أشهر الهجمات السيبرانية
2. يُعرِّف الهجمات السيبرانية
3. يذكر كيفية التصدي للهجمات السيبرانية
4. يبين مدي أهمية الدراسات التحليلية للهجمات السيبرانية
5. يوضح أهداف الدراسات التحليلية للهجمات السيبرانية
6. يشعر بدور الدراسات التحليلية للهجوم السيبراني

تشمل الوحدة على المواضيع الفرعية التالية "

الدرس الأول / دراسة تحليلية لهجمات أرامكو السيبرانية

الدرس الثاني / دراسة تحليلية لهجمات استونيا السيبرانية والآثار المترتبة عليها

الدرس الثالث / دراسة تحليلية لهجمات مختلفة في أنحاء العالم

الدرس الرابع / تحليل لأهم المواقع الإحصائية للهجمات السيبرانية

الدرس الأول / دراسة تحليلية لهجمات أرامكو السيبرانية

أرامكو السعودية تحوز جائزة دولية مرموقة لدورها الريادي في مجال الأمن السيبراني

سلّطت منظمة دولية معنية بالتحول الرقمي وتعزيز الأمن السيبراني في كل المشهد الصناعي العالمي، الضوء على الجهود المتطورة لإدارة أمن المعلومات في أرامكو السعودية.

وحصل برنامج الأمن السيبراني الذي طورته إحدى الشركات المتعاونة مع أرامكو السعودية لحمايتها من التهديدات السيبرانية، على جائزة (سي إس أو 50) المرموقة لعام 2020م من شركة تقنيات الاتصال التابعة لمجموعة البيانات الدولية. وعُقدت مراسم التكريم عن بُعد بسبب القيود المستمرة التي فرضتها جائحة فيروس كوفيد-19.

وقد أدخل برنامج إدارة أمن المعلومات آليات للحوكمة والحماية في كل سلسلة الإمداد في أرامكو السعودية لحمايتها ضد المخاطر السيبرانية المتزايدة.

ولا يقتصر الهدف الرئيس للبرنامج على حماية الشركة فحسب؛ فهو يشتمل أيضًا على زيادة وعي الأطراف الأخرى التي تعمل مع أرامكو السعودية بالأمن السيبراني وتعريفهم بقدراته وإمكانياته.

وتعد جائزة سي إس أو 50 جائزةً دوليةً مرموقةً تُمنح لأفضل 50 مشروعًا متميزًا كان له أكبر أثر إيجابي على قوة الأمن السيبراني في الشركة، ومجتمع المعنيين بالأمن السيبراني، ومنظومة الأمن السيبراني .

حماية بيانات وأصول الشركة

وبهذه المناسبة، أعرب كبير مسؤولي أمن المعلومات، الأستاذ خالد الحربي، عن فخره بالجائزة وبجهود فريقه، وقال:

وهو شعار يسلط الضوء على الدور الذي يسهم به كل موظف في حماية بيانات وأصول الشركة".

ويزداد المستوى الفني للهجمات السيبرانية تطورًا، فبدلًا من أن يستغل المهاجمون الثغرات الأمنية الموجودة في التقنيات والأنظمة الأمنية، أصبحوا يستخدمون تقنيات الهندسة الاجتماعية المصممة لدفع المستخدمين لكشف بياناتهم، أو لنشر برمجيات خبيثة، أو للحصول على حق الولوج إلى أنظمة محظورة.

وأضاف الحربي: "التقنيات المتقدمة والممارسات الأمنية - مهما كانت متطوّرة- ستظل دائمًا مقيدة بالعامل البشري. ولذلك فنحن ملتزمون بمواصلة جهودنا لتعزيز ثقافة أمن سيبراني مرنة في أرامكو السعودية من خلال برنامج إدارة سلوك الأمن السيبراني" .

إدارة السلوك

ويمر البرنامج بمرحلة مهمة لخلق ثقافة الحذر والتيقظ، حيث يتحول إلى برنامج تعاوني يتمحور حول السلوك.

وأوضح الحربي أن الإدارة دأبت على تكثيف جهودها من خلال التعاون مع الجهات الحكومية ومؤسسات البنية التحتية الوطنية الحيوية لتعزيز سلوكيات الأمن السيبراني الإيجابية على مستوى الدولة.

وقال: "نتعاون حاليًا مع منتدى الاقتصاد العالمي في قيادة أبحاث عالمية عن المرونة السيبرانية لقطاع النفط والغاز، وتكثيف الجهود على التصدي للمخاطر السيبرانية التي تواجهها البنية التحتية لتقنية المعلومات والمعدات التقنية. ويمثل هذا البحث جهدًا جماعيًا عالميًا لمجتمع الأمن السيبراني بمصلحة مشتركة والتزام بتقوية قدرات الأمن السيبراني" .

وتقود أرامكو السعودية بصفتها عضوًا مؤسسًا في مركز الأمن السيبراني التابع للمنتدى الاقتصادي العالمي؛ جنبًا إلى جنب مع المركز)يعرف الاثنان بمسمى "سي فور سي ("C4C: برنامجًا سيبرانيًا مرنًا يركز تحديدًا على قطاع النفط والغاز .

المرونة السيبرانية

وتعمل كلٌّ من أرامكو السعودية والمنتدى الاقتصادي العالمي على وضع مبادئ توجيهية بشأن المرونة السيبرانية لمجالس الإدارة لإحداث تغيير تنظيمي وسلوكي في قطاع النفط والغاز. ويُنشئ البرنامج شبكة تعاون موثوقة لترسيخ الأمن السيبراني عبر كامل منظومة النفط والغاز.

وأضاف الحربي: "سعت الشركة لتقوية مرونتها السيبرانية لضمان إيجاد قدرات أمن سيبراني للشركة ومنظومتها الرقمية".

كما أدركت أرامكو السعودية أن هذه المرونة تعتمد على جهد جماعي يُبنى على اكتساب حلفاء أقوى في كل سلسلة الإمدادات. وسدًا لهذه الفجوة، ظهرت الحاجة في عام 2016م لبرنامج أمن سيبراني.

التعاون القوي مع الشركاء

وقالت رئيسة مجموعة تطوير برامج أمن المعلومات، ظبي الراشد، إن طبيعة أعمال أرامكو السعودية كشركة عالمية تتطلب تعاونًا قويًا بين الشركة وشركائها للتصدي لتحديات الأمن السيبراني بفاعلية. وأضافت قائلة: "نعتمد على عديد من الموردين من شركائنا ومن أطراف ثالثة لتحقيق أهداف أعمالنا. وذلك يتضمن تبادل البيانات والتواصل المكثف، مما يرفع بطبيعة الحال من مستوى الخطورة حول حوكمة وأمن البيانات. ويسعى البرنامج لمواجهة استباقية للمخاطر السيبرانية التي تفرضها أطراف خارجية من خلال إدراج الأمن السيبراني في كل مرحلة من مراحل مشاركة شركات الطرف الثالث" .

وقد وضعت إدارة أمن المعلومات أول شهادة رقمية لشركات الطرف الثالث التي تتعامل معها الشركة تحت مسمى "شهادة الالتزام بالأمن السيبراني"؛ والتي تسعى للارتقاء بقدرات الأمن السيبراني عبر سلسلة الإمداد في أرامكو السعودية لضمان التقيد بمعايير أفضل الممارسات.

وركز رئيس سلسلة الإمداد ومجموعة التزام الأطراف الثالثة، علي العسيري، على المنفعة المتبادلة للتعاون، وعن أهميتها الرئيسة في تقوية أمن المنصات الإلكترونية، فقال: "أثارت إدارة أمن المعلومات مناقشات مع أطراف ثالثة واستضافت عدة جلسات تعاونية على مستوى المملكة لتوحيد الجهود الوطنية في التعامل مع مخاطر سلسلة الإمداد ورفع معايير الأمن

أُستحدث برنامج اعتماد الالتزام بضوابط الأمن السيبراني (CCC) لضمان التزام جميع الأطراف الخارجية لدى أرامكو السعودية لمتطلبات الأمن السيبراني الواردة في معيار أرامكو السعودية للأمن السيبراني للأطراف الخارجية رقم 002.(SACS-002)

ما الهدف من برنامج اعتماد الالتزام بضوابط الأمن السيبراني(CCC) ؟

أُستحدث برنامج اعتماد الالتزام بضوابط الأمن السيبراني(CCC) لضمان حصول جميع الأطراف الخارجية على شهادة الالتزام بضوابط الأمن السيبراني من شركات التدقيق المعتمدة، لتأكيد التزامهم بمتطلبات الأمن السيبراني كما هو منصوص عليه في معيار أرامكو السعودية للأمن السيبراني للأطراف الخارجية رقم 002(SACS-002) ، لمزاولة الأعمال مع أرامكو السعودية.

ما الفرق بين من شهادة الالتزام بضوابط الأمن السيبراني (CCC) وشهادة الالتزام بضوابط الأمن السيبراني بلس(CCC+) ؟

يتطلب الحصول على شهادة الالتزام بضوابط الأمن السيبراني (CCC) من الجهة الخارجية إجراء تقييم التزام ذاتي بضوابط النطاق الموضحة في معيار أرامكو السعودية للأمن السيبراني رقم 002(SACS-002) ، والتحقق من إجراءات تقييم الالتزام عن طريق إحدى شركات التدقيق المُعتمدة عن بُعد.

بينما يتطلب الحصول على شهادة الالتزام بضوابط الأمن السيبراني بلس (CCC+) حضور إحدى شركات التدقيق المُعتمدة للموقع لإجراء تقييم للجهة الخارجية وفقًا لضوابط النطاق وحسبما هو موضح في معيار أرامكو السعودية للأمن السيبراني رقم 002 .(SACS-002) تُطلب شهادة الالتزام بضوابط الأمن السيبراني بلس (CCC+) من الأطراف الخارجية التي تندرج تحت تصنيف الاتصال المباشر ومعالج البيانات الهامة، في حين تُطلب شهادة الالتزام بضوابط الأمن السيبراني (CCC) من الأطراف الخارجية المتبقية التي لا تندرج تحت التصنيفات المذكورة أعلاه.

ما نوع الشهادة التي تنطبق على شركتي؟

يعتمد الأمر على التصنيف الذي ستقرره الدائرة المعنية في أرامكو السعودية، وصاحب المقاولة، وذلك وفقًا لمعيار أرامكو السعودية للأمن السيبراني للأطراف الخارجية رقم 002(SACS-002) ، حيث سيُحدد التصنيف نوع الشهادة المطلوبة من شركتك .

كم مدة سريان شهادة الامتثال بضوابط الأمن السيبراني(CCC) ؟

ستكون الشهادة سارية لمدة عامين من تاريخ الإصدار، بشرط عدم تغيير تصنيف الجهة الخارجية خلال فترة العامين.

هل يتوجب على الحصول على شهادة التزام (CCC) جديدة في كل مرة أتقدم فيها للحصول على عقد جديد؟

يعتمد الأمر على طبيعة عملك، ففي حال كنت تندرج تحت نفس التصنيف، فلن تحتاج إلى التقدم للحصول على شهادة جديدة، بخلاف ذلك، ستحتاج إلى التواصل مع شركة التدقيق لإجراء تقييم التزام بضوابط الأمن السيبراني حسب الضوابط المتعلقة بالتصنيف المحدث الذي سيغطي الفئة الأصلية، بالإضافة إلى الفئة الجديدة

ماهي شركة التدقيق التي يجب أن نختارها؟

التدقيق التي يجب أن نختارها؟ ليس لدى أرامكو السعودية أية تفضيلات بخصوص اختيار شركة التدقيق، طالما أنك ستعمل مع إحدى شركات التدقيق المعتمدة المدرجة في هذا الموقع.

كيف يمكنني تقديم الشهادة فور حصولي عليها من شركة التدقيق؟

يتوجب عليك تقديم شهادة التزام الأطراف الخارجية بضوابط الأمن السيبراني، وتقرير شهادة الالتزام بضوابط الأمن السيبراني إلى أرامكو السعودية من خلال نظام.e-marketplace

»أرامكو» السعودية توسع استراتيجيتها السيبرانية لتحصين إمدادات الطاقة

الناصر: العمل التكاملي مطلب تجاه المخاوف الأمنية المهددة للأعمال

المهندس الناصر متحدثًا للحضور خلال المنتدى الدولي للأمن السيبراني (الشرق الأوسط)

- الرياض» :الشرق الأوسط«

نُشر: 15:25-1 نوفمبر 2023 م ـ 17 ربيع الثاني 1445 هـ

أعلن رئيس أرامكو السعودية وكبير إداريها التنفيذيين، المهندس أمين الناصر، توسيع استراتيجية الشركة في مجال الأمن السيبراني للتقليل من أيّ تهديدات للإمدادات الثابتة من الطاقة، مؤكداً أن هذا النهج يعد تسخيرا للإمكانات القوية للابتكارات الرقمية.

جاء ذلك خلال فعاليات الدورة الثالثة للمنتدى الدولي للأمن السيبراني، المقام حالياً في الرياض، بمشاركة نخبة من القادة وصنّاع القرار والمديرين التنفيذيين من المنظمات الدولية ذات الصلة بمجال الأمن السيبراني، يمثلون مختلف القطاعات الحكومية والأكاديمية وأبرز الشركات العالمية.

وتأتي مشاركة «أرامكو» السعودية في المنتدى كشريك استراتيجي للتركيز على أهمية العمل الجماعي، ومنح الأمن السيبراني الأولوية القصوى لمجابهة الهجمات الإلكترونية.

وقال المهندس الناصر «إذا نظرنا إلى الطفرات التقنية الجديدة والتطورات الرقمية المتسارعة بما فيها تصاعد استخدام الذكاء الاصطناعي التوليدي والمخاطر المحتملة، يصبح من الضروري التعاون بين جميع أصحاب المصلحة في القطاعين العام والخاص والمجتمعات لإيجاد حلول تجاه المخاوف الأمنية التي تسبب تهديدات للأعمال والمجتمعات.

وواصل أن المنتدى يمثل فرصة مهمة لمناقشة وتطوير وتكامل المعايير الدولية، والاستفادة من تجارب الآخرين، والتعرّف على أفضل الممارسات في الأمن السيبراني.

وكشف الناصر عن استثمار «أرامكو» في منصات مثل مركز الأمن السيبراني التابع للمنتدى الاقتصادي العالمي الذي يُعد أحد المراكز الفكرية العالمية الرائدة في هذا المجال.

وأفصح أيضاً عن توسيع استراتيجية الشركة في مجال الأمن السيبراني للتقليل من أيّ تهديدات للإمدادات الثابتة من الطاقة، وأن هذا النهج تسخير للإمكانات القوية للابتكارات الرقمية.

وتتبنّى «أرامكو» السعودية تقنيات متقدمة في جميع مرافقها وأعمالها لاستكشاف المهددات السيبرانية في ظل القدرات الهائلة التي أطلقتها الثورة الصناعية الرابعة.

كما أنشأت الشركة برنامج اعتماد الالتزام بضوابط الأمن السيبراني، والذي يهدف إلى ضمان التزام جميع الأطراف الخارجية بمعيار «أرامكو» السعودية للأمن السيبراني، والذي يتطلب من الموردين الذين يتعاملون معها الحصول على شهادة اعتماد تُجدد كل عامين تضمن مواكبتهم لأي تهديدات سيبرانية محتملة.

وأسّست «أرامكو» السعودية شركة «الحلول السيبرانية» لتقديم مجموعة من خدمات الأمن السيبراني المتخصصة لمساعدة الشركات على حماية عملياتها وبياناتها.

ويُعد المنتدى الدولي للأمن السيبراني فعالية سنوية تنظمها الهيئة الوطنية للأمن السيبراني تحت رعاية خادم الحرمين الشريفين الملك سلمان بن عبد العزيز.

ويمثّل المنتدى إحدى المنصات العالمية التي تجمع نخبة من صناع القرار والرؤساء التنفيذيين، وكبار المسؤولين الحكوميين، وممثلي أبرز الشركات العالمية، والمنظمات غير الحكومية، والأوساط الأكاديمية حول العالم والمهتمة بتطوير الآفاق المعرفية بشأن موضوعات الأمن السيبراني، وبناء أسس التعاون في ظل المتغيرات الجيوسياسية والاستراتيجية المتسارعة، وآفاق تشكيل مستقبل الأمن السيبراني.

الدرس الثاني / دراسة تحليلية لهجمات أستونيا السيبرانية والآثار المترتبة ليها

نظرًا للتعرض لحملات تضليل متكررة، ترى دولة إستونيا الصغيرة الواقعة على بحر البلطيق أن التثقيف الإعلامي جزء من ثقافتها الرقمية وأمنها القومي.

استمرت أعمال الشغب لمدة يومين في العاصمة الإستونية تالين، واشتبك المتظاهرون مع الشرطة وانتشر اللصوص بعد اندلاع أعمال العنف بسبب الجدل حول قرار نقل تمثال عسكري أقيم خلال الحكم السوفيتي. واشتعلت نيران الغضب بين الأقلية الناطقة باللغة الروسية في إستونيا بسبب انتشار أخبار كاذبة على شبكة الإنترنت وفي تقارير إخبارية روسية.

ثم تصاعدت حملة التضليل الإعلامي إلى ما يُعتبر أول هجوم إلكتروني ضد دولة بأكملها. وأدى الهجوم، الذي كان مرتبطا بروسيا، إلى إغلاق المواقع الإلكترونية التابعة للحكومة الإستونية والبنوك ووسائل الإعلام.

وفي أعقاب هذا الهجوم في عام 2007، قررت إستونيا اتخاذ بعض الإجراءات، وأصبحت الآن دولة رائدة في مجال الأمن السيبراني، وتعمل على حماية بنيتها التحتية الإلكترونية من الهجمات المستقبلية.

لكن الدولة فعلت شيئًا آخر في محاولتها لحماية نفسها من العدوان الرقمي - تستخدم تلك الدولة الصغيرة الواقعة على بحر البلطيق تعليم محو الأمية الإعلامية لمساعدة مواطنيها على اكتشاف المعلومات المضللة والحذر منها.

ومنذ عام 2010، تقدم المدارس العامة الإستونية - من روضة الأطفال حتى المدرسة الثانوية - لتلاميذها دروسا في محو الأمية الإعلامية. ويشارك الطلاب في الصف العاشر أيضًا في دورة إلزامية مدتها 35 ساعة حول "الإعلام وتأثيره".

ويُقبل تعليم محو الأمية الإعلامية الآن "بنفس أهمية الرياضيات أو الكتابة أو القراءة"، كما يقول سيم كومباس، المستشار السابق للحكومة الإستونية للمعلومات الاستراتيجية. وعُين كومباس مؤخرًا كمسؤول سياسات في خدمة العمل الخارجي الأوروبي، وهي الخدمة الدبلوماسية للاتحاد الأوروبي.

مصدر الصورة، RAIGO PAJULAR/AFP/GETTY IMAGES

أدى الهجوم الإلكتروني الذي نشر معلومات مضللة في إستونيا في عام 2007 إلى احتجاجات عنيفة في شوارع العاصمة تالين

تحتل إستونيا مرتبة عالية في مجال حرية الإعلام والتعليم، و"تضع شروطًا مسبقة قوية للتعامل مع المعلومات المضللة"، كما تقول مارين ليسينسكي، مديرة برنامج في معهد المجتمع المفتوح ومقره صوفيا ببلغاريا، والذي ينشر مؤشرًا سنويًا لمحو الأمية الإعلامية. وتضيف: "التعليم الجيد يخلق تفكيرًا نقديًا أقوى أو مهارات أفضل للتحقق من الحقائق".

وجرى تسليط الضوء على التهديد القوي الذي تشكله المعلومات المضللة عبر الإنترنت في أعقاب الانتخابات الرئاسية الأمريكية لعام 2016، إذ جرى استهداف الناخبين بمعلومات مضللة من قبل المتصيدين الذين لديهم صلات بالاستخبارات الروسية. واتهم تقرير لاحق نشرته لجنة الاستخبارات بمجلس الشيوخ الأمريكي، روسيا بشن "حملة حرب معلومات" تهدف إلى نشر معلومات مضللة وتقسيم المجتمع الأمريكي.

وأدت المحاولات الواضحة لتعطيل الانتخابات الديمقراطية، جنبًا إلى جنب مع المعلومات المضللة التي انتشرت خلال وباء كورونا، إلى ادعاءات بأن العالم يواجه "وباء معلومات" أو وباء المعلومات الخاطئة، على حد تعبير هيلاري كلينتون.

وفي يوليو/تموز 2021، تصدر الرئيس الأمريكي جو بايدن عناوين الصحف عندما قال إن منصات وسائل التواصل الاجتماعي مثل فيسبوك "تقتل الناس" من خلال نشر معلومات مضللة عن لقاحات فيروس كورونا.

لكن على الرغم من التهديد، ليس هناك حل حاسم لهذه المشكلة المتفشية. وتناقش بعض البلدان مثل الولايات المتحدة وضع لوائح جديدة للإنترنت وفرض عقوبات على منصات التواصل الاجتماعي التي تنشر محتوى ضارًا، بينما تحاول شركات الإنترنت نفسها والمؤسسات الإعلامية اتخاذ خطواتها الخاصة لمعالجة المشكلة خوفًا من فقدان ثقة جمهورها.

وأقرت ألمانيا في عام 2017 قانون تنظيم الإنترنت "نتيز دي جي"، وهو قانون يهدف لمواجهة خطاب الكراهية عبر الإنترنت، كما وسعت العام الماضي اللوائح بموجب هذا القانون.

وفي ربيع عام 2021، اقترحت المملكة المتحدة "مشروع قانون أمان الإنترنت"، وأطلقت لاحقًا استراتيجية جديدة لتنسيق مبادرات محو الأمية الإعلامية.

ازداد القلق بشأن المعلومات المضللة التي تُنشر عبر الإنترنت وعلى وسائل التواصل الاجتماعي خلال وباء كورونا

قد تكون محاولات إستونيا المستمرة منذ عقد من الزمان لتعليم شعبها التمييز بين المعلومات الموثوقة والأكاذيب جزءًا مهمًا في هذا الصدد، وقد بدأ يؤتي ثماره بالفعل.

وفي العام الماضي، احتلت هذه الدولة الصغيرة المرتبة الثالثة في مؤشر محو الأمية الإعلامية لعام 2021، الذي تعده مبادرة السياسات الأوروبية التابعة لمعهد المجتمع المفتوح، بعد فنلندا والدنمارك. ووفقًا للمؤشر الذي يضم 35 دولة أوروبية، فإن الدول ذات التصنيف الأعلى هي التي تتمتع بأعلى الإمكانات لمواجهة المعلومات المضللة والمعلومات الخاطئة بناءً على جودة التعليم ووسائل الإعلام الحرة والثقة العالية بين الناس، وفقًا لمعهد المجتمع المفتوح.

ويأتي مركز إستونيا المتقدم في المؤشر على الرغم من أن متوسط دخلها السنوي أقل من نصف مثيله في الدول الأوروبية الغنية ذات التصنيف الأعلى. وعلى الرغم من أن عدد سكان إستونيا يبلغ 1.3 مليون نسمة فقط، إلا أنها تعد واحدة من أكثر دول العالم تقدمًا رقميًا. كما أن ثقافة محو الأمية الإعلامية و"الكفاءة الرقمية" تمثلان جزءًا من هوية إستونيا كدولة رائدة في التكنولوجيا ورقمنه التصويت، وتقديم الضرائب، ومعظم جوانب الحياة المدنية.

وتحاول دول أخرى أيضًا التعلم من نهج إستونيا. وقبل انتخابات نوفمبر/تشرين الثاني 2020، زار مسؤولون عسكريون أمريكيون إستونيا للتعرف على طرق مواجهة الحرب الإلكترونية الروسية. واستمع برلمان المملكة المتحدة أيضًا في عام 2020 إلى كومباس وهو يقدم أدلة من الحكومة الإستونية للتعرف على برامج محو الأمية الإعلامية في البلاد وكيفية مساعدة المواطنين "على فهم الدعاية الرقمية في موقعها كجارة قريبة لروسيا".

وقال كومباس أمام لجنة البرلمان البريطاني المعنية بالديمقراطية والتقنيات الرقمية إن المهارات الجيدة لمحو الأمية الإعلامية "تجعل شعبنا أكثر مرونة، ليس فقط في مواجهة التدخل العدائي في المجال الرقمي، ولكن أيضًا أمام الضوضاء والوقاحة والصحافة السيئة وكل شيء آخر".

وكانت ممارسات الأمن السيبرانى الوطنية فى إستونيا مدفوعة بعلاقتها المشحونة تاريخياً مع روسيا. واستعادت البلاد استقلالها من

الحكم السوفيتي في عام 1991 ووجدت نفسها منذ ذلك الحين بين أهداف العدوان الروسي.

ومنذ الهجوم الإلكتروني على إستونيا عام 2007، اتُهمت روسيا أيضًا بالعدوان الإلكتروني ضد دول مجاورة أخرى مثل جورجيا، وأوكرانيا على وجه التحديد التي تعرضت لضغوط متزايدة من جارتها الأكبر هذا الشتاء.

وتنفي الحكومة الروسية باستمرار أي تورط لها في الهجمات الإلكترونية، لكن مع تجمع القوات الروسية بالقرب من الحدود مع أوكرانيا في يناير/كانون الثاني، ذهبت وزارة الخارجية الأمريكية إلى حد نشر صحيفة وقائع حول المعلومات الروسية المضللة بشأن أوكرانيا.

وأصدرت المملكة المتحدة أيضًا توجيهات جديدة تحث المنظمات البريطانية على تعزيز دفاعاتها ضد الهجمات الإلكترونية.

يقول كومباس: "لم نُفاجأ كثيرًا بما حدث في جورجيا عام 2008، أو أوكرانيا عام 2014، أو الولايات المتحدة عام 2016". وقال كومباس لأعضاء البرلمان البريطاني إن هذه التهديدات أكدت على حاجة إستونيا لمساعدة مواطنيها على حماية أنفسهم من التدخل الروسي.

التثقيف حول مخاطر المعلومات المضللة وكيفية اكتشافها يبدأ في سن مبكرة في إستونيا من خلال الرسوم الكرتونية التي تهدف إلى زيادة وعي الأطفال

إن مفهوم "إستونيا الإلكترونية" والمجتمع الرقمي المتطور متأصل بعمق في المواطنين. تقول ماريا موروما مينغيل، محاضرة في جامعة تارتو ومُدرسة سابقة لمحو الأمية الإعلامية في إحدى المدارس الثانوية لمدة 15 عاما: "تُقال لنا هذه القصة مرات عديدة، ونحن معتادون على هذه الفكرة. يتعين علينا أن نفكر في كل شيء من الناحية السيبرانية والرقمية". وتُعد مينغيل دورات في الإعلام ومحو الأمية الرقمية في جامعة تارتو والمدارس الثانوية.

وفي المدارس الابتدائية والإعدادية الإستونية، لا يوجد مقرر دراسي محدد حول محو الأمية الإعلامية. وبدلا من ذلك، تُدمج مثل هذه المفاهيم في المواد الدراسة الأخرى. على سبيل المثال، قد يتعمق معلمو الرياضيات في الإحصائيات، التي يمكن إساءة فهمها أو التلاعب بها. وتحلل دروس الرسم الصور وكيف تجعل الإعلانات أو صور وسائط معينة المشاهدين يرون أشياء بعينها. كما يمكن أن تركز دروس مادة الدراسات الاجتماعية على الدعاية الحربية.

ويشير كومباس إلى أنه في رياض الأطفال، قد يلعب الأطفال بألعاب ذات مقابض توجه الحشرة للقيام بأشياء مختلفة. ويشير إلى أن هذا درس مبكر في أساسيات الترميز ومفهوم الخوارزميات.

ويتعلم الأطفال الصغار كيفية إنشاء المحتوى الرقمي، وكذلك كيفية استخدام الإنترنت بأمان، كما تقول بريت جارفيت، مستشارة التخطيط الاستراتيجي في وزارة التعليم في إستونيا.

وتضع المعايير التعليمية الوطنية في إستونيا للمدارس أهدافًا ونتائج دراسية محددة يجب الوصول إليها. وتقرر المدارس نفسها كيفية الوصول إلى الأهداف، لذلك يتمتع المعلمون بالمرونة عند اختيار المواد والأساليب الدراسية.

لكن دورة "الإعلام وتأثيره" الإلزامية في المدارس الثانوية في إستونيا تركز على دور الإعلام والصحافة في المجتمع، بما في ذلك كيفية عمل وسائل التواصل الاجتماعي، وكيفية عمل الروبوتات والمتصيدين وكيفية الحماية منهم. ويتعلم الطلاب التفرقة بين الحقائق والرأي، والمصادر الموثوقة والمصادر المشكوك فيها، بالإضافة إلى أدوات أخرى للتحليل النقدي.

وبالإضافة إلى هذه الدورة الإلزامية، تقدم المدارس الثانوية عادةً دروسًا اختيارية إضافية حول الإعلام. تقول ليزا كويك، معلمة محو الأمية الإعلامية في مدرسة ثانوية في إستونيا، إنه في العديد من هذه الدورات، يصنع الطلاب الوسائط الإعلامية بأنفسهم. وتقول إن هذا يساعدهم على معرفة كيفية إنشاء المحتوى، سواء كان في شكل مقاطع فيديو أو صور أو منشورات على وسائل التواصل الاجتماعي أو مدونات - وكيف يمكن تصميمه للإقناع أو التلاعب.

الهجمات الإلكترونية على أستونيا عام 2007: الحرب الإلكترونية الأولى

قبل بدء السباق الرئاسي الأميركي بتسعة أعوام، كانت روسيا متورطة في فضيحة أخرى كبيرة تتعلق بأستونيا. تعد أستونيا، الدولة الأوروبية الصغيرة، التي كانت جزءا من الاتحاد السوفياتي سابقا وأصبحت في الوقت الحالي عضوا في كل من الاتحاد الأوروبي وحلف الناتو، أحد مؤيدي الحوكمة الإلكترونية. وفقا لخطة «أستونيا الإلكترونية»، تحولت الدولة إلى «مجتمع إلكتروني» بمعنى أن جميع أعمال الحكومة والبنوك تتم دون إجراءات ورقية. وحتى التصويت في الانتخابات يتم عبر الإنترنت. وكانت الدولة التي يبلغ تعدادها 1.3 مليون نسمة أول بلد يجعل الاتصال بالإنترنت حقا إنسانيا. وفي عام 2016، كانت 99.6 في المائة من التعاملات تتم عن طريق خدمات مصرفية إلكترونية، وأعلن 96 في المائة من السكان عن دخلهم إلكترونيا.

ولكن أدت طموحات أستونيا بإحداث ثورة في الحوكمة الإلكترونية إلى تعرُّض البلاد إلى مخاطر غير مسبوقة. في عام 2007، في جزء من محاولاتها للتخلي عن إرثها من الاتحاد الأوروبي، قررت الحكومة نقل نصب تذكاري من الحرب السوفياتية من وسط مدينة تالين. ثار الغضب الروسي وانهالت تهديدات بفرض العقوبات عقب تلك الخطوة. واعتدى مشاغبون على السفير الأستوني في موسكو، وسريعا ما أصيبت مواقع الأجهزة الحكومية الأستونية والصحف والبنوك في البلاد بالتعطل. استمرت الهجمات الإلكترونية لمدة ثلاثة أسابيع، وكانت تأتي على دفعات لتصيب أستونيا بشلل فعلي. أرسل مخترقو الإنترنت كميات كبيرة من المعلومات إلى المواقع الإلكترونية المستهدفة في وقت واحد، مما أدى إلى زيادة الأحمال عليها وتوقفها في النهاية. ووردت تقارير بأن قراصنة الإنترنت اخترقوا ما يصل إلى ربع أجهزة الكومبيوتر في العالم (حيث حولوها إلى أجهزة زومبي)، واستعانوا بروبوت برمجي لإغراق المواقع الأستونية بمعلومات وهمية عن وقوع هجوم حجب الخدمة (وهو هجوم يستهدف وقف خدمة إلكترونية ما بإغراقها بسيل من المعلومات من مصادر متعددة). بالإضافة إلى ذلك، انضم إلى القراصنة أشخاص عاديون حصلوا على تعليمات من مواقع روسية بشأن كيفية شن هجوم حجب الخدمة. وتم اختراق بعض المواقع وإعادة توجيه مستخدميها إلى صور لجنود سوفيات ومقولات لمارتن لوثر كينغ عن مقاومة «الشر». تزامن مع تلك الهجمات نشر معلومات خاطئة، حيث نشرت مواقع إلكترونية أخرى مخترقة أخبارا كاذبة بأن الحكومة الأستونية طلبت العفو من روسيا ووعدتها بإعادة النصب التذكاري إلى موقعه الأصلي.

شبهت حكومة أستونيا هذه الهجمات الإلكترونية التي استغرقت ثلاثة أسابيع بالأعمال الإرهابية. وكانت تلك العمليات أولى حالات «الحرب الإلكترونية» وكان ذلك المصطلح حديثا في عام 2007، كما كان الحال مع «الإرهاب الإلكتروني». وفي حين استطاع مسؤولون أستونيون تعقب بعض عناوين الآي بي الأصلية الخاصة بالمخترقين وصولا إلى الحكومة الروسية والإدارة الرئاسية، فإنهم واجهوا صعوبة في إثبات تنفيذ الحكومة الروسية لتلك الهجمات. ومع ذلك تقدمت أستونيا بطلب رسمي إلى الناتو لتفعيل المادة الخامسة التي تلزم الحلف بالرد على أي هجمات تستهدف أيا من الدول الأعضاء. وكشف ذلك الحادث عن نقاط ضعف مهمة في النظام الذي يقوم على القواعد الدولية. لقد اتضح أن تلك القواعد ليست مصممة على نحو يتناسب مع تحديات القرن الحادي والعشرين، مثل الحرب الإلكترونية. وكان إخفاء الهوية في هذا النوع من الإرهاب الإلكتروني مناسبا للمسؤولين الروس الذين نفوا تورطهم به.

في عام 2007، كتبت آن أبلباوم أن «الهجمات (كانت) 'اختباراً' روسياً لاستعداد الغرب للحرب الإلكترونية في العموم، ولالتزام الناتو تجاه أحدث وأضعف أعضائه بوجه خاص». في ذلك الحين، أخفق الغرب في الاختبار، حيث استطاعت روسيا الخروج من المأزق في النهاية بلا مساس. وكانت صلاحية المادتين الرابعة والخامسة من حلف الناتو غير واضحة بما يكفي لاتخاذ رد فعل ممكن تجاه هذا النوع من المواقف.

ومع ذلك، تلقى المجتمع الدولي بعض الدروس المستفادة من «الحرب الإلكترونية الأولى» في أستونيا. في قمة بوخارست التي عقدها الناتو في عام 2008، أنشأ الحلف مركز تميز الدفاع الإلكتروني التعاوني في تالين بأستونيا. وأنشأ أيضا سلطة جديدة لإدارة الدفاع الإلكتروني في بروكسل. وعلى مدار الأعوام التالية، تأثر عمل الناتو نحو تحسين الأمن الإلكتروني للدول الأعضاء بتجربة أستونيا. سمح ذلك لأستونيا بمواصلة التحول الرقمي لحكومتها ومجتمعها دون حدوث اضطرابات أخرى. وتعد الدولة حاليا من أبرز أعضاء الناتو في مجال الحوكمة الإلكترونية والأمن الإلكتروني.

في الوقت الذي تصارع فيه الحكومات حول العالم تحديات تكنولوجية، بما في ذلك جمع البيانات والذكاء الاصطناعي والتهديدات السيبرانية، تقدم إستونيا نموذجا لكيفية بناء مجتمع رقمي، ونظرا لكونها دولة صغيرة، وضعت إستونيا بصمة كبيرة على الساحة العالمية، حسب تقرير لشبكة "سي إن بي سي".

اجتذبت الدولة الواقعة في منطقة البلطيق التي يبلغ عدد سكانها 1.3 مليون نسمة اهتمام قادة العالم والأكاديميين بفضل مجتمعها الرقمي المتطور.

