القمة العالمية للحكومات
WORLD GOVERNMENT SUMMIT

بالتعاون مع

EY
نبني عالماً أفضل للعمل

الاستمرارية والمرونة الإلكترونية في العصر الرقمي

الفهرس

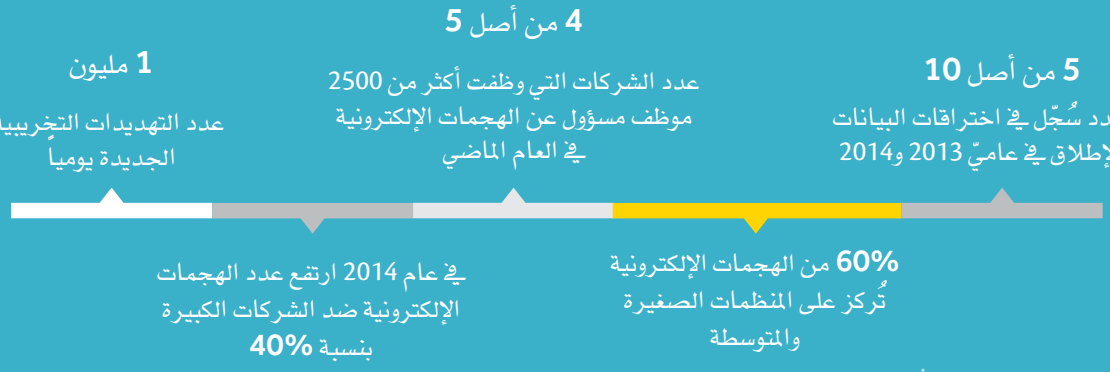
الملخص التنفيذي

تؤدي عملية الرقمنة المتسارعة للاقتصاد العالمي إلى زيادة كبيرة في التهديدات الأمنية الإلكترونية. وقد وظفت كل أربع منظمات من أصل خمس، في جميع أنحاء العالم، أكثر من 2،500 كادر وظيفي للتصدي للهجمات الإلكترونية في عام 2015، وقد تم تقدير الأثر المالي لذلك بما يتجاوز 440 مليار دولار.

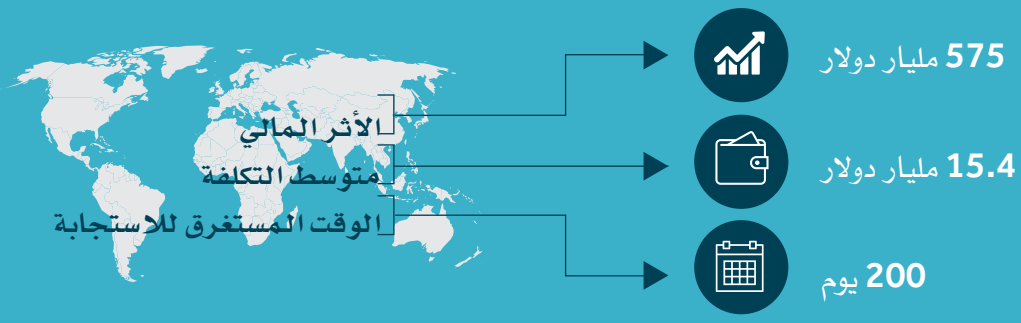
يتطلع المواطنون والزوار إلى أن توفر لهم حكوماتهم بيئة اقتصادية آمنة وقوية في الشركات التي تستثمر في التكنولوجيا الرقمية مع الشعور بالأمن والراحة في تخزين وتبادل المعلومات؛ نظراً لأنهم أصبحوا أكثر اعتماداً بشكل متزايد على التكنولوجيا في الأنشطة اليومية الخاصة بهم، كما يرغب المواطنون والزوار على حد سواء أن يكون هناك حماية قوية ضد كافة أنواع التهديدات، بما في ذلك التهديدات التي يواجهها العالم الرقمي الخاص بهم (التهديدات الإلكترونية).

وفي الوقت نفسه، تعتمد الحكومات على الابتكارات الرقمية للمساعدة في خدمة أصحاب المصالح والحد من التكاليف وتوفير ميزة تنافسية في السوق العالمية. وتُشير هذه الاتجاهات إلى أن هناك ضرورة مُلحّة لأن يكون هناك مرونة في التصدي للتهديدات الإلكترونية في العصر الرقمي، وينبغي على الحكومات والمنظمات في القطاعات الخاصة والعامة والأفراد ينبغي أن يكون لكل من الأفراد و الحكومات والمنظمات في القطاعين الخاص والعام دوراً في إنشاء النظم التي تتسم بالمرونة عند التصدي للتهديدات الإلكترونية.

الهجمات الإلكترونية وأثرها



المصدر: تقرير التهديدات الأمنية الإلكترونية، سيمانتيك



المصدر: معهد Ponemon

دراسة تكلفة اختراق البيانات لعام 2015: التحليل العالمي

ماذا تعني المرونة في سياق التكنولوجيا الرقمية؟ يمكننا تعريف المرونة الإلكترونية بأنها القدرة التنظيمية على استشعار الأحداث المتعلقة بالتهديدات الإلكترونية التخريبية ومقاومتها والرد عليها، والتعافي منها في فترة زمنية مناسبة. وقد أصبح الاقتصاد الرقمي في الوقت الحالي متغيراً ولا حدود له أكثر من أي وقت مضى؛ ولذلك فبدلاً من بناء حماية منيعة حول الوجود الرقمي في أي بلد، فالأفضل من ذلك هو وجود القدرة على إمكانية استباق التهديدات لاستيعاب أثر الهجمات الالكترونية والرد عليها بطريقة سريعة ومرنة لضمان أن النظم والعمليات الرئيسية في الدول لا تزال تعمل بشكل سلس.

ومع استخدام التقنيات الذكية، مثل الذكاء الاصطناعي والتعلم الآلي ونظم المؤسسات؛ فستكون الأنظمة الخاصة بالأمن الإلكتروني قادرة على التعافي من أي هجوم وإيجاد وسائل حماية أقوى ضد مثل هذه الهجمات في المستقبل.

تلعب الحكومات دوراً حاسماً في المساعدة على نشر ثقافة إلكترونية مرنة، حيث قد تلقّى الأفراد والمنظمات تعليماً توعوياً بشأن مخاطر التهديدات الإلكترونية. ويُمكن للحكومات أن تضع الأساس الفعال واللازم للمنظمات والمواطنين والزوار، والذي يقوم على القوة والثقة.

وهناك تهديدات إلكترونية حقيقية من شأنها أن تكون مدمرة، مثل مخاطر الارهاب والحوادث الكارثية. ويُمكن للحكومات تصميم إطار عمل تتعاون من خلاله المنظمات لتعزيز قدرتها على مواجهة الهجمات الإلكترونية، لأن الحكومات قادرة على رؤية الصورة الأكبر للتهديدات المحتملة وآثارها. وعندما تتعرض منظمة ما لهجوم إلكتروني، فمن المرجح أن يتم الهجوم عليها باعتبارها لا تستطيع التصدي للهجوم أو الرد عليه، ولكن الحكومات قادرة على وضع هذا الهجوم في سياق وطني والرد عليه على المستوى الوطني أو الدولي، إذا اقتضت الحاجة لذلك.

وفي حال نجحت الحكومات في هذا المسعى؛ فإن الأشخاص سيشعرون بأمانٍ أكثر تجاه حصانة البيانات الخاصة بهم، وسوف يزدهر الابتكار والاستثمار في التكنولوجيا في بيئة ترعاها الحكومات الذكية والقوية.

> "نحن نقف على حافة ثورة تكنولوجية من شأنها أن تُحدث تغييراً جذرياً في أسلوب العمل والتفاعل بين الفرد ومؤسسة المجتمع المدني، وسيكون هذا التحوّل في مُجمَله ونطاقه وتعقيده على عكس ما شهدته البشرية من قبل، فهو تحوّلٌ لم يسبق له مثيل".
>
> (المنتدى الاقتصادي العالمي، 2016)

وسيتم التطرّق في هذا التقرير إلى النقاط التالية:

- الدور الحاسم الذي تلعبه الحكومات في إعداد وتنفيذ استراتيجية خاصة بالمرونة الإلكترونية.
- ضرورة وجود رؤية واضحة بشأن التهديدات الإلكترونية المتغيرة باستمرار، وحماية المجالات الأكثر حيوية وعُرضة للهجوم والتهديد الإلكتروني.
- استبدال استراتيجيات الحماية التقليدية لفقدان فعاليتها، حيث أن مُوجهي التهديدات الناشئة وسرعة التغيير التي أوجدتها الثورة الرقمية لا يُمكن معالجتها بهذه الوسائل التقليدية.