وقالت رئيسة إستونيا "كرستي كالجوليد" في مقابلة سابقة مع الشبكة الإخبارية: "لدينا جيل نشأ وهو يعلم أنك تتواصل رقميا مع مدرستك لأنا نملك نظاما تعليما رقميا، وحتى مع طبيبك تتواصل عن طريق برامج الصحة الإلكترونية".

وتوضح "كالجوليد": "الحكومة الإستونية تقدم للمواطنين ما لا يمكن أن يقدمه إلا القطاع الخاص".

تستطيع تقديم إقرارك الضريبي عبر الإنترنت في أقل من 5 دقائق، وتتوفر 99% من الخدمات الحكومية عبر الإنترنت على مدار 24 ساعة، وفي الانتخابات يصوت ثلث المواطنين تقريبا عبر الإنترنت.

أكثر كفاءة وأقل تكلفة

- استقلت إستونيا عن الاتحاد السوفيتي عام 1991، وشرعت البلاد في سلسلة من الإصلاحات السريعة لتحديث الاقتصاد، متخذة منذ البداية نهجا رقميا واضحا.

- قالت "كالجوليد": "كانت إستونيا دولة فقيرة نسبيا، وأراد قطاعنا العام وحكومتنا تقديم خدمات عالية الجودة للمواطنين، ولذا وفرنا خدماتنا رقميا على الفور، لأنها كانت ببساطة أرخص وأسهل".

- بدأت مبادرة رئيسية في مجال التعليم، حيث تعهدت إستونيا بوضع أجهزة كمبيوتر في كل فصل، وبحلول عام 2000، كانت كل مدرسة متصلة بشبكة الإنترنت.

- وقدمت الحكومة تدريبا مجانيا على الكمبيوتر لقرابة 10%من السكان البالغين، ساعدت هذه المبادرة في زيادة نسبة المواطنين الذين يستخدمون الإنترنت من 29%في عام 2000 إلى 91% في 2016.

هوية رقمية وأخرى افتراضية

- في عام 2002 ، أطلقت إستونيا نظام هوية وطنية عالي التقنية، حيث ربطت بطاقات الهوية بالتوقيعات الرقمية ليصبح من الممكن دفع الضرائب والتصويت والقيام بالخدمات المصرفية عبر الإنترنت والوصول إلى سجلات الرعاية الصحية.

- وأطلقت برنامج الإقامة الافتراضية، وهي أول مبادرة من نوعها تتيح للأفراد بدء أعمال تجارية في البلاد دون العيش فيها.

- تقدم أكثر من 50 ألف شخص من جميع أنحاء العالم بطلب للاستفادة من هذه المبادرة منذ إطلاقها في عام 2014، ويقدم البرنامج مدخلا للشركات التي تتطلع إلى القيام بأعمال تجارية في الاتحاد الأوروبي والاستفادة من السوق الموحدة.

تأشيرة عمل افتراضية

- تطلق إستونيا الآن تأشيرة تجوال رقمية، للموظفين الذين يعملون عن بعد، وتعد التأشيرة مثالاً للشراكة بين القطاعين العام والخاص مثل التي بين الحكومة الإستونية وشركة "جوبيتيكال"، وهي شركة توظيف عبر الحدود.

- وفي هذا الصدد يقول المستشار القانوني للهجرة بوزارة الداخلية "كيلو فانتسي: "ما نقوم به مع تأشيرة التجوال الرقمية يعكس ما تدور حوله سياسة الهجرة بأكملها، نريد أن نجذب الأشخاص الموهوبين ورجال الأعمال الذين يفيدون مجتمعنا واقتصادنا."

- وتحث الرئيسة التنفيذية لشركة "جوبوتيكال" "كارولي هيندريكس" الدول الأخرى أن تتطلع لنموذج إستونيا وتوظفه في مواجه تحديات مثل شيخوخة السكان ونقص العمالة الماهرة.

- خلقت إستونيا مناخا جاذبا للأعمال، ما شجع الشركات الناشئة على اختيارها، وتم إطلاق منصة "سكايب" لخدمة الدردشة المرئية من إستونيا في عام 2003، قبل أن تشتريها شركة "مايكروسوفت".

- واليوم تفتخر الحكومة بأنها موطن لأكبر شركات تكنولوجيا اليونوكورن حول العالم (شركات ناشئة تقدر قيمتها بأكثر من مليار دولار).

- أحد المنضمين حديثا لقائمة الشركات الناشئة الناجحة هناك هي شركة المدفوعات النقدية "ترانسفر وايز" و"تاكسيفاي" المنافسة لأوبر.

- وتنافس شركات البلوك تشين والأغذية العضوية على أن تكون هي قصة النجاح القادمة التي تبدأ من إستونيا.

الرحلة لم تكن دائما بلا عوائق

- في عام 2007، تعرضت البلاد لاختراق كبير على شبكة الإنترنت أسقط معظم بنيتها التحتية الرقمية.

- في أعقاب الهجوم الذي كان درسا قاسيا، أصبحت إستونيا موطنا لمركز التميز للدفاع السيبراني التعاوني التابع لحلف شمال الأطلسي (الناتو)، والذي يجري تدريبات دفاعية على الإنترنت واسعة النطاق.

-وفي خطوة احترازية، أنشأت الحكومة سفارة للبيانات في لوكسمبورج حيث تقوم بتخزين نسخ من جميع بياناتها.

- ومع ذلك، اضطر المسؤولون إلى التعامل مع أكثر من 10 آلاف حادثة عبر الإنترنت في إستونيا في 2017.

- وحذرت أكبر هيئة تنظيمية في البلاد في الآونة الأخيرة من أن قواعد البيانات على الإنترنت وبرامج مثل الإقامة الافتراضية جعلت إستونيا عرضة للأموال المشكوك في مصدرها والتحايل على العقوبات.

- ويعترف المسؤولون الحكوميون بأن كون المجتمع رقميا فهذا يعني أن عليه الاستعداد دائما للتهديدات السيبرانية، فالحفاظ على الأمن السيبراني مثل النظافة تماما، وعليك أن تغسل يديك دائما، حيث لا تتوقف الجراثيم عن الانتشار ومهاجمتك.

الدرس الثالث / دراسة تحليلية لهجمات مختلفة في مختلف أنحاء العالم

شهد القرن الماضي عدة هجمات سيبرانية (إليكترونية) شنّتها الحكومة الروسيّة ضد دول أجنبيّة، تارة بهدف تقديم المُساعدة أو إلحاق الضرر بمُرشّحين سياسيين مُعيّنين، فيما وتارة أخرى بغرض إحداث الفوضى، غير أنها كانت ترمي جميعها إلى استعراض القوة الروسيّة.

واستعرضت شبكة NBC الإخباريّة الأمريكيّة أبرز الهجمات السيبرانيّة التي شنّتها روسيا على دول أخرى على مدى العشرة أعوام الماضية في تسلسل زمني:

أبريل - مايو 2007: استشاطت موسكو غضبًا من إستونيا، دولة البلطيق الصغيرة (والتي تضم ثلاث دول في أوروبا الشمالية وهي إستونيا ولاتفيا ولتوانيا) التي وقعت تحت قبضة احتلال الاتحاد السوفيتي حتى عام 1991، بسبب خططها الرامية إلى نقل النصب التذكاري للحرب العالمية الثانية الروسية ومقابر الجنود الروس. فما كان من روسيا إلا أن تنتقم بشنّ هجمة إلكترونية تسبّبت في حدوث عُطل مؤقت بخدمة الإنترنت في إستونيا، في هجوم يُعرف باسم هجوم حجب الخدمة أو هجمات الحرمان من الخدمة (DDOS)، مُستهدِفة المكاتب الحكوميّة والمؤسّسات المالية، ما أدى إلى تشويش الاتصالات.

يونيو 2008: قام مُخترقون روس بطمس وتشويه صفحات الويب الحكومية، بعد حظر الحكومة الليتوانية عرض الرموز السوفيتية.

أغسطس 2008: شنّ مُخترقون روس هجمة على خدمة الإنترنت في جورجيا، أدت إلى توقّف الاتصالات الداخليّة في جورجيا، ردًا على إرسال الحكومة الجورجية الموالية للغرب قوات للحكومة الانفصالية المدعومة من موسكو.

يناير 2009: توقّف اثنين من مزوّدي خدمة الإنترنت في قرغيزستان عن العمل، بعد قيام قراصنة روس بشن هجمة DDOS، في إطار الجهود التي كانت تبذلها روسيا آنذاك من أجل الضغط على رئيس قرغيزستان لإزالة قاعدة عسكرية أمريكيّة. بيد أن تلك الهجمة قد أتت ثمارها بعد قيام الجمهورية القيرغيزية بإزالة القاعدة الأمريكيّة، وهو ما دفع الكرملين إلى منح قرغيزستان قروضًا ومساعدات مالية بقيمة 2 مليار دولار لاحقًا.

أبريل 2009: بعد قيام إحدى وسائل الإعلام في كازاخستان بنشر بيان للرئيس الكازاخستاني ينتقد فيه روسيا، طالت هجمات DDOS تلك الوسيلة، على يدّ عناصر من الهاكرز الروس، أدت في نهاية المطاف إلى توقّف الوسيلة الإعلامية عن العمل.

أغسطس 2009: أغلق قراصنة روس موقعيّ تويتر وفيسبوك في جورجيا؛ إحياءاً للذكرى الأولى للغزو الروسي.

مايو 2014: قبل ثلاثة أيام من انتخاب الرئيس الأوكراني، قامت مجموعة من القراصنة الروس باختراق الحواسيب المُسجّل عليها بيانات التصويت والاقتراع، في محاولة للتلاعُب في النتائج وإحداث الفوضى، فيما تمكّن خبراء الحاسب الأوكرانيون من استعادة النظام قبل يوم الانتخابات. وقالت الشرطة الأوكرانيّة إنها ألقت القبض على الهاكرز الذين حاولوا التلاعب في نتيجة الانتخابات التي خسر فيها المُرشّح المدعوم من قِبل روسيا في نهاية الأمر.

مارس 2014: قامت الحكومة الروسية بالتعاون مع الهاكرز لشن هجوم DDOS يُعد أعنف 32 مرة من الهجوم المُماثِل الذي تم شنّه على جورجيا في 2008، تسبب في توقّف خدمة الإنترنت في أوكرانيا في الوقت الذي كان المتمرّدون الروس المُسلّحون الموالون لروسيا يتحكّمون سيطرتهم على شبه جزيرة القرم.

مايو 2015: اكتشف مُحقّقون ألمان تعرّض شبكة الكمبيوتر الخاصة بالبرلمان الألماني (البوندستاغ) للاختراق من جانب مجموعة من الهاكرز، في هجوم سيبراني يُعد الأبرز في تاريخ ألمانيا. وقال دائرة الاستخبارات الاتحادية الألمانية BfV، لاحقًا، إن روسيا كانت تقف وراء هذا الهجوم في مسعى للحصول على معلومات لا تتصل بأعمال مجلس النواب الاتحادي الألماني فقط، بل معلومات تخُص القادة الألمان، وحلف شمال الأطلنطي (الناتو) أيضًا. وقال خبراء الأمن إن الهاكرز حاولا اختراق أجهزة الحاسب الخاصة حزب الاتحاد الديمقراطي المسيحي للمستشارة الألمانية أنجيلا ميركل.

ديسمبر 2015: سيطر هاكرز روس على محطة توليد الطاقة بأوكرانيا، وهو ما تسبّب في ترك 235 ألف منزل بدون كهرباء في أوكرانيا.

يونيو 2015 – نوفمبر 2016: في الولايات المتحدة، اخترق هاكرز روس حواسيب الحزب الديمقراطي، ونجحوا في الوصول إلى عناوين البريد الإلكتروني الشخصيّة للمسؤولين الديمقراطيين، التي تم توزيعها بعد ذلك إلى وسائل الإعلام من قِبل ويكليكس، بغية إحداث الفوضى والتأثير على نتيجة الانتخابات الأمريكية التي انتهت بفوز الجمهوري دونالد ترامب رئيسًا لأمريكا.

أكتوبر 2015: قال خبراء أمنيّون إن الحكومة الروسية حاولت اختراق أجهزة الكمبيوتر الخاصة بالحكومة الهولنديّة من أجل سحب التقرير الخاص بإطلاق مقاتلة أوكرانية صاروخ على طائرة الركاب الماليزية MH17، سقطت في يوليو 2014، ما أدى إلى سقوط 298 قتيلًا كانوا على متنها.

يناير 2016: خرجت شركة أمنية تُعرب عن اعتقادها "وقوف قراصنة روس وراء الهجمات التي وقعت على وزارة الخارجيّة الفنلنديّة قبل بِضعة أعوام".

ديسمبر 2016: في وقت مبكر هذا الشهر، خرج رئيس دائرة الاستخبارات الاتحادية الألمانية BfV، جورج هانز ماسين، يُحذّر من "مُحاولات مُحتملة للتلاعب في الانتخابات الاتحاديّة العام المُقبِل"، في إشارة إلى الانتخابات البرلمانيّة الألمانيّة المُرجّح إجراؤها في سبتمبر 2017. وبشكل أكثر تحديدًا، ذكر ماسين أن روسيا ستكون مصدر هذه الهجمات المُتوقّعة، وأضاف: "نتوقع زيادة غير مسبوقة في الهجمات السيبرانيّة الروسية خلال الفترات التي تسبق الانتخابات".

ويعتقد خبراء الأمن أن الروس يحاولون تدمير المُستشارة الألمانيّة الحالية أنجيلا ميركل، على خلفيّة مواقفها الداعمة لفرض عقوبات ضد الرئيس الروسي فلاديمير بوتين بعد ضم روسيا لشبه جزيرة القرم.

تشير أبحاث وتقارير الأمن السيبراني الصادرة خلال النصف الأول من العام الجاري (2019) إلى تزايد معدلات الهجمات السيبرانية على اختلاف طبيعتها، وطبيعة الفاعل الذي تستهدفه، والهدف من ورائها. وفي ضوء صعوبة حصر كافة تلك الهجمات على وجه الدقة، يمكن تسليط الضوء على أبرز هذه الهجمات، للوقوف على دلالاتها وملامحها المستقبلية.

أبرز الهجمات السيبرانية خلال الربع الأول من عام 2019

شهد الربع الأول من عام 2019 جملةً من الهجمات السيبرانية التي استهدفت عددًا كبيرًا من الدول، بما في ذلك ألمانيا، وكوريا الجنوبية، وإندونيسيا، وغيرها. فمع بداية العام، تم كشف بيانات مئات الساسة الألمان على تويتر؛ بما في ذلك "أنجيلا ميركل"، وأعضاء البرلمان الألماني، والبرلمان الأوروبي، والمسئولون المحليون على مستوى الحكومة الاتحادية وحكومات الولايات .

وبالتزامن مع بداية العام أيضًا، أعلنت وزارة العدل الأمريكية عن عملية لتعطيل روبوتات تابعة لكوريا الشمالية، والتي كانت مخصصة لاستهداف الشركات في قطاعات الإعلام، والفضاء، والمالية، والبنية التحتية الحيوية. كما كشفت اللجنة الوطنية الديمقراطية الأمريكية عن استهدافها من قبل متسللين روس خلال الأسابيع التي تلت انتخابات التجديد النصفي لعام 2018. وبالمثل أعلنت وزارة الدفاع الوطني في كوريا الجنوبية عن خرق قراصنة مجهولين أنظمة الحاسوب في مكتب المشتريات بالوزارة. وتم الكشف عن مشاركة إيران في حملةٍ عالمية تستهدف مقدمي خدمات الاتصالات والبنية التحتية للإنترنت، بالإضافة إلى الجهات الحكومية في الشرق الأوسط، وأوروبا، وأمريكا الشمالية.

وقد شهد شهر فبراير من هذا العام عددًا من الهجمات السيبرانية التي استهدفت كوريا الجنوبية؛ حيث استهدف قراصنة تابعون لكوريا الشمالية عدة مؤسساتٍ تابعة لكوريا الجنوبية بالتزامن مع قمة فيتنام التي جمعت كلًّا من "كيم جونج أون" ودونالد ترامب". كما استهدف المتسللون المرتبطون بأجهزة المخابرات الروسية أكثر من (1000) فرد في أوروبا ممن يعملون في منظمات المجتمع المدني المعنية بأمن الانتخابات وتعزيز الديمقراطية .

وفي الشهر نفسه، تم القبض على بعض المتسللين الذين استهدفوا أنظمة الحاسب الآلي في البرلمان الفيدرالي الأسترالي. كما كشفت شركة إيرباص الفضائية الأوروبية عن استهدافها من قبل قراصنة صينيين قاموا بسرقة المعلومات الشخصية لبعض الموظفين بها .

واستهدفت مجموعة تجسس إلكترونية إيرانية، في شهر مارس، البنية التحتية الرقمية الحكومية والصناعية في المملكة العربية السعودية، والولايات المتحدة. وفي الشهر ذاته، اخترق جهاز المخابرات الإيراني الهاتف المحمول لرئيس جيش الدفاع الإسرائيلي السابق وزعيم المعارضة الإسرائيلية "بيني غانتز" قبيل الانتخابات الإسرائيلية في أبريل. كما استهدف قراصنة من كوريا الشمالية شركةً أمنيةً إسرائيليةً كجزءٍ من حملة تجسس صناعية. واستهدف المتسللون الروس عددًا من الوكالات الحكومية الأوروبية قبل انتخابات الاتحاد الأوروبي.

وفي مارس الماضي أيضًا، أفادت لجنة الانتخابات الوطنية في إندونيسيا بأن المتسللين الصينيين والروس بحثوا في قاعدة بيانات الناخبين في إندونيسيا قبل الانتخابات الرئاسية والتشريعية في البلاد. واستهدف قراصنة إيرانيون الآلاف من الأشخاص في أكثر من (200) شركة للنفط والغاز والآلات الثقيلة في جميع أنحاء العالم، لسرقة أسرار الشركات ومسح البيانات من أجهزة الكمبيوتر.

أبرز الهجمات السيبرانية في الربع الثاني من عام 2019

شهد الربع الثاني من العام -على غرار مثيله الأول- جملةً من الهجمات السيبرانية التي استهدفت بالمثل عددًا كبيرًا من الدول بما في ذلك: فنلندا، وليتوانيا، وإيران، وغيرها. ففي أبريل، أعلن مكتب منظمة العفو الدولية في هونج كونج عن وقوعه ضحية هجوم من قراصنة صينيين تمكنوا من الوصول إلى المعلومات الشخصية للعاملين بالمكتب. واستهدفت المنظمات العسكرية والحكومية الأوكرانية إحدى الحملات التي قام بها قراصنة من "جمهورية لوهانسك الشعبية" (التي أعلنت استقلالها عن أوكرانيا في عام 2014). وقام المتسللون بحملة تضليل في ليتوانيا لتشويه سمعة وزير الدفاع من خلال نشر شائعاتٍ تتهمه بالفساد.

كما حققت الشرطة الفنلندية في إحدى هجمات رفض الخدمة التي استخدمت لنشر قوائم الأصوات في الانتخابات الفنلندية. وتزايدت الشكوك بشأن قيام الإيرانيين بحملة قرصنة ضد البنوك، وشبكات الحكومة المحلية، والهيئات العامة الأخرى في المملكة المتحدة. وأعلنت شركة الأدوية "باير" أنها منعت هجومًا قام به قراصنة صينيون يستهدفون بيانات حول ملكية فكرية حساسة .

وشهد شهر مايو الماضي ثلاث هجماتٍ سيبرانية كبرى؛ حيث طورت إيران شبكة من المواقع والحسابات لنشر معلوماتٍ كاذبة عن كلٍّ من: الولايات المتحدة، وإسرائيل، والمملكة العربية السعودية، بينما شن جيش الدفاع الإسرائيلي غارةً جوية على حماس بعد اختراق عدة أهداف إسرائيلية. وأفادت التقارير -في الشهر ذاته- بأن قراصنة تابعين للمخابرات الصينية استخدموا أدوات القرصنة التابعة لوكالة الأمن القومي منذ عام 2016.

ومؤخرًا، تجلى الصراع السيبراني بين الولايات المتحدة وإيران كبديل للأداة العسكرية، حيث يُعتقد قيام إيران باستهداف الوكالات الحكومية الأمريكية، فضلًا عن قطاعات الاقتصاد بما في ذلك القطاعات المالية، والنفط، والغاز، وذلك من خلال عدد من رسائل البريد الإلكتروني المخادعة. وفي الوقت ذاته، سمحت الولايات المحددة للقيادة السيبرانية الأمريكية بشن هجومٍ سيبراني انتقامي لاختراق أنظمة الكمبيوتر الإيرانية التي كانت تتحكم في منصات إطلاق الصواريخ والقذائف. كما استهدفت الهجمات أنظمة الكمبيوتر التابعة للحرس الثوري الإيراني، وأنظمة الأسلحة الإيرانية، وأنظمة مراقبة الصواريخ الإيرانية، وشبكة تجسس مسئولة عن تعقب السفن في مضيق هرمز الاستراتيجي .

الفعل ورد الفعل

على الرغم من الوقوف على الحالات السابقة؛ إلا أن الحصر الدقيق لكافة الهجمات السيبرانية أمرٌ معقد، خاصةً في ظل استحالة الكشف عن بعضها، وعدم الإبلاغ عن بعضها الآخر؛ فقد تتعرض الدول أو المؤسسات أو الأفراد لهجماتٍ سيبرانية دون أن يدركوا وقوعها. وهو الأمر الذي يثير التساؤل عن كيفية الاستجابة لها، خاصة في ظل غياب الأدلة القاطعة التي لا تقبل الجدل عن هوية مرتكبيها على وجه الدقة، وغياب الرد المضاد نتيجة لذلك.

ويُستثنى من ذلك بطبيعة الحال استهداف إسرائيل لمقر الوحدات السيبرانية التابع لحركة حماس بغارةٍ جوية، بعد أن ادّعى جيش الاحتلال الإسرائيلي قيام حركة حماس بهجومٍ سيبراني على أهدافٍ مدنية. إذ تُعد تلك الغارة هي الأولى من نوعها في حوادث الانتقام الجسدي والعنيف ضد المتسللين وقراصنة المعلومات، خاصة أن جيش الاحتلال أعلن عن توقف الهجوم السيبراني قبل قصف المقر، ما يعني أنه لم يكن هناك مبرر للقصف. ولم يسبق لجيشٍ نظامٍ استخدام القوة العسكرية للرد على هجومٍ سيبراني.

وقد أثار ذلك جدلًا واسعًا بين فريقين؛ يرى أولهما أن هجوم جيش الدفاع الإسرائيلي يُعد نقطة تحول حاسمة في الحروب السيبرانية، لأن الهجوم دار بالأساس بين جيش نظامي من ناحية، وقراصنة الإنترنت من ناحيةٍ أخرى، ولأن قواعد القانون الدولي تحظر استخدام القوة العسكرية إلا في حالات الدفاع الشرعي عن النفس، وفي إطار جملةٍ من الضوابط التي يأتي في مقدمتها التناسب، وهو ما لم يتحقق. فرغم تنوع وتعدد وتكرار وقوع الهجمات السيبرانية، إلا أن الدول عادةً ما تتعاطى معها بأدواتٍ غير عسكرية. فقد

طورت إسرائيل والولايات المتحدة فيروس "ستكسنت" لتخريب أجهزة الطرد المركزي النووية الإيرانية، وانخرطت الصين في عمليات تجسس سيبرانية لسنوات؛ إلا أن ذلك لم يُسفر عن الاستخدام الفعلي للقوة العسكرية، وتم التعاطي معها جميعًا من خلال المفاوضات الدبلوماسية، والعقوبات الاقتصادية، وغيرها لتجنب تصعيد الصراع.

أما الفريق الثاني فيرى أن الهجوم الإسرائيلي لم يكن له علاقة بالمجال السيبراني، وأن المقر الذي تم استهدافه استخدمه عملاء المخابرات التابعون لحماس. لذا لا يمثل هجوم جيش الدفاع الإسرائيلي سابقةً، خاصة مع استمرار حالة الصراع المسلح الحالي بين الجانبين. ومع الاعتراف بالمجال السيبراني كمجالٍ للحرب -على شاكلة البر والبحر والجو- من الطبيعي أن يتحول قراصنة المعلومات إلى أهدافٍ في القريب العاجل .

الدلالات المستخلصة

مما سبق تتضح خطورة التهديدات السيبرانية مقارنة بمثيلتها التقليدية، ففي حين تنصبّ التهديدات العسكرية التقليدية على استهداف الدول وجيوشها العسكرية وإقليمها الجغرافي بالأساس، تستهدف الهجمات السيبرانية أنظمة المعلومات والشبكات الإلكترونية التي تعتمد عليها الدول بشكل رئيسي مخلفةً نتائج تتراوح بين الأضرار المادية الطفيفة، وتدمير البنية التحتية، وتسريب معلومات سرية، وسرقة البيانات، والمساس بالأمن القومي للدول.

كما يتضح أيضًا تعدد أنماط تلك الهجمات من حالةٍ إلى أخرى، واختلاف أهداف كل منها، لتشمل: التجسس، واستعراض القوة، والانتقام، وإلحاق أضرارٍ مادية بالخصم، وغيرها، مما يعني تباين الآثر التدميري لتلك الهجمات من حالةٍ إلى أخرى، وإن كان أخطرها هو الهجمات المدمرة الصريحة ضد البنية التحتية الحيوية. أضف إلى ذلك طول أمد الفترة الزمنية بين وقوع الهجمة السيبرانية من جانب، واكتشاف وقوعها من جانبٍ آخر، والرد عليها من جانبٍ ثالث. وقد لا يُكتشف عددٌ منها ابتداءً، وحتى وإن تم اكتشافها فإن كافة الدول التي توجه إليها أصابع الإتهام تُنكر قيامها بشنها .

وتأخذ الهجمات السابقة شكل المنحنى الآخذ في الصعود، وهي الهجمات التي لا يُمكن للدول أو الشركات الكبرى بما في ذلك: ماريوت، وإيكوفاكس، وياهو، وفيسبوك، أن تنأى بنفسها عنها. والأكثر خطورة من ذلك، قدرتها على استهداف العمليات الانتخابية لأعرق الديمقراطيات. وكما يتضح، تتعدد أسباب تلك الهجمات لتشمل ثغرات الأمن السيبراني، مثل: البرامج غير المرخصة، وشهادات الأمان منتهية الصلاحية، وتدابير الأمن السيبراني غير الكافية، وغيرها .

كما تكشف الهجمات عن اتجاهاتٍ ودوافع جديدة من التشفير إلى الفدية، إلى استغلال نقاط ضعف الأجهزة المحمولة للهجمات من أجل المصالح الوطنية. وشملت الهجمات كذلك البنية التحتية لتكنولوجيا المعلومات، والمستشفيات، والموانئ، والمطارات، والصحف، وغيرها. وأصبحت البرمجيات الخبيثة أيضًا متعددة الوظائف في منهجيتها وأغراضها، مما أدى إلى حدوث هجمات هجينة تجمع بين برامج التشفير والتشفير الخبيث .

الاتجاهات المحتملة

نظرًا لاستمرار نمو سوق إنترنت الأشياء، واستخدام التطورات التكنولوجية في مختلف المجالات تقريبًا، يتوقع الخبراء تزايد الهجمات السيبرانية والخسائر الناجمة عنها في النصف الثاني من 2019 وفقًا لوتيرةٍ متسارعة، بل وفي السنوات القادمة أيضًا. وتشير إحصاءات العام الجاري إلى احتمالات تزايد تكلفة الهجمات السيبرانية لتصل إلى (6) تريليونات دولار سنويًا بحلول عام 2021، بزيادة قدرها 3 تريليونات دولار عن توقعات عام 2015. وهو ما يعني تزايد الآثار الناجمة عنها، ومن ثم ربحيتها لمرتكبيها مقارنة بعددٍ من الأنشطة غير المشروعة مثل تجارة المخدرات على سبيل المثال .

ويقدر تقرير الجريمة السنوية لمشروعات الأمن السيبراني Cybersecurity Ventures Annual Crime Report متوسط تكلفة الجرائم السيبرانية لمختلف المنظمات بحوالي)13(مليون دولار سنويًّا، وذلك وفقًا للدراسة العالمية التي أجرتها .Accenture ووفقًا للتقرير السنوي للأمن السيبراني الصادر عن شركةBulletproof ، قد يكلف هجوم الحرمان من الخدمة الشركات الكبرى أكثر من مليوني دولار، والشركات الصغرى ما يزيد عن 120 ألف دولار بنهاية عام 2019. ناهيك عن ارتفاع تكلفة هجمات الفدية لتصل إلى)11.5 (مليار دولار سنويًّا بنهاية هذا العام، و(20) مليار دولار سنويًّا بحلول عام 2021، مما يجعل ذلك النوع من الهجمات هو الأسرع نموًّا. إذ تعتبر هجمات الأمن السيبراني -بشكلٍ عام- من أسرع الجرائم نموًّا في العالم، سواء نفذت من قبل مجرمي الإنترنت أو الدول القومية. وهو ما يؤكد عليه اختراق (1.16) مليار عنوان بريد إلكتروني وكلمة مرور في عام 2019 في خرقٍ هائل سُمي "Collection 1"، بجانب اختراق بيانات أكثر من نصف مليار مستخدم من مستخدمي الفيسبوك في عام 2019، وعرض تلك البينات علنًا في قواعد البيانات التابعة لأمازون.ختامًا، هناك حاجة إلى تعزيز الجهود العالمية لمكافحة الهجمات السيبرانية، خاصة أنها باتت تطال الدول الكبيرة والصغيرة على حدّ سواء في ضوء تسارع التطورات التكنولوجية والتقنيات المستخدمة في هذا المجال.

الدرس الرابع / تحليل لأهم المواقع الإحصائية للهجمات السيبرانية

تعد الهجمات السيبرانية المتقدمة أحد التحديات الكبرى التي تواجهها المؤسسات والأفراد في العصر الرقمي الحديث. فمع تطور التكنولوجيا، أصبحت الهجمات السيبرانية أكثر تطورًا وتعقيدًا، مما يتطلب استراتيجيات تصدي متقدمة ومتعددة الأطراف. يهدف هذا المقال إلى دراسة حالة للهجمات السيبرانية البارزة وتقديم نظرة شاملة حول كيفية التصدي لها.

الهجمات السيبرانية المتقدمة

سنستعرض بعض الهجمات السيبرانية المتقدمة التي وقعت في السنوات الأخيرة وأثرت على المؤسسات والأفراد. واحدة من الهجمات البارزة هي هجمات الفدية(Ransomware) ، حيث يتم اختراق أنظمة المؤسسات وتشفير البيانات مع مطلب فدية لاستعادتها. كما نجد هجمات التصيد الاحتيالي (Phishing) التي تستخدم رسائل البريد الإلكتروني المزيفة للحصول على معلومات شخصية ومالية من الضحايا. بالإضافة إلى ذلك، هجمات الإنكار الخدمي الموزع (DDoS) تستهدف المواقع والخوادم بتكديس حركة المرور وتعطيلها. وأخيرًا، هجمات استغلال الثغرات الأمنية (Exploits) تستغل الثغرات في البرمجيات والنظم للوصول غير المشروع والتحكم فيها.

استراتيجيات التصدي للهجمات السيبرانية

في هذا الجزء، سنركز على كيفية التصدي للهجمات السيبرانية المتقدمة.

أولاً، يجب تعزيز الوعي الأمني لدى المؤسسات والأفراد من خلال توفير تدريبات وورش عمل حول التهديدات السيبرانية وكيفية التعامل معها.

ثانيًا، ينبغي تطبيق سياسات الأمان القوية وتنفيذ أفضل الممارسات مثل تحديث البرامج والنظم بانتظام لسد الثغرات الأمنية.

ثالثًا، يمكن استخدام تقنيات التحليل السلوكي لاكتشاف الأنشطة الضارة والمشتبه بها داخل الشبكة، مما يمكن من رصد ومنع الهجمات قبل وقوعها.

أخيرًا، ينبغي إقامة شراكات استراتيجية مع شركات الأمن السيبراني المتخصصة لتوفير حلول متقدمة وتحليل استراتيجي للتهديدات.

دراسة حالة لاستراتيجية التصدي لهجمة سيبرانية متقدمة

دراسة حالة لاستراتيجية التصدي لهجمة سيبرانية متقدمة. لنفترض أن مؤسسة X تعرضت لهجمة فدية حيث تم اختراق أنظمتها وتشفير بياناتها. كيف يمكن للمؤسسة التصدي لهذه الهجمة؟

1- العزل والاستجابة السريعة:

يجب على المؤسسة عزل الأنظمة المصابة فورًا لمنع انتشار الهجمة. ينبغي أيضًا تشكيل فريق استجابة سريعة للتعامل مع الهجمة وتقييم الأضرار ومحاولة استعادة البيانات.

2- إعادة التشغيل من النسخة الاحتياطية:

في حالة حدوث هجمة فدية، يكون الحل الأمثل هو استعادة البيانات من نسخة احتياطية موثوقة. يجب على المؤسسة المحتجزة للبيانات الاحتفاظ بنسخ احتياطية منتظمة واختبار فعالية استعادتها.

3- تحليل الأمان وتدقيق الثغرات:

بعد التعامل مع الهجمة، يجب على المؤسسة تحليل سبب الاختراق وتقييم الثغرات الأمنية التي تم استغلالها. يمكن أن يساعد تدقيق الثغرات في اكتشاف الثغرات وتقديم توصيات لتعزيز الأمان.

4- تعزيز الأمان والتدريب المستمر:

يجب أن تتخذ المؤسسة إجراءات لتعزيز أمان أنظمتها وشبكتها. يمكن أن تتضمن هذه الإجراءات تحديث البرامج والنظم بانتظام، وتطبيق سياسات الأمان القوية، وتوفير تدريبات مستمرة للموظفين حول التهديدات السيبرانية وكيفية التعامل معها.