دور الحكومات في إعداد استراتيجية المرونة الإلكترونية

تلعب الحكومات دوراً هاماً في تشكيل المستقبل الرقمي لبلدانها، وينبغي وجود رؤية واضحة فيما يتعلق بالاحتياجات الرقمية للمجتمع، بحيث تُمكّن من تحقيق التحوّل الرقمي بنجاح. وفي حين أن الاقتصاد الرقمي قد بدأ بالازدهار؛ فأصبح يتعين على الحكومات إيجاد بيئة مُناسبة تساعد في نمو العمل ونجاح الابتكار.

ويُمكّن التقدم السريع في مجال التكنولوجيا الرقمية الحكومات من توفير خدمات أكثر كفاءة وتحسين تجربة المستخدمين، كما تحتاج الحكومات إلى إنشاء نظام مستدام من شأنه زيادة القدرة على مواجهة الهجمات والكوارث سواء كانت طبيعية أو من فعل الإنسان.

الأمور التي يأخذها النظام الرقمي بعين الاعتبار

إن الاستفادة من الفرص التي توفرها الثورة الرقمية تتطلب من الحكومات وضع سياسة خاصة بالثقافة والتوعية الرقمية ووضع خطة لكيفية تلبية احتياجات المهارات، وذلك من خلال تعليم الطلاب الذين سيدخلون سوق العمل وإعادة تدريب الأشخاص العاملين الذين يحتاجون إلى مزيد من الوعي الإلكتروني للتكيّف مع الثقافة الجديدة.

ونظراً لجمع المزيد من البيانات وتخزينها وتبادلها بشكل إلكتروني؛ سيترتب على الحكومات مسؤوليات جديدة، مثل ضمان خصوصية البيانات وضمان الأمن الإلكتروني. ويتطلب التحول الرقمي من الحكومات إعداد إطار عمل قانوني ورقابي مُناسب بحيث تتمكن الشركات والأفراد من العمل من خلاله بشكل قانوني.

المحاور الرقمية الأربعة التي تعكس مجموعة شاملة من التحديات والفرص التي توفرها عملية الرقمنة

تحسين الخدمات في المدن الذكية

- كيف يُمكن لعملية الرقمنة أن تعالج المشكلات المتعلقة بمسألة التحضر؟
- كيف يُمكن لعملية الرقمنة أن تُساعد الحكومات على الاستفادة بأقصى قدر ممكن من إمكانات البنية التحتية للنقل في زيادة الكفاءة ورضا الركاب على حد سواء؟

تحسين خدمة العملاء

- كيف يُمكن لعملية الرقمنة أن تُساعد القطاعات على تكوين علاقة أفضل مع العملاء وجعلها "علامة تجارية موثوق بها"؟
- كيف يُمكن لعملية الرقمنة أن تُساعد القطاعات والحكومات على تحسين مشاركة المواطنين الدائمة في بناء اقتصاد ومجتمع أفضل؟

إنشاء مجتمع واقتصاد رقمي

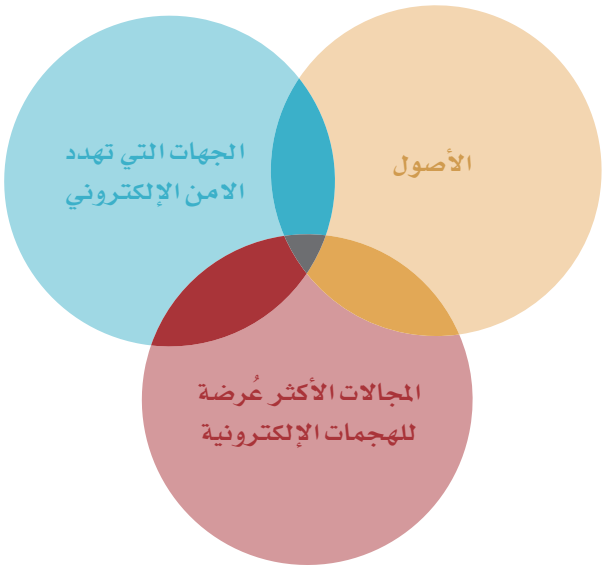
- كيف يُمكن للحكومات بناء اقتصاد ومجتمع رقمي شامل؟
- كيف يمكن لعملية الرقمنة أن تُساعد قطاع التعليم في بناء المهارات والقدرات المناسبة والمطلوبة في البيئة الرقمية المتطورة أكثر من أي وقت مضى؟

تطوير القطاعات والحكومات الذكية

- كيف يُمكن لعملية الرقمنة أن تُساعد القطاعات والحكومات في إعادة تحديد طريقة تقديم الخدمات وجعل المواطنين أكثر سعادة من خلال تقليل تكلفتها؟
- كيف يمكن لعملية الرقمنة تحسين كفاءة وفعالية القطاعات والحكومات؟

سيؤدي التطور السريع الذي يشهده المجال الرقمي إلى إعادة تشكيل وظيفة رئيس قسم التكنولوجيا لتجعله يقوم بدور استراتيجي أكبر من الدور المُوكَل إليه مُسبَقاً، وذلك بصفته وكيلاً للتغيير وأحد قادة التحوّل الرقمي، كما عليه أن يضع في اعتباره أنه سيكون هناك آثاراً بعيدة المدى على الاقتصاد. ولا بد لرئيس قسم التكنولوجيا في الحكومة أن يكون مؤيداً هاماً لإنشاء نظام يتسم بالمرونة، وأن يلعب كذلك دوراً هاماً في إعداد السياسة الخاصة بهذا النظام.

عناصر الحوادث الإلكترونية



عملية الرقمنة تغير خطة التهديدات الإلكترونية

يُتيح التحول الرقمي فرصاً استثمارية جديدة كل يوم، كما يؤدي في الوقت نفسه إلى مجموعة من التهديدات الإلكترونية الجديدة. وتمتد الابتكارات الرقمية لتنتشر في المجال المستهدف من قِبَل الهجمات الإلكترونية التي يقوم بها المخترقون وغيرهم من الجهات التي تقوم بالتهديدات الأمنية، والذين يعملون على إيجاد طرق جديدة لاختراق شبكات المعلومات بهدف التخريب أو السرقة؛ لذلك فإنه ينبغي على الحكومات أن تكون على دراية بالمجالات الأكثر عُرضةً للهجمات الإلكترونية ووضع استراتيجية قوية لإدارة المخاطر الإلكترونية والمساعدة في توفير الظروف المُستدامة لاستمرار التحوّل الرقمي.

عناصر الحوادث الإلكترونية

لا بد من إعداد استراتيجية ناجحة تستند على فهم واضح لثلاثة عناصر يقوم عليها الهجوم الإلكتروني (انظر الشكل في الصفحة رقم 6)، وستكون الحكومات بحاجة إلى تقييم ورصد كافة العناصر الثلاثة بشكل مستمر من أجل تحقيق المرونة الإلكترونية.