1. أنواع تغطيات تأمين السايبر (المخاطر الالكترونية):	: Types of Cyber Insurance Coverage
1.1 تغطية خصوصية البيانات	Data Privacy Coverage
1.2 تغطية المسؤولية عن الخسارة أو خرق البيانات	Liability Coverage for Loss or Breach of Data
1.3 تغطية تكاليف المعالجة / مثل إخطار العميل والتحقيقات الجنائية	Coverage for Remediation Costs such as Customer Notification and Forensic Investigations
1.4 تغطية غرامات الجهات الرقابية و / أو العقوبات المرتبطة بخروقات البيانات	Coverage for Regulatory Fines and/or Penalties Associated with Data Breaches
2. أنواع أخرى من تغطيات تأمين السايبر (المخاطر الالكترونية):	Other Types of Cyber Coverage:

2.1 التكاليف والمسئوليات الناشئة عن حوادث الأمن الالكتروني التي لا تنطوي على خروقات البيانات.	Costs and Liability Arising out of Cybersecurity Incidents not involving Data Breaches
2.2 الأعمال التجارية وانقطاع الأعمال المحتمل.	Business and Contingent Business Interruption
2.3 الابتزاز.	Cyber Extortion
2.4 المسؤولية الإعلامية.	Media Liability
3. تغطية الازمات للطرف الأول	First-Party Coverage Crisis
3.1 عملية الادارة واسترجاع هوية المؤسسة بعد حادث السرقة : نفقات الاتصالات لإخطار العملاء المتضررين، وتقديم خدمات مراقبة الائتمان، وإجراء تحقيقات الطب الشرعي، والنفقات المتكبدة في الابقاء على إدارة الأزمات أو تكاليف الحصول على شركة العلاقات العامة لغرض حماية أو استعادة سمعة المنظمة.	Management & Identity Theft Response: Expenses for communications to notify affected customers, provide credit monitoring services, conduct forensic investigations, and for expenses incurred in retaining a crisis management or public relations firm for the purpose of protecting/ restoring the organization's reputation.
3.2 الابتزاز: نفقات دفع الفدية أو التحقيق في تهديدات إطلاق السراح، الإفشاء، النشر،التدمير، السرقة أو استخدام المعلومات السرية. إدخال الشفرات الخبيثة في نظام الكمبيوتر. فساد أو تلف أو تدمير نظام الكمبيوتر . تقييد أو عرقلة الوصول إلى نظام الكمبيوتر.	Cyber Extortion: Expenses to pay ransom or investigate a threat to release, divulge, disseminate, destroy, steal or use confidential information; introduce malicious code into a computer system; corrupt, damage or destroy a computer system; or restrict or hinder access to a computer system.
3.3 حماية أصول البيانات:	Data Asset Protection:

استرداد التكاليف والنفقات التي تكبدتها المنظمة لاستعادة أو إعادة إنشاء أو استعادة الوصول إلى أي برامج أو بيانات إلكترونية من النسخ الاحتياطية أو من النسخ الأصلية. أو معاً تجميع وإعادة إنشاء مثل هذه البرمجيات أو البيانات الإلكترونية من مصادر أخرى إلى المستوى أو الحالة التي كانت موجودة عليها مباشرة قبل تغييرها، أوفسادها، أوتدميرها، أوحذفها أو الحاق اضرار بها.	Recovery of your costs and expenses incurred to restore, recreate or regain access to any software or electronic data from back-ups or from originals or to gather, assemble and recreate such software or electronic data from other sources to the level or condition in which it existed immediately prior to its alteration, corruption, destruction, deletion or damage.
3.4 انقطاع شبكة الأعمال: تسديد خسارة الدخل و / أو النفقات الإضافية نتيجة لانقطاع أو تعليق الأنظمة.	Network Business Interruption: Reimbursement for loss of income and/or extra expenses resulting from an interruption or suspension of systems.
4. تغطية الطرف الثالث	Third-Party Coverage
4.1 مسؤولية أمن الشبكة: تغطي المطالبات من الأطراف الثالثة الناشئة عن خرق في أمن الشبكة أو نقل البرمجيات الخبيثة / الفيروسات إلى أجهزة كمبيوتر وانظمة الطرف الثالث.	Network Security Liability: Covers claims from third parties arising from a breach in network security or transmission of malware/viruses to third-party computers and systems.
4.2 مسؤولية الخصوصية: تغطي المطالبات من أطراف ثالثة نتيجة لعدم التعامل بشكل صحيح مع إدارة، تخزين أو حماية المعلومات الشخصية/التعريفية الأخرى. سرية معلومات الشركة والانتهاك غير المقصود للوائح الخصوصية.	Privacy Liability: Covers claims from third parties as a result of a failure to properly handle, manage, store or otherwise protect personally identifiable information, confidential corporate information and unintentional violation of privacy regulations.
5. الاستثناءات الرئيسية / الحدود الفرعية	Key Exclusions/Sub Limits[8]

5.1 استبعاد الأجهزة الإلكترونية المحمولة: إذا كان الجهاز الذي أدي إلى خرق الكتروني هو جهاز محمول، العديد من الوثائق يمكن أن تستبعد التغطية تماما عن أي خسارة ناتجة.	Portable Electronic Device Exclusion: If the device leading to a cyber breach is portable, many policies could exclude coverage completely for any resulting loss.
5.2 اعمال الاستبعاد المقصودة: مرة اخري، الفجوة هنا هي افضل توضيح لسيناريوهات التناقض بين الانواع المختلفة لمنتجات التأمين وبالذات منتج المسئولية أمام منتج الجريمة. وثيقة الجريمة أوالامانه تغطي بشكل عام خسارة الطرف الاول للمؤمن له حتى لو الخسارة حدثت بسبب المؤمن له أما وثائق المسئوليات بشكل عام تغطي الاضرار أو الخسائر التي سببها المؤمن له للطرف الثالث. معظم وثائق تأمين السايبر (الاخطار الالكترونية) لا تقدم على نحو كاف للطرف الاول والثالث. على سبيل المثال، تستثني وثائق المسؤولية تغطية الأضرار أو الخسائر التي يتسبب فيها المؤمن له عمداً. وبالتالي، إذا تسبب الموظف عن طريق الخطأ في حدوث خرق إلكتروني، فسيتم تغطية الخسارة الناتجة (إما تحت مسؤولية عامة أو تحت مظلة الوثيقة التي لا تستثني مخاطر السيبر(المخاطر الالكترونية) أو بموجب وثيقة إلكترونية مستقلة). ومع ذلك، إذا تسبب موظف اخر في نفس الخرق الإلكتروني عن عمد، فإن الخسارة الناتجة سيتم رفضها بموجب وثيقة المسؤولية العامة إذا كان هذا الاستثناء موجود.	Intentional Acts Exclusion: Again, the gap here is best outlined in a scenario that contrasts different types of insurance products, namely a liability product against a crime product. A crime or fidelity policy generally covers first-party loss to the Insured even where such loss is caused by the Insured, while liability policies generally provide for damages or losses the Insured causes to a third party. Most cyber insurance policies do not adequately provide for both first-party and third-party loss. For example, liability policies typically exclude coverage for damages or losses intentionally caused by an Insured. Thus, if an employee accidentally caused a cyber breach, the resulting loss would be covered (either under a general liability or umbrella policy that does not exclude cyber perils or under a stand-alone cyber policy). However, if a different employee caused the exact same cyber breach intentionally, the resulting loss would be denied under a

general liability policy if this exclusion is present.	
Nation / State, Terrorism, Cyber Terrorism / Acts of God Exclusions: Similar to the previous scenario, where coverage was precluded simply based on whether the breach was caused intentionally or unintentionally, nation/state and terrorism as well as Acts of God exclusions can result in coverage being precluded simply based on who or what caused the breach to occur.	5.3 الأمة / الدولة، الإرهاب، استبعادات الإرهاب الإلكتروني / القضاء والقدر: وعلى غرار السيناريو السابق، يستثني من التغطية - سواء إذا كان الخرق ناجما عن قصد أو عن غير قصد- كل من الاحداث المتعلقة بالدولة ، الإرهاب وكذلك الاحداث القدرية وبالتالي يمكن أن تؤدي العناصر السابقة إلى منع التغطية ببساطة بناء على من أو ما الذي تسبب في حدوث الخرق .
Negligent Computer Security Exclusion: Some policies exclude coverage if data is unencrypted or if the Insured has failed to appropriately install software updates or security patches.	5.4 تجاهل او اهمال في امن الكمبيوتر: تستبعد بعض الوثائق التغطية إذا كانت البيانات غير مشفرة أو إذا فشل المؤمن له في تثبيت تحديثات البرامج أو تصحيحات الأمان بشكل مناسب.
Sublimits: Many policies also have sublimits that may apply for things like breach notification costs, forensic expenses, credit monitoring costs, business or network interruption and extra expenses. In addition, business or network interruption coverage may have a larger deductible or include a time element component (i.e., business or network must be down for a certain number of hours before business interruption coverage will be triggered).	5.5 الحدود الفرعية: العديد من الوثائق لديها أيضا حدود فرعية يتم تطبيقها على أشياء مثل تكاليف الاخطار بالاختراق أو الانتهاك، ومصاريف مراقبة الائتمان، الاعمال وانقطاع الأعمال أو انقطاع الشبكة، والنفقات الاضافية. بالإضافة إلى ذلك، قد تكون تغطية الأعمال أوانقطاع الشبكة لديها خصم اكبر أو تتضمن عنصر الوقت (أي، يجب أن يحدث للاعمال أو الشبكة سقوط/ توقف لعدد معين من الساعات قبل أن يتم تشغيل تغطية انقطاع الأعمال).

5.6 خدمات ما بعد الخرق: بعض شركات التأمين بدأت في شراكة مع المتخصصين في الأمن الالكتروني لمساعدة العملاء الذين حدثت لهم تجربة خرق عبر الإنترنت / خرق إلكتروني وذلك لتقديم تحقيقات الطب الشرعي، واستراتيجيات الاستجابة للحوادث الاستباقية، والتدريب وذلك لأنها تدرك فائدة ذلك لكل من العملاء والشركة نفسها في الاستجابة بسرعة وبكفاءة بقدر الإمكان إلى الخرق الالكتروني /عبر الإنترنت للحفاظ أو تثبيت التكاليف الناتجة عن وقوع الحدث ،والمطالبات، والأضرار لتكون جميعها منخفضة بقدر الإمكان.	Post-Breach Services: Some insurers are starting to partner with cybersecurity specialists to assist customers who experience a cyber breach with forensic investigations, proactive incident response strategies, and training as they realize the benefit both to the customer and themselves in responding as quickly and efficiently as possible to a cyber breach to keep resulting costs, claims, and damages as low as possible.
5.7 المسؤولية غير المباشرة/ البائعون: العديد من وثائق السيبر(التأمين ضد المخاطر الالكترونيه) القياسية تستثني تغطية البيانات التي عهدت بها المنظمة إلى بائع طرف ثالث الذي تم اختراقه.	Vicarious Liability/Vendors: Many standard Cyber policies exclude coverage for data an organization has entrusted to a third-party vendor who is breached.
6. الاعتبارات العامة الأخرى للوثيقة:	Other Policy Considerations:
6.1 يجب ان تتم مراجعة البنود بعناية. 6.2 إذا كنت لا تفهم معني شئ ما ، هذا يعني غالباً أن هذا الجزء ليس واضحا ويمكن أن يؤدي إلى رفض التغطية أو التقاضي على الشروط. من المهم أن نفهم شروط الوثيقة وعادةً يقوم المكتتبين بتفسير كل النقاط التي تحتاج الي توضيح، لذلك يجب ان يتم الاستفسار. 6.3 في ما يلي بعض العناصر الأخرى التي يجب مراعاتها أثناء مراجعة بنود وثيقتك: Û التهديدات الداخلية :هل تشمل التغطية حوادث مخالفات داخلية؟	Carefully review the terms of your policy. If you do not understand what something means, that often means it is not clear and could lead to coverage denial or litigation over the terms. It is important to understand the terms of the policy and underwriters will typically explain their position, so just ask. Below are some other items to consider while reviewing the terms of your policy: · Insider Threats. Does your coverage include incidents of insider malfeasance?

Û بيانات عن الأجهزة غير المشفرة أو BYOD :لا تغطي بعض الوثائق الأجهزة غير المشفرة أو الأجهزة التي لا تملكها الشركة. Û المعلومات التي تخزنها أو تحتفظ بها من قبل أطراف ثالثة: فهم ما إذا كانت وثيقتك لديها تغطية توسعيه في حال وجود خرق في أحد موردي المؤسسة. Û تكاليف استبدال أو تحديث أو تطوير أو تحسين أو صيانة نظام الكمبيوتر: وكثيرا ما تكون التغطية غير متاحة لاستبدال أو تطوير الأنظمة التي تعاني من نقاط ضعف، ولا توفر التغطية سوى تكاليف الاستبدال للبنية التحتية القائمة. Û تغطية للتحقيقات المحتملة للجهات التنظيمية /الرقابية والغرامات. Û الأضرار التي لحقت بعملاء الشركة. في كثير من الأحيان تمتد تغطية السيير فقط للمستهلكين الأفراد وليس للطرف الثالث من عملاء الشركة. Û الحدود الإقليمية: تقتصر بعض التغطيات فقط على الحوادث التي تحدث داخل الدولة/الولاية وقد تحتاج المؤسسة إلى تغطية إضافية اعتماداً على مكان البيانات المخزنه. Û تكاليف مراقبة الائتمان. وعادة ما تنص وثائق تأمين السيير على تقديم سنة واحدة من مراقبة الائتمان للمستهلكين المتضررين.	· Data on unencrypted devices or BYOD. policies do not cover devices that Some unencrypted or non company-owned are devices. · Information maintained and stored by third parties. Understand whether your policy will extend coverage if there is a breach at one of the organization's vendors. · Costs to replace, upgrade, update, improve or maintain a computer system. coverage is not available to replace or Often upgrade systems that have vulnerabilities coverage only provides and the replacement costs for the existing infrastructure. · Coverage for potential regulator investigations and fines. · Damages to corporate clients. Often cyber coverage extends only to individual consumers and not to third party corporate clients. · Territorial limits. Some coverage is limited only to incidents that occur in the United States and an organization may need additional coverage depending on where stored. data is · Credit monitoring costs. Cyber insurance policies typically provide for the offering of one year of credit monitoring to affected consumers.

تغطيات اخري متخصصة بكبري شركات التأمين الامريكية [9]

سيبر إيدج CyberEdge هي تغطية تقدمها كبري شركات التأمين الامريكية AIG تتضمن العديد من الحلول المرنة التي تسمح للشركات بالحصول على التغطية التي تتطابق مع متطلباتهم.

وفيما يلي بعض نماذج التغطية المتاحة:

نماذج التغطية المقدمة

الاستجابة الأولى First Response

عندما يشتبه في انتهاك الامن السيبراني (الالكتروني) فإن معظم الاعمال ليس لديها القدرة على تشخيص المشكلة والاستجابة السريعه لها. تغطية سيبر ايدج للاستجابة الاولي تغطي الوصول في حالات الطوارئ الي مستشار قانوني ومتخصص في تكنولوجيا المعلومات من اللذين يمكنهم تقديم الدعم الحاسم والتنسيق المطلوب.

ادارة الحدث Event Management

بعد الهجوم السيبراني (الالكتروني) تطلب المنظمات مجموعة من الخدمات لوضع أو الرجوع بأعمالهم مرة اخري للمسار الصحيح.

تدفع سيبرايدج لادارة الحدث لكل من الخدمات القانونية وتكنولوجيا المعلومات والعلاقات العامة ، كذلك هو الحال لخدمات مراقبة الائتمان والهوية بالاضافة الي ذلك استعادة البيانات وتكاليف الاخطار بالخرق.

المسئوليات وحماية البيانات Data Protection & Cyber Liability

تقوم التغطية بالاستجابة لتعويضات / مطالبات مسئولية الطرف الثالث الناشئة عن الفشل في امن الشبكات ويتضمن ذلك تغطية تكاليف الدفاع ومطالبات / تعويضات المسئولية الناتجة عن خرق سرية البيانات الي جانب تكاليف الدفاع والغرامات القابلة للتأمين التي تتكبدها الشركة اثناء التحقيقات أو التي تطلب منها من قبل المنظم / المراقب.

انقطاع الشبكة Network Interruption

غالبا جميع المستهلكين من الشركات تعتمد على البيع المباشر عبر المواقع الالكترونية وادارة علاقات العملاء Customers Relationship Management وحتي الصناعات التقليدية مثل التصنيع والنقل تتطلب الاتصال بالشبكة للعمل بكفاءة - لذلك فإن تغطية انقطاع الشبكة تغطي فقد / خسارة الدخل ونفقات التخفيف عند توقف العمل أو تعليقه بسبب حادث أمن سيبراني / الكتروني.

انقطاع الشبكة: الاستعانة بمصادر خارجية من مقدمي الخدمات Network Interruption: OSP

الاستعانة بمصادر خارجية من مقدمي الخدمات Outsourced Service Providers (OSPs) للمؤسسات المتضررة للقيام باعمال مثل استضافة المواقع – معالجة عمليات الدفع – جمع وتخزين البيانات.

يمتد ذلك ليشمل تغطية انقطاع الشبكة ليشمل الخسائر وتكاليف التخفيف الناشئة عن استخدام خدمات ال OSP بسبب سقوط الشبكة / النظام.

انقطاع الشبكة : فشل النظام Network Interruption: System Failure

ليس كل فشل أو سقوط بالنظام يكون بسبب خرق الأمن السيبراني، ولكن الانقطاع غير المقصود وغير المخطط بسبب اي عوامل اخري بخلاف الاختراق يمكن أن يؤدي أيضا إلى حدوث خسائر انقطاع الشبكة أو سقوط النظام .

تقدم تغطية فشل النظام / انقطاع الشبكة تغطية الخسائر وتكاليف التخفيف الناتجة عن فشل / سقوط النظام الداخلي الذي لا ينشأ عن خرق الأمن السيبراني ولكن يمكن ان يكون بسبب خطأ بشري او مشكلة في البرامج.

حادثة البيانات الإلكترونية Electronic Data Incident

خرق الأمن السيبراني الالكتروني ليس هو السبب الوحيد الذي يمكن أن يتسبب في ضياع البيانات أو فسادها.

الارتفاع في الطاقة/ الكهرباء ، والكوارث الطبيعية، وارتفاع درجة الحرارة والتخريب المادي يمكن ايضا ان يؤدي إلى عدم إمكانية الوصول إلى البيانات .

نموذج تغطية حادثة البيانات الالكترونية يقوم ببساطة باضافة حادث مؤمن منه الي قسم ادارة الحدث Event Management ويغطي هو الضرر العرضي أو خطر تدمير نظام الكمبيوتر للشركة.

وسائل الاعلام الرقمية Digital Media

في بيئة رقمية سريعة التحرك، أصبح من الأسهل الآن اكثر من أي وقت مضى على الشركات أن تنتهك / تتعدي عن غير قصد على العلامات التجارية inadvertently infringe on trademarks، أو تختلس المواد الإبداعية misappropriate creative material، أو تتفحص الحقائق بشكل غير كاف.

تغطي تغطية وسائل الإعلام الرقمية الأضرار والخسائر وتكاليف الدفاع فيما يتعلق بانتهاك حقوق الملكية الفكرية لطرف ثالث أو الإهمال فيما يتعلق بالمحتوى الإلكتروني.

الابتزاز السيبراني / الالكتروني Cyber Extortion

قد تجد الشركات / الاعمال نفسها هدف لمجرمي الإنترنت الذين يقوموا بتشفير البيانات الخاصة بالشركات ليجبروهم على دفع فدية لشراء مفتاح لفتح هذه البيانات.

يغطي ال Cyber Extortion الخسائر الناجمة عن الابتزاز والتهديد.

وهذا يشمل الفدية لإنهاء الابتزاز فضلا عن الرسوم المتكبدة من المستشارين المتخصصين في الابتزاز السيبراني.

قرصنة الهاتف Telephone Hacking

بالاضافة الي القرصنة على الانترنت ، تواجه الشركات قرصنة الهواتف ويشار اليها باتصال الـ PBX من خلال الاحتيال.

هذا ويستهدف المحتالين أنظمة الهواتف لاجراء مكالمات من خلال مجموعة من الارقام المميزة .

وتقدم تغطية القرصنة للهواتف الرسوم المترتبة على الوصول غير المصرح به واستخدام انظمة هواتف الاعمال التجارية .

جريمة الحاسوب Computer Crime :

ويقصد هنا استخدام اجهزة الحاسوب في عمليات الغش لتحويل الأموال حيث يستخدم المجرمين التفاصيل التي تم الحصول عليها من خرق الأمن السيبراني لاجهزة الحاسوب لنقل الأموال بشكل احتيالي من حساب في مؤسسة مالية الي حساب اخر في جهة اخري .

يقدم هذا النوع تغطية الخسائر المالية المباشرة من تحويلات الأموال الإلكترونية الاحتيالية الناشئة عن خرق الأمن السيبراني.

مفاهيم وتعريفات هامة يجب التعرف عليها لفهم الاخطار الالكترونية "السيبرانية"

1- **الفضاء السيبراني Cyberspace**: فضاء افتراضي يسعى إلى ضم العالم بأسره، ويختلف عن الفضاء الحقيقي وتوجد فيه العديد من المجتمعات الموزعة على نحو غير متساوٍ باستخدام بيئة تقنية - الإنترنت فى المقام الأول - حيث يستفيد المواطنون والمؤسسات من تكنولوجيا المعلومات والاتصالات في تفاعلاتهم.

2- **الأمن السيبراني Cybersecurity** : مصطلح جامع لمجال واسع من القضايا بدءاً من أمن تكنولوجيا المعلومات، ومروراً بأمن المعلومات أو المحتويات، ووصولاً إلى التدابير الأمنية الرامية إلى مكافحة إساءة استخدام الإنترنت والجرائم السيبرانية.

ملحوظة: نظراً إلى أن معمارية الإنترنت Internet architecture لم تراع الأمن السيبراني، فإن إدراج الحماية الأمنية يتطلب إجراء تعديلات جوهرية في البنى التحتية للإنترنت وفي مجموعة بروتوكولات الإنترنت (TCP/IP) تشمل ما يلي:

- إدراج الأمن في التصميم،
- أمن البنية،
- الآليات العتادية التي تحمي الحواسيب والبيانات،
- نظم التشغيل الآمنة،
- الترميز الآمن،
- القدرات وقوائم التحكم في النفاذ،

وتطرأ تغيرات متواصلة على التوازن بين الأمن السيبراني وحقوق الإنسان، ولا سيما الحق في الخصوصية، وحرية التعبير.

3- **تكنولوجيا المعلومات والاتصالات Information and communication technologies (ICT)**:

إدماج الاتصالات السلكية واللاسلكية وأجهزة الحاسوب فضلاً عن البرمجيات والتخزين والأنظمة السمعية والبصرية على نحو يتيح للمستخدمين الوصول إلى المعلومات وتخزينها ونقلها و معالجتها.

4- **أمن المعلومات** Information Security: مجموع العمليات والتقنيات المستخدمة لحماية موارد المعلومات من الاستحواذ غير المرخص به، أو الانكشاف أو التلاعب بها أو تغييرها أو إتلافها وفقدها.

ملحوظة: يشير أمن المعلومات من جهة إلى ضمان عدم فقدان البيانات عندما تطرأ أمور حرجة مثل الكوارث الطبيعية، أو أعطال الحاسوب/الخادم، أو السرقات المادية، أو غيرها. ويشير من جهة أخرى إلى النفاذ غير المرخص به إلى البيانات واستخدامها وكشفها أو عرقلة تداولها أو تغييرها أو الاطلاع عليها أو فحصها أو تسجيلها أو تدميرها.

5- **الإنترنت Internet** : شبكة عالمية عمومية تربط شبكات الحواسيب وتوفر إمكانية الانتفاع بعدد من خدمات الاتصالات والمعلومات مثل شبكة الوِب والبريد الإلكتروني.

6- **إنترنت الأشياء** Internet of things : تكنولوجيا الإنترنت ، التوجه إلى ربط الأشياء بالإنترنت عن طريق إدماج أجهزة استشعار وأجهزة أخرى فضلاً عن إضفاء قدرة التواصل مع بقية العناصر عليها، ومن ثم تحويل العالم المادي نفسه إلى نظام ضخم من المعلومات والمعرفة. ويمكّن ذلك الأشياء أو العناصر من تمييز الأحداث والتغيرات في البيئة المحيطة بها ومن التصرف والتفاعل بطريقة مناسبة دون تدخل بشري.

7- **الإنترنت المحمول / الإنترنت الجوَّال** Mobile Web / Mobile Internet: يشير هذا المصطلح إلى النفاذ إلى شبكة الوِب(World Wide Web (WWW عن طريق استخدام خدمات الإنترنت المعتمدة على المتصفح من خلال أي جهاز محمول باليد (مثل الهواتف الذكية أو الهواتف ذات الخواص المميزة) أو أجهزة الحاسوب المحمولة أو الحواسيب اللوحية وما شابهها والتي تتصل بشبكة هواتف محمولة أو بأي شبكة لاسلكية أخرى.

8- **البنية التحتية للاتصالات** Telecommunication infrastructure : نظام لوسائط النقل والإرسال - مثل أسلاك الهواتف، وأسلاك الألياف الضوئية، والسواتل، والموجات الدقيقة، والوصلات اللاسلكية - يمكن بناءً عليه تقديم خدمات الاتصال ومن ثم تيسير الاندماج بين خدمات الإنترنت والاتصال عن بعد وتكنولوجيا الوسائط المتعددة وتطبيقاتها.

9- **الحوسبة السحابية** Cloud computing : خدمة من خدمات تكنولوجيا المعلومات والاتصالات لتقديم برمجيات التطبيقات أو الخدمات أو المحتويات إلى المستخدمين النهائيين من خلال النفاذ إلى مَعِين تشاركي من الموارد الفعلية أو الافتراضية قابل للتمديد ومرن يمكن إدارته ذاتياً حسب الطلب.

10- **إساءة استخدام الإنترنت** Internet misuse : الاستخدام غير اللائق للإنترنت ولما يرتبط بها من تكنولوجيا المعلومات والاتصالات، الذي قد يتسبب في خسارة مادية أو يلحق أذى جسدياً بالأفراد.

ملحوظة: لا يوجد خط فاصل بين إساءة استخدام الإنترنت والجرائم السيبرانية .ووفقاً لدرجة الخسارة المادية أو الأذى الجسدي الذي يلحق بالأفراد، قد يُعدُّ التعدي - أي انتهاك القانون أو الحقوق - أو مخالفة اللوائح أو مدونات الممارسات الأخرى من خلال إساءة استخدام الإنترنت فيما يتعلق بحقوق الإنسان الأساسية جريمة من الجرائم السيبرانية.

11- **الجرائم السيبرانية** Cybercrime :أي جريمة تنطوي من حيث الوسيلة أو الهدف على أي ما يلي:

- منظومة حواسيب (الجرائم التي تُرتكب عبر الحواسيب أو الجرائم المتعلقة بالحواسيب بمعناها الضيق)،

- تكنولوجيات الربط الشبكي (جرائم الشبكات بالمعنى الضيق)،
- أو كليهما.

ملحوظة : تُعدُّ اتفاقية بودابست بشأن جرائم الفضاء السيبراني أول معاهدة دولية تُعنى بالجرائم المرتكبة عن طريق الإنترنت وشبكات الحاسوب الأخرى، عن طريق مواءمة القوانين الوطنية، وتحسين أساليب التحري، وزيادة التعاون بين الدول.

12- الهجمات السيبرانية Cyberattack :أحد ضروب إساءة استخدام الإنترنت أو ارتكاب الجرائم السيبرانية تُستغل فيه مواطن الضعف في الإنترنت لشن أنواع مختلفة من الهجمات تستهدف أساساً أجهزة أو برمجيات تكنولوجيا المعلومات والاتصالات، أو تهدف في المقام الأول إلى إيذاء الأشخاص.

ملحوظة: ثمة أنواع مختلفة من الهجمات السيبرانية (لكل منها أنواع فرعية):

- الهجمات الفاعلة وغير الفاعلة؛
- الهجمات الرامية إلى الحرمان من الخدمة؛
- الهجمات الرامية إلى استبدال صفحات الوِب؛
- هجمات باستخدام برمجيات خبيثة؛
- اختراق الفضاء السيبراني؛
- البريد الواغل والتصيّد؛
- إساءة استخدام بعض بروتوكولات الاتصالات، ... وصولاً إلى الحرب السيبرانية الشاملة.

13- **البرمجيات الخبيثة** Malware / Malicious software: برنامج من قبيل الفيروس أو الدودة الحاسوبية أو حصان طروادة، أو أي برمجية أخرى من برمجيات الهجوم التي تعمل على نحو مستقل إلى حد ما ويمكنها إيقاف أو تعطيل عمل الحاسوب، وجمع معلومات ذات طبيعة حساسة، أو النفاذ إلى نظم حاسوبية خاصة.

ملحوظة: تعد البرمجيات الخبيثة تهديداً لأمن المعلومات وحماية البيانات.

14- .**برمجيات الجريمة** Crimeware: فئة من البرمجيات الخبيثة مصممة خصيصاً لأتمتة الجرائم السيبرانية، بغية (أ) ارتكاب أفعال غير مشروعة، أو (ب) سرقة معلومات شخصية، أو (ج) أتمتة الجرائم المالية.

ملحوظة: قد تشمل برمجيات الجرائم برمجيات التجسس، وبرمجيات مراقبة لوحة المفاتيح والتلصص. وفي معظم الأحيان، تُستخدَم برمجيات الجرائم في ما يلي: (1) جمع معلومات سرية، مثل كلمات السر أو أرقام بطاقات الائتمان؛ أو (2) السيطرة على أجهزة الحاسوب وتنفيذ الأوامر عن بعد.

15- **برمجيات التجسس** Spyware : برمجيات خبيثة تراقب أنشطة المستخدمين دون علمهم، وتجمع معلومات مثل الأنشطة عبر الإنترنت، والمعلومات السرية والشخصية، وتنقل تلك المعلومات إلى صاحب برمجية التجسس.

ملحوظة: ُتعد برمجيات التجسس تهديداً لحماية البيانات..

16- **الحرب السيبرانية / الحرب المعلوماتية** Cyberwar / Cyberwarfare : نشاط منطوٍ على إساءة لاستخدام الإنترنت عابر للحدود الدولية لأغراض سياسية من خلال استهداف مواطن الضعف فى البنى التحتية الوطنية الحيوية والبيانات الوطنية.

ملحوظة :على الصعيد الدولي، تنخرط جهات فاعلة حكومية وغير حكومية على حد سواء في إساءة استخدام الإنترنت، بما في ذلك التجسس (عن طريق برمجيات التجسس مثلاً)، والحرب السيبرانية وغير ذلك من أوجه إساءة استخدام الإنترنت عبر الحدود أو الجرائم السيبرانية وصولاً إلى الحرب المعلوماتية الشاملة. ولذلك، فإن الحرب السيبرانية تُعدُّ أحد أهم شواغل الأمن القومي.

17- **الإرهاب السيبراني** Cyberterrorism: نمط من الإرهاب تُستغل فيه موارد الفضاء السيبراني وتكنولوجيا المعلومات والاتصالات لمهاجمة البنى التحتية الحرجة أو لتنفيذ أعمال الإرهاب التقليدية على النحو الأمثل.

18- **المطاردة السيبرانية** Cyberstalking: أحد ضروب إساءة استخدام الإنترنت لمطاردة الآخرين ومضايقتهم أو الإساءة إليهم.

ملحوظة: تقترن أنشطة الكثيرين من مرتكبي أعمال المطاردة أو المتحرشين على الإنترنت بأشكال تقليدية من المطاردة أو التحرش (الاتصال هاتفياً بالمجني عليهم مثلاً).

19- **هجمات الحرمان من الخدمات أو هجوم حجب الخدمة** A Distributed Denial of Service (DDoS) هو محاولة لجعل خدمات الانترنت (الاون لاين) غير متوفرة عن طريق إغراقها بسيل من البيانات غير اللازمة يتم إرسالها من مصادر متعددة . وهذا النوع من الهجمات يستهدف مجموعة واسعة ومتنوعة من الموارد الهامة، من البنوك إلى المواقع الإخبارية، ويشكل هذا النوع من التهديدات تحديا كبيراً من حيث تأمين قدرة الافراد على النشر والوصول الي المعلومات الهامة.

Source: UNESCO_ Internet Governance Glossary

بعض الجهود المصرية في دعم الامن السيبراني (على سبيل المثال)

"أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي ، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه ، على النحو الذي ينظمه القانون " مادة (31) من الدستور المصري (يناير 2014)

1. تأسيس المركز المصري للاستجابة لطوارئ الإنترنت والحاسب" المجلس الأعلى للأمن السيبراني" التابع لوزارة الاتصالات وتكنولوجيا المعلومات بجمهورية مصر العربية مسؤولاً عن الاستجابة لحوادث أمن الكمبيوتر والمعلومات، وتوفير الدعم والدفاع والتحليل في مجال الهجمات السيبرانية والتعاون مع الهيئات الحكومية والمالية وأي قطاعات معنية بالبنية التحتية المعلوماتية الحرجة، كما يوفر المركز أيضاً الإنذار المبكر ضد انتشار البرمجيات الخبيثة والهجمات السيبرانية الضخمة ضد البنية التحتية للاتصالات في مصر.

2. في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري، ومع تزايد التهديدات والتحديات المستقبلية في المجال السيبراني والمجتمع الرقمي ولرصد ومجابهة المخاطر والتهديدات المتزايدة، قام المجلس الأعلى للأمن السيبراني التابع لرئاسة مجلس الوزراء برئاسة وزير الاتصالات وتكنولوجيا المعلومات ، بوضع الاستراتيجية الوطنية للأمن السيبراني (2017-2021).

3. اصدار قانون مكافحة جرائم تقنية المعلومات المعروف إعلامياً بـ"مكافحة جرائم الإنترنت ".

سوق التأمين المصري والتأمين السيبراني

كشفت دراسة استطلاعية أجرتها "كاسبرسكى" حول "حالة الأمن الإلكتروني في القطاع الصناعي 2018" ، عن أبرز الدول العربية التي تعرضت لهجمات إلكترونية على شبكاتها وأنظمتها الصناعية، وهى كل من الجزائر بنسبة 66.2% والمغرب بنسبة 60.4% ومصر بنسبة 57.6% والمملكة العربية السعودية بنسبة 48.4% في طليعة البلدان التي تواجه مثل تلك الهجمات.

ورغم ذلك لايزال موضوع توفير تأمين للمنتجات المتصلة بالمخاطر الالكترونية "السيبرانية" أمر غير منتشر بسوق التأمين المصري بشكل كبير .

ومما لا شك فيه انه يجب على كل المؤسسات والقطاعات تأمين تعاملاتها الإلكترونية في المستقبل ضد الاختراقات، خصوصًا أن هناك توسعا واضحا في الاعتماد على التكنولوجيا في ظل الثورة الصناعية الرابعة.

هذا وقد أعلن الدكتور محمد عمران رئيس الهيئة العامة للرقابة المالية ،أن هناك شركتين تقدمتا إلى الهيئة بوثائق تأمين جديدة ضد الهجمات الإليكترونية (السيبرانية)، إحداهما مصرية، والثانية أجنبية، للإسراع بطرحها في السوق، سعيا لإيجاد تأمين ضد مخاطر القرصنة الإلكترونية.

كما أن هناك مباحثات مستمرة مع البنك المركزي لبحث أطر التأمين، على الهجوم الإلكتروني، الذي يستهدف تأمين البنوك ضد مخاطر هذا النوع من الهجمات، ووضع آليات التنفيذ مع البنوك المصرية.

حيث أن البنوك تمتلك قاعدة بيانات كبيرة وتقوم بعدد كبير يوميًا من عمليات نقل البيانات، ومن ثم فإنها تحتاج تأمينًا قويًا للحفاظ على أرصدة العملاء، وهذا نظام موجود فى القطاعات المصرفية بمختلف دول العالم، وجارى تفعيلة فى مصر على جميع البنوك العاملة.

ومما لا شك فيه ان هذه الجهود يمكن ان تكون نواة جيدة لبدأ العديد من الشركات العاملة بسوق التأمين المصري في طرح منتجاتها للتأمين السيبراني ضد المخاطر الالكترونية.

دور الاتحاد المصري للتأمين

قدم الاتحاد المصري للتأمين ندوة عن "التأمين على الجرائم الإلكترونية" cyber risks والتي قدمتها اللجنة العامة لتأمينات الحوادث المتنوعة بالاستعانة ببعض الخبراء الدوليين خلال العام الماضي ، هذا بالإضافة الي تناول هذا الموضوع اكثر من مرة خلال المؤتمرات والاحداث المختلفة بالاتحاد المصري للتأمين.

كما قام الاتحاد المصري للتأمين بنشر مجموعة من النشرات المميزة حول هذا الموضوع الهام.

كما قدمت اللجنة العامة لتأمينات الحوادث المتنوعة بالاتحاد المصري للتأمين ورقة بحثية حول اهم التغطيات التأمينية التي يمكن ان يتم تقديمها لمنظومة الدفع الالكتروني التي تسعي الدولة الي الانتقال لها تدريجيا خلال الفترة القادمة وذلك برعاية المجلس القومي للمدفوعات.