الأصول

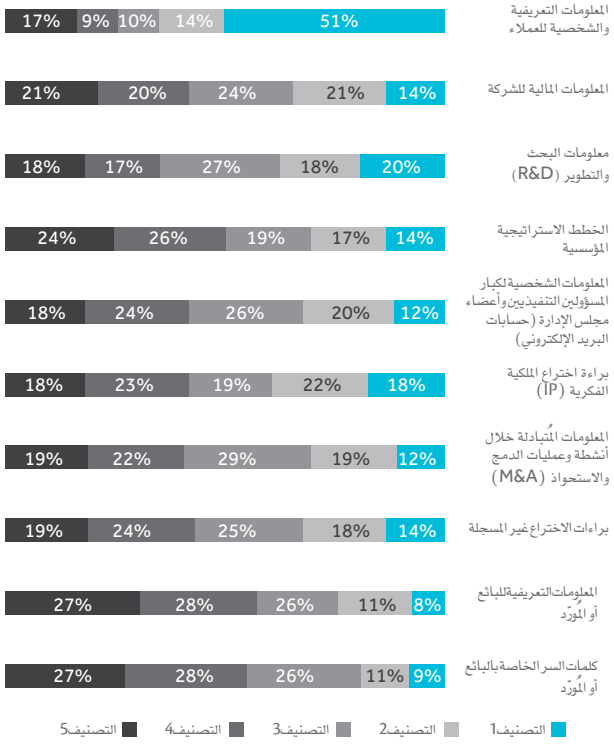
عند حدوث الهجمات الإلكترونية، فإنه بإمكان الجهات التي تقوم بالتهديدات الأمنية أن تستهدف أصولاً حساسة، وتتخذ هذه الأصول أشكالاً مختلفة، بما في ذلك البيانات (مثل معلومات بطاقة الائتمان والسجلات الصحية الشخصية وأوراق اعتماد المستخدم الخاصة والملكية الفكرية) والمال والنظم التي تتحكم في البنية التحتية الوطنية الهامّة في البلاد (مثل شبكات الاتصالات السلكية واللاسلكية وشبكة الكهرباء ونظم النقل). وينبغي على الحكومات إنشاء قاعدة بيانات للأصول الوطنية التي ستتطور بالتدريج مع عملية رقمنة الاقتصاد، كما يجب أن تكون قاعدة البيانات هذه مرنة بما فيه الكفاية لتتماشى مع استراتيجية المرونة الإلكترونية، ويعد كذلك تحديد الأصول الرقمية الهامّة للبلاد خطوة ضرورية جداً لفهم المخاطر المحتملة التي يتعين على الحكومة إدارتها.

المجالات الأكثر عُرضة للهجمات الإلكترونية

تتجه معظم الحكومات والمنظمات إلى حماية أنظمتها التقنية القابلة للتعرض إلى الهجمات الإلكترونية من خلال التركيز على إصلاح البرامج المُعطلة وإرسال التحذيرات والتنبيهات، وذلك لتأمين الشبكات الأكثر عُرضة للهجمات الإلكترونية.

استبيان إرنست ويونغ (EY) السنوي حول أمن المعلومات العالمية (GISS) لعام 2015

"ما هي المعلومات التي تُعتَبر الأكثر قيمة في مؤسستكم بالنسبة لمجرمي الإنترنت؟"



تعتمد الجهات التي تهدد الأمن الإلكتروني بشكل كبير على الأساليب التنظيمية الاجتماعية للبحث عن المجالات الأكثر عُرضةً للهجوم الإلكتروني، وهذا يدل على أنها تستخدم أساليب مختلفة كالاحتيال وطلب فدية وسرقة الهوية للوصول إلى أغلى وأثمن الموجودات في الشركة أو الدائرة الحكومية. وهناك حملة وطنية ترعاها الحكومة لرفع مستوى الوعي بأكثر المجالات المُعرّضة للهجمات الإلكترونية والتي من شأنها أن تساعد في تثقيف الأشخاص بشأن هذه المخاطر، وسيؤدي تبادل المعلومات التقنية حول الأمن الإلكتروني بين المسؤولين عنه إلى زيادة الثقة بين الأفراد والمنظمات وتسريع تبني التحوّل الرقمي.

تستحق البنية التحتية الوطنية الحرجة، مثل شبكة الكهرباء، اهتماماً وثيقاً بشكل خاص نظراً لأن التقنية التشغيلية (OT) وتكنولوجيا المعلومات (IT) لا ترتبط بشكل مادي او افتراضي، وطالما أن هذه البنية التحتية تعمل بشكل مستمر فستشكل تحديثات نظم التقنية التشغيلية (OT) مشكلة كبيرة، حيث قد يستغرق الاختبار الشامل لهذه لتحديثات مدة زمنية يُمكن أن تصل إلى 18 شهراً، وستكون الأنظمة حينها عُرضة للهجمات الإلكترونية، لذلك فإن الحكومات ستكون بحاجة إلى العمل بشكل وثيق مع مُوزعي نظم التقنية التشغيلية (OT) المتخصصين لتحسين عملية التحديث.