هذا ويسعي الاتحاد المصري للتأمين في الفترة القادمة الى دراسة التغطيات المختلفة لهذا النوع التأميني الهام باللجان الفنية للاتحاد المصري للتأمين بهدف تقديم نماذج لتغطية مخاطر هذا النوع من التأمين والتبادل المعرفي ونشر ثقافة الوعي وتعزيزها في مجال التأمين السيبراني

الوحدة الثالثة : فيروسات الفدية

الأهداف التفصيلية للوحدة :

أن يكون المتدرب في نهاية الوحدة قادرا على:

8- **يوضح تعريف فيروسات الفدية**

9- **يُعرِّف آلية عمل فيروسات الفدية**

10- **يبين الهدف من الهجمات المرتكبة بفيروسات الفدية**

11- **يوضح كيفية التعامل مع الهجمات**

12- **يبين الطرق المستخدمة للوقاية من الفيروسات**

تشمل الوحدة على المواضيع الفرعية التالية "

1- التعريف بفيروسات الفدية

2- آلية عمل فيروسات الفدية والهدف من الهجمات المرتكبة

3- هجمات فيروسات الفدية وكيفية عملها واستراتيجية التعامل معها

4- كيفية التعامل مع الهجمات والوقاية منها

الدرس الأول / التعريف بفيروسات الفدية

ما هو فيروس الفدية

"فيروس الفدية" هو نوع خبيث من البرامج يقفل أجهزة الحاسوب الشخصي أو اللوحي أو الهواتف الذكية - أو يضع تشفيراً على ملفاتك ثم يطلب منك فدية مقابل إعادتها إليك في حالة سليمة؛ هناك نوعان أساسيان من فيروسات الفدية.

النوع الأول هو فيروسات التشفير، أي: التي تضع شفرة على الملفات بحيث لا يمكن الوصول إليها؛ ويتطلب فك تشفير الملفات امتلاك المفتاح الذي تم استخدامه في تشفيرها – وهذا هو ما تدفع مبلغ الفدية للحصول عليه.

النوع الثاني هو فيروسات الحجب، التي ببساطة تحجب الكمبيوتر أو الأجهزة الأخرى مما يجعلها غير صالحة للعمل؛ وفي الواقع، تُعد حالات فيروسات الحجب أفضل من فيروسات التشفير، ففرص الضحايا في إزالة الحجب واستعادة

"فيروس الفدية" الضار هو أحد الأشكال الجديدة للبرامج الضارة التي تتسبب في إغلاق ملفات المستخدمين أو أجهزتهم، ومطالبتهم بعد ذلك بدفع فدية عبر الإنترنت لاسترداد الوصول.

كل ما تريد أن تعرفه عن فيروسات الفدية الضارة

هل تساءلت يومًا عن سبب كل هذه الضجة التي تدور حول فيروسات الفدية الضارة؟ لقد سمعت عنها في المكتب أو قرأت عنها في الأخبار. ربما ظهرت الآن على شاشة جهاز الكمبيوتر الخاص بك رسالةً تحذرك من أحد فيروسات برنامج الفدية الضار. حسنًا، إذا كنت مهتمًا بمعرفة كل المعلومات التي تتعلق ببرامج الفدية الضارة، فقد أتيت للمكان المناسب. سنخبرك عن الأنواع المختلفة لفيروسات الفدية الضارة، وكيف تصيب جهازك، ومن أين تأتي، ومن المستهدف، وما الإجراءات التي يتعين عليك القيام بها لحماية جهازك منها.

ما هو فيروس الفدية الضار؟

فيروس الفدية الضار، أو Ransomware، هو أحد أنواع البرامج الضارة التي تمنع المستخدمين من الوصول إلى الأنظمة الخاصة بهم أو ملفاتهم الشخصية وتطلب دفع فدية لاستعادة الوصول. ظهرت أول أنواع لبرامج الفدية الضارة في أواخر ثمانينيات القرن العشرين، وكان يتم إرسال الفدية عبر البريد التقليدي. اليوم، يطلب منفذو الهجمات باستخدام برامج الفدية الضارة، إرسال الأموال بالعملة المشفرة أو باستخدام البطاقة الائتمانية.

الدرس الثاني / آلية عمل فيروسات الفدية والهدف من الهجمات المرتكبة

كيف يصيب فيروس الفدية جهاز المستخدم؟

ثمة طرق متنوعة عدة تستطيع منها خلال برامج الفدية الضارة إلحاق الضرر بجهاز الكمبيوتر الخاص بك. وتتمثل أحد الوسائل الأكثر انتشارًا اليوم في البريد العشوائي الضار أو malspam ، وهو بريد غير مطلوب يُستخدم لإرسال برامج ضارة. وقد يتضمن البريد الإلكتروني مرفقات خداعية، مثل ملفات PDFs أو مستندات .Word وربما يتضمن أيضًا روابط توجهك إلى مواقع ويب ضارة.

يستخدم البريد العشوائي الضار الهندسة الاجتماعية لخداع الأشخاص بفتح المرفقات أو النقر فوق الروابط التي تظهر كمرفقات أو روابط قانونية سواء كان ذلك يبدو واردًا من إحدى المؤسسات الموثوقة أو أحد الأصدقاء. يستخدم مجرمو الفضاء الإلكتروني الهندسة الاجتماعية في أنواع أخرى من هجمات فيروسات الفدية الضارة، مثل انتحال صفة أحد أفراد مكتب التحقيقات الفيدرالي لبث الخوف في نفوس المستخدمين وإجبارهم على دفع مبلغ من المال لإلغاء قفل الملفات الخاصة بهم.

ومن بين الوسائل الأخرى الشائعة والمستخدمة في إلحاق الضرر، والتي وصلت ذروتها في عام 2016، الإعلانات الضارة (malvertising)الإعلانات الضارة (Malvertising) أو الدعاية الضارة، وتتمثل في استخدام الإعلانات عبر الإنترنت لتوزيع البرامج الضارة مع إشراك المستخدم إشراكًا جزئيًا أو عدم إشراكه. وأثناء استعراض مواقع الويب، وحتى المواقع السليمة، يمكن أن يتم توجيه المستخدمين إلى أجهزة سيرفر إجرامية دون النقر على أحد الإعلانات. تجمع أجهزة السيرفر هذه التفاصيل بشأن أجهزة الكمبيوتر الخاصة بالضحية، وموقعه، وتحدد بعد ذلك نوع البرنامج الضار المناسب للإرسال. وكثيرًا، ما يكون هذا البرنامج الضار هو فيروس الفدية الضار.

كثيرًا ما تستخدم الإعلانات الضارة إطار مضمن ضار، أو عنصر صفحة ويب غير مرئي، لكي تتمكن من أداء عملها. يقوم الإطار المضمن بإعادة التوجيه إلى صفحة متنقلة لفيروس معطل للأمان، وتهاجم إحدى التعليمات البرمجية الضارة النظام من صفحة متنقلة عبر

مجموعة فيروسات معطلة للأمان. يحدث كل ذلك دون معرفة المستخدم، وهو ما يُشار إليه كثيرًا باسم التنزيل غير المقصود-drive) by-download)

أنواع فيروس الفدية

توجد ثلاثة أنواع رئيسية من فيروسات الفدية الضارة، تتراوح في درجة خطورتها بين الإزعاج المتوسط وأزمة الصواريخ الكوبية الخطيرة. وهي على النحو التالي:

- البرامج المخيفة(Scareware)

إن البرامج المخيفة، كما يتضح، غير مخيفة. وتتضمن برامج أمان احتيالية ورسائل دعم تقني. ربما تصلك رسالة منبثقة تزعم أنه قد تم الكشف عن أحد البرامج الضارة وليست هناك طريقة للتخلص منها سوى دفع مبلغ من المال. وإذا لم تفعل شيئًا، فربما يستمر إرسال الرسائل المنبثقة لك، إلا أن الملفات الخاصة بك تظل آمنة تمامًا.

لن يطلب برنامج الأمن الإلكتروني السليم من العملاء دفع أي شيء بهذه الطريقة. إذا لم يكن لديك بالفعل هذا البرنامج الخاص بالشركة على جهازك، فلن يراقب البرنامج جهاز الكمبيوتر الخاص بك للكشف عن فيروسات برامج الفدية الضارة. إذا كان برنامج الأمان مُثبتًا على جهازك، فلن تكون مضطرًا لدفع أي أموال لإزالة هذا الفيروس لأنك قد سددت بالفعل قيمة البرنامج حتى يُنفذ تلك المهمة على الوجه الأكمل.

- شاشات القفل(Screen lockers)

التحديث إلى التحذير ذات اللون البرتقالي لهؤلاء المجرمين. حين يتعرض جهاز الكمبيوتر الخاص بك لفيروس الفدية الضار باستخدام شاشة القفل، فهذا يعني أنك لن تتمكن من استخدام الجهاز الكمبيوتر الخاص بك تمامًا. بمجرد تشغيل جهاز الكمبيوتر الخاص بك، ستظهر شاشة بالحجم الكامل، وكثيرًا ما تكون مصحوبة بختم يبدو رسميًا من مكتب التحقيقات الفيدرالي أو وزارة العدل، وتزعم تلك الشاشة أن نشاطًا غير مشروع قد تم اكتشافه على جهاز الكمبيوتر الخاص بك ويجب أن تدفع غرامة. لكن، مكتب التحقيقات الفيدرالي لن يمنعك من استخدام جهاز الكمبيوتر الخاص بك أو يطلب منك دفع أموال لأي نشاط غير مشروع. إذا اشتبه مكتب التحقيقات أنك تقوم بأعمال القرصنة أو تستغل الأطفال في المواد الإباحية أو الجرائم الإلكترونية الأخرى، فسيلتزم بالقنوات القانونية ذات الصلة.

- برامج الفدية الضارة المُشفِّرة(Encrypting ransomware)

ويُعد هذا النوع مخيفًا للغاية. وهؤلاء هم المهاجمون الذين يقومون بسرقة ملفاتك وتشفيرها، ويُطالبونك بعد ذلك بدفع أموال لفك تشفيرها وإعادة إرسالها. ويكمن سبب الخطورة الشديدة لهذا النوع من فيروسات الفدية الضارة في أن مجرمو الفضاء الإلكتروني يسرقون ملفاتك، ولا توجد برامج أمان أو برامج استعادة النظام، يمكنها إعادتها لك. إذا لم تدفع الفدية، ففي الغالب لن تحصل عليها مرة أخرى. وحتى إذا قمت بدفع الفدية، فلا يوجد ضمان أن مجرمو الفضاء الإلكتروني سيعيدون تلك الملفات لك مرة أخرى.

أحدث الهجمات باستخدام فيروس الفدية

- ✓ اليوروبول :(Europol) تظل برامج الفدية الضارة على رأس التهديدات في تقرير تقييم تهديدات الجرائم المنظمة الإلكترونية(IOCTA)
- ✓ تواصل فيروسات الفدية الضارة مهاجمة المدن والشركات
- ✓ تصدرت فيروسات حصان طروادة، وبرامج الفدية الضارة مشهد التهديدات بالتعليم لعامي 2018 و2019

تاريخ فيروسات الفدية الضارة

تم تكوين أول فيروس فدية ضار، والمعروف باسم PC Cyborg أوAIDS ، في أواخر ثمانينيات القرن العشرين. يُمكن أن يُشفِّر فيروس الفدية الضار PC Cyborg جميع الملفات في دليل قرص :C بعد 90 عملية إعادة تشغيل للجهاز، ويطلب من المستخدم بعد ذلك تجديد رخصته وإرسال 189 دولارًا أمريكيًا عبر البريد إلى شركة .PC Cyborg كان التشفير المُستخدم بسيطًا بما يكفي للتبديل، ولذلك كان يمثل تهديدًا بسيطًا على هؤلاء الذين تم اختراق أجهزة الكمبيوتر الخاصة بهم.

ومع انخفاض أنواع برامج الفدية الضارة خلال فترة 10 سنوات، لم تظهر أي تهديدات لبرامج الفدية الضارة على المشهد حتى عام 2004، حين استخدم فيروس الفدية الضار GpCode تشفير RSA الضعيف لسرقة الملفات الشخصية وإعادتها بعد دفع الفدية.

في 2007، كان فيروس الفدية الضار WinLock يشير إلى ظهور نوع جديد من برامج الفدية الضارة، والتي تقوم بقفل أجهزة سطح المكتب الخاصة بالمستخدمين بدلاً من تشفير الملفات. استولى فيروس الفدية الضارWinLock على شاشة الضحية وعرض عليها صورًا إباحية. وبعد ذلك، طلب البرنامج دفع أموال وإرسال رسائل نصية صغيرة بالمبلغ لإزالة الشاشة.

ومع تطور عائلة برامج الفدية الضارة Reveton في 2012، ظهر نوع جديد من برامج الفدية الضارة ألا وهو برنامج الفدية الضار لإنفاذ القانون .كان يتم إقفال أجهزة سطح المكتب الخاصة بالضحايا وتظهر صفحة تبدو رسمية تتضمن بيانات اعتماد لهيئات إنفاذ قانون مثل مكتب التحقيقات الفيدرالي ومنظمة الشرطة الجنائية الدولية. وكان فيروس الفدية الضار يطلب من المستخدم ارتكاب جريمة، مثل اختراق جهاز كمبيوتر أو تنزيل ملفات غير مشروعة أو حتى الاشتراك في استغلال الأطفال لنشر مواد إباحية. كانت معظم عائلات برامج الفدية الضارة لإنفاذ القانون، تشترط دفع غرامة تتراوح بين 100 دولار أمريكي و3,000 دولار أمريكي باستخدام بطاقة مسبقة الدفع مثل UKash أو.PaySafeCard

لم يكن المستخدمون العاديون يعرفون ما يتعين عليهم القيام به حيال ذلك وكانوا يعتقدون أنهم يخضعون بالفعل للتحقيقات من إحدى هيئات إنفاذ القانون. إن أسلوب الهندسة الاجتماعية هذا، والمُشار إليه الآن باسم الإقرار بالذنب ضمنيًا، يجعل المستخدم يتساءل ما إذا كانوا بريئًا أم لا، وبدلاً من التحقق من النشاط الذي ليس مسؤولاً عنه، يدفع الفدية لإخفاء الأمر.

في عام 2013 أعاد Crypto Locker طرح فيروسات الفدية الضارة المُشفِّرة على العالم، وكانت هذه المرة فقط أكثر خطورة. استخدم فيروس الفدية الضار Crypto Locker تشفيرًا عسكريًا وقام بتخزين مفتاح المرور اللازم لإلغاء قفل الملفات على جهاز سيرفر بعيد. وكان ذلك يعني أنه من المستحيل عمليًا حصول المستخدمين على البيانات الخاصة بهم دون دفع الفدية. لا يزال هذا النوع من فيروسات الفدية الضارة المُشفِّرة يُستخدم حتى اليوم، حيث ثَبُت أنه أداة فعالة للغاية لمجرمي الفضاء الإلكتروني في الحصول على الأموال. في حالات كثيرة، استخدمت برامج فدية ضارة، مثل WannaCry في مايو 2017 و Petyaفي يونيو 2017، برامج ضارة مُشفِّرة للإيقاع بالمستخدمين والشركات في جميع أنحاء العالم.

في أواخر 2018، تصدر Ryuk مشهد فيروسات الفدية الضارة بسلسلة من الهجمات على وكالات الصحف الأمريكية فضلاً عن شركة مرافق المياه في ولاية كارولاينا الشمالية. وفي تطور مثير للاهتمام، تم اختراق الأنظمة المستهدفة أولاً باستخدام Emotet أو Trick Bot، اثنين من فيروسات حصان طروادة لسرقة المعلومات والمستخدمين الآن لإرسال أشكال أخرى من البرامج الضارة مثلRyuk ، على سبيل المثال. مديرMalwarebytes Labs ، السيد آدم كوجاوا يعتقد أن Emotet و TrickBotيُستخدمان للبحث عن الأهداف بالغة الأهمية. بعد أن يتم اختراق أحد الأنظمة وتوضع عليه علامة تفيد أنه هدف جيد لكي تخترقه برامج الفدية الضارة، تقوم برامج Emotet/TrickBotبإعادة اختراق النظام مرة أخرى باستخدام.Ryuk

في الأخبار الأخيرة، بدأ المجرمون المسؤولون عن برنامج الفدية الضار) Sodinokibi أحد البرامج التي تزعم أنها تابعة لبرنامج GandCrab، استخدام شركات الخدمات المُدارة (MSP) لنشر الفيروسات. في أغسطس 2019، اكتشفت المئات من عيادات طب الأسنان في جميع أرجاء البلد، أنها لم تعد قادرة على الوصول إلى سجلات المرضى. استخدم المهاجمون إحدى شركات الخدمات

المُدارة المخترقة(MSP) ، وفي تلك الحالة إحدى شركات برامج السجلات الطبية، لاختراق أكثر من 400 عيادة لطب الأسنان مستخدمين في ذلك برامج لحفظ السجلات.

فيروسات الفدية الضارة في أجهزة Mac

لا أحد بمنأى عن التهديدات الالكترونية وتهديدات فيروسات الفدية الضارة، فقد نشر أصحاب البرامج الضارة أول برنامج فدية ضار في نظام التشغيل Mac OSes وذلك في عام 2016. هذا البرنامج الذي يُطلق عليهKe Ranger ، فيروس الفدية الضارة المخترق لأحد التطبيقات التي يطلق عليهاTransmission ، وعند تشغيله، يقوم بنسخ ملفات ضارة تظل تعمل في الخلفية سرًا لمدة ثلاثة أيام حتى تنتشر ويقوم بتشفير الملفات. ولحسن الحظ، أصدر البرنامج المضمن للحماية من البرامج الضارة XProtect منApple ، تحديثًا بعد فترة قصيرة من اكتشاف فيروس الفدية الضار ومنعه من اختراق أنظمة المستخدمين. ورغم ذلك، لم تعد برامج الفدية الضارة بأجهزة Macنظرية.

برامج الفدية الضارة بالهواتف المحمولة

ولم تكن كذلك حتى ظهر البرنامج الضار المشهور Crypto Locker والعائلات الأخرى المشابهة في 2014 وحينها انتشرت فيروسات الفدية الضارة على نطاق واسع في أجهزة المحمول. تقوم برامج الفدية الضارة للهواتف المحمولة بعرض رسالة تفيد أن الجهاز قد تم إقفاله نظرًا لوجود نشاط غير مشروع. وُتبين الرسالة أن الهاتف سيتم إلغاء قفله بعد دفع الغرامة. كثيرًا ما يتم إرسال فيروسات الفدية الضارة للهواتف المحمولة عبر تطبيقات ضارة، وتتطلب منك تشغيل الهاتف في الوضع الآمن وحذف التطبيقات المخترقة لاستعادة الوصول إلى هاتفك المحمول.

من الذي يستهدفه أصحاب فيروس الفدية؟

عند نشر فيروس الفدية الضار (وإعادة نشره بعد ذلك)، كان يستهدف في البداية أنظمة الأفراد) أشخاص عاديين .(aka ومع ذلك، بدأ مجرمو الفضاء الإلكتروني العمل بكامل طاقتهم عندما قاموا بنشر فيروسات الفدية الضارة في الشركات. وحقق فيروس الفدية الضار نجاحًا كبيرًا ضد الشركات، وتسبب في وقف الإنتاج، وفقدان البيانات والعائدات، وقام المهاجمون بتحويل معظم هجماتهم تجاه الشركات. في نهاية 2016، بلغت نسبة عمليات الكشف عن البرامج الضارة في المؤسسات العالمية، 12.3 في المائة وكانت البرامج الضارة عبارة عن فيروسات فدية ضارة، بينما بلغت نسبة عمليات الكشف عن البرامج الضارة في أجهزة الأفراد 1.8 في المائة وكانت البرامج الضارة عبارة عن برامج فدية ضارة في جميع أنحاء العالم. وبحلول عام 2017، تعرضت الشركات الصغيرة ومتوسط الحجم والتي بلغت نسبتها 35 في المائة، إلى هجوم بفيروس الفدية الضار.

جغرافيًا، لا تزال الهجمات الالكترونية وبرامج الفدية الضارة تركز على الأسواق الغربية، وتتصدر المملكة المتحدة، والولايات وكندا، على التوالي، قائمة الدول المستهدفة. وفيما يتعلق بعوامل التهديد الأخرى، سيحاول أصحاب فيروسات الفدية الضارة جمع الأموال، ولذلك سيبحثون عن المناطق التي ينتشر بها استخدام أجهزة الكمبيوتر والغنية بالثروات. ومع ظهور أسواق في قارتي آسيا وأمريكا الجنوبية وتحريكها للنمو الاقتصادي، من المتوقع أن نرى هناك أيضًا زيادة في فيروسات الفدية الضارة (والأشكال الأخرى من البرامج الضارة).

الدرس الثالث / هجمات فيروسات الفدية وكيفية عملها واستراتيجية التعامل معها

تعريف برامج الفدية الضارة

برامج الفدية الضارة هي نوع من البرامج الضارة أو البرامج الخبيثة، التي تهدد الضحية من خلال تدمير أو منع الوصول إلى البيانات أو الأنظمة الهامة حتى يتم دفع فدية. وقد جرت العادة أن تستهدف معظم برامج الفدية الضارة الأفراد، ولكن في الآونة الأخيرة، أصبحت برامج الفدية الضارة بشرية الإدارة التي تستهدف المؤسسات تمثل التهديد الأكبر والأكثر صعوبة في منعه وإنهائه. من خلال برامج الفدية الضارة بشرية الإدارة، يستخدم مجموعة من المهاجمين ذكاءهم الجماعي للوصول إلى شبكة المؤسسة. بعض الهجمات من هذا النوع مُطورة للغاية لدرجة أن المهاجمين يستخدمون المستندات المالية الداخلية التي تم الكشف عنها لتحديد سعر الفدية.

هجمات برامج الفدية الضارة في الأخبار

لسوء الحظ، أصبح ذكر تهديدات برامج الفدية الضارة في الأخبار أمراً شائعاً الآن. أثرت هجمات برامج الفدية الضارة عالية المستوى الحالية على البنية الأساسية الهامة وقطاع الرعاية الصحية وموفري خدمات تكنولوجيا المعلومات. ونظراً لأن تلك الهجمات أصبحت أكثر جرأة في نطاقها، فقد أصبحت آثارها غير متوقعة بشكل أكبر. نتناول

فيما يلي نظرة سريعة حول بعض هجمات برامج الفدية الضارة وتأثيرها على المؤسسات:

- في مارس 2022، وقع نظام البريد اليوناني كفريسة لبرامج الفدية الضارة. أدى هذا الهجوم إلى تعطيل تسليم البريد مؤقتاً وأثر على معالجة العمليات المالية.
- كما تعرضت إحدى أكبر شركات الطيران في الهند لهجوم برامج الفدية الضارة في مايو 2022. وأدى هذا الحدث إلى تأخير وإلغاء الرحلات، فضلاً عن تقطع السبل بمئات الركاب.
- تعرضت شركة موارد بشرية عملاقة لهجوم من برامج الفدية الضارة في ديسمبر 2021، حيث تأثر نظام كشف الرواتب والإجازات الخاص بالعملاء الذين يستخدمون خدماتها السحابية.
- في مايو 2021، أوقف خط أنابيب الوقود الأمريكي خدماته لمنع التعرض للمزيد من الانتهاكات بعد اختراق هجمات برامج الفدية الضارة لآلاف المعلومات الشخصية لموظفيه. كما أدت الآثار المترتبة على ذلك إلى ارتفاع أسعار الغاز في جميع أنحاء الساحل الشرقي.
- تعرضت شركة توزيع مواد كيميائية ألمانية لهجوم من برامج الفدية الضارة في أبريل 2021. أدى هذا الهجوم الإلكتروني إلى سرقة تواريخ ميلاد أكثر من 6000 شخص وأرقام الضمان الاجتماعي وأرقام رخصة القيادة بالإضافة إلى بعض البيانات الطبية.
- كما أصبح أكبر موردي اللحوم في العالم هدفاً لهجوم برامج الفدية الضارة في مايو 2021. وبعد إيقاف تشغيل موقع الويب مؤقتاً وإيقاف الإنتاج، انتهى الأمر بالشركة بدفع فدية قدرها 11 مليون دولار في Bitcoin.

كيف تعمل برامج الفدية الضارة؟

تعتمد هجمات برامج الفدية الضارة على الاستيلاء على بيانات الأفراد أو المؤسسات كوسيلة للمطالبة بالمال. في السنوات السابقة كانت هجمات الانتحال بالهندسة الاجتماعية هي الأكثر انتشاراً، ولكن مؤخراً أصبحت برامج الفدية بشرية الإدارة شائعة لدى المجرمين بسبب احتمالية الحصول على تعويضات ضخمة.

برامج الفدية الضارة للانتحال بالهندسة الاجتماعية

تستخدم هذه الهجمات التصيد الاحتيالي—وهو شكل من أشكال الخداع حيث يتظاهر المهاجم بأنه شركة أو موقع ويب شرعي - لخداع الضحية للنقر فوق ارتباط أو فتح مرفق بريد إلكتروني، مما يؤدي إلى تثبيت برامج الفدية الضارة على الأجهزة. غالباً ما تقوم الهجمات بإرسال رسائل تُنذر بالخطر تدفع الضحية إلى التصرف بدافع الخوف. على سبيل المثال، قد يتظاهر مجرم إلكتروني بأنه بنك معروف ويرسل بريداً إلكترونياً ينبه شخصاً ما بأن حسابه قد تم تجميده بسبب نشاط مشبوه، ويحثه على النقر فوق ارتباط في البريد الإلكتروني لمعالجة المشكلة. بمجرد نقر الرابط، يتم تثبيت برامج الفدية الضارة.

برامج الفدية الضارة بشرية الإدارة

غالباً ما تبدأ برامج الفدية الضارة بشرية الإدارة هجماتها من خلال بيانات اعتماد الحساب المسروقة. بمجرد أن يتمكن المهاجمون من الوصول إلى شبكة مؤسسة بهذه الطريقة، فإنهم يستخدمون الحساب المسروق لتحديد بيانات اعتماد الحسابات ذات نطاقات الوصول الأوسع والبحث عن البيانات والأنظمة المهمة للأعمال ليكون لديهم إمكانية تحقيق مكاسب مالية عالية. ثم يقومون بعد ذلك بتثبيت برامج الفدية الضارة على هذه البيانات الحساسة أو الأنظمة المهمة للأعمال، على سبيل المثال، عن طريق تشفير الملفات الحساسة حتى لا تتمكن المؤسسة من الوصول إليها حتى تدفع فدية. يميل المجرمون الإلكترونيون إلى طلب الدفع بعملة رقمية حتى لا يتم الكشف عن هويتهم.

يستهدف هؤلاء المهاجمون المؤسسات الكبيرة التي يمكنها دفع فدية أعلى من الفرد العادي، وأحياناً يطلبون ملايين الدولارات. نظراً للمخاطر الكبيرة الناتجة عن انتهاك هذا النطاق، تختار العديد من المؤسسات دفع الفدية بدلاً من تسريب بياناتها الحساسة أو المخاطرة بالتعرض للمزيد من الهجمات من المجرمين الإلكترونيين على الرغم من أن الدفع لا يضمن منع أي من النتيجتين

مع تزايد هجمات برامج الفدية الضارة بشرية الإدارة، أصبح المجرمون القائمون على تلك الهجمات أكثر تنظيماً. في الواقع، تستخدم العديد من عمليات برامج الفدية الضارة الآن برامج الفدية الضارة كنموذج خدمة، مما يعني أن مجموعة من المطورين المجرمين ينشئون برامج الفدية الضارة نفسها ثم يوظفون شركاء مجرمين إلكترونيين آخرين لاختراق شبكة مؤسسة وتثبيت برنامج الفدية الضارة، وتُقسم الأرباح بين المجموعتين بنحو مُتفق عليه

الأنواع المختلفة من برامج الفدية الضارة

تنقسم برامج الفدية الضارة إلى نوعين رئيسيين: برامج الفدية الضارة المشفِرة للملفات (Crypto) وبرامج الفدية الضارة المغلِقة للملفات (Locker)

- ### برامج الفدية الضارة المُشفِرة للملفات

عندما يقع فرد أو مؤسسة ضحيةً لهجمات برامج الفدية الضارة المُشفِرة للملفات، يقوم المهاجم بتشفير البيانات أو الملفات الحساسة للضحية حتى لا يتمكن من الوصول إليها إلا إذا دفع الفدية المطلوبة. نظرياً بمجرد أن يدفع الضحية الفدية، يحصل على مفتاح تشفير يمكنه من الوصول إلى الملفات أو البيانات. حتى إذا دفع الضحية الفدية، فليس هناك ما يضمن أن المجرم الإلكتروني سيرسل مفتاح التشفير أو يتخلى عن السيطرة. برنامج Doxware هو شكل من أشكال برامج الفدية الضارة المُشفِرة للملفات الذي يقوم بتشفير المعلومات الشخصية للضحية ويُهدد بالكشف عنها، وعادة ما يكون ذلك بهدف إهانة وإذلال الضحية لدفع الفدية.

- ### برامج الفدية الضارة المغلِقة للملفات

هجمات برامج الفدية الضارة المغلِقة للملفات تمنع الضحية من الوصول إلي أجهزته و تجعله غير قادر على تسجيل الدخول. سيظهر للضحية على الشاشة إشعار دفع فدية يوضح أنه قد تم إغلاق ملفاته، ويتضمن تعليمات حول كيفية

دفع فدية لاستعادة الوصول. لا يتضمن هذا النوع من برامج الفدية الضارة عادةً التشفير، لذلك بمجرد استعادة الضحية إمكانية الوصول إلى أجهزته، يتم الاحتفاظ بأي ملفات وبيانات حساسة.

الاستجابة لهجمات برامج الفدية الضارة

إذا وقعت ضحيةً في براثن هجوم برامج الفدية الضارة، فلديك خيارات للرجوع والإزالة.

- **كن حذراً بشأن دفع الفدية**

على الرغم من أنه قد يكون من المغري دفع الفدية على أمل التخلص من المشكلة، إلا أنه لا يوجد ضمان بأن المجرمين الإلكترونيين سوف يوفون بكلامهم ويمنحونك إمكانية الوصول إلى بياناتك. يوصي خبراء الأمن ووكالات تطبيق القانون بأن لا يدفع ضحايا هجمات برامج الفدية الضارة الفدية المطلوبة، لأن القيام بذلك قد يترك الضحايا عُرضة للتهديدات المستقبلية ويُدعم بشكل فعال المجال الإجرامي. إذا كنت قد دفعت بالفعل، فاتصل على الفور بالبنك الذي تتعامل معه فقد يكون قادراً على إيقاف عملية الدفع إذا كنت تدفع ببطاقة ائتمان.

- **اعزل البيانات المصابة**

بمجرد أن تتمكن من ذلك، اعزل البيانات المخترقة للمساعدة في منع انتشار برامج الفدية الضارة في مناطق أخرى في الشبكة.

- **تشغيل برنامج الحماية من البرامج الضارة**

يمكن التعامل مع العديد من هجمات برامج الفدية الضارة عن طريق تثبيت برامج الحماية من البرامج الضارة لإزالة برامج الفدية الضارة. بمجرد اختيار برنامج موثوق للحماية من البرامج الضارة مثلMicrosoft Defender ، تأكد من تحديثه وتشغيله دائماً حتى تتمتع بالحماية من أحدث الهجمات.

- **أبلغ عن الهجوم**

اتصل بجهات إنفاذ القانون المحلية أو الفيدرالية للإبلاغ عن الهجوم. في الولايات المتحدة، هذه هي مكاتب الميدانية المحلية لمكتب التحقيقات الفيدرالي، أوIC3، أو الخدمة السرية .على الرغم من أن هذه الخطوة لن تحل على الأرجح أياً من المخاوف الحالية، إلا أنها مهمة لأن هذه السلطات تتعقب وتراقب بشكل نشط الهجمات المختلفة. قد يكون تقديم تفاصيل لهم عن تجربتك مفيداً لهم في العثور على المجرمين الإلكترونيين وملاحقتهم ومقاضاتهم.

ما الإجراءات التي ينبغي أن أقوم بها إذا تعرضت لمحاولة اختراق؟

القاعدة الأولى، إذا اكتشفت أنك قد تعرضت لعملية اختراق بأحد فيروسات الفدية الضارة، فلا تدفع فدية. (وهذه هي نصيحة أقرها مكتب التحقيقات الفيدرالي.) كل ذلك يُشجع مجرمي الفضاء الإلكتروني على شن المزيد من الهجمات ضدك أو ضد أحد الأشخاص الآخرين. ورغم ذلك، قد تكون قادرًا على استعادة بعض الملفات المشفرة باستخدام برامج فك التشفير المجانية.

وحتى تكون الأمور واضحة: لا توجد برامج فك تشفير لجميع عائلات فيروسات الفدية الضارة، في العديد من الحالات لأن فيروس الفدية الضار يستخدم خوارزميات متقدمة ومتطورة. وحتى إذا كان هناك برنامج لفك التشفير، فليس واضحًا دائمًا ما إذا كان هو الإصدار المناسب لصد البرنامج الضار أم لا. أنت لا تريد مزيدًا من التشفير لملفاتك باستخدام برنامج نصي خاطئ للتشفير. ولذلك، سيتعين عليك إيلاء اهتمام كبير لرسالة الفدية ذاتها، أو ربما طلب نصيحة أحد اختصاصي الأمان أو تكنولوجيا المعلومات قبل محاولة القيام بأي شيء.

وتوجد طرق أخرى للتعامل مع فيروس برنامج الفدية الضار وتتضمن تنزيل برنامج أمان معروف للمعالجة وإجراء فحص لإزالة التهديد. قد لا تتمكن من استعادة الملفات مرةً أخرى، لكن بوسعك أن تطمئن أن الفيروس سيتم إزالته. فيما يتعلق بفيروسات الفدية التي تقوم بإقفال الشاشة، ربما يكون حل استعادة النظام بالكامل حلاً مناسبًا. وإذا لم ينجح ذلك، فبوسعك إجراء فحص من أحد الأقراص القابلة للتشغيل أو محرك أقراص USB

إذا كنت تريد تجربة نشر أحد فيروسات برنامج الفدية الضار المُشفِّر ومنعه من اختراق جهازك، فسيتعين عليك توخي الحذر. إذا لاحظت وجود بطء في نظامك دون وجود أي سبب ظاهر، فقم بإيقاف تشغيله وقطع اتصاله بالإنترنت. إذا قمت بالتشغيل ذات مرة وكان البرنامج الضار لا يزال نشطًا، فلن يتمكن من إرسال أو استقبال تعليمات من جهاز السيرفر المتحكم الذي يعطي الأوامر. ويعني

ذلك أنه إذا لم يكن هناك مفتاحًا أو طريقةً للحصول على الأموال، فقد يظل خامل. وفي هذه المرحلة، قم بتنزيل وتثبيت برنامج أمان وقم بإجراء فحص كامل.

الدرس الرابع / كيفية التعامل مع الهجمات والوقاية منها

الحماية من برامج الفدية الضارة

نظراً لتزايد هجمات برامج الفدية الضارة عن أي وقت مضى الحماية، وأصبح الكثير من المعلومات الشخصية للأشخاص مضمنة رقمياً، فإن التداعيات المحتملة للهجوم باتت مروعة. لحسن الحظ، يوجد عدة طرق للحفاظ على حياتك الرقمية، وليس حياة شخص آخر. وإليك كيفية الشعور براحة البال من خلال الحماية من برامج الفدية الضارة الاستباقية.

- #### تثبيت برنامج الحماية من البرامج الضارة

الوقاية هي أفضل وسيلة للحماية. يمكن الكشف عن العديد من هجمات برامج الفدية الضارة ومنعها من خلال خدمة موثوق بها للحماية من البرامج الضارة، مثل Microsoft Defender لنقطة النهاية أو Microsoft Defender XDR أو Microsoft Defender for Cloud. عندما تستخدم برنامج حماية من برامج الفدية الضارة، يقوم جهازك أولاً بفحص أي ملفات أو ارتباطات تحاول فتحها للمساعدة على التأكد من أنها آمنة. إذا كان الملف أو موقع الويب ضاراً، فسينبهك برنامج الحماية من البرامج الضارة ويقترح عليك عدم فتحه. يمكن لهذه البرامج أيضاً إزالة برامج الفدية الضارة من جهاز مصاب بالفعل.

- #### عقد دورات تدريبية منتظمة

احرص على إطلاع الموظفين بكيفية اكتشاف علامات التصيد الاحتيالي وهجمات برامج الفدية الضارة الأخرى من خلال الدورات التدريبية المنتظمة. لن تقتصر هذه الدورات التدريبية على تعليم الموظفين الممارسات الأكثر أماناً في العمل فقط، بل ستشمل أيضاً طرق حماية أنفسهم بشكل أكبر عند استخدام أجهزتهم الشخصية.