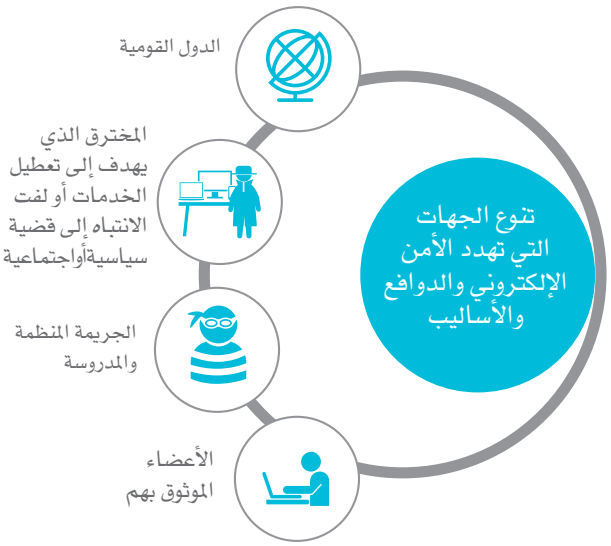
ويستحق انترنت الأشياء «Internet of Things» وجميع الأجهزة المتصلة اهتمام خاص وذلك بسبب تعرضه لهجوم إلكتروني واسع النطاق. وقد نشرت بعض الحكومات مؤخراً معايير خاصة بصناعة أجهزة التقنيات التشغيلية للتأكد من أن الأجهزة المتصلة بالإنترنت ستكون أكثر أمناً في المستقبل بعد التصدي لهجوم قطع الخدمة الموجهة من خلال هذه الأدوات.

معايير التكنولوجيا الناشئة والمناهج الخاصة بالمرونة الإلكترونية

لقد اتبع القطاع الإلكتروني مجموعة متنوعة من الوسائل التي تمكنه من معالجة مسألة المرونة فيه، وقد أصدرت منظمة المعايير الدولية مشروعاً حول ISO 23316 يشتمل على القواعد والمبادئ التوجيهية المتعلقة بالمرونة التنظيمية. وقد نشر المعهد الوطني الأمريكي للمعايير والتكنولوجيا تقريراً 53–800يتناول فيه قدرة البنية التحتية الوطنية الهامة. وعملت جامعة »كارنيجي ميلون« مع »معهد هندسة البرمجيات« على تطوير نموذج إدارة المرونة الذي تم تحديثه في عام 2016 (v1.2). وبالمثل، فقد قامت مجموعة من الهيئات الوطنية والإقليمية بتطوير وتعزيز المعايير المختلفة والوثائق التوجيهية بشأن المرونة الإلكترونية، بما في ذلك وزارة الأمن الداخلي الأمريكية ووكالة الاتحاد الأوروبي لامن المعلومات.