- #### النقل إلى السحابة

عندما تقوم بنقل البيانات إلى خدمة مستندة إلى السحابة، مثل خدمة النسخ الاحتياطي على السحابة في Azure أو النسخ الاحتياطي في Azure Block Blob Storage ، ستكون قادراً على نسخ البيانات احتياطياً بسهولة للتأكد من حمايتها. إذا تعرضت البيانات للاختراق من قبل برامج الفدية الضارة، فإن هذه الخدمات تضمن لك استرداداً فورياً وشاملاً للبيانات.

- #### اعتماد نموذج أمان الثقة المعدومة

يقوم نموذج أمان الثقة المعدومة بتقييم جميع الأجهزة والمستخدمين بحثاً عن المخاطر قبل السماح لهم بالوصول إلى التطبيقات والملفات وقواعد البيانات والأجهزة الأخرى، مما يقلل من احتمالية وصول أي هوية أو جهاز ضار إلى الموارد وتثبيت برامج الفدية الضارة. على سبيل المثال، تبين أن تنفيذ مكون نموذج أمان الثقة المعدومة "المصادقة متعددة العوامل" يقلل فعالية هجمات الهوية لأكثر من 99٪ بالمائة. لتقييم مستوى فعالية نموذج "الثقة المعدومة" في مؤسستك، قم بإجراء تقييم فعالية نموذج الثقة المعدومة" من Microsoft.

- #### الانضمام إلى مجموعة مشاركة المعلومات

تشجع مجموعات مشاركة المعلومات، التي يتم تنظيمها باستمرار حسب المجال أو الموقع الجغرافي، المؤسسات ذات الهيكلية المماثلة على العمل معاً لإيجاد حلول للأمان عبر الإنترنت. تقدم المجموعات أيضاً للمؤسسات مزايا مختلفة، مثل الاستجابة للتنبيهات وخدمات الأدلة الجنائية الرقمية، والأخبار المتعلقة بأحدث التهديدات، ومراقبة نطاقات ومجالات IP العامة.

- #### الاحتفاظ بنسخ احتياطية في وضع عدم الاتصال بالإنترنت

نظراً لأن بعض برامج الفدية الضارة ستحاول البحث عن أي نسخ احتياطية عبر الإنترنت قد تكون لديك وتحذفها، فمن الجيد الاحتفاظ بنسخة احتياطية محدثة للبيانات الحساسة دون الاتصال بالإنترنت التي تختبرها بانتظام للتأكد من قابلية استعادتها إذا تعرضت لهجوم من البرامج الضارة. لسوء الحظ، لن يؤدي الاحتفاظ بنسخة احتياطية دون الاتصال بالإنترنت إلى حل

المشكلة إذا تعرضت لهجوم برامج الفدية الضارة المُشفِرة للملفات، ولكن يمكن أن يكون أداة فعالة لاستخدامها في هجوم برامج الفدية الضارة المغلِقة للملفات.

- **المداومة على تحديث البرنامج**

بالإضافة إلى تحديث أي حلول لبرنامج الحماية من الفيروسات (ومراعاة اختيار التحديثات التلقائية)، تأكد من تنزيل وتثبيت أي تحديثات أخرى للنظام وتصحيحات البرامج بمجرد توفرها. يساعد هذا في تقليل أي ثغرات أمنية قد يستغلها المجرمون الإلكترونيون للوصول إلى الشبكة أو الأجهزة.

- **وضع خطة للاستجابة للتنبيهات**

على غرار خطة طوارئ الخروج من المنزل في حالة الحريق، التي تجعلك أكثر أماناً وأكثر استعداداً، فإن وضع خطة استجابة للحوادث لما يجب فعله عند التعرض لهجوم برامج الفدية الضارة سيوفر لك خطوات فعلية يجب اتباعها للتعامل مع سيناريوهات الهجوم المختلفة حتى تتمكن من العودة إلى العمل بشكل طبيعي وآمن في أسرع وقت ممكن.

كيف أحمي نفسي من فيروسات الفدية؟

يرى خبراء الأمان أن أفضل طريقة للحماية من فيروسات الفدية الضارة تتمثل في منعه من الحدوث في المقام الأول.

رغم وجود أساليب للتعامل مع فيروس برنامج الفدية الضار، لكنها حلول غير متكاملة، وكثيرًا ما تتطلب مهارات تقنية كثيرة تفوق مهارات المستخدم العادي لجهاز الكمبيوتر. ولذلك سنقدم فيما يلي النصائح التي ينبغي أن يلتزم بها الأفراد لتجنب النتائج التي قد تترتب على هجمات فيروس الفدية الضارة.

وتتمثل الخطوة الأولى لمنع فيروسات الفدية الضارة في ضخ الاستثمارات في أمن الفضاء الإلكتروني وهو برنامج مزود بحماية في الوقت الفعلي ومصمم لمنع هجمات البرامج الضارة المتطورة مثل فيروسات الفدية الضارة. كما يتعين عليك البحث عن الميزات التي ستحمي البرامج المعرضة للتهديدات (تكنولوجيا ضد الفيروسات المعطلة للأمان) فضلاً عن منع فيروسات الفدية الضارة من سرقة الملفات (مكون ضد فيروسات الفدية الضارة). إن العملاء الذين كانوا يستخدمون الإصدار المتميز من برنامج MalwarebytesلنسخةWindows ، على سبيل المثال، كانوا بمنأى عن جميع الهجمات الرئيسية لبرامج الفدية الضارة في عام 2017.

بعد ذلك، وعلى قدر الألم الذي قد يصيبك، يتعين عليك إنشاء نسخ احتياطية مؤمنة من بياناتك على أساس منتظم. ونوصي باستخدام مساحة تخزين سحابية مُزودة بتشفير ذي مستوى عالٍ ومصادقة ذات عوامل متعددة. ورغم ذلك، يمكنك شراء أجهزة USB أو محرك أقراص ثابتة خارجي حيث يمكن أن تحفظ ملفات جديدة أو ملفات مُحدثة ولكن عليك أن تتأكد بشكل ملموس من فصل الأجهزة من جهاز الكمبيوتر الخاص بك بعد إجراء عملية النسخ، وإلا فمن الممكن أن يتم اختراقها بفيروسات الفدية الضارة، أيضًا.

بعد ذلك، تأكد من تحديث الأنظمة والبرامج. لقد استغلت الأنواع المختلفة من برنامج فيروس الفدية الضارWannaCry ، الثغرات في برنامج .Microsoft ورغم أن الشركة قد أصدرت حزمة تصحيح برمجي لثغرة الأمان في مارس 2017، لم يقم الكثير من الأشخاص بتثبيت التحديث وهو ما عرضهم للهجمات. نتفهم أنه من الصعب الحفاظ على تثبيت قائمة متزايدة من التحديثات لقائمة متزايدة من البرامج والتطبيقات في حياتك اليومية. وهذا هو السبب في أننا نوصي بتغيير إعداداتك لتمكين التحديث التلقائي.

وأخيرًا، كن مطلعًا على المستجدات. واحدة من أكثر الأساليب المعتادة لاختراق برامج الفدية الضارة لأجهزة الكمبيوتر تكمن في استخدام الهندسة الاجتماعية. علّم نفسك (والموظفين معك إذا كنت صاحب شركة) كيفية الكشف عن البريد العشوائي الضار، ومواقع الويب الضارة، والرسائل الأخرى. وقبل كل ذلك، تدرب على الحس الفطري. إذا كان يبدو مصدرًا للشك، فهو كذلك

كيف يمكن ان يخترق فيروس الفدية شركتي؟

GandCrab ، وSamSam، وWannaCry، وNotPetya، هي أنواع مختلفة لفيروسات الفدية الضارة وتلحق أضرارًا جسيمة بالشركات. في الحقيقة، ارتفعت نسبة هجمات الفدية الضارة على الشركات إلى .88% في النصف الثاني من عام 2018 عندما قام مجرمو الفضاء الإلكتروني بتحويل محور الأهداف بعيدًا عن الهجمات المركزة على المستهلكين. أدرك مجرمو الفضاء الإلكتروني أن الشركات الكبيرة تترجم إلى أموال كبيرة، ولذلك قاموا باستهداف المستشفيات، والهيئات الحكومية، والمؤسسات التجارية. خلاصة القول، تبلغ تكلفة اختراق البيانات، ويشمل ذلك المعالجات، والغرامات، والمقابل المادي لبرامج الفدية الضارة، 3.86 ملايين دولارات أمريكية.

لقد تم تحديد غالبية حالات برامج الفدية الضارة مؤخرًا على أنها برنامج .GandCrab إن برنامج GandCrab الذي تم اكتشافه لأول مرة في يناير 2018، قد مَرَّ بالفعل بعدة إصدارات حيث يعمل أصحاب التهديدات على زيادة درجة تعقيد برامج الفدية الضارة الخاصة بهم لكي تدافع عن نفسها وتقوي تشفيرها. تشير التقديرات إلى أن البرنامج الضار GandCrab قد حصد بالفعل في مكان ما مبلغ وصل إلى 300$ مليون دولار أمريكي مدفوعة في شكل فدية، إضافةً إلى فدية تراوحت بين 600 دولار أمريكي و700,000 دولار أمريكي.

في هجوم آخر ملحوظ وقع في مارس 2018، تسبب برنامج الفدية الضار SamSamفي شل حركة مدينة أتلانتا وذلك من خلال تعطيل العديد من الخدمات الرئيسية بالمدينة بما في ذلك تحصيل الإيرادات ونظام حفظ السجلات الشرطية. خلاصة القول، كلف هجوم SamSam قيمة بلغت 2.6 ملايين دولارات أمريكية للقيام بالمعالجة.

وبالنظر إلى سلسلة هجمات برامج الفدية الضارة والتكلفة الباهظة المرتبطة بها، الآن هو الوقت المناسب للتحلي بالحكمة بشأن حماية شركتك من فيروسات الفدية الضارة. لقد قمنا بتغطية الموضوع بالتفصيل من قبل

لكن فيما يلي نظرة سريعة على كيفية حماية شركتك من البرامج الضارة.

- إجراء النسخ الاحتياطي للبيانات الخاصة بك. لنفترض أن لديك نسخ احتياطية متاحة، ستكون معالجة الآثار المترتبة على هجوم فيروس الفدية الضار بسيطة مثل مسح وإعادة تصوير الأنظمة المخترقة. ربنا تريد إجراء الفحص للنسخ الاحتياطية الخاصة بك حتى تتأكد من عدم اختراقها، لأن بعض فيروسات الفدية الضارة مصممة للبحث عن مشاركات الشبكات. وبناء على ذلك، من الأفضل أن تقوم بتخزين النسخ الاحتياطية للبيانات على جهاز سيرفر سحابي آمن مُزوَّد بتشفير ذي مستوى عالٍ ومصادقة ذات عوامل متعددة.
- إجراء التحديثات البرمجية وتحديث البرامج الخاصة بك. كثيرًا ما تعتمد فيروسات الفدية الضارة على مجموعات الاختراق للحصول على وصول غير مشروع لأحد الأنظمة أو الشبكات) على سبيل المثال .(GandCrab وطالما أن جميع البرامج في شبكتك مُحدثة، لا يمكن أن تتسبب هجمات برامج الفدية الضارة القائمة على الاختراق، في إلحاق الضرر بك. وفي ذلك الصدد، إذا كانت شركتك تُثبِّت برامج غير حديثة أو قديمة فأنت بذلك معرض لخطر التعرض لفيروسات الفدية الضارة، لأن الشركات المنتجة للبرامج لا تطرح تحديثات أمان. تخلص من abandonware واستبدله ببرامج لا تزال تدعمها الشركة المنتجة.
- علّم المستخدمين النهائيين لديك كيفية اكتشاف البريد العشوائي الضار وإنشاء كلمات مرور قوية. يستخدم مجرمو الفضاء الإلكتروني في المؤسسات والمسؤولون عنEmotet ، فيروس حصان طروادة السابق بالبنوك كوسيلة إرسال لفيروسات الفدية الضارة. يعتمد Emotet على البريد العشوائي الضار لاختراق المستخدم النهائي والحصول على موطئ قدم في شبكتك. بعد أن يتواجد برنامج Emotet في شبكتك، يقوم بإظهار تصرفات مثل الدودة وينتشر من نظام إلى نظام

باستخدام قائمة من كلمات المرور الشائعة. بعد تعلم كيفية الكشف عن البريد العشوائي الضار واستخدام مصادقة ذات عاملين، سيكون المستخدمون النهائيون لديك متقدمين خطوة عن مجرمو الفضاء الإلكتروني.

- استثمر في التكنولوجيا الجيدة لأمن الفضاء الإلكتروني Malwarebytes Endpoint Protection. وResponse، على سبيل المثال، يُوفِّران لك إمكانات الاكتشاف، والاستجابة والمعالجة عبر أحد العوامل المناسبة في شبكتك بالكامل.

ما الإجراءات التي ينبغي أن أقوم بها إذا وقعت بالفعل ضحية لفيروس الفدية؟ لا أحد يريد أن يتعامل مع فيروسات الفدية الضارة بعد التعرض لها.

1. تحقق وتأكد ما إذا يتوفر برنامج لفك التشفير أم لا. في بعض الحالات النادرة قد تكون قادرًا على فك تشفير بياناتك دون دفع أموال، لكن تهديدات برامج الفدية الضارة تتطور باستمرار بهدف زيادة درجة صعوبتها وصعوبة فك تشفير ملفاتك ولذلك لا ترفع من سقف آمالك.
2. لا تدفع فدية. لطالما نادينا بعدم دفع الفدية ووافق مكتب التحقيقات الفيدرالي (بعد عدة مناقشات). ليس لدى مجرمي الفضاء الإلكتروني أي وازع ولا يوجد ضمان أنك ستحصل على ملفاتك مرة أخرى. وفضلاً عن ذلك، حين تدفع الفدية فأنت تثبت لمجرمي الفضاء الإلكتروني أن هجمات فيروس الفدية الضارة مثمرة.

الوحدة الرابعة : الجهود الدولية والوطنية لحماية الأمن السيبراني

الأهداف التفصيلية للوحدة :

أن يكون المتدرب في نهاية الوحدة قادرا على:

1- يتعرف علي الحماية الدولية للأمن السيبراني

2- يتعرف علي قواعد الحروب السيبرانية

3- يوضح الطرق المستخدمة لحماية البيانات

4- يتعرف علي جهود الانتربول في حماية الأمن السيبراني

تشمل الوحدة على المواضيع الفرعية التالية "

1- الحماية الدولية للأمن السيبراني وتنظيم قواعد الحروب السيبرانية (لجنة تالين للأمن السيبراني)

2- دور الإتحاد الدولي للاتصالات في تقييم الجاهزية السيبرانية مع الهجمات السيبرانية

3- جهود الإنتربول في حماية السيبراني

الدرس الأول / الحماية الدولية للأمن السيبراني وتنظيم قواعد الحروب السيبرانية (لجنة تالين للأمن السيبراني)

الجريمة السيبرانية والهجوم السيبراني في سياق الأمن السيبراني

يعتبر تنفيذ "الهجمة السيبرانية " واقع نتيجة "عمل مقصود" لهذا الهدف، حيث ينبغي ربط مفهوم هذا المصطلح بسلوك أو نتيجة لوقوع فعل الجريمة الإلكترونية / السيبرانية. وقد أصبحت هذه الجريمة منظمة عابرة للحدود والقارات، وتهدد شريحة كبيرة من سكان العالم، لأن الجناة يلجؤون إلى وسائل متعددة ومتنوعة عند القيام بها .

تُفهم الجريمة الإلكترونية عمومًا على أنها "استخدام وسيلة قائمة على استخدام الحواسب الآلية لارتكاب عمل غير قانوني. يصف أحد التعريفات النموذجية الجريمة السيبرانية بأنها "أي جريمة يتم تسهيلها أو ارتكابها باستخدام جهاز حاسوب آلي أو شبكة أو جهاز أخر لإفشاء او استيلاء على معلومات أو تعطيل أو النفاذ الى أجهزة او شبكات دون مسوغ قانوني. وعلى هذا النحو، فإنه يشمل مجموعة واسعة من الأنشطة غير المشروعة ".

يُفهم عمومًا، بالطريقة التقليدية، أن مرتكبي الجريمة السيبرانية هم أفراد وليست دول. لقد تغير هذا الفهم بشكل ذاتي لأننا لم نشهد فقط تهديدات في أشكال حملات خاصة بهدف مالي أو ابتزاز للمعلومات من مجرمي الأنترنت، ولكن هويات أفراد من هذه الجماعات تهاجم لأسباب جغرافية سياسية .

أنواع التهديدات السيبرانية التي يتصدى لها الأمن السيبراني ثلاثة:

1. تشمل الجرائم الإلكترونية جهات فاعلة فردية أو مجموعات تستهدف أنظمة لتحقيق مكاسب مالية أو إحداث اضطراب.
2. غالبًا ما تنطوي الهجمات الإلكترونية عبر الإنترنت على جمع معلومات ذات دوافع سياسية.
3. يهدف الإرهاب الإلكتروني إلى تقويض الأنظمة الإلكترونية لإحداث حالة من الذعر أو الخوف.

وتتراوح الهجمات السيبرانية المنظمة عالمياً بين ثلاثة أقسام وهي:

١- الإرهاب السيبراني

هو الهجوم المنظم من الجماعات الإرهابية على البنى التحتية والأنظمة والشبكات بهدف التخريب والإرهاب، حيث استطاعت الجماعاتُ الإرهابية استخدام الانترنت في التواصل مع بعضها بعضاً عبر القارات، وهو الأمر الذي كان يستغرق شهوراً في الماضي. ليس هذا فحسب، بل استطاعت الجماعات الإرهابية تبادل المعارف بطرق جديدة، وبذلك يكون الانترنت قد وفّر لهذه الجماعات مساحات افتراضية للتدريب، ووفرّ كذلك مصدر منخفض التكلفة لجمع المعلومات الاستخباراتية حول أهدافها عن طريق استخدام تقنيةGoogle Earth .

٢- الحروب السيبرانية

تستخدم مصطلح "الحرب السيبرانية" لوصف كل شيء متعلق بحملات التخريب وتعطيل الإنترنت، وصولاً إلى حالة الحرب الفعلية باستخدام الوسائل الالكترونية، ويذهب بعض الخبراء لتوسيع هذا المفهوم ليشمل عمليات تزوير بطاقات الائتمان، وقد تم اعتماد الحرب السيبرانية كغيرها من الحروب التقليدية مثل (الحرب البرية، الجوية، البحرية والفضاء) من قبل العديد من الحكومات.

٣- التجسس السيبراني

يُعد أحد أنواع التجسس التقليدي باستخدام وسائل التكنولوجيا الفائقة؛ و معظم الهجمات السيبرانية المتطورة التي أطلقت تقع ضمن هذه الفئة حيث يتم التحصل على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية اقتصادية، أو استراتيجية، أو عسكرية، ومن أشهر الهجمات الهجوم على "اكويفاكس" والذي تسبب في ضياع معلومات شخصية لـ ١٤٣ مليون مستهلك أمريكي،

وأيضاً هجمات فيروس "الفدية" الالكترونية التي تعرض لها عدد كبير من دول العالم.

التمييز بين **الجريمة الإلكترونية والهجوم السيبراني** أمر بالغ الأهمية، فإننا ندرك أنه من الصعب في كثير من الأحيان معرفة ما إذا كان الحدث السيبراني واحدًا أو آخر (أو كلاهما)، في وقت وقوع الحدث - ويرجع ذلك جزئيًا إلى أن هوية الفاعل والقصد قد لا يكون واضحً. ونظرًا للغموض الذي يحيط بهذا الأمر، يوصى برد فعل عاجل ومناسب على الجرائم السيبرانية أو الهجوم السيبراني

أما عن التعريف الشائع للجرائم الإلكترونية :

الجرائم الإلكترونية :

يُشار أيضًا إلى **جرائم الإنترنت** على أنها جرائم متعلقة بالكمبيوتر والشبكة عبر الفضاء السيبراني ويُعتبر أي نشاط إجرامي يتم باستخدام الكمبيوتر (أو أجهزة أخرى مماثلة مثل اللاب توب والهواتف المحمولة وغيرها) والإنترنت جريمة إلكترونية ، بمعنى آخر الجريمة الإلكترونية هي أي عمل غير قانوني يتم فيه استخدام أجهزة الكمبيوتر والإنترنت إما كأداة أو هدف أو كليهما والحاجة للأمن السيبراني اليوم في عصر التكنولوجيا حيث تنجذب جميع جوانب الحياة بما في ذلك المهنية والشخصية والمالية والتعليمية نحو الرقمنة وبسبب هذا الاعتماد الشديد على أجهزة الكمبيوتر (وغيرها من أجهزة الحوسبة المماثلة) والشبكات نقوم بتخزين ونقل البيانات الغزيرة على أساس منتظم يمكن أن يكون جزء من هذه البيانات خاصًا وحساسًا ويجب الاحتفاظ به بطريقة لا يتم فيها تغيير الخصوصية والسرية والنزاهة ولكن العديد من المستخدمين يفشلون في الحفاظ على هذه الخصوصية أثناء اتباع مسار الرقمنة وينسى الكثير من المستخدمين الانتباه إلى جانب مهم من جوانب الفضاء الإلكتروني يُعرف بالأمن السيبراني مما يجعلهم أكثر عرضة من أي وقت مضى للهجمات الضارة وانتهاكات الخصوصية والاحتيال وغيرها من الأمور غير السارة .

بالإضافة إلى الجريمة الإلكترونية، يمكن أيضًا ربط الهجمات السيبرانية بالحرب الإلكترونية أو الإرهاب الإلكتروني، لا سيما في الحالات التي يكون فيها المهاجمون جهات فاعلة تابعة للدولة أو مجموعات أو منظمات تابعة .

يعمل المركز الوطني للأمن السيبراني عن كثب مع إدارة الجرائم الإلكترونية في الإدارة العامة لمكافحة الفساد والأمن الاقتصادي والإلكتروني بوزارة الداخلية في مملكة البحرين، لان هذه التهديدات و المخاطر تمس بالأمن القومي، بالإضافة في حالات التهديد المتزايد الموجه للأفراد أو القطاعات.

الممارسات التي يجب وضعها في الاعتبار لتقليل احتمالية وجود جريمة إلكترونية :

- **المصادقة الثنائية :**

يمكن للمصادقة الثنائية (2FA) (أى طريقة أمان لإدارة حسابك الخاص وهى تتطلب شكلين من أشكال التعريف للوصول إلى الموارد والبيانات) أن تحميك من المتسللين وهي أفضل طريقة لحماية حساباتك على الإنترنت فهي تضيف طبقة إضافية من الأمان إلى عملية المصادقة لأنه يضيف خطوة ثانية في عملية تسجيل الدخول المعتادة ومن ثم يصبح من الصعب على المهاجم الوصول إلى جهاز الشخص أو حساباته عبر الإنترنت لأن معرفة كلمة مرور الضحية وحدها لا يكفي لاجتياز فحص المصادقة

- **استخدم Bluetooth و GPS بأمان :**

يمكن للقراصنة اختراق نظامك باستخدام GPSأو Bluetoothفي جهازك ويمكن للقراصنة استخدامها للوصول إلى جهازك واستغلاله فإذا كان نظام تحديد المواقع العالمي (GPS)قيد التشغيل فيمكن للمتسللين تتبع موقعك بالضبط لذا قم بإيقاف تشغيله عندما لا يكون قيد الاستخدام .

- **تجنب رسائل البريد الإلكتروني والنصوص المشبوهة :**

إذا لم تتمكن من التعرف على عنوان البريد الإلكتروني أو رقم هاتف المرسل فلا تفتحه ولا ترد فقد تكون محاولة لخداع التصيد الاحتيالي أو هجوم سرقة الهوية فإذا فتحت أي رابط مشبوه في جهازك فقد يؤدي ذلك إلى هجوم فدية أو سرقة البيانات لذا تجنب فتح مثل هذه الروابط المشبوهة .

- **استخدم برنامج مكافحة فيروسات عالي الجودة :**

يحمي برنامج مكافحة الفيروسات جهازك من البرامج الضارة ومجرمي الإنترنت فهو يبحث عن التهديدات المحددة مسبقًا وإذا تم العثور على أي سلوك مشبوه يقوم برنامج مكافحة الفيروسات بوضع علامة عليه .

- **لا تفقد أجهزتك :**

أسهل طريقة لدخول المتسللين إلى جهازك هي الاستيلاء عليه فعليًا والوصول أو التلاعب ببياناتك لتجنب ذلك راقب أجهزتك دائمًا وقم بحمايتها باستخدام كلمات مرور قوية وأيضًا في حالة فقدها لا تنس الإبلاغ عنها على الفور

حفظ على تحديث أجهزتك :

تبقي نفسك على اطلاع دائم بما يجري في مجال الأمن السيبراني ونوع الجرائم الإلكترونية التي تحدث بسبب وجود جرائم إلكترونية جديدة تحدث كل يوم كلما حافظت على تحديثك للجرائم السيبرانية والمزيد من المعلومات التي تعرفها عن التطورات في مجال الأمن السيبراني يمكنك حماية نفسك بشكل أفضل في الفضاء الإلكتروني

الحرب السيبرانية

يقصد بالحرب السيبرانية اساليب الحرب ووسائلها التي تعتمد على تكنولوجيا المعلومات وتستخدم في سياق نزاع مسلح.

اي هي الهجمات والعمليات التي ترتكب ضد او بواسطة شبكات الحواسيب وانظمة البيانات بين الدول أو الجماعات المسلحة المنظمة في سياق نزاع مسلح، او سياسات الردع المتبادل.

وتعد الحروب السيبرانية ميدان رابع من ميادين الحروب فهي حروب خفية تقتحم الأنظمة الإلكترونية وتسبق العمل العسكري.

تستهدف الحرب السيبرانية استهداف الأنظمة العسكرية والبنية التحتية الحيوية للدولة فضلا عن الشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA) التي تسمح لها بالعمل والدفاع عن نفسها.

تصنف الهجمات السيبرانية ضمن أبرز المخاطر التي تحيط بالدول، حيث زادت حجم الهجمات السيبيرانية بين الدول في الفترة الحالية . لذلك قامت الدول بتخصيص وحدات إلكترونية خاصة بالأمن السيبراني وزادت من حجم صلاحياتها.

الأمن السيبراني

الأمن السيبراني هو ممارسة حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. وعادة ما تهدف هذه الهجمات الإلكترونية إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها، ابتزاز المال من المستخدمين، أو مقاطعة العمليات التجارية العادية.

البيئة الرقمية

تعرف البيئة الرقمية على انها سياق او مكان يتم تمكينه بواسطة التكنولوجيا والأجهزة الرقمية، التي غالباً ما تنتقل عبر الإنترنت، أو غيرها من الوسائل الرقمية، مثل شبكة الهاتف المحمول. تشكل السجلات والأدلة على تفاعل الفرد مع البيئة الرقمية بصمتها الرقمية.

ثانيا: خصائص الارهاب السيبراني

للارهاب السيبراني العديد من الخصائص التي تميّزه عن الإرهاب في صورته التقليدية، والتي تسعى في نهاية الأمر لتحقيق أهداف غير مشروعة، وهي:

1. **أن الإرهاب السيبراني إرهاب عابر للقارات والحدود، وغير خاضعة لنطاق اقليمي محدود.**
2. **صعوبة اكتشاف أثر الجاني في مرتكب واقعة الإرهاب السيبراني، حيث يوجد العديد من الصعوبات التي تقف حائلًا دون الوصول لدليل مادي يربط الجاني بالواقعة.**
3. **الارهاب السيبراني يعد أحد أخطر أنواع الإرهاب، إذ انه يؤثر بالسلب على الأمن القومي للدولة المستهدفة. وفي هذا الصدد يقول بيتر غرابوسكي أن طريقة توظيف تقنية المعلومات الواسعة تعتبر وسيلة لتسهيل الإرهاب، ومن ذلك قرصنة المعلومات الاستخباراتية، واستخراج البيانات، وجمع الأموال، والتوظيف والتعبئة والتدريب عن بعد، مثل التدريب على استخدام تقنية الهجوم ومهاراته، ومشاركة المعلومات، ونشر الأدلة، مثل أدلة صنع الأسلحة وغيرها.**

4. الارهاب السيبراني لا يحتاج عند ارتكابه الى العنف والقوة بل يتطلب حاسب الي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة، لذا يوصف بأنه من قبيل الجرائم الناعمة التي لا تتطلب استخداما للقوة في معناها العنيف أو المسلح.
5. مرتكب الجريمة السيبرانية لديه الخبرة في استخدام تكنولوجيا المعلومات، وبالتالي تكون أهدافه ليست صعبة، وبالتالي صعوبة الاثبات قيامه بالجريمة، نظرا لسرعة غياب الدليل الرقمي وسهولة اتلافه وتدميره.

ثالثا: مخاطر الارهاب السيبراني

في عام 2019 أكّد تقرير المخاطر العالمية الصادر عن المنتدى الاقتصادي العالمي، أن الإرهاب السيبراني أصبح واقعا لا مفر منه.

ويصف التقرير الهجَماتِ السيبرانيةَ بأنها تلك الهجَماتُ التي تتسبَّب في أضرار اقتصادية كبيرة، أو اضطرابات جيوسياسية، أو مشاهدَ ومواقف تتصدع فيها الثقة بشبكة الإنترنت على نطاق شاسع.

وتتمثل الهجَمات الإرهابية واسعة النطاق بأفراد أو جماعات غير الحكومية ذات أهداف سياسية أو دينية أو اجتماعية تهدف إلى إلحاق أضرار بشرية أو مادية واسعة النطاق.

وفي هذا الاطار كشف تقرير المنتدى الاقتصادي العالمي عن مخاطرَ عميقة للهجوم الإرهابي السيبراني، حيث أنه له صلة وثيقة بانهيار البِنية التحتية للمعلومات الهامة، وخطر إطلاق أسلحة الدمار الشامل. وقد تتعدد طرائق العمل من استعمال البرامج التخريبية الخبيثة و(فيروسات) البرامج، إلى حجب الخِدْمات، والأعمال الاستخباراتية التجسُّسية على الشبكة وغيرها.

المنتدى الدولي
للأمن السيبراني

الدرس الثاني / دور الإتحاد الدولي للاتصالات في تقييم الجاهزية السيبرانية مع الهجمات السيبرانية

جهود الدولة لتأمين البنى التحتية للإتصالات والمعلومات

1 - تشكيل المجلس الأعلى للأمن السيبرانى فى مصر 2014 :

- تم تشكيل المجلس الأعلى للأمن السيبراني في مصر، بقرار من رئيس الوزراء الأسبق المهندس إبراهيم محلب، في ديسمبر 2014، و يهدف إلى حماية المعلومات والبيانات لدى الجهات مع الاهتمام بإدارات المعلومات والاتصالات في الوزارات والجهات المختلفة، والتأكد من توافر التمويل اللازم لضمان تنفيذ منظومة الأمن السيبرانى، مع ضرورة وضوح الإطار التشريعى الخاص به، ويضم تشكيله وزير الاتصالات وتكنولوجيا المعلومات رئيسا للمجلس، وعضوية ممثلين عن وزارات: الدفاع، والخارجية، والداخلية، والبترول والثروة المعدنية، والكهرباء، والصحة، والموارد المائية والري، والتموين، والاتصالات، وجهاز المخابرات العامة، والبنك المركزي، و3 أعضاء من ذوي الخبرة .

- في يناير 2015 أصدر المهندس إبراهيم محلب رئيس الوزراء الأسبق، قرارًا بضم ممثل عن وزارة المالية، وممثل عن وزارة التخطيط والمتابعة والإصلاح الإداري، لعضوية المجلس ، كما أصدر المهندس شريف إسماعيل رئيس الوزراء السابق فى 19 يناير 2016، قراراً بتعيين ممثل عن رئاسة الجمهورية عضواً بالمجلس يتولي وضع استراتيجية لمواجهة الأخطار السيبرانية والإشراف على تنفيذها .

ونشرت الجريدة الرسمية قراراً للمهندس شريف إسماعيل رئيس مجلس الوزراء السابق بشأن الأمن السيبراني، في عددها رقم 17 مكرر

(ب) بتاريخ 2 مايو2017، وتنص المادة الأولى للقرار على التزام كافة الجهات الحكومية بكافة مستوياتها وشركات قطاع الأعمال العام بتنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني، فيما يتعلق بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات الخاصة بها، واتخاذ كافة الإجراءات الفنية والإدارية لمواجهة الأخطار والهجمات السيبرانية وتنفيذ الاستراتيجية الوطنية للأمن السيبراني، وقد نصت المادة الثانية للقرار على أن يتولى وزير الاتصالات وتكنولوجيا المعلومات وضع وتحديد قواعد وإجراءات تأمين البنية المعلوماتية الحرجة لقطاعات الدولة، ومتابعة تنفيذ قرارات وتوصيات المجلس الأعلى للأمن السيبراني وتطبيق أحكام هذا القرار

2 – اطلاق الاستراتيجية الوطنية للأمن السيبراني:

أطلق المجلس الأعلى للأمن السيبراني، التابع لرئاسة مجلس الوزراء، برئاسة وزير الاتصالات وتكنولوجيا المعلومات، الاستراتيجية الوطنية للأمن السيبراني (٢٠١٧- ٢٠٢١)، وهي تهدف إلى تأمين البني التحتية للاتصالات والمعلومات بشكل متكامل لتوفير البيئة الآمنة لمختلف القطاعات لتقديم الخدمات الإلكترونية المتكاملة، وذلك في إطار جهود الدولة لدعم الأمن القومي وتنمية المجتمع المصري.

3 - المركز المصري للاستجابة لطوارئ الحاسب الآلي "سيرت "

قام الجهاز القومي لتنظيم الاتصالات بتأسيس المركز المصري للاستجابة لطوارئ الحاسب الآلي "سيرت" في أبريل 2009، حيث يعمل به فريق من ستة عشر متخصصاً ، ويقدم الفريق الدعم الفني على مدار 24 ساعة لحماية البنية التحتية الحيوية للمعلومات .

- يقدم المركز منذ عام 2012 الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية والحكومية من أجل مساعدتهم على مواجهة تهديدات الأمن السيبراني بما في ذلك هجمات الحرمان من الخدمة .

- يتكون المركز من أربع إدارات رئيسية، وهي مراقبة المخاطر والتعامل مع الحوادث السيبرانية، وتحليل الأدلة السيبرانية، وتحليل البرمجيات الخبيثة، وفحص الثغرات واختبارات الاختراق.

- تتمحور مهمة المركز المصري للاستجابة لطوارئ الإنترنت والحاسب حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية، ويعمل المركز حالياً على التوسع في تطوير مختبراته في الإدارات التشغيلية الرئيسية الأربعة، ويجرى التخطيط لمختبرات إضافية للأمن السيبراني في مجال الهاتف المحمول والأمن السيبراني في أنظمة التحكم الصناعية .

- تتركز المهمة الرئيسية للمركز المصري للاستجابة للطوارئ المعلوماتية (سيرت) حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الالكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية، ومن أهداف المركز أيضاً: وضع إطار تشريعي ملائم للأمن السيبراني، بمشاركة القطاع الخاص والمجتمع المدني واسترشادا بالخبرة الدولية والمبادرات ذات الصلة، ووضع إطار تنظيمي مناسب لإنشاء نظام وطني للأمن السيبراني ومراكز استجابة للطوارئ، وتأسيس البنية التحتية اللازمة لضمان الثقة في المعاملات الالكترونية وحماية الهوية الرقمية، مثل البنية التحتية للمفاتيح العامة ومكاتب الائتمان بمشاركة القطاع الخاص، وجمع المعلومات حول الحوادث الأمنية وتحليلها، والتنسيق والوساطة بين كافة الأطراف لحل مثل تلك الحوادث ، بالإضافة إلى التعاون الدولي مع مختلف الفرق الأخرى.