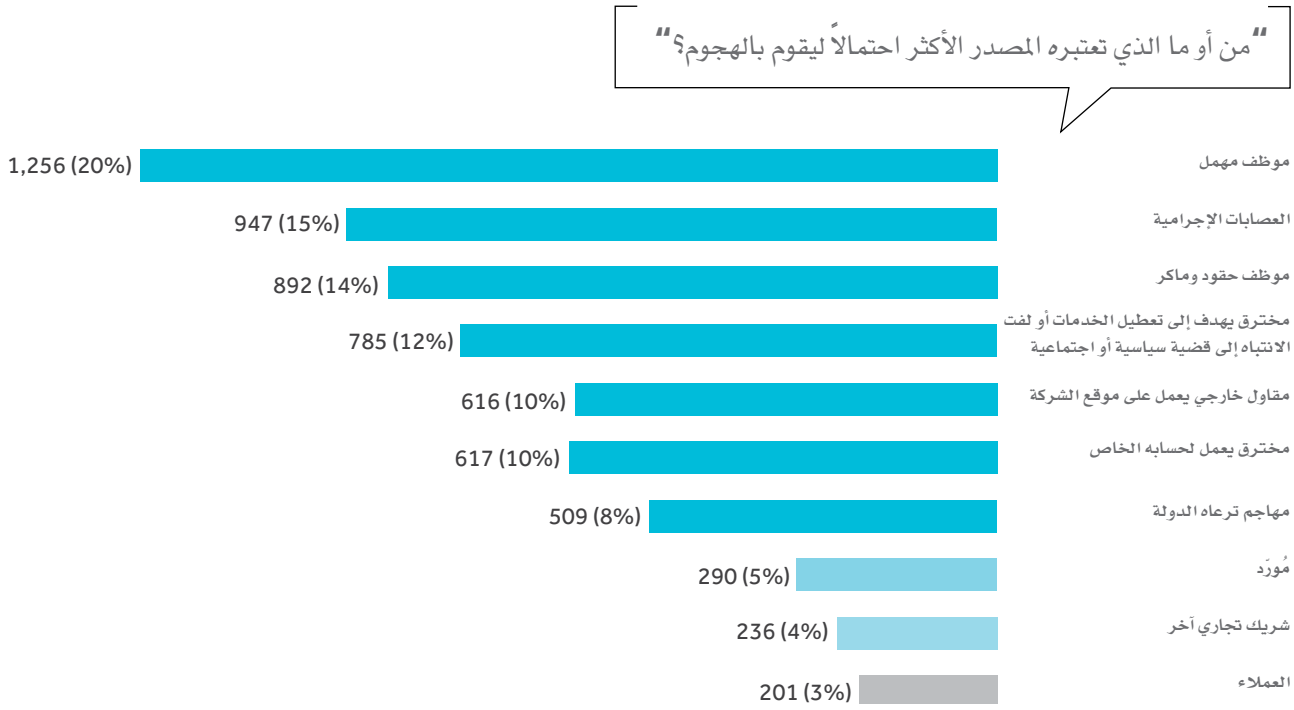
الجهات التي تهدد الأمن الإلكتروني

لقد مالت الحكومات والقطاع الخاص إلى التركيز على الأصول والمجالات الأكثر عُرضة للهجمات الإلكترونية، وقاموا أيضاً بإجراء تقييم للجهات التي تهدد الأمن الإلكتروني بشكل فعلي أو محتمل على حد سواء، إذ في النهاية فإن الحكومات والقطاعات لن تبدأ بالإجراء اللازم قبل أن تفهم ماهيّة تلك التهديدات والمخاطر المحتملة. وعندما يتم انخراط الأشخاص في مثل هذه الأمور، فستكون الحكومات حينها بحاجة إلى فهم دوافع ونوايا الجهات التي تهدد الأمن الإلكتروني والأساليب والتقنيات التي تتبعها، وهذه جميعها تتغير مع مرور الوقت وكيفية استجابة الحكومات لتغيرات وسائل الحماية الإلكترونية.



وبالمقارنة مع القطاع الخاص؛ فإن الحكومات لديها القدرة على مراقبة النظام إذا اقتضى الأمر، وذلك من خلال سنّ التشريعات الفرعية، كما يتعيّن على الحكومات أن تضع في اعتبارها المخاوف والمخاطر المتعلقة بالخصوصية في حال تم اتباع نهج غير مناسب من شأنه أن يُعيق الابتكار والاستثمار. ويُمكن للحكومات كذلك رصد أنشطة الجهات التي تهدد الأمن الإلكتروني، والبحث عن الهجمات الإلكترونية السابقة التي قامت بها، وتحديد التغييرات التي أحدثتها هذه الجهات في الأساليب والتقنيات والإجراءات الخاصة بها. ويكمن التحدي، إذن، في نشر المعلومات حول الجهات التي تهدد الأمن الإلكتروني دون تنبيه المخترقين أو الكشف عن مصادرهم، ولكنه لا يزال يتعين على المنظمات أن تقوم بالدور المُوكل إليها كذلك، إذ أن وجود حكومة يقظة ومتنبهة لا يُغني عن ضرورة قيام المنظمات بمراقبة البيئة المحيطة بها بشكل مستمر.