4- مؤتمر أمن المعلومات والأمن السيبراني "CAISEC'22 "

قامت مصر باقامة وعقد معرض ومؤتمر أمن المعلومات والأمن السيبراني ""CAISEC'22 على مدار يومي 13و 14 يونيو 2022 تحت عنوان "الأمن السيبراني وقت الأزمات" برعاية ودعم من وزارات مختلفة، كما شاركت شركات عملاقة مثل: دل تكنولوجيز ومجموعة بنية وإى فاينانس وشركات مايكروسوفت وسيسكو وهواوي وانتل واورنج والبنك التجاري الدولي وشركات ستار لينك وسايشيلد وفي إم وير وكاسبرسكي واكسكلوسيف نتوركس وبروف بوينت وساير فورس وسيتريكس وألكان تليكوم وفيكسد جروب وبرق ولوجريثم وفيس بوينت وفيكتوري لينك وتاليس ونت سكاوت وانومالي وتوب تك.

ناقش المؤتمر مجموعة من القضايا الأكثر أهمية من خلال لقاءات وجلسات تفاعلية بين المؤسسات الحكومية والشركات المصرية والعالمية الرائدة في أمن المعلومات، حيث ناقش المؤتمر خلال جلساته ملف الجيل الخامس من الحروب وهو الحرب السيبرانية في محاضرة متخصصة لاول مرة يلقيها ممثل عن القوات المسلحة المصرية، كما ناقش المؤتمر الأمن السيبراني والمرونة الإلكترونية، وكذا

جلسة عن الأمن السيبراني والخدمات المصرفية المفتوحة والرقمية.

كما تتضمن المؤتمر جلسة للتباحث فيما يخص حماية الأصول العينية باستخدام خطط الأمن السيبراني ، بالإضافة إلى جلسة أخرى لمناقشة بناء وتأمين أنظمة البنية التحتية الحيوية، وأخرى فتحت ملف الحاجة إلى تشييد مركز عمليات الأمن، وعلى مدار يومين من التباحث المشترك بين مؤسسات وشركات القطاعين العام والخاص يناقش المؤتمر أيضاً تحليل الأمن السيبرانى والحلول السحابية وكيفية إدارة مخاطر سلسلة التوريد للأمن السيبراني.

كما انعقدت على هامش المؤتمر معرض أمن المعلومات والأمن السيبراني CAISEC'22 ، لاستعراض أحدث ما توصلت إليها الشركات المصرية والعالمية في مجالات حماية البيانات والأمن السيبرانى وما تقدمه من خدمات مستحدثة لمختلف القطاعات.

الأبعاد الاجتماعية للأمن السيبراني (المخاطر الاجتماعية) .

١ -استحداث الجرائم السيبرانية

وزيادة معدلاتها مع الاعتماد المتزايد، في الحياة اليومية، على الأنظمة المعلوماتية، والأجهزة المتصلة بالشبكة الدولية للمعلومات، وتشعب طبيعة هذه الأجهزة من هواتف خلوية، وأجهزة حوسبة شخصية، يزداد عدد المتصلين بالفضاء السيبرانى، .وتسهل سبل التجسس الاقتصادى وتزداد احتمالات الاعتداءات والجريمة، وتؤثر على عمليات الحكومة مثل الفيروسات وهجمات منع الخدمة وسرقة البيانات والرسائل الاقتحامية والتدليس، وكلها تقوض مصداقية تكنولوجيا المعلومات والاتصالات وقدرة المجتمعات على العمل.

وقد أشار تقرير صادر عن مؤسسة ماكينزى، إلى توقع زيادة المعلومات الرقمية، بمعدل ٤٤،٪ خلال الأعوام الممتدة من ٢٠٠٩ إلى ٢٠٢٠ .

وكذلك من أبرز التهديدات السيبرانية المحتمل تزايدها فى السنوات القادمة، هجوم الفدية (war Ransom)، (هي نوع من البرمجيات الضارة أو الخبيثة) التي يستخدمها المجرمون الإلكترونيون. إذا تمت إصابة جهاز كمبيوتر أو شبكة ببرنامج فدية، يعمل ذلك الفيروس على حجب الوصول إلى النظام أو يقوم بتشفير البيانات الموجودة. يطلب المجرمون الإلكترونيون مبلغ فدية من ضحاياهم مقابل فك التشفير عن البيانات) الذى وصفته وزارة العدل الأمريكية بأنه نموذج عمل جديد للجريمة السيبرانية. ويقدر مكتب التحقيقات الفيدرالى الأمريكى أن المبلغ الإجمالى من مدفوعات الفدية يقترب من مليار دولار سنويا، حيث كان من المتوقع أن الشركات التجارية سوف تقع ضحية لهجوم ٍالفدية كل ١٤ ثانية بحلول ٢٠١٩ .وتشير التقارير الدولية إلى أن فيروس الفدية تسبب فى خسائر مالية تفوق الخمسة مليارات دولار أثناء عام ٢٠١٧، وهو معدل مرتفع جدا خلال عام واحد.

ومن أمثلة الهجوم الإلكترونى ما ٍأصاب شبكة الكهرباء الأوكرانية والذى تسبب فى بقاء أُوكرانيا لساعات فى الظلام. وبذا، تخطت الحروب الإلكترونية والهجمات السيبرانية حاجز البيانات والمعلومات والمواقع الإلكترونية لتصل للبنية التحتية والأنظمة الحيوية مثل المفاعلات النووية وأنظمة الكهرباء والأنظمة الطبية والنقل وغيرها من القطاعات التى تعد ركائز أساسية للدول، مما يرفع مستوى الخطورة على الدول .ومن المتوقع أن ترتفع التحديات والمخاطر فى الفترة القادمة لاسيما بعد أن أوضح تقرير " Council Advisory Security Overscan"عام ٢٠١٦، أن الهجوم السيبرانى على شركة أرامكو السعودية قد كلفها تغيير ٥٠ ألف قرص صلب لأجهزتها الحاسوبية، ولم تستطع استخدام الإنترنت لمدة خمسة أشهر تقريبا. كما أشار تقرير شركة نورتون الأمريكية (سمنتك) خلال شهر أغسطس ٢٠١٦ إلى أن هناك 262، 538، 6 فردا فى المملكة كانوا ضحايا هجمات ٍ سيبرانية أو تأثروا بجرائم سيبرانية. كذلك ذكر التقرير أن نسبة ٨٥ ٪من السكان تعرضوا لهجمات سيبرانية وهذه النسبة تعد أعلى من النسبة العالمية بما يعادل ١٠٪ .

ومن أشهر الاختراقات، ما حدث من سرقة حسابات شركة ياهو (Yahoo)حيث بلغ عدد الحسابات المسروقة ثلاثة مليارات حساب، وكذلك اختراق إكيفاكس Equifax)فى عام ٢٠١٧ ،حيث تأثر 5،145 مليون عميل، وذلك يتطلب بشكل ملح إفساح المجال وبشدة للأمن السيبرانى تقنيا وتنظيمياً ٍوتشريعيا ونشر ثقافة المواطنة الرقمية لزيادة سلامة التعامل ٍالسيبرانى .

ولذا، حذر القائمون على مؤتمر أمن المعلومات السنوى بمنطقة الشرق الأوسط وشمال أفريقيا ٢٠١٧ من أن المنطقة تواجه تحديات شديدة الأهمية تتعلق بتأمين المعلومات والبنية التحتية من الهجمات الإلكترونية التى يرتكبها القراصنة كالتخريب أو الابتزاز أو الاحتيال على ضحاياهم . وتشير التقارير إلى توالى حوادث اختراق الأنظمة وسرقة البيانات وتسربها، كاختراق أنظمة معلومات سونى، التى نتج عنها تسرب بيانات مليون مستخدم.

ومما يزيد الأمر تعقيدا، ظهور ما يسمى بالويب العميق (Web Deep)والمعروف باسم الويب المظلم (Web Dark)،)وهى شبكة خفية تستخدم فى تعزيز الأنشطة الإجرامية الشنيعة.

فمع تزايد أعداد المشتركين والمستخدمين للتقنية فى الوطن العربى، ارتفعت معدلات الجريمة الإلكترونية، وظهرت مجموعة من الظواهر السلبية الإلكترونية من قبيل التنمر والاحتيال والابتزاز الإلكترونـى وغيرهـا مـن ممارسـات تتسبب فى العديـد مـن المشكلات الاجتماعية ، فقد تطورت المعارك فى الفضاء الإلكترونى، حتى باتت أخطرعلى أمن الدول من المعارك المباشرة. كما كشفت دراسة حديثة أن أكثر من ٦٥ ٪من خبراء تكنولوجيا المعلومات فى دول مجلس التعاون الخليجى يعتقدون أن المنطقة تشكل هدفا رئيسا للجرائم الإلكترونية.

٢ -استهداف الأمن القومى

يلاحظ أن التهديدات الأمنية قد ازدادت بطرق متسارعة لم يشهدها العالم من قبل حتى شملت السياحة والتجارة والاقتصاد، وطالت أمن الدول والمجتمعات .وفى هذا الخصوص، أشار تقرير صادر عن وكالة الأمن القومى الأمريكى إلى أن هناك ٢٣٢ جهاز حاسب آلى تتعرض لاختراقات وهجمات سيبرانية فى كل دقيقة على امتداد العالم مما أضاف صعوبة عالية فى المقدرة على اللحاق بمجرى السيبر فنيا وتقنيا ،كما أكدت الدراسات التى أصدرها الاتحاد الدولى للإتصالات (ITU) فى يوليو ٢٠١٧ أن هناك ضرورة ملحة فى مجالات التعليم والتدريب والدراسات لرفع مستوى المهارات والمعرفة فى الأمن هذا إلى جانب إن هناك أربع فئات رئيسة للتهديدات السيبرانية للأمن القومى هى :

الحرب السيبرانية والتجسس الاقتصادى، وهما يرتبطان الى حد كبير بالدول، وفئة الجريمة السيبرانية، والإرهاب السيبرانى، اللذين يرتبطان فى الأغلب بجهات فاعلة غير تابعة لدولة معينة.

٣ -تهديد القيم والأخلاق

ومـن الأبعاد الاجتماعيـة الحمايـة من تدنـى المستويين القيمى والأخلاقى، فالمحتويات غير المشروعة وغير المرغوب بها ذات تأثير سلبى على أخلاقيات المجتمع وعلى ارتفاع نسبة الممارسات الإجرامية كالإباحية، والترويج للإتجار بالممنوعات، والدعارة، والإرهاب، والتجنيد لقضايا تمس الأمن والسلام الدوليين .وعليه، لا بد من بناء مجتمع مسئول، ومدرك لمخاطر الفضاء السيبيرانى، قادر على التعامل مع قواعد السلامة ومدرك للعواقب القانونية التى يمكن أن تترتب على التعرض لسلامة الأفراد والمؤسسات ورؤوس الأموال.

٤ -تدمير البنية التحتية

لا يشمل مفهـوم الحـرب السيبرانية استهـداف المقـدرات والأنظمة العسكرية وحسب، ولكن أيضا استهداف البنية التحتية الحيوية للمجتمع- بما فى ذلك ٍالشبكات الذكية وشبكات المراقبة الإشرافية وحيازة البيانات (SCADA)التى تسمح لها بالعمل والدفاع عن نفسها ، ومن ثم يتمخض النزاع السيبرانى عن عواقب تهدد الحياة إذا تم إفساد البنية التحتية للمعلومات.

ولذلك ورد فى تقرير ITU 2017 بالمؤتمر العالمى لتنمية الاتصالات فى مشروع الخطة الاستراتيجية للاتحاد "ضرورة وجود بنية تحتية حديثة وآمنة للاتصالات وتكنولوجيا المعلومات وضرورة تعزيز تنمية البنية التحتية والخدمات بما فى ذلك بناء الثقة والأمن فى استخدام الاتصالات و تكنولوجيا المعلومات. وضرورة وجود بيئة تمكينية وتعزيز بيئة تنظيمية وسياسات مؤاتية .

وقد تواجه المجتمعات خسائر اقتصادية واجتماعية فادحة للتنمية المستدامة للاتصالات وتكنولوجيا المعلومات، إذا تعرضت شبكات اتصالاتها أو بنيتها التحتية الأخرى للهجوم والأعطال. وسوف يزيد التطور التكنولوجى من هذه الخسائر فى حالة عدم إيلاء اهتمام ٍكاف الخسائر فى بالأمن والبنية التحتية، إذ أن تنامى الاستغلال السيئ والمنحرف للشبكات الإلكترونية لتحقيق أهداف إجرامية يؤثر سلبا على سلامة البنى التحتية للمعلومات وهذا الخطر لا يقتصر فقط على المؤسسات بل يطول الأفراد على حساباتهم الخاصة للنيل منهم.

٥ -تصدير أزمة ثقة

إن المخاطر طويلة الأجل للمجتمع تمثل عنصرا جوهريا يجب دراسته فقد تستمر الهجمات لبضع ثوانٍ ، ولكنها تحدث آثارا واسعة. وقد تتطلب الخسارة المجتمعية للثقة في هذه الثوانى سنوات لإعادة بنائها وتقويض الثقة بين المواطنين والشركات وبين الدول نفسها يمكن أن يولد آثارا مدمرة على المجتمعات وعلى الاستقرار العالمى فى الأجل الطويل. ووقتها لا نستطيع أن نتحمل تكلفة الركو فى هذا المجال بسبب ضياع الثقة ويرجع ذلك لأسباب من أهمها نقص الخبرة فى التعامل مع مثل هذه القضايا وقلة الوعى من قبل المستهدفين، مما يزيد فرص وجود الجرائم الإلكترونية بشكل كبير، ولمحاربتها يجب تطبيق سياسة الأمن السيبر.

الأبعاد القانونية للأمن السيبرانى

١ -الإطار التشريعى والإطار التنظيمى

تتمثل المخاطر القانونيــة، بشكل أساسى، فى غياب الإطاريـن التشريعى والتنظيمى المناسبين للتعامل مع نتائج الأعمال القانونية وغير القانونية منها، والتى تتم فى الفضاء السيبرانى. ويتطلب النشاط الاقتصادى والتجارى وغيرهماء تحديدا واضحا، للواجبات والحقوق، فمستخدمو هذه التقنيات، عبر الفضاءء السيبرانى .بحاجة إلى إطار يؤمن حماية استخدامهم، ففى حالة غياب الأطر التشريعية تؤثر الجرائم السيبرانية على عمليات معلوماتية تخص حقوق الإنسان الدولية وتدفع على العنف وتسبب ضررا اقتصاديا خطيرا، فضمان إدارة مخاطر الأمن السيبرانى على نحو ممنهج يهدف إلى حماية الأصول المعلوماتية والتقنية وفقا للسياسات والإجراءات التنظيمية والمتطلبات التشريعية .

٢ -الأمن القانونى

من هذا المنطلق، تتمثل المخاطر القانونية، فى غياب الأمن القانونى، أو حتى فى تناقض الأحكام والقوانين، وتنازع الأنظمة القانونية، فيؤدى إلى ارتفاع منسوب المخاطر، مع انعدام ملاحقة فاعلة، تتلاءم وطبيعة الأعمال والجرائم والاعتداءات السيبرانية، العابرة للحدود، وللأنظمة القانونية، بحيث تطال أى مواطن فى أية بقعة من الأرض، بما يطال الدول وأمنها واستقرارها ، وتعد المخاطر التى يتعرض لها الأفراد والدول مخاطر هائلة وغير مقيدة بالأطر القانونية الجارية التى لا تستوعب العصر السيبرانى بالقدر الكافى. وهناك حاجة عاجلة إلى الخطى السريعة التى تقيم بها البلدان القيادات السيبرانية وتوسع قدراتها العسكرية لتشمل النزاع السيبرانى، ويجب أن تتوازن بعدم تعارض للقوانين والتشريعات.

٣ -التعاون الدولى

نظرا لطبيعة مجتمع الفضاء السيبرانى العابرة للحدود، يعترف قطاع تنمية ونظرا الاتصالات بأهمية التعاون الدولى فى تعزيز الموثوقية فى استخدام تكنولوجيات المعلومات والاتصالات وتوافر هذه التكنولوجيات وأمن استخدامها. وعليه، يعترف قطاع تنمية الاتـصالات بالحاجـة الملحة لدعـم الـدول لوضـع تدابيـر محددة لتنفيذ أطرها الوطنية المتعلقة بالأمن السيبرانى من أجل معالجة شواغل أصحاب المصلحة المختلفين بهذا الشأن، ومن أجل إفساح المجال أمام تبادل أفضل الممارسات على المستوى العالمى السيبرانية من أى مكان ويمكن أن تصدر الهجمات من أى مكان ، مما يجعل هذه التهديدات دولية بطبيعتها، وتتطلب التعاون الدولى والمساعدة فى التحقيق والأحكام الإجرائية والموضوعية المشتركة ولمعالجتها على نحو ملائم. ، وإضافة إلى ذلك، من المعترف به على نطاق واسع أن التعاون الدولى يمثل أحد المتطلبات الرئيسة لضمان الأمن السيبرانى، وفى عامى ٢٠٠٣ و٢٠٠٥ ،اتفقت الدول فى القمة العالمية لمجتمع المعلومات (WSIS) على ضرورة وضع أدوات تتسم بالفعالية والكفاءة على المستويين الداخلى والخارجى للنهوض بالتعاون الدولى بشأن الأمن السيبرانى ، ولذلك ينبغى أن يكون هذا التعاون، بدافع الرغبة المشتركة فى السلام، وبدافع المصلحة الفردية المستنيرة لكل بلد. وكذلك دعا المؤتمر الإقليمى الخامس للأمـن السيبرانـى والذى أعـده المركز العربى الإقليمى -ARCC) (ITUالتابع للاتحاد الدولى للاتصال، لتوحيد التعاون فى المنطقة العربية وتعزيز دور الاتحاد الدولى للاتصالات فى بناء الثقة والأمن على مستوى تقنية المعلومات والاتصالات فى المنطقة العربية والشرق الأوسط.

٤ -استحداث اتفاقيات للمكافحة

عمدت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية، إلى إيراد ما تعده أعمالا غير مشروعة، تحت عناوين تناولت، الجرائم ضد سرية الأنظمة والبيانات وسلامتها وتوفرها، والجرائم المتصلة بالأجهزة، والجرائم الخاصة بالمحتوى،والجرائم الخاصة بالملكية الفكرية.

٥ -إقرار سياسات وقائية ودفاعية

تمثل ذلك فى بناء الثقة والاطمئنان والأمن فى استعمال الاتصالات وتكنولوجياء عن حماية البيانات الشخصية وهى من الأولويات التى تستدعى تعاونا وتنسيقا دوليين بين الحكومات والمنظمات ذوات الصلة وشركات القطاع الخاص والكيانات المعنية فى مجال بناء القدرات وتبادل أفضل الممارسات من أجل وضع السياسات العامة والتدابير القانونية والتنظيمية والتقنية التى تتناول حماية البيانات الشخصية، لضمان موثوقية وأمن شبكات وخدمات تكنولوجيا المعلومات والاتصالات ولذلك اتجهت معظم الدول المتقدمة إلى إقرار سياسات وقائية ودفاعية، ضد الهجمات السيبرانية وخصصت بعض الدول مثل الولايات المتحدة الأمريكية وأستراليا وانجلترا مبالغ طائلة، لمعالجة مسائل الأمن السيبرانى، وليست هذه الحقيقة، سوى مؤشر، إلى مدى الاهتمام الذى توليه هذه الدول، لإرساء الثقة والاستقرار، فالعلاقات الدولية، مهددة فى كل لحظة نتيجة الاختراقات والاعتداءات على الشبكة العالمية للمعلومات، وعلى الأنظمة المعلوماتية، وقواعد المعلومات ولم تتأخر الإدارة الأمريكية، عن استحداث قيادة عسكرية جديدة، مختصة بأمن الفضاء السيبرانى ، وقد اقترح الاتحاد الدولى للاتصالات بالفعل عملية كاملة لوضع خطة وطنية للأمن السيبرانى وتنفيذها [ICEGOV1] ، ولكن هذه العملية استعراض تتطلب استراتيجية شاملة تتضمن استعراضا أولياء واسعا لمدى ملاءمة الممارسات الوطنية .

٦ -إنشاء وحدات خاصة للمكافحة

كثرت النشاطات العسكرية فى هذا المجال، والتى تشمل الحماية، والقيام بمناورات مكامن الضعف، والتدريب على آليات الرد. ويتم ذلك، فى إطار استراتيجية أعدتها وزارة الدفاع الإنجليزى فى عام ٢٠١١ حول كيفية العمل فى . الفضاء السيبرانى، وكان رئيس الوزراء، "جوردن براون"، قد أعلن عن إنشاء وحدة خاصة، لمكافحة الجريمة السيبيرانية ، وعلى نفس النهج أنشأت مصر وحدة لطوارئ الإنترنت والحاسب الآلى ٢٠١٢ وتسمى (CERT).

٧ -تنفيذ القوانين وفاعلية التشريعات

يأتى فى هذا الإطار، تقاعس الإدارات أو عجزها، حتى عن تنفيذ القوانين التى وضعت آليات تنفيذها، كما هو الحال مثلا، مع قوانين حماية الملكية الفكرية والأدبية، حيث تنتشر ظاهرة قرصنة البرامج، بشكل كثيف، فى مختلف الدول العربية ويعود ذلك إما لغياب إدارة متخصصة بالملاحقة واما لعدم إمكانية الإدارة المعنية، متابعة الوضع بشكل فاعل، نتيجة عدم توافر الإمكانات التقنية، والمادية والبشرية. وغياب القدرة على الضبط والتحقيق، ورغم إنشاء عدد من مراكز الاستجابة لطوارئ الإنترنت، فى البلدان العربية، فإن بعضها مازال غير فاعل بشكل كاف ، كما أن القوانين المنسقة بشأن الجريمة السيبرانية تنهض بالتحقيقات وتقديم المجرمين السيبرانيين إلى القضاء. ويتعين القيام بالكثير من العمل فى كل مجال من هذه المجالات .

واقع الأمن السيبرانى فى مصر بالنسبة الى العالم "بالأرقام" :

مؤشر «الأمن السيبراني « GCI الصادر عن الاتحاد الدولي للاتصالات أعلن عن حصول مصر خلال 2020 على المركز 23الـ عالميا بين 182 دولة بـ 95.45 درجة، بينما تصدرت أمريكا المؤشر بـ 100 درجة، تلتها بريطانيا في المركز الثاني بـ 99.54 درجة، ثم السعودية في المركز الثاني مكرر بـ 99.54 درجة، كاشفا عن أن مصر اتخذت خطوات هامة لدعم الأمن السيبراني من أهمها: تأسيس مجلس أعلى للأمن السيبراني في عام 2015 ووضع استراتيجية وطنية للأمن السيبراني 2017-2021، إلى جانب تأسيس المركز الوطني للاستعداد لطوارئ الحاسبات والشركات EG-CERT ، كما جاءت مصر في المرتبة الأولى عالميًا في تنافسية قطاعي الإنترنت والهاتف خلال 2021 وفقًا لمؤشر المعرفة العالمي .

جدير بالذكر أن الاتحاد الدولى للاتصالات التابع للأمم المتحدة يصدر المؤشر العالمى للأمن السيبرانى بشكل دورى كل عامين، ويعتمد المؤشر فى ترتيب الدول من 100 درجة على 5 معايير منها السياسات التنظيمية والتشريعات والإطار المؤسسى وبناء القدرات البشرية وتوافر القدرات التقنية والفنية اللازمة.

نفّذت الهيئة الوطنية للأمن السيبراني "تمرين الأمن السيبراني" بمشاركة المسؤولين المنتخبين وكبار مديري وكالة الأمم المتحدة المتخصصة بالاتصالات وتقنية المعلومات "الاتحاد الدولي للاتصالات"، وحضور الأمين العام للاتحاد الدولي للاتصالات دورين بوجدان مارتن؛ وذلك في مقر الوكالة بجمهورية سويسرا الاتحادية.

وأوضحت الهيئة أن التمرين يهدف إلى رفع مستوى الجاهزية السيبرانية، وتبادل المعلومات والخبرات في مجال الأمن السيبراني، والإلمام بآخر الأساليب المستخدمة في الهجمات السيبرانية، وتناولَ التمرينُ إجراء محاكاة لأنواع مختلفة من الهجمات والحوادث السيبرانية الواقعية، وتطبيق آلية الاستجابة لها؛ بما يسهم في تعزيز الصمود السيبراني .

وبيّنت الهيئة أن التمرين يأتي في إطار جهود الهيئة الدولية ومبادراتها في دعم وتوحيد المساعي المشتركة في مجالات الأمن السيبراني على المستوى الدولي، ويُعد امتدادًا للنجاح الذي تَحقق في "تمرين الأمن السيبراني" الذي نفّذته خلال شهر مايو الماضي على هامش القمة العالمية لمجتمع المعلومات 2023 بمشاركة أكثر من 40 دولة ومنظمة حول العالم.

ويأتي تنفيذ هذا التمرين عبر منصة متخصصة تم بناؤها واستضافتها وتشغيلها محليًا بالتعاون مع الذراع التقني للهيئة، الشركة السعودية لتقنية المعلومات (سايت)، يتم من خلالها تصميم تمارين سيبرانية وتطوير سيناريوهات تحاكي آخر التطورات في الأساليب المستخدمة في التهديدات والهجمات السيبرانية والتزود باستراتيجيات التعامل معها.

الهيئة الوطنية للأمن السيبراني تنفذ «تمرين الأمن السيبراني» في مقر الاتحاد الدولي للاتصالات

نفذت الهيئة الوطنية للأمن السيبراني «تمرين الأمن السيبراني» بالتعاون مع وكالة الأمم المتحدة المتخصصة بالاتصالات وتقنية المعلومات (الاتحاد الدولي للاتصالات)، وذلك عبر منصة متخصصة مستضافة في المملكة

أهداف التمرين

- تعزيز الجهود الدولية في الأمن السيبراني
- تبادل الخبرات وأفضل الممارسات في مجال الأمن السيبراني
- رفع مستوى الجاهزية السيبرانية

المشاركـون

المسؤولون المنتخبون وكبار مديري الاتحاد الدولي للاتصالات

تضمن التمرين

- إجراء محاكاة لأنواع مختلفة من الهجمات السيبرانية
- تطبيق آلية الاستجابة للحوادث السيبرانية

عن منصة التمارين السيبرانية

منصة متخصصة تم بناؤها واستضافتها وتشغيلها محلياً بالتعاون مع الذراع التقني للهيئة، الشركة السعودية لتقنية المعلومات (سايت)، يتم من خلالها تصميم تمارين سيبرانية وتطوير سيناريوهات تحاكي آخر التطورات في الأساليب المستخدمة في التهديدات والهجمات السيبرانية

SITE

NCA_KSA
NCA.GOV.SA

ITU | الهيئة الوطنية للأمن السيبراني

الدرس الثالث / جهود الانتربول في حماية الأمن السيبراني

تنسيق الإجراءات على الصعيد العالمي لمكافحة تهديدات الجريمة السيبرانية

لا تحدّ الفضاء السيبراني أيّ حدود، فالتهديدات والاعتداءات يمكن أن تأتي من كل حدب وصوب وفي كل الأوقات، ما يطرح تحديات بالنسبة للشرطة لأن هذه الحوادث قد تتعلق بمشتبه فيهم وضحايا وجرائم، وتمتد إلى عدة بلدان.

ويقدم الإنتربول المساعدة للبلدان الأعضاء في كشف التهديدات السيبرانية وتصنيفها حسب الأولوية وتنسيق إجراءات التصدي لها.

ومن خلال التعاون مع الشركاء من القطاع الخاص في مجال الأمن السيبراني الذين يزودوننا ببيانات محدثة عن التهديدات والاتجاهات والمخاطر، نكفل حصول الشرطة على أحدث المعلومات صلة بهذه التهديدات من أجل توجيه دفة عملها.

ونستخدم هذه البيانات من أجل الحصول على معلومات استخباراتية سيبرانية تساعد البلدان في وضع استراتيجيات للوقاية من التهديدات الأشد إلحاحا والتصدي لها، والاستعداد في الوقت نفسه لمواجهة أيّ تهديدات جديدة.

المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرانية

يضم المركز المتعدد الاختصاصات لمكافحة الجريمة السيبرانية خبراء في شؤون الإنترنت من أجهزة إنفاذ القانون والقطاع الخاص لجمع وتحليل جميع المعلومات المتاحة عن الأنشطة الإجرامية المرتكبة في الفضاء السيبراني بهدف تزويد البلدان بمعلومات استخباراتية متسقة يمكن ترجمتها إلى تحرك عملي.

وينشر المركز تقارير لتنبيه البلدان إلى تهديدات سيبرانية جديدة وشيكة أو متطورة. وشملت التقارير السابقة تهديدات محددة، ولا سيما برمجيات خبيثة، ورسائل تصيّد احتيالي، ومواقع إلكترونية حكومية مخترقة، واحتيال باستخدام أساليب الهندسة الاجتماعية وغير ذلك. ومنذ عام 2017، أصدرنا ما يزيد على 800 تقرير موجه للشرطة في أكثر من 150 بلدا.

الاتفاقيات الدولية في مكافحة الجرائم السيبرانية.

معاهدة بودابست لمكافحة جرائم الانترنت

تعد هذه الإتفاقية هي أولى الإتفاقيات العالمية المتعلقة بجرائم الانترنت، وقعت الإتفاقية في العاصمة المجرية بودابست في 23 نوفمبر 2001، بهدف التعاون والتضامن الدولي في محاربة الجرائم الإلكترونية.

وقعت 26 دولة أوروبية على هذه الإتفاقية بالإضافة إلى الولايات المتحدة الامريكية، كندا واليابان، جنوب أفريقيا.

وبالرغم من ان هذه الاتفاقية أوروبية المنشأ، إلا ان عضويتها مفتوحة لجميع الدول التي تريد الانضمام إليها لتعم الفائدة.

وعلى الرغم من أن هذه الإتفاقية لا تعالج الإرهابَ السيبراني على وجه الخصوص، إلا أنها صيغت بطريقة قادرة على تتبع نطاق تهديدات الإرهابيين، لتشمل جريمة الإرهاب السيبراني.

في عام 2016 أصدرت لجنةُ اتفاقية الجرائم السيبرانية مذكرةً توجيهية تتعلّق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تعلن فيها أن "الجرائم الموضوعية في الإتفاقية قد تكون أيضًا أعمالا إرهابية على النحو المحدد في القانون المعمول به". وجاءت هذه المذكرة الإضافية بموجب الإتفاقية في الوقت المناسب، لتسلط المذكرة الضوء على أن هذه الإتفاقية ليست معاهدة مختصة بالإرهاب، إلا أنه يمكن القول: إن الجرائم الموضوعية في الإتفاقية يمكن أن تنفذ على أنها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانبُ التمويلي، أو الأعمال التحضيرية.

الجهود الماليزية في مجال مكافحة جريمة الارهاب السيبراني

تتعدد الجهود التي تبذلها الدول في مجتمع المعلومات العالمي من اجل العمل على تنظيم عملية وضع السياسات المثلى للتعامل مع الارهاب السيبراني من قبل الحكومات.

قد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الاقليمي وذلك من أجل حماية البنية التحتية الكونية للمعلومات من خطر التعرض لمثل تلك الاخطار.

ففي ظل التحولات الرقمية التي يعيشها العالم بوجه عام وماليزيا بوجه خاص ظهر نوع جديد من التهديدات الأمنية التى تعتبر البيئة الرقمية عاملا هاما في انتشارها، وقد أصبحت هذه التهديدات تمس ليس فقط أمن المؤسسات وإنما أمن الأفراد وبذلك تكون شكلت تحديا للدوله في سعييها لتحقيق أمنها القومي.

وقد استمرت الدولة الماليزية في تطوير سياسات وبرامج تساعدها في تعزيز أمنها السيبراني في إطار رؤية 2020.

ويجدر بالذكر أن الهدف من إطلاق رؤية ماليزيا 2020 هو أن تصبح دولة متقدمة واعتناق الاقتصاد القائم على المعرفة كوسيلة لتحقيق ذلك.

ومن خلال الاختيار الواعي لاستخدام تكنولوجيا المعلومات والاتصالات كأداة للتنمية، فقد أدى ذلك إلى زيادة استخدام أنظمة المعلومات الرقمية في جميع أنحاء الصناعة والمنظمات الخاصة والعامة والمجتمع ككل.

ومما شك فيه إن الاعتماد على أنظمة المعلومات الرقمية يجلب معه نقاط الضعف والمخاطر المتزايدة، لا سيما للبنية التحتية للمعلومات الوطنية الحرجة (CNII) والتي تشمل من بين أمور أخرى الجرائم الإلكترونية مثل القرصنة والتطفل والاحتيال والمضايقة والرموز الضارة وهجمات الحرمان من الخدمة، كل ذلك يزيد التهديدات السيبرانية التي تهدد السيادة الإلكترونية للدولة.

تم إنشاء العديد من مواقع الانترنت لمكافحة الإرهاب السيبراني والأمن الرقمي، حيث أصبحت بمثابة مؤسسات فكرية وفنية لدعم الأمن الرقمي، وكانت تلك المواقع إما بمبادرة حكومية او من القطاع الخاص او من المجتمع المدني ، فضلا عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات.

تعد ماليزيا إحدى الدول التي كثفت جهودها في هذا المجال منذ وقت مبكر، كونها دخلت المجتمع المعلوماتي في وقت متزامن مع العديد من دول العالم المتقدم، فقد تم تصنيفها من قبل الخبراء والمتخصصين في مرتبة متقدمة نظرا للانجازات التي حققتها حتى الآن للإندماج في مجتمع المعلومات.

منذ عام 1987 دخلت خدمة الانترنت إلى ماليزيا من قبل المعهد الماليزي للأنظمة الإلكترونية الدقيقة، وذلك من خلال مشروع رنجكوم Rangkom، الذي قام بربط عدة جامعات ماليزية في شبكة واحدة.

في عام 1991 تحول مشروع رنجكوم Rangkom إلى مزود خدمة يعرض خدماته لعدد محدود من العامة.

وفي عام 1992 تم إطلاق أول مزود ماليزي لخدمات الانترنت RARING، أطلقه المعهد الماليزي للانظمة الإلكترونية الدقيقة.

حيث تفوقت ماليزيا على دول الاسيان بما في ذلك تايلاند التي جاءت في المرتبة الـ 13 وفيتنام التي جاءت في المرتبة الـ 14 والفلبين التي جاءت في المرتبة الـ 18 واندونسيا جاءت في المرتبة الـ 20.

وقد ازداد ظهور أنشطة الإرهاب السيبراني بوضوح في ماليزيا في العِقد الماضي، ورفعت دعاوى قضائية بموجب قانون العقوبات في البلاد وتصنف الأحكام تحت الرقم (ج-031) والرقم (ي-031) مختلِف الأعمال المرتكبة في سياق الأعمال الإرهابية.

سعت الدولة الماليزية الى تكثيف جهودها الرامية إلى مكافحة الجرائم الإلكترونية أو استخدام الإنترنت لأغراض إرهابية، بما في ذلك تعزيز المرافق الأمنية للإنترنت وتشديد الرقابة على أنظمة التواصل الإلكتروني.

تضع ماليزيا الأمن السيبراني نصب أعينها وتحاول أن تكون نموذجاً لمنطقة آسيا والمحيط الهادي، حيث أنها تقدم ما يقرب من اثنتي عشرة خدمة تلبي احتياجات القطاع العام والقطاع الخاص ومستخدمي الانترنت.

تشريعات وقوانين مكافحة الارهاب السيبراني في ماليزيا

تعد ماليزيا واحدة من اولى الدول في جنوب شرق آسيا التي سنت قوانين وتشريعات الفضاء السيبراني، فهناك عدة قوانين وتنظيمات تبنتها الدولة الماليزية للتعامل مع الارهاب السيبراني والتي كان من أهمها:

1- قانون جرائم الكمبيوتر عام 1997 :

هو أول تشريع محدد على الإطلاق يتم في ماليزيا لمكافحة الجرائم الإلكترونية. يجرم عمل القراصنة ونشر الفيروسات على اجهزة الكمبيوتر والاتصال غير المشروع للوصول إلى أجهزة الكمبيوتر وارتكاب الجرائم الإلكترونية.

2- قانون التوقيع الرقمي عام 1997.

التوقيع الرقمي هو توقيع إلكتروني يستخدم للتحقق من هوية المرسل / الموقّع للرسالة وأيضًا لضمان صحة المعلومات في المعاملات الإلكترونية، ويمكن أن يفي استخدام التوقيع الرقمي المعترف به بمتطلبات السرية ، ومصادقة الهوية، وعدم التنصل، وسلامة المعلومات.

دخل قانون التوقيع الرقمي لعام (DSA) حيز التنفيذ في 1 أكتوبر 1998، بهدف تنظيم استخدام التوقيع الرقمي في ماليزيا، ويضمن أمن القضايا القانونية المتعلقة بالمعاملات الإلكترونية ويتحقق من استخدام التوقيعات الرقمية من خلال الشهادات الصادره عن المرجع المصدق المرخص (CA).

تعتبر هيئة الاتصالات والوسائط المتعددة الماليزية (MCMC) مسؤولة عن إدارة وتنفيذ أحكام DSA 1997 لغرض المراقبة والإشراف على أنشطة CAs.

1- قانون الاتصالات والوسائط المتعددة عام 1998:

تم سنّ القانون في عام1 نوفمبر 1998 - كان بمثابة تشريع في عام 1997- وقد أجريت تعديلات المره الاولى في عام 2002 والمره الثانية في 1 يناير 2006.

ونص على إنشاء لجنة الاتصالات والوسائط المتعددة الماليزية مع صلاحيات الإشراف على الاتصالات والأنشطة المتعددة الوسائط في وتنظيمها، وتطبيق قوانين الاتصالات والوسائط المتعددة.

2- قانون حماية البيانات الشخصية عام 2010:

يهدف قانون حماية البيانات الشخصية الصادر في عام 2010 إلى ضمان عدم إساءة أستخدام أي بيانات شخصية يتم جمعها كما يفرض على الشركات الحصول على موافقة من الأفراد قبل جمع بيانتهم الشخصية أو مشاركة بيناتهم مع أطراف أخرى، فضلا القانون وضع شروط تسجيل لمستخدمي البيانات في صناعات معينة وإلا فإن ذلك قد يعرضهم لعقوبة جنائية بحد أقصى 500000 رينغيت ماليزي أو ما يصل إلى ثلاث سنوات في السجن، أو كليهما.

تحديات الأمن السيبراني في ماليزيا والتهديدات الدولية المتزايدة عبر الإنترنت

وفقاً لدراسة أجراها الاتحاد الدولي للاتصالات (ITU) تعد ماليزيا واحدة من أكبر عشر دول مستهدفة بهجمات البرامج الضارة على مستوى العالم.

شهدت ماليزيا خرقًا هائلاً للبيانات التي نشأت بسبب البرامج الخبيثة، وكان التأثير المالي ضخمًا بسبب اختراق البيانات. كما أن الوعي بالأمن السيبراني في ماليزيا لم يتم توصيله بشكل جيد لجميع المواطنين.

وفقاً لاحصائية قدمها فريق الاستجابة لحالات طوارئ الكمبيوتر، والذي يعمل في إطار Cyber Security Malaysia أن هناك من 2.7 مليون من هجمات الربوتات الآلية وهجمات عدوى البرامج الضارة بواسطة بروتوكولات الانترنت الفريدة IPS)(

كما كشفت إحصائيه أخرى أنه تم الإبلاغ عن أكثر من 9000 قضية تتعلق بالأمن السيبراني في ماليزيا، مثل المضايقات الإلكترونية والاحتيال والتطفل والرموز الخبيثة ورفض الخدمة والمحتوى المرتبط بالبريد العشوائي.

تزايدت حوادث الجرائم الإلكترونية بمعدل ينذر بالخطر في ماليزيا ومنطقة جنوب شرق آسيا حيث شهدت المنظمات المزيد من الهجمات الإلكترونية، حيث يستغل مجرمو الإنترنت في ماليزيا الخوف وعدم اليقين المحيطين بتفشي فيروس كورونا.

تم اكتشاف 20 برنامجًا ضارًا مختلفًا مرتبطًا بفيروس كورونا من قبل متخصصي الأمن السيبرانيKaspersky، وذكرت مجلة Forbesأن ماليزيا هي واحدة من أكثر خمس دول في العالم مستهدفة من قبل مجرمي الإنترنت أثناء تفشي المرض واصبح معدل الهجمات الإلكترونية في تزايد عن زي قبل.

وكشفت شركة Microsoft في دراسة أجريت عام 2018 أن ماليزيا قد عانت من خسائر اقتصادية بلغت 12.2 مليار دولار أمريكي بسبب الجرائم السيبرانية

واكتشفت شركة Technisanct الناشئة للأمن السيبراني أن أكثر من 35000 بطاقة ائتمان من عدد من البنوك قد تم اختراقها في ماليزيا وتم بيعها على شبكة الإنترنت.

وقد اطلقت أحدى الشركات التكنولوجية حلاً أطلق Linkdood منصة اتصالات صممها خبراء الأمن السيبراني لتمكين الموظفين من تخزين الملفات والتعاون بأمان باستخدام تقنية السحابة الخاصة.

أطلقت LGMS، وهي شركة محلية للأمن السيبراني ، مختبرًا للأمن السيبراني مع مزود الخدمة النمساوي TÜV Austria

قال سفير النمسا في ماليزيا الدكتور مايكل بوستل: "هذه الشراكة لديها القدرة على ترسيخ ماليزيا كمركز لاختبار واعتماد الأمن السيبراني لمنطقة آسيا والمحيط الهادئ."

وقد حققت شركة البيانات الماليزية Strateq أيضًا نجاحًا مؤخرًا عندما أعلنت شركة الاتصالات السنغافورية StarHub أنها ستدفع ما يصل إلى 82 مليون دولار سنغافوري مقابل حصة تبلغ 88٪ في الشركة.

وتعمل ماليزيا على إنشاء نظام دفاع إلكتروني متطور اكتمل الآن بنسبة 90٪ بعد ثلاث سنوات من العمل، وإذا سار العمل وفقًا للخطة ، فستكون ماليزيا في طريقها لتصبح واحدة من أفضل القدرات في المنطقة.

وقد وقعت منظمة Cyber Security Malaysiaالمرتبطة بالحكومة أيضًا اتفاقية مع Blackberry لحماية بعض البيانات الأكثر أهمية وحساسية في ماليزيا من مجرمي الإنترنت.

تظهر ماليزيا بوادر تحسن في الحرب ضد مجرمي الإنترنت وجدت دراسة حديثة أجرتها شركة Cisco أن الشركات في ماليزيا تلقت تنبيهات إلكترونية أقل بنسبة 3٪ في عام 2019 مقارنة بعام 2018 ، وهو أفضل من المتوسط في منطقة آسيا والمحيط الهادئ. وذكرت الدراسة أيضًا أن الانتهاكات التي تكلف الشركات مليون دولار أمريكي أو أكثر انخفضت من 50٪ في 2018 إلى 23٪ فقط في 2019.

لكن المعركة لم تنته بعد. ما زال أمام ماليزيا ومنطقة آسيا والمحيط الهادئ طريق طويل لتقطعه، ولا تزال المنطقة تتلقى المزيد من التنبيهات على أساس يومي أكثر من المناطق الأخرى التي شملتها الدراسة التي أجرتها شركة Cisco .

بينما شهد عدد التنبيهات التي تم التحقيق فيها أيضًا انخفاضًا في جميع أنحاء المنطقة منذ عام 2018.

وضعت الدولة للمستهلكين والعملاء ومستخدمي الإنترنت عدد من الطرق التي يمكن من خلالها المساعدة في منع الجرائم الإلكترونية منها:لابد من استخدام كلمة مرور مختلفة لكل حساب، تجنب الوصول إلى المعلومات الحساسة وحفظ التفاصيل الخاصة بك عند استخدام شبكة WiFi العامة، قراءة رسائل البريد الإلكتروني بعناية لتجنب هجمات التصيد الاحتيالي، لابد من مراجعة عناوين مواقع الويب والتحقق مما إذا كانت آمنة.

أهم الاستراتيجيات والسياسات التي تَبَنَّتْها الدولة لمكافحة الإرهاب السيبراني

تعد ماليزيا أكثر دول جنوب شرق اسيا تقدما في استراتيجية الأمن السيبراني وإن ريادة ماليزيا في هذا المجال تنبثق من تأسيس وكالة وطنية لتعزيز وتنسيق جدول أعمال الأمن السيبراني وصياغة القوانين والخطة الشاملة لتنمية المهنيين في المجال نفسه.

الهجمات السيبرانية العابرة للحدود تفتح مجالا لهذه البلاد للتعاون مع خبراء الأمن السيبراني وصانعي السياسة ورواد الأعمال وصناع القرار التجاري في هذه المنطقة من أجل تعزيز مرونة الآسيان.

منذ التسعينات والدولة الماليزية تحاول تكييف سياساتها لتستجيب للتهديدات الجديدة المرافقة للبيئة الرقمية، ووسعت دائرة التعاون مع القطاع الخاص، فضلاً عن أنها وضعت عددا مهما من التنظيمات القانونية لتعزيز أمنها السيبراني.

ولحماية الحكومة والشركات من أي الهجمات السيبرانية تنفذ وزارة الدفاع الماليزية السياسة الأمنية لتكنولوجيا المعلومات، من بين مهامها ضمان سلامة الشبكات ومنع الحوادث الإلكترونية من إحداث آثار اقتصادية ضارة.

في عام 2006 أعلنت ماليزيا إطلاق مبادرة تحت مسمى " الشراكة الدولية متعددة الأطراف لمكافحة الإرهاب الالكتروني IMPACT، وقد تضمن تلك المبادرة انشاء أربعة مراكز وهي: مركز تنمية المهارات والتدريب، مركز لشهادات الامن والبحث والتنمية، مركز دعم التعاون الدولي، مركز الاستجابة والطوارئ الدولية.

لمكافحة الارهاب السيبراني تم إنشاء العديد من مواقع الانترنت بمبادرة من الحكومة او القطاع الخاص أو مؤسسات المجتمع المدني فضلا عن مواقع الشركات العاملة في تكنولوجيا الاتصال والمعلومات، وأصبحت بمثابة مؤسسات فكرية لدعم الأمن الرقمي.

وضعت وزارة الاتصالات والوسائط المتعددة استراتيجية 2019- 2023تركزعلى تعزيز أمن الفضاء الإلكتروني في البلاد وزيادة الوعي العام بالاستخدام الحكيم والأخلاقي للأجهزة الرقمية.

وفي 2020 اطلقت ماليزيا مشروع تجريبي لأمن الانترنت والنهوض بالمهارات في مجال الأمن الالكتروني والصناعة، ويعزز من كفاءة ممارسي الأمن الإلكتروني الحاليين، ويساهم في رعاية جيل جديد من المتخصصين الموثوق بهم في مجال الأمن الإلكتروني وبالتالي يعزز القدرة التنافسية في الدفاع عن الفضاء الإلكتروني الوطني".

وفي سعي الدولة لتعزيز التأهب الوطني للأمن السيبراني تم تكليف وزارة الاتصالات والوسائط المتعددة والوكالة الوطنية للأمن السيبراني بمهمة صياغة خطة العمل متوسطة الأجل، فضلًا عن تنفيذها وتنسيقها.

مبادرات الحكومة الماليزية في مكافحة الجرائم السيبرانية:

تحت إشراف وزارة الوسائط المتعددة والاتصالات (MCMC) ، تم تأسيس CyberSecurity Malaysia باعتبارها وكالة متخصصة في الأمن السيبراني لتقديم مجموعة واسعة من الخدمات وتعزيز اعتماد ماليزيا على ذاتها في الفضاء الإلكتروني.

وتقوم المنظمة بمساعدة وكالات إنفاذ الطب الشرعي والتحليل السيبراني، مثل تحليل الأدلة وتوفير خبراء لقضايا الجرائم الإلكترونية، فضلا عن ترسيخ ثقافة الأمن من خلال برامج التوعية.

إلى جانب CyberSecurity Malaysia ، هناك أيضًا العديد من المنظمات الفرعية والخدمات المقدمة لتلبية حاجة ماليزيا المتزايدة للأمن عبر الإنترنت.

وبالرغم من أن المعلومات حول الارهابيين السيبرانيين تعتبر في الغالب معلومات سرية ولا يمكن الكشف عنها بسهولة إلا أنه يمكننا أستنتاج وجود هذا النوع من التهديد في ماليزيا وذلك من خلال بعض الاحداث التي وقعت وأربكت الحكومة الماليزية.

وقد جاءت تلك الهجمات بعد تحذير جماعة أطلقت على نفسها " المجهول Anonymous، والتي قالت أنها ستهاجم البوابات الرئيسية للحكومة لمعاقبتها على فرض رقابة على موقع ويكيليكس الذي يقوم بتسريب الوثائق السرية للشركات متعددة الجنسيات والحكومات.

ومن أهم الانشطة السيبرانية كانت نشاطات حركة "التنظيف Persih"، والتي تبنت أستخدام وسائل الإعلام الرقمية منذ أن تأسست في 23 نوفمبر 2006 ، وخلال السنوات التالية شهدت عملياتها في الوسائط الرقمية تطورا كبيرا.

فقد جعلت هذه الحركة من استخدام المواقع والمدونات واليوتيوب أدوات رئيسية للتداول والتعبئة مع استخدامات متقطعة لـ Flickr.

وقد كان التدوين خياراً طبيعاً أضافة إلى إدماج يوتيوب وفليكر في عام 2006، والفيسبوك في 2008، وتويتر في 2011، الذي لم يكن مفاجئا في ظل شعبية هذه المنصات بين الماليزيين وخاصة الشباب.

في عام 2011 نظمت حركة Persh، حمله احتجاجية من أجل الإصلاح الديمقراطي في ماليزيا وأستخدمت فيها بشكل واسع الهواتف الذكية وشبكات التواصل الاجتماعي.

هناك العديد من السياسات والبرامج التي وضعتها الحكومة الماليزية للتصدي للارهاب السيبراني نذكر منها ما يلي:

1. **السياسة الوطنية للأمن السيبراني (NCSP):**

اتخذت الحكومة مبادرات للتخفيف من الهجمات الإلكترونية ومكافحتها. إحدى المبادرات التي تم اتخاذها هي تطوير السياسة الوطنية للأمن السيبراني (NCSP)، والتي أقرتها الحكومة في مايو 2006.

وهي عباره عن تطبيق مالي شامل للأمن السيبراني يتم تنفيذه بطريقة متكاملة لضمان حماية البنيه التحتية الوطنية Critical National Information Infrastructure (CNII) إلى مستوى يتناسب مع المخاطر التي تواجهها، عبر الأجهزة الحكومية، واجتذب التنفيذ العديد من الوزارات والوكالات للعمل معًا لتلبية رؤية وجود CNII مضمون ومرن ومعتمد على الذات من شأنه في النهاية تعزيز الاستقرار والرفاهية الاجتماعية وخلق الثروة للبلد.

يتكون برنامج NCSP من ثمانية (8) توجهات سياسية وهي:

- **الحوكمة الفعالة.**
- **الإطار التشريعي والتنظيمي.**
- **إطار تكنولوجيا الأمن السيبراني.**
- **ثقافة الأمن وبناء القدرات.**
- **البحث والتطوير نحو الاعتماد على الذات.**
- **الامتثال والتنفيذ.**
- **الجاهزية للطوارئ الأمنية السيبرانية والتعاون الدولي.**

وبعد 4 سنوات من تنفيذ برنامج NCSP ، يُنظر الآن إلى الأمن السيبراني في ماليزيا على أنه شيء لا يستهان به، حيث تم إنجاز الكثير ولا يزال يتعين القيام بالمزيد مع تغير مشهد التهديدات السيبرانية مع تطور التقنيات والأدوات الجديدة.

2. **البنية التحتية الوطنية الحرجة للمعلومات.**

تُعرَّف البنية التحتية للمعلومات الوطنية الحاسمة (CNII) بأنها تلك الأصول (الحقيقية والافتراضية) والأنظمة والوظائف الحيوية للدول التي سيكون لعجزها أو تدميرها تأثير على القوة الاقتصادية الوطنية، الدفاع والأمن القومي، وقدرة الحكومة على العمل بكفاءة، الصحة العامة والسلامة.

- **برنامج الامن السيبراني الماليزي:**

تم تصميم CyberSecurityMalaysia ، وهو برنامج تابع لوزارة العلوم والتكنولوجيا والابتكار الماليزية، لتكون قادرة على التخفيف من التهديدات السيبرانية.

لهذا السبب، تسعى CyberSecurity Malaysia إلى إقامة شراكات وتعزيز جهود التعاون مع الدول والمنظمات الدولية.

تحاول ماليزيا إنشاء منصات متعددة الأطراف للأمن السيبراني مثل مركز آسيا والمحيط الهادئ (APCERT) ومنظمة التعاون الإسلامي (OIC-CERT)، من أجل التخفيف من التهديدات السيبرانية الدولية.

برنامج التوعية المعروف باسم CyberSAFE - Cyber Security Awareness For Everyone ، هو مبادرة CyberSecurity Malaysia لتثقيف وتعزيز وعي الجمهور بالمسائل التكنولوجية والاجتماعية التي تواجه مستخدمي الإنترنت، ولا سيما بشأن مخاطر الاتصال بالإنترنت. CyberSAFE في المدارس. فضلا عن أن البرنامج يهدف إلى الوصول إلى جيل الشباب في المدارس لآنها تضم الجزء الأكبر من مستخدمي الإنترنت.

3. الحضيرة الماليزية لتكنولوجيا الدفاع Malaysia Defence Technology Park MDSTP

تعتبر الحضيرة الاولى من نوعها في منطقة الاسيان -وفق تصريح لوزير الدفاع الماليزي Zahid Hamide- لتلبية الطلب واحتياجات الصناعة الدفاعية وألامنية المتزايدة، وتهدف إلى تحقيق مجموعة من الاهداف لعل أهمها يتمثل في:

- دفع ماليزيا إلى اقتصاد قائم على الابتكار، وذلك من خلال استضافة المركز الأكثر تقدمًا وتكاملاً للبحث والتطوير، وإنتاج منتجات مبتكرة ذات صلة بصناعة الدفاع.
- تسهيل أنشطة البحث والتطوير الدفاعي والابتكار والتسويق من خلال توفير البنية التحتية والمعدات والمرافق المتطورة.
- تعزيز تطوير بيئة مواتية لتقنيات ومنتجات الدفاع الفكرية والإبداعية والمبتكرة.
- تسهيل الشراكات الذكية بين الحكومة والقطاع الخاص في تطوير تكنولوجيا الدفاع وتسويق نتائج البحوث.
- إعداد مزودي صناعة الدفاع المحليين للمشاركة في مناقصة العقود العالمية.
- تمكين مزود الصناعات الدفاعية المحلي والدولي من تصنيع منتجات للسوق المحلي والإقليمي والعالمي.

4. فريق الاستجابة لطوارئ الكمبيوتر الماليزي MYCERT

يعد فريق الاستجابة للطوارئ الحاسوبية في ماليزيا ('MyCERT') ذراع الاستجابة للأمن السيبراني في ماليزيا، لتوفير نقطة اتصال لمستخدمي الإنترنت المتأثرين بالحوادث المتعلقة بالأمن.

مركز المساعدة Cyber999

تتوفر خبرة الاستجابة للطوارئ مساعدة الجمهور الماليزي على اكتشاف وتفسير والاستجابة لحوادث أمن الكمبيوتر مثل المضايقات الإلكترونية والبرامج الضارة والهجمات المستهدفة.

CyberCSI

خدمات الطب الشرعي الرقمي ذات النطاق الكامل، والتدريب والشهادات ، بالإضافة إلى استعادة البيانات، وتعقيم البيانات، وخدمات التقاضي للحكومة ووكالات إنفاذ القانون والمنظمات الخاصة.

Cyber DEF

الكشف عن التهديدات والقضاء على التهديدات وتحليل الأدلة الجنائية المخصص لتأمين البنى التحتية الوطنية للأمن السيبراني.

وفي عام 2015 أنشأت القوات المسلحة الماليزية وحدة دفاع الكتروني لحماية المعلومات السرية المتعلقة بنظام الدفاع من التسريب أو الاختراق. وتراقب هذه الوحدة عن كسب الأنشطة الإلكترونية التي تشكل تهديداً محتملاً لنظام الدفاع في البلاد.

كما أنها تعمل أيضا من أجل تعزيز نظام الدفاع السيبراني وإجراء عمليات تدقيق الموقف الأمني بالأضافه إلى الطب الشرعي الالكتروني.

تخضع وحدة الدفاع السيبراني لسلطة شعبة استخبارات أركان الدفاع *، وهي وكالة المخابرات العسكرية التابعة للقوات المسلحة.

تهدف الوكالة إلى عولمة الأمن السيبراني، وتوسيع المبادرات من خلال التعاون الثنائي والمتعدد الأطراف مع الوكالات المحلية والدولية وذلك لتعزيز استراتيجيات الأمن السيبراني للدولة.

على الرغم من الجهود التى تبذلها الدولة الماليزية في مكافحة الارهاب السيبراني إلا أن هناك العديد من التحديات التي تواجه الدوله في مكافحة استخدام تكنولوجيات المعلومات والاتصالات للأغراض الإجرامية لعل من أهمها:

نقص الموارد البشرية لدى وكالات إنفاذ القانون يشكل تحدِّياً تواجهه السلطات الوطنية، اذ انبعض وكالات إنفاذ القانون في ماليزيا لا يوجد لديها فريق مكرس للتركيز على التحقيقات في الجرائم السيبرانية.

حاجة الدولة إلى رفع مستوى مهارات وكفاءات القضاة والمدعين العامين وتعزيز معارفهم بشأن أساسيات تكنولوجيات المعلومات والاتصالات والأمن السيبراني، بما في ذلك معرفة المصطلحات المتعلقة بالنظم الحاسوبية والشبكات.

على أجهزة إنفاذ القانون الحصول على الأدلة الرقمية عبر الحدود من خلال قناة رسمية، وهي المساعدة القانونية المتبادلة، لكي تكون الأدلة مقبولة في المحكمة. وقد يستغرق تلقي الردود من خلال هذه المساعدة وقتاً طويلاً للغاية، مما قد يطيل إجراءات المحكمة. وبالإضافة إلى ذلك، لا تزال طلبات الحصول على الأدلة خارج الولاية القضائية تخضع لمسألة ازدواجية التجريم.

أن الشركات الماليزية الصغيرة والمتوسطة من المحتمل أن يكون 33% منها عرضة للهجمات الإلكترونية ويرجع السبب في ذلك إلى عدم وعيهم بأمن المعلومات مما يؤدي إلى إدارة عشوائية لمعلوماتهم وأصولهم الرقمية.

ماليزيا بحاجة إلى تطوير نظام بيئي وطني للابتكار في مجال الأمن السيبراني للاستجابة للتهديدات السيبرانية المتزايدة التعقيد

الوحدة الخامسة : قواعد الأمن السيبراني في المؤسسات

الأهداف التفصيلية للوحدة :

أن يكون المتدرب في نهاية الوحدة قادرا على:

يوضح الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات

يتعرف علي مهددات المن السيبراني في المؤسسات الصناعية والحيوية

يبين مدي خطورة الهجمات الموجهة لنظم المعلومات

يتعرف علي قواعد الاستخدام الآمن لنظم المعلومات في المؤسسات

تشمل الوحدة على المواضيع الفرعية التالية "

1- الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات

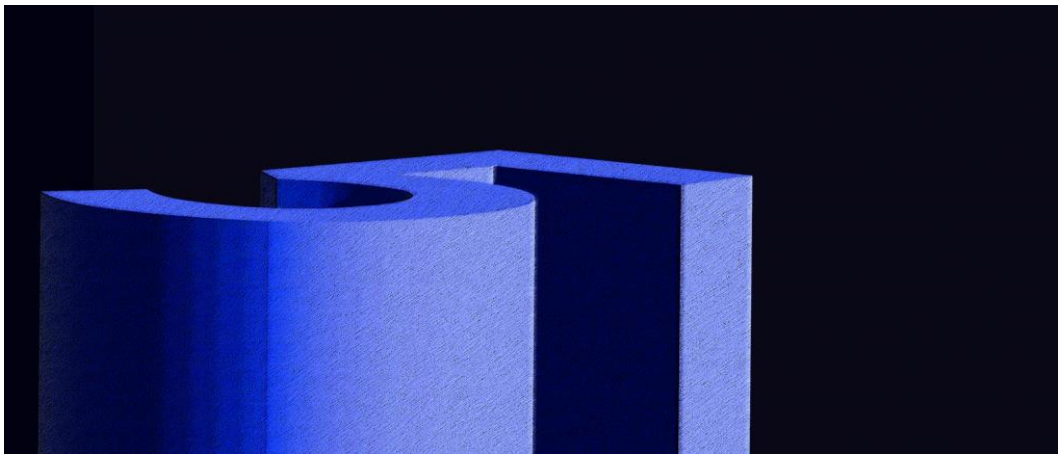
2- مهددات الأمن السيبراني في المؤسسات الصناعية والحيوية

3- الحروب السيبرانية والهجمات الموجهة لنظم المعلومات

4- قواعد الاستخدام الآمن لنظم المعلومات في المؤسسات

الدرس الأول / الأصول الفنية للتعامل مع نظم المعلومات في المؤسسات

ما أهمية نظم المعلومات للمنظمات؟ وماهي مكوناتها الخمس؟



نظم المعلومات الإدارية(Management Information System)

تلك الوسائط التي تتعامل وتحكم التدفق المستمر للبيانات لدى منظمة ما بين إداراتها وأقسامها الداخلية والخارجية، ويعد اتساق الإدارة التنظيمية والمالية مع توفر البيانات ونظم المعلومات الفعالة بمثابة خارطة الطريق لتحقيق النجاح للمنظمات بنسبة كبيرة، وربما ندرك أهمية ودور نظم المعلومات إذا كان لدينا بعض المهام المكلفين بإنجازها وفجأة حدثت مشكلة توقف النظام (System Failure)كما يشيع وصفها في أوساطنا العربية، والتي ينتج عنها تباطؤ في سير العمل بشكل بالغ وربما توقفه في بعض الأحيان بشكل كامل، مما قد يؤثر على جودة وكفاءة الخدمة المقدمة حال عدم وجود حلول بديلة.

أهمية نظم المعلومات للمنظمات

تمثل نظم المعلومات للمنظمات أهمية بالغة، حيث تعمل تلك الأنظمة على معالجة البيانات وتوفيرها بشكل سريع دون المساس بالدقة والموثوقية في نتائجها، كما تضمن تحقيق هدفين أساسيين هما تقليل الأخطاء البشرية وزيادة كفاءة العمل عبر تنظيم البيانات وتخزين المعلومات، وتحليل العمليات لتوقع المكانة المستقبلية للمنظمة بين المنافسين، والتي لن تتمكن أي إدارة من التعرف عليها دون وجود نظام معلومات شامل منسق وجيد التصميم.

وتُمكن نظم المعلومات من متابعة اتجاه سير العمل وإحراز التقدم المستهدف في عمل المنظمة بوجه عام أو في معدلات تقدم العمليات والمهام بشكل تفصيلي مع التنبؤ بالفرص والمعوقات المستقبلية، كما توفر الوقت والجهد وتُسهل الاحتفاظ بالبيانات رقميًا وتصنيفها حسب التاريخ والنوع بدلًا من الطرق التقليدية المهدرة للوقت مثل السجلات والتدوين اليدوي، والتي قد تُعرض بعض البيانات الهامة للفقد أو صعوبة الوصول إليها والمراجعة والأرشفة، ويمكن من خلال قواعد البيانات المتطورة بتلك الأنظمة الوصول إلى ما تحتاجه الأطراف المشتركة والمسموح لها بالتعامل مع معلومات المنظمات.

وتساهم نظم المعلومات في تجنب الأزمات التي قد تواجهها المنظمة، خاصة فيما يخص أسواق الأسهم على سبيل المثال، والتي تتيح نظم المعلومات الإدارية لها متابعة ورصد توقعات صعود وهبوط الأسهم والاطلاع على أدائها السابق، ومعدلات الأرباح والخسائر، وبالتالي يمكن اعتبار "نظام المعلومات" نوع من الاستثمار أو أحد الحلول الداعمة لمواجهة المخاطر المحتملة التي قد تواجه المنظمات وتهدد استقرارها ومركزها المالي وقيمتها السوقية .

وتسهل الخصائص والتمكين من البيانات التي توفرها نظم المعلومات من عملية اتخاذ القرار بسهولة ودقة في المواقف التي تتطلب حلولًا عاجلة، وهو ما يدعم تلك العملية التي تعد أحد شقي معادلة النجاح التي تتمثل في الخطط الاستراتيجية و جودة القرارات المتخذة من قبل إدارة المنظمة، كما تساهم نظم المعلومات في دعم وضع الرؤى والخطوات المقبلة في مستقبل المنظمات المهني.

وتساعد نظم المعلومات الإدارية (MIS) بصفة خاصة في تحسين المكانة السوقية والقدرة التنظيمية لأي شركة أو جهة، وذلك عبر استخدام الأساليب التحليلية للتعرف على وجمع المعلومات حول المنافسين، والتخطيط وقياس مدى التقدم في الوصول إلى النتائج المستهدفة، وتشترط نظم المعلومات لضمان استقرارها توفر فريق جيد من التقنيين المتخصصين لمتابعة سير النظم وثباتها والتصدي لأي معوقات قد تعرقل عملها بكفاءة.

وتتعامل المنظمات التي تعتمد نظم المعلومات المستقرة في عملها بشكل أساسي على اعتبارها بمثابة شريان سير البيانات داخلها الذي يمثل توقفه تهديدًا لدورة العمل وربما كيان المنظمة بالكامل.

مكونات نظم المعلومات

تشمل مكونات نظم المعلومات باقة متكاملة من الأجهزة والتجهيزات والبرمجيات وشبكات الاتصالات السلكية واللاسلكية، والتي تعمل كمنظومة متكاملة للوصول إلى جمع وإنشاء وتوزيع البيانات وضبط تدفق المعلومات داخل النظام في المنظمة .

وتضم نظم المعلومات 5 مكونات أساسية هي:

1. أجهزة الحاسب الآلي

وهي تعد المكون المادي الأساسي لنظم المعلومات وتختلف خصائصها حسب طبيعة المنظمة ونشاطها، وتعمل أجهزة الحاسب الآلي ومكوناتها على تولي تلقى وتنفيذ المهام عبر الإجراءات التي تتيحها المنظمة.

2. برامج وتطبيقات الحاسب الآلي

يمكن تقسيم البرامج بوجه عام إلى 3 أنواع وهي برامج النظام، تطبيقات البرمجيات، والإجراءات، وتختلف عنها البرامج والنظم الخاصة بالمعلومات لدى المنظمات في تنفيذ مهام التحليل ومعالجة البيانات والمعلومات التي تختلف حسب طبيعة عمل المنظمة.

3. قواعد البيانات

هي برامج تستخدم في تنظيم وخدمة البيانات الخاصة بالمستخدم وإدارتها وتخزينها من الموارد الافتراضية للبيانات، وتشمل البيانات المادة الخام من الحقائق والأرقام غير المنظمة التي يتم معالجتها في وقت لاحق لإنتاج المعلومات، وتتيح إدارة البيانات باستخدام نظام إدارة قواعد البيانات تحقيق كفاءة الوصول .

يشمل مفهوم الشبكات بشكل موسع شبكات الاتصالات مثل الشبكة الداخلية، الخارجية وشبكة الإنترنت، والتي تعمل جميعها على تسهيل تدفق البيانات في المنظمة، وتشمل مكوناتها كروت الشبكات والكابلات والبرامج وأجهزة نقاط الاتصال وخوادم البيانات والتطبيقات، كما تشمل وسائل الاتصال و دعم الشبكة.

4. الموارد البشرية

تتكامل الموارد البشرية مع الأنظمة، حيث توفر القوى العاملة المطلوبة لتشغيل وإدارة النظام، ويعد الناس هم المستفيد النهائي من نظم المعلومات لتحقيق مطالبهم ومهامهم سواء الخاصة أو العملية، ويمكن اعتبار أن مفهوم "الناس" يمثل المستخدم النهائي الذي يمكن أن يكون مشغل الكمبيوتر والمبرمج، مهندس، بائع، محاسب، مدير، وربما العميل العادي.

كيف تحسن نظم المعلومات في مؤسستك؟

هناك العديد من التطبيقات التي يمكن أن تساعد مؤسستك على إدارة البيانات بطريقة فعالة. إليك بعض النصائح في هذا الخصوص:

إنشاء خطة تقنية شاملة

يجب أن تتناول هذه الخطة طرق الاستبدال المنهجية لتقييم التقنيات الناشئة، حيث يجب أن يوفر خريطة لكيفية عمل نظام المعلومات الخاص بك في الوقت الحالي وفي المستقبل، مع الأخذ في الاعتبار الطبيعة المتغيرة بسرعة للصناعة.

استشارة الخبراء

استشر إحدى الشركات التي توفر وحدات التخزين الاحتياطي خارج الموقع لمستنداتها وقواعد بياناتها الرئيسية. عادةً ما تكون هذه الخدمة سهلة التثبيت وتوفر لك استردادًا سهلاً في حالة الكوارث إذا كنت تعاني من مشكلة كبيرة في النظام.

البرمجيات كخيارات خدمة للوظائف

توفر هذه الخدمة إصدارات تستند إلى الويب للحلول التي تقوم بتثبيتها عادةً على كل محطة عمل، وتجعل هذه الخدمة البيانات متاحة بشكل أكبر في جميع أنحاء متجرك وفي منزلك. استخدم البرامج المجانية لتقليل ميزانيتك لترقية الأجهزة بشكل أسرع.

يعرف العديد من أصحاب الأعمال أن التكنولوجيا يجب أن تكون على رأس أولوياتهم لتعزيز عملياتهم وزيادة الإيرادات وتأمين مستقبلهم. سيؤدي امتلاك أنظمة المعلومات الخاصة بك ودمجها مع أنظمة أخرى مثل CRMو PIMو ERPإلى تحسين كفاءتك وضمان فهم أفضل للأعمال وقدرتها على الأداء في مواجهة المواقف الأكثر صعوبة.

الدرس الثاني / مهددات الأمن السيبراني في المؤسسات الصناعية والحيوية

أدى التطور السريع للتقنية في السنوات الأخيرة إلى اعتبار هذه النهضة بأنها حقبة جديدة للتقدم الصناعي، ويُشار إلى هذه الحقبة بالثورة الصناعية الرابعة، والتي ترتبط فيها الآلات مع البشر في منظومةٍ رقميةٍ متكاملةٍ تولّد البيانات وتحللها وتنقلها بكل سلاسةٍ، وتتميز فيها الآلات بقدرتها على اتخاذ القرارات بنفسها بناءً على تلك البيانات دون الحاجة إلى أي تدخلٍ بشريٍّ، وذلك باستخدام التقنيات المتقدمة كإنترنت الأشياء (IoT) والذكاء الاصطناعي (AI) والحوسبة السحابية في عمليات التصنيع.

ورغم توقع أن تحدث هذه التقنيات طفرة في المجال الصناعي كما أحدثه المحرك البخاري قبل نحو قرنين، إذ أنها أدت إلى تحسيناتٍ كبيرةٍ في الكفاءة والإنتاجية والربحية، إلا أنها تطرح أيضاً تحدياتٍ أمنيةً جديدةً تتعلق بأمن البيانات الحساسة وتعرضها للتسريب أو الاختراق، نظراً للكم الهائل من الأجهزة المرتبطة بالإنترنت. ولهذا، يعد تبني تقنيات الأمن السيبراني عاملاً مهماً لنجاح واستدامة أعمال المنشآت التجارية، نظراً لكون القطاع الصناعي مجالاً خصباً للهجمات ومحاولات سرقة البيانات.