استبيان إرنست ويونغ (EY) السنوي حول أمن المعلومات العالمية (GISS)، لعام 2016



تمتلك الحكومات الوسائل المناسبة لاتخاذ إجراءات مُعاكِسة ضد الجهات التي تهدد الأمن الإلكتروني، ويجب على المسؤولين النظر في وضع قنوات الاتصال وصياغة مذكرة تفاهم بين الحكومات والمنظمات لتبادل المعلومات قبل اتخاذ تدابير وإجراءات معاكسة. ويتعين على الحكومات أيضاً تحديث إطار العمل القانوني الذي سيُقاضي الجهات التي تهدد الأمن الإلكتروني. وسوف يشمل ذلك الإجراءات المتعلقة بتسليم الفاعل وتطبيق العقوبة الفعلية عليه وفقاً للمعايير القانونية الدولية، ويجب أن تتطرق سياسة الحكومة وتأخذ بعين الاعتبار إجراءات المنظمات الخاصة، مثل الشركات، والنظر فيما إذا كانت قد فشلت في الامتثال للأنظمة واللوائح ذات الصلة. وفي حال كانت السياسة صارمة جداً؛ فإن ذلك من شأنه أن يحول دون التطوير التجاري للتكنولوجيا الرقمية.

وسائل الحماية الإلكترونية وفقدان فعاليتها

لقد تم حفظ معلومات بالغة الأهمية في قواعد البيانات والشبكات الداخلية التي تعمل بشكل ذاتي بعيداً عن أعين المتطفلين في الماضي القريب، وقامت المنظمات بحماية البيانات من خلال برنامج جدار الحماية (Firewall) لديها. وبما أن الأنظمة أصبحت مرتبطة بالشبكات الخارجية؛ فقد قامت المنظمات باعتماد نموذج أمني »يقوم على الحماية المُعمّقة للمعلومات« ، بحيث أنه في حال وقوع اختراق لحدود المعلومات فسيكون هناك مستويات حماية أمنية إضافية لحماية المعلومات الحرجة والهامّة من الوقوع في الأيدي الخطأ.

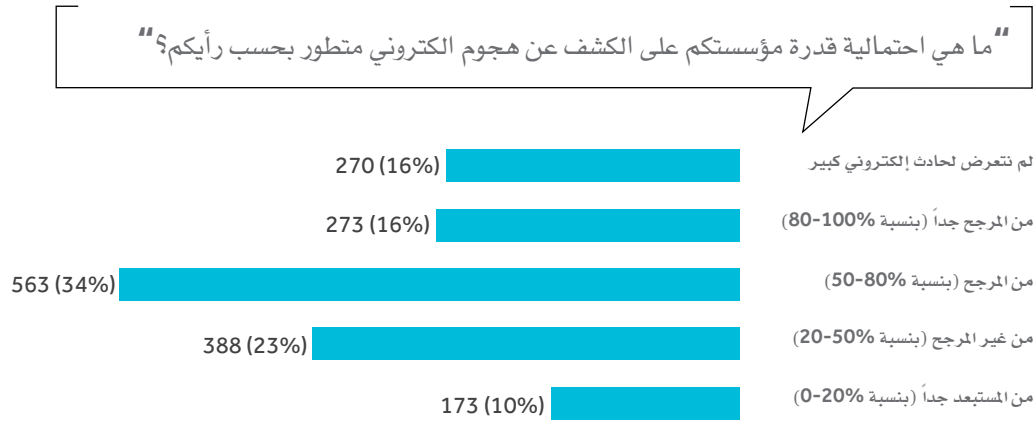
وقد تم الاستمرار في استخدام برامج جدار الحماية (Firewalls) ولكن مع إضافة أساليب جديدة، مثل الحماية من عدم فقدان البيانات، وذلك لتَتَبُّع وحماية المعلومات وهي تنتقل عبر الشبكات. ولكن هذه الإجراءات والبرامج لم تعد توفر الحماية الكافية ضد الهجمات الإلكترونية.

وقد بدأت المنظمات تُدرك بأن