أبرز التحديات التي تواجه الأمن السيبراني للصناعة

يزداد تعقيد النظام بزيادة عدد الأجهزة والنظم الأخرى المرتبطة به. ومع هذا التعقيد، تكثر نقاط الضعف الأمنية التي يعاني منها هذا النظام. وفيما يلي أبرز المخاطر التي تتعرض لها المنشآت عند تبني تقنيات الثورة الصناعية :

- الحرمان من الخدمة: يمكن أن تُحجب الخدمات السحابية التي تقدمها بعض الأنظمة بسبب الطلب الكبير عليها والضغط الكبير على الخادم، وهو ما قد يؤدي إلى تعطلها وتلفها، ما يكلف الجهة الكثير من الوقت والمال والفرص الضائعة لإصلاحه.

- عدم توفر معيار موحد: تتطلب تقنيات الصناعة 4.0 تكامل أنظمةٍ وتقنياتٍ مختلفةً، والتي تأتي غالباً من بائعين ومزودي خدمة مختلفين. ويمكن أن يؤدي عدم وجود معيارٍ موحدٍ للبروتوكولات الأمنية إلى صعوبة بالغة في إدارة هذه الأنظمة وتأمينها بشكلٍ فعال.

- الأخطاء البشرية: فعلى الرغم من استخدام التقنيات المتقدمة، يظل البشر جزءاً لا يتجزأ من أنظمة الصناعة 4.0، فقد يقوم أحد الموظفين عن غير قصدٍ بخرق أنظمة الأمن عن طريق تنزيل برامج ضارة أو عدم اتباع البروتوكولات الأمنية التي وضعتها الجهة المختصة.

- التجسس السيبراني: هناك العديد من الشركات والمؤسسات والهيئات الحكومية التي تعمل في نطاق حساسٍ، ما يحفز المخربين على التنافس أو التعاون فيما بينهم لسرقة وتسريب البيانات المهمة وسرقة الملكية الفكرية.

● الحوادث والهجمات السيبرانية: تشكل الهجمات الإلكترونية وتفشي الفيروسات والبرامج الضارة أكبر تهديد متزايد يهدد أنظمة الصناعة 4.0، حيث تزايدت الهجمات بنسبة ٢٤٠٪ بالمقارنة مع عام ٢٠١١م.

يمكن للمهاجمين استغلال الثغرات الأمنية في أجهزة إنترنت الأشياء والشبكات وبرامج الوصول إلى الأنظمة غير المصرح بها وسرقة البيانات وتعطيل العمليات، وتعاني الشركات التي تتعرض للهجمات السيبرانية من أضرارٍ تلحق بعمليات الإنتاج وهو ما يكلفها الكثير من المال. حيث تقدر خسائر قطاع الأعمال في ولاية كاليفورنيا بـ٢٥٠ مليار دولارٍ سنوياً، وتعد الشركات الصغيرة والمتوسطة أكبر المتضررين من هذه الهجمات نظراً لعدم قدرتها على تحمل الخسائر المالية التي تلحق بها. وبالإضافة إلى ذلك، لا تأخذ الكثير من الشركات الصغيرة والمتوسطة تدابير الأمن السيبراني بعين الاعتبار، ظناً منهم أن المهاجمون السيبرانيون ينظرون نحو كبرى الشركات ولا يهتمون بالشركات الناشئة. إذ أظهرت إحدى الدراسات أن الرد الأكثر شيوعاً الذي يقدمه من يدير البنية التحتية لشبكة الشركة هو: "لسنا ناسا أو بنكاً"، وهو ما يتعارض مع طبيعة الهجمات التي لا تستبعد أي شركة.

الحلول التي يقدمها الأمن السيبراني لقطاع الصناعة

بالرغم من المخاطر التي تتعرض لها المنشآت التجارية باستمرار، إلا القليل من الشركات لديها وعي بأهمية الأمن السيبراني لحماية الأجهزة المتصلة بالشبكة، فمعظم المنشآت لا تؤسس لأنظمة الحماية بالشكل الصحيح إلا بعد هجوم المخربين، ما يتسبب بالكثير من الأضرار وتعطل الإنتاج وفقدان أو ترسب البيانات. إذ تظهر الإحصائيات أن ٧٥٪ من المنشآت معرضة للهجوم السيبراني لأكثر من مرة، ولهذا فإن من الضروري أن تعي المنشآت أهمية بناء بنية تحتية قوية، وأن تدرك حجم المشاكل التي ستواجهها حال تعرضها للهجمات. ومن بين الإجراءات التي يمكن للمنشآت اتخاذها:

● الاستثمار: بحيث يكون الاستثمار استباقياً لا تفاعلياً، عبر توظيف المنشآت للأفراد ذوي الكفاءة والخبرة العالية، وإعداد الأنظمة لمنع الحوادث. فبعكس الاستثمار التفاعلي الذي يأتي كاستجابة متأخرة للتهديدات، فإن الاستثمار الاستباقي يعمل على صد الهجمات قبل حدوثها، ما يقلل من التكلفة التي تلحق بالمنشآت.

● تجزئة الشبكة: تتمثل إحدى الطرق الفعالة لتحسين أمن أنظمة الصناعة 4.0 في تجزئة الشبكة، حيث يشمل ذلك تقسيم الشبكة إلى أجزاءٍ أصغر، ولكلّ منها بروتوكولات أمنٍ خاصةٍ بها وضوابط للوصول، ويمكن أن يساعد ذلك في احتواء أي انتهاكات أمنية ومنع المخربين من اختراق الشبكة.

● استخدام التشفير: يمكن استخدام التشفير لحماية البيانات أثناء نقلها أو تخزينها، ويتضمن ذلك تشفير البيانات بحيث لا يمكن قراءتها إلا باستخدام مفتاحٍ خاصٍ للوصول، بحيث لن يتمكن المهاجم من قراءة البيانات حتى لو تمكن من الوصول إليها.

● تدريب الموظفين وتوعيتهم: غالباً ما يكون الموظفون هم الحلقة الأضعف في أمن أنظمة وبرامج الصناعة 4.0. إلا أنه عن طريق تقديم برامج التدريب والتوعية في تثقيف الموظفين حول أهمية الأمن السيبراني، ومخاطر التصيد الاحتيالي والهجمات الإلكترونية، أن تحافظ على سلامة وأمن الأنظمة.

● اتخاذ معيار موحد لأمن البيانات: نظراً لطبيعة أنظمة الصناعة 4.0 المعقدة وغير المتجانسة، فإن إدارة البيانات وتخزينها قد يؤدي إلى ضعف حمايتها وإمكانية تعرضها للمخاطر. لذا من المهم تبني معيارٍ موحدٍ لحماية المعلومات التي تخص الشركة وإدارتها بشكلٍ فعال. ويعد معيار IEC 62443 الدولي للأمن السيبراني هو المعيار الدفاعي الأفضل الذي يمكن تنفيذه في القطاع الصناعي، رغم كونه معروفاً لدى القليل من الشركات. حيث يغطي هذا المعيار جميع المراحل والخطوات التي تمر بها عمليات إجراء الأمن السيبراني، والتي تتضمن مرحلة التقييم لتحليل أي ثغرة أمنية، بالإضافة إلى التنفيذ والصيانة اللاحقة لأداء السلامة ضد التهديدات السيبرانية.

● إجراء الأبحاث: أدى تبني التقنيات الصاعدة إلى العديد من التغيرات التي أثرت بشكلٍ كبيرٍ على القطاع التقني والاقتصاد والمجتمع أيضاً. ولذا، يجب أن تُكثف الأبحاث لمواكبة التغيرات وحماية البيانات والمعلومات. حيث إن التخلف في فهم الطبيعة المتقلبة لهذه التقنيات التي تمتاز بكثرة الأجهزة والنظم المرتبطة ببعضها سيؤدي إلى ضعفٍ في حماية أسرار المنشأة، ما يجعلها عرضةً سهلةً للمخربين والهجمات الإلكترونية.

الأمن الإلكتروني الصناعي

نوفر للمؤسسات الصناعية تدارك للأخطاء ومواصلة النشاط التجاري، مما يمنع الوصول غير المصرّح به إلى إدارة النظام والمعلومات التقنية.

أمان عقدة SCADA (نظام التحكم وتحصيل البيانات) الطرفية

يعالج حل الأمن الإلكتروني الصناعي تحديدًا التهديدات على مستوى المُشغل في بيئات .ICS وهو يؤمّن خوادم ICS/SCADA وأنظمة HMIs ومحطات العمل من التهديدات الإلكترونية. يتميز أمان عقدة SCADA (نظام التحكم وتحصيل البيانات) الطرفية بالتوافق التام مع أنظمة التشغيل التلقائي الصناعية، مثل SCADA و PLCوDCS.

يعمل الحل في طبقة بروتوكول الاتصالات الصناعيةModbus) ، وIEC stack، وISO، وما إلى ذلك(، ويبحث عن حالات غير طبيعية في حركة المرور الصناعية عبر تقنية DPI (فحص الحزمة العميق) المتقدمة.

التهديدات والمخاطر التي تمت إزالتها

- تنفيذ البرنامج غير المُصرح به
- Cryptors، برامج الفدية، البرامج الضارة
- جهاز غير مُصرح به أو اتصالات لاسلكية
- انتحال برامجPLC
- خصائص نظام — ICS الفجوات الهوائية؛ النتائج الإيجابية الزائفة لعملية/برنامجCS ، وما إلى ذلك
- ظهور اتصالات أو أجهزة شبكة غير مُصرح بها على الشبكة الصناعية
- هجمات الشبكة
- أوامر PLC الضارة (التي أجراها المُشغل عن طريق الخطأ، بسبب إجراءات الاحتيال أو البرامج الضارة)

تقييم أمان أنظمة التحكم الصناعية(ICS)

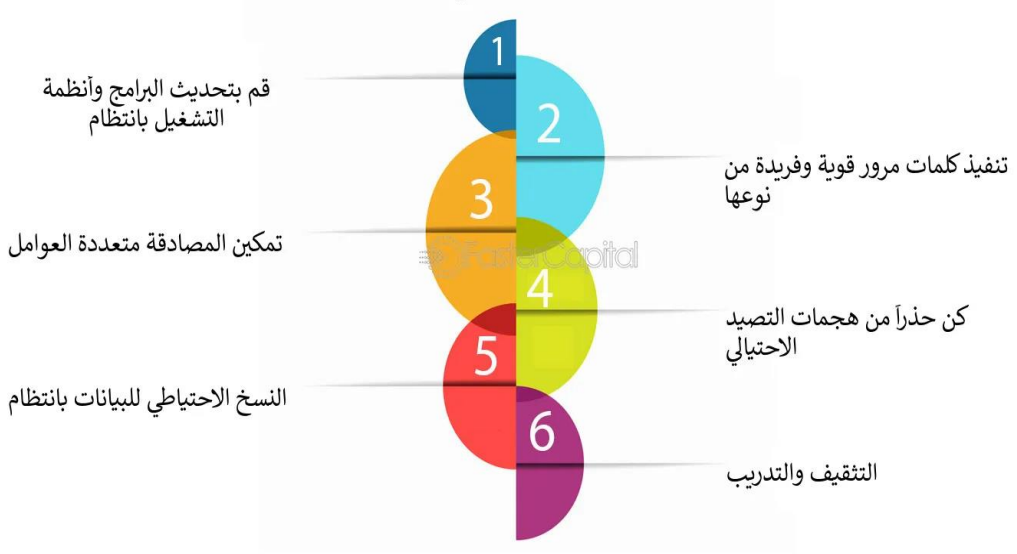
يقدم تقييم أمان أنظمة التحكم الصناعية (ICS) تقييمًا شاملاً لبرنامج أمان ICS ومراجعة تقنية لبنية ICS لديك. تكمن النتائج في جوهر المخطط الاستراتيجي لتحسين أمان نظامي ICS و.SCADA

يمكن أن يحلل خبراؤنا أنظمة التحكم الصناعية في أي مجال: توليد الطاقة ونقلها، وأنظمة النقل، وإنتاج النفط والغاز، وعمليات التعدين، والعديد من المجالات الأخرى. قد نستخدم نُهج تقييم أمنية مختلفة، اعتمادًا على البنية الأساسية والاحتياجات.

ونتيجة لخدمة تقييم أمانICS ، يمكن تحديد نقاط ضعف مختلفة تؤدي إلى الحصول على وصول غير مُصرح به إلى مكونات الشبكة الهامة، بما في ذلك:

- عدم كفاية الأمان المادي لمعداتICS
- بنية شبكة ضعيفة، وحماية شبكة غير كافية) بما في ذلك العيوب في فصل شبكة ICS عن شبكات أخرى(
- نقاط ضعف تؤدي إلى اعتراض حركة مرور الشبكة وإعادة توجيهها (بما في ذلك نقاط الضعف في بروتوكولات الاتصالات الصناعية)
- نقاط الضعف في مكوناتICS ، مثلSCADA ، وPLC، أجهزة القياس الذكية، وما إلى ذلك.
- مصادقة وتخويل غير كافيين في خدمات مختلفة
- بيانات اعتماد المستخدم ضعيفة
- عيوب التكوين، بما في ذلك امتيازات المستخدم الزائدة، بالإضافة إلى عدم الامتثال لمعايير الأمان وتوصيات البائعين
- نقاط الضعف في الاتصالات بين نظام ICS الذي تم تحليله والأنظمة الأخرى) من خلال MES وما إلى ذلك(
- نقاط الضعف الناجمة عن الأخطاء في رمز التطبيقات (عمليات إدخال التعليمة البرمجية، واجتياز المسار، ونقاط الضعف من جانب العميل، وما إلى ذلك)
- نقاط الضعف الناجمة عن استخدام إصدارات البرامج والأجهزة القديمة دون آخر تحديثات الأمان
- الإفصاح عن المعلومات

أفضل ممارسات الأمن السيبراني للأفراد والشركات



الدرس الثالث / الحروب السيبرانية والهجمات الموجهة لنظم المعلومات

الحرب السيبرانية أوCyber War ، وهي عبارة عن هجمات إلكترونية بقيادة عسكرية تقوم باختراق الأنظمة الإلكترونية العالمية، وكل ما يعتمد على التكنولوجيا، وذلك بهدف إلحاق الضرر بالحواسيب والأجهزة التي تستخدم شبكة الإنترنت العالمية.

وكلمة سيبراني، تعني الإلكترونية، وقد أُصطلح على أن تُطلق كلمة "سيبراني" على كل ما يتعلق بالشبكات الإلكترونية الحاسوبية، وشبكة الإنترنت، والإنترنت، والتطبيقات المختلفة..

كيف تتم الحرب السيبرانية؟

الحرب السيبرانية هي حرب افتراضية، تتميز بأسلحتها الرقمية، وبجنودها الجالسين أمام الكمبيوتر. تعمل هذه الحرب على خرق الشبكات الأجنبية دون أن يلاحظها أحد، وتتلاعب بالبنى التحتية الحيوية مثل شبكات الكهرباء أو الاتصالات..

كما أنها قد تؤدي إلى نتائج كارثية، كسرقة بيانات خاصة، وغيرها من الكوارث التي قد تكون عالمية مثل الحروب النووية وغيرها..

الحروب الإلكترونية

الحروب الإلكترونية هي احد أنواع الصراعات والاشتباكات القائمة على استخدام التكنولوجيا الإلكترونية والمعلوماتية بهدف تحقيق أهداف سياسية، عسكرية أو اقتصادية. تشمل هذه الحروب استخدام الحواسيب، والشبكات، والبرمجيات، والاتصالات السلكية واللاسلكية، والأنظمة الإلكترونية في جميع جوانبها.

أولا: مفهوم الحرب الإلكترونية

عرف كل من (Richard A. Clarke & Robert knake) الحرب الالكترونية على أنها "أعمال تقوم بها دولة تحاول من خلالها اختراق أجهزة الكمبيوتر والشبكات التابعة لدولة أخرى بهدف تحقيق أضرار بالغة أو تعطيلها".

كما تعرف الحرب الالكترونية بانها مجموعة من الاجراءات التي تنفذ بهدف الاستطلاع الالكتروني للنظم والوسائل الالكترونية المعادية، واخلال عمل هذه النظم والوسائل الالكترونية، ومقاومة الاستطلاع الالكتروني المعادي، وتحقيق استقرار عمل النظم الالكترونية الصديقة تحت ظروف استخدام العدو اعمال الاستطلاع، والاعاقة الالكترونية.

كذلك تعرف انها "مفهوم يشير إلى أي نزاع يحدث في الفضاء الإلكتروني ويكون له طابع دولي".

ان تطور تكنولوجيا الحروب الإلكترونية ، واعتمادها على استخدام تقنيات متقدمة مثل الذكاء الاصطناعي وتحليل البيانات الكبيرة وتسخير الأقمار الصناعية المتقدمة لتنفيذ الهجمات والتجسس وتعزيز الدفاع. كما تلعب هذه الأنشطة دورا مهما في الأمن القومي والسياسة العالمية، وتتطلب تعاون دوليا لمكافحتها وتأمين البنية التحتية الرقمية لها.

من المتوقع أن تصبح الحرب الإلكترونية نموذجا تسعى إليه العديد من الجهات نظرا للخصائص العديدة التي تنطوي عليها، ومنها:

الكلفة المادية: حيث تعتبر حروب لا تناظرية، فالتكلفة المتدنية نسبيا للأدوات اللازمة لشن هكذا حروب مقارنة بالكلفة التي تقوم بها الدول لتصنيع أسلحة مكلفة جدا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدا خطيرا وحقيقيا على دولة اخرى.

افضلية المهاجم على المدافع: في بيئة مماثلة يتمتع بها المهاجم بأفضلية، فالتحصين سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق وبالتالي المزيد من الضغط.

صعوبة الردع : مفهوم الردع في الحرب التقليدية يختلف عن مفهومه في حروب الإنترنيت، على عكس الحروب التقليدية حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة تحديد موقع الهجمات الإلكترونية، وهو ما يلغي مفعول الردع وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، وفي هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.

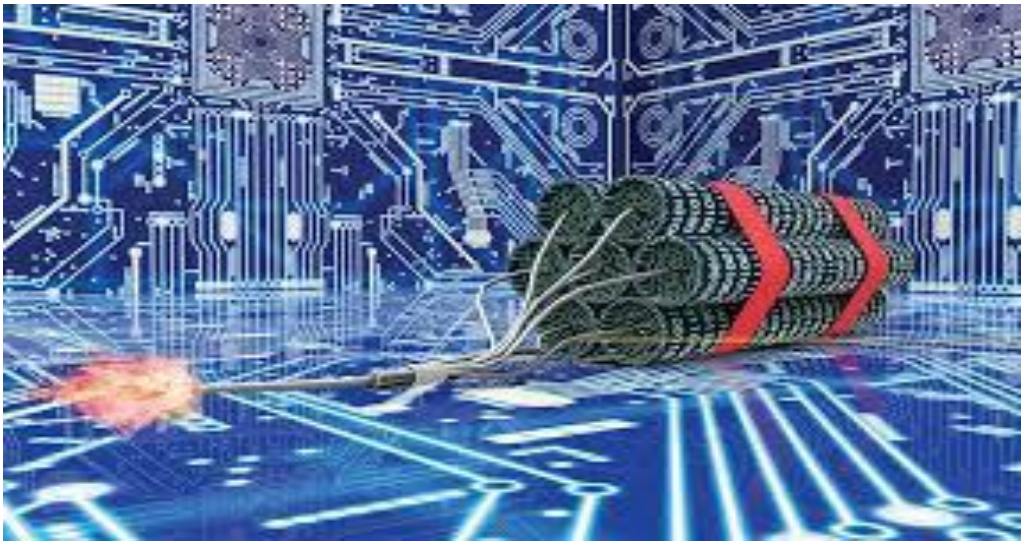
تنوع الجوانب المستهدفة: لا ينحصر إطار حروب الإنترنيت باستهداف المواقع العسكرية، فهناك استهداف البنى التحتية المدنية والحساسة في البلدان المستهدفة، في ظل القدرة على استهداف شبكات الكهرباء والطاقة وشبكات النقل والنظام المالي والمنشآت الحساسة . اضف الى ذلك استهداف مجتمعات تلك الدول من خلال بث الاشاعات وتغيير الرأي العام ضد الدولة او بث الرعب والفوضى بين المواطنين.

وتشير العديد من التقارير إلى تزايد أعداد الهجمات الإلكترونية التي تتم في العالم اليوم والتي يقوم بتنفيذها بها مجموعات أو حكومات

في عام 2007 استهدفت أستونيا هجوم الكتروني الذي يكاد يكون الأول الذي يتم على هذا المستوى ويستخدم لتعطيل المواقع الإلكترونية الحكومية والتجارية والمصرفية والإعلامية مسببا خسائر بعشرات الملايين من الدولارات.

وفي عام 2009، أوردت الحكومة الكورية الجنوبية تقريرا عن تعرضها لهجوم نفذه قراصنة كوريين شماليين بهدف سرقة خطط دفاعية سرية .

وفي عام 2010، واجهت المانيا عمليات تجسس شديدة لكل من الصين وروسيا والتي كانت تستهدف القطاعات الصناعية والبنى التحتية الحساسة في البلاد ومن بينها شبكة الكهرباء.



ثانيا: أنواع حرب المعلومات

1- حرب المعلومات الدفاعية:

حرب المعلومات الدفاعية هي استراتيجية تستخدمها الدول والمؤسسات لحماية أنظمتها وبياناتها من الهجمات والتهديدات السيبرانية. يشمل الدفاع في حرب المعلومات مجموعة من الإجراءات والتقنيات التي تهدف إلى تعزيز الأمان السيبراني والتصدي للتهديدات الإلكترونية.

أهم المفاهيم المتعلقة بحرب المعلومات الدفاعية:

1- تقييم الأمن السيبراني:(Cybersecurity Assessment)

والذي يتضمن تقييم الأمان السيبراني عن طريق تحليل النقاط الضعيفة في الأنظمة والشبكات وتصنيف التهديدات المحتملة.

2- تطوير سياسات الأمان:(Security Policies Development)

إنشاء سياسات وإجراءات تأمينية وتحدد كيفية التعامل مع البيانات والمعلومات الحساسة وكيفية الوصول إليها وحمايتها.

3- استخدام أدوات أمان سيبراني:(Cybersecurity Tools)

استخدام برامج وأدوات أمان سيبراني مثل أنظمة اكتشاف التهديدات وجدران الحماية وبرمجيات مكافحة الفيروسات.

4- التحديث والتصحيح:(Patch and Update Management)

ضمان تحديث البرامج وأنظمة التشغيل بانتظام لسد الثغرات الأمنية المعروفة.

5- تدريب الموظفين:(Employee Training)

تدريب الموظفين على أمور الأمان السيبراني وكيفية التعامل مع التهديدات المحتملة.

6- التشفير والحماية البيانية:(Encryption and Data Protection)

استخدام تقنيات التشفير لحماية البيانات والمعلومات الحساسة.

7- التحقق من الهوية والوصول:(Identity and Access Management)

وذلك عن طريق تنظيم منح الوصول إلى الأنظمة والبيانات بناء على صلاحيات الهوية ومستوى السماح.

8- استراتيجية الاحتياطي واستعادة الكوارث:(Backup and Disaster Recovery Strategy)

ويكون عن طريق إعداد خطة للاحتياطي واستعادة البيانات في حالات الكوارث وفقدان البيانات.

ويتم تصميم اساليب مواجهة حرب المعلومات بما يحقق توافر المعلومات اللازمة، وهذا يتطلب التعرف الدقيق على مصادر ومستوى التهديد المعلوماتي، وذلك من خلال فهم العناصر الآتية:

- هوية ونوايا الاعداء المحتملين.
- اساليب وطرق الهجوم المتوقعة.
- الاهداف المتوقع الهجوم عليها.

2- حرب المعلومات الهجومية:

وتشمل وضع الخطط واتخاذ الاجراءات لإتلاف او تزييف والاستحواذ على المعلومات المسجلة على انظمة الحاسوب والاتصالات المستخدمة في نظم المعلومات في كافة المجالات العسكرية والمدنية، وتتطلب:

1- المعرفة الدقيقة للبنية المعلوماتية والمعدات والموصفات الفنية المستخدمة لدى العدو.
2- اسلوب نقل المعلومات خلال قنوات الاتصال.

3- التطبيقات والبرامج الاساسية المستخدمة في انظمة العدو.

وسائل تحقيق اهداف الهجوم الالكتروني:

- الهجوم الالكتروني (Electronic Attack) ومن امثلته التشويش والخداع الالكتروني والصواريخ المضادة للإشعاع الكهرومغناطيسي.
- العمليات الفسلجية (Psychological Operation) وتنفذ هذه العمليات بواسطة وسائل الاعلام المرئية والمسموعة والمقروءة او توزيع منشورات والذي تودي الى زعزعة الثقة لدى الخصم بقدراته وبث الفرقة بين صفوفه.
- الهجمات على شبكات الحاسوب (Computer Network Attack) : وهذه تشمل اختراق الشبكات والحاسبات المركزية لحقن الحاسبات ببيانات ومعلومات مزيفة ونشر الفايروسات.

ويمكن تنفيذ حرب المعلومات الهجومية من خلال شل فعاليات انظمة معلومات العدو، واعداد مسرح العمليات، بحيث اذا ما تطور النزاع او الازمة الى مواجهة عسكرية فانه يمكن تنفيذ سيناريو حرب المعلومات الهجومية.

الدرس الرابع / قواعد الاستخدام الآمن لنظم المعلومات في المؤسسات

تعريف أمان المعلومات

يشير أمان المعلومات إلى مجموعة من الإجراءات والأدوات الأمنية التي تحمي على نطاق واسع معلومات المؤسسة الحساسة من سوء الاستخدام أو الوصول غير المصرح به أو التعطيل أو الإتلاف. يشمل أمان المعلومات الأمن المادي والبيئي والتحكم في الوصول، والأمان عبر الإنترنت. غالباً ما يتضمن أمن المعلومات تقنيات مثل وسطاء أمان الوصول إلى السحابة(CASB) ، وأدوات كشف الخداع، والكشف التلقائي والاستجابة على النقط النهائية(EDR) ، واختبار الأمان لـ (DevSecOps) DevOps والمزيد.

العناصر الرئيسية لأمن المعلومات

تضم سياسة أمان المعلومات مجموعة من أدوات وحلول وعمليات الأمان التى تحافظ على أمان معلومات المؤسسة عبر الأجهزة والمواقع، مما يساعد على الحماية من الهجمات الإلكترونية أو الأحداث التخريبية الأخرى

- أمان التطبيقات

النُهج والإجراءات والأدوات وأفضل الممارسات التي يتم وضعها لحماية التطبيقات وبياناتها.

- الأمان السحابي

النُهج والإجراءات والأدوات وأفضل الممارسات التى يتم وضعها لحماية السحابة ككل، بما فى ذلك الأنظمة والبيانات والتطبيقات والبنية الأساسية.

- التشفير

هو طريقة قائمة على الخوارزمية لتأمين الاتصال تهدف إلى ضمان اقتصار عرض رسالة معينة وفك تشفيرها على مستلمين بعينهم.

- الإصلاح بعد كارثة

هو عبارة عن طريقة لإعادة إنشاء أنظمة تكنولوجية فعالة في أعقاب حدث مثل كارثة طبيعية أو هجوم إلكتروني أو حدث تخريبي آخر.

- التصدي للحوادث

خطة المؤسسة للاستجابة لتداعيات أي هجوم عبر الإنترنت أو تسرب للبيانات أو حدث تخريبي آخر ومعالجته وإدارته.

- أمان البنية الأساسية

الأمان الذي يشمل البنية الأساسية التكنولوجية الكاملة للمؤسسة، بما في ذلك أنظمة الأجهزة والبرامج.

- إدارة الثغرات الأمنية

هي العملية التي تجريها المؤسسة لتحديد وتقييم ومعالجة الثغرات الأمنية في نقاط النهاية والبرامج والأنظمة الخاصة بها.

الركائز الثلاثة لأمن المعلومات : السرية والتكامل والتوافر(CIA)

تمثل عناصر "السرية" و"التكامل" و"التوافر" الركائز الأساسية حماية البيانات، والتي تشكل بدورها أساس البنية الأساسية الأمنية للمؤسسة. تعمل تلك العناصر الثلاثة "السرية" و"التكامل" و"التوافر" بمثابة مبادئ توجيهية لتنفيذ خطة أمان المعلومات.

- السرية

تمثل الخصوصية مكوناً رئيسياً لأمان المعلومات، ويجب على المؤسسات أن تضع إجراءات تسمح فقط للمستخدمين المصرح لهم بالوصول إلى المعلومات. يمثل تشفير البيانات و المصادقة متعددة العوامل وتفادي فقدان البيانات جزءاً من الأدوات التي يمكن للمؤسسات استخدامها للمساعدة في ضمان سرية البيانات.

- التكامل

يجب أن تحافظ المؤسسات على تكامل البيانات طوال دورتها بالكامل. ستدرك الشركات التي تتمتع بميزة أمان المعلومات الفعالة أهمية البيانات الدقيقة والموثوقة، ولن تسمح لأي مستخدم غير مُخوَّل بالوصول إليها أو تغييرها أو التدخل فيها بأي طريقة أخرى. تساعد أدوات مثل أذونات الوصول إلى الملفات وإدارة الهوية وعناصر التحكم في وصول المستخدم في ضمان تكامل البيانات.

- التوافر

تتضمن سياسة أمان المعلومات صيانة الأجهزة المادية باستمرار واستكمال ترقيات النظام بانتظام لضمان حصول المستخدمين المعتمدين على وصول متسق يمكن الاعتماد عليه إلى البيانات التي يحتاجون إليها.

المخاطر الشائعة لأمان المعلومات

هجمات المخاطر المستمرة والمتقدمة:(APT)

عبارة عن هجوم إلكتروني متطور يحدث على مدى فترات طويلة، ويكتسب خلاله مهاجم مخفية (أو مجموعة) الوصول إلى شبكة المؤسسة والبيانات.

الحواسيب الموبوءة:(Botnet)

مشتق من المصطلح Robot Network" (شبكة الروبوت)" ويشير إلى شبكة من الأجهزة المتصلة التى يصيبها المهاجم بعناصر تحكم عن بُعد وشفرة ضارة.

هجمات الموزعة لحجب الخدمة:(DDoS)

تستخدم الهجمات الموزعة لحجب الخدمة الحواسيب الموبوءة للسيطرة على موقع الويب أو التطبيق الخاص بالمؤسسة، مما يؤدي إلى تعطل أو حجب الخدمة عن المستخدمين أو الزوار الصالحين.

هجمات لتنزيل البرامج الضارة دون قصد:

جزء خبيث من التعليمات البرمجية يتم تنزيله تلقائياً على جهاز المستخدم عند زيارة أحد مواقع الويب، مما يجعل هذا المستخدم عُرضة لمزيد من التهديدات الأمنية.

مجموعة أدوات الاستغلال:

هي مجموعة شاملة من الأدوات التي تستخدم عمليات الاستغلال لاكتشاف الثغرات الأمنية وإصابة الأجهزة بالبرامج الضارة.

المخاطر الداخلية :

تشير إلى احتمالية استغلال مستخدم داخلي للوصول المصرح به عن قصد أو بغير قصد لإلحاق الضرر أو جعل أنظمة وشبكات وبيانات المؤسسة عُرضة للخطر.

هجمات الدخيل:(MitM)

يقاطع المهاجم الضار خط اتصال أو نقل بيانات منتحلاً صفة مستخدم صالح لسرقة المعلومات أو البيانات.

هجمات التصيد الاحتيالي:

تنتحل هجمات التصيد الاحتيالي صفة منظمات أو مستخدمين شرعيين لسرقة المعلومات عبر البريد الإلكتروني أو الرسائل النصية أو طرق الاتصال الأخرى.

برامج الفدية الضارة:

هجوم ابتزازي من البرامج الضارة يعمل على تشفير معلومات مؤسسة أو شخص ما، ويمنع الوصول إليها حتى يتم دفع فدية.

الانتحال بالهندسة الاجتماعية:

هي هجمات إلكترونية تنشأ عن تفاعل بشري، حيث يكتسب المهاجم ثقة الضحية من خلال الاصطياد أو التخويف أو التصيد الاحتيالي، ويجمع المعلومات الشخصية ويستخدمها لتنفيذ هجوم.

هجمات عبر وسائل التواصل الاجتماعي:

الهجمات الإلكترونية التي تستهدف منصات التواصل الاجتماعي، أو تستغل هذه المنصات كآليات تسليم أو تسرق معلومات المستخدم وبياناته.

الفيروسات والفيروسات المتنقلة:

البرامج الضارة الخبيثة التي لم يتم اكتشافها والتي يمكن نسخها ذاتياً عبر شبكة أو نظام المستخدم.

التقنيات المستخدمة لأمن المعلومات

وسطاء أمان الوصول إلى السحابة(CASB)

نقاط فرض نهج الأمان الموضوعة بين مستخدمي المؤسسات وموفري الخدمات السحابية التي تجمع بين نُهج أمان مختلفة ومتعددة، ابتداءً من المصادقة وتعيين بيانات الاعتماد ووصولاً إلى التشفير واكتشاف البرامج الضارة والمزيد. يعمل وسطاء أمان الوصول إلي السحابة CASB عبر التطبيقات المصرح بها وغير المصرح بها والأجهزة المُدارة وغير المُدارة.

تفادي فقدان البيانات

يشمل تفادي فقدان البيانات (DLP)

النُهج والإجراءات والأدوات وأفضل الممارسات التي تم وضعها لتفادي فقدان البيانات الحساسة أو إساءة استخدامها. تتضمن الأدوات الرئيسية كلاً من التشفير أو تحويل النص العادي إلى نص مشفر عبر الخوارزمية والترميز المميز أو تعيين مجموعة من الأرقام العشوائية لجزء من البيانات واستخدام نواة قاعدة البيانات الرمزية لتخزين العلاقة.

الكشف التلقائي والاستجابة على النقط النهائية(EDR)

يُعد الكشف التلقائي والاستجابة على النقط النهائية EDR بمثابة حل أمني يستخدم مجموعة من الأدوات لكشف التهديدات في أجهزة نقطة النهاية وفحصها والاستجابة لها.

التجزئة الدقيقة

تُقسم التجزئة الدقيقة مراكز البيانات إلى مناطق وأجزاء كثيرة ومتعددة المستويات وآمنة، مما يُخفف من مستويات المخاطر.

اختبار الأمان لـ(DevSecOps) DevOps

DevSecOps هو عملية دمج الإجراءات الأمنية في كل خطوة من خطوات عملية التطوير، وزيادة السرعة وتقديم عمليات أمان محسّنة وأكثر استباقية.

تحليلات استخدامات المستخدمين والكيانات(UEBA)

تُعد عملية تحليلات استخدامات المستخدمين والكيانات بمثابة عملية مراقبة سلوك المستخدم النموذجي وكشف الإجراءات التي تخرج عن الحدود الطبيعية، مما يساعد المؤسسات على تحديد التهديدات المحتملة.

أمن المعلومات ومؤسستك

يُمكن للشركات استخدام أنظمة إدارة أمان المعلومات (ISMS) لتوحيد عناصر التحكم في الأمان عبر المؤسسة، وإعداد معايير مخصصة أو معايير المجال للمساعدة في ضمان أمن المعلومات و إدارة المخاطر .سيساعد استخدام نهج منظم لأمان المعلومات في حماية المؤسسة من المخاطر غير الضرورية بشكل استباقي والسماح لفريقك بمعالجة التهديدات بكفاءة عند ظهورها.

الاستجابة لمخاطر أمن المعلومات

بمجرد تحول فريق الأمان لديك إلى فريق لمكافحة تهديدات أمان المعلومات، اتبع الخطوات التالية:

- قم بتجميع فريقك وتحدث معهم عن خطة الاستجابة للحوادث الخاصة بك.
- حدد مصدر التهديدات.
- نفذ الإجراءات لاحتواء ومعالجة التهديدات.
- قيم أي ضرر.
- أخطر الأطراف ذات الصلة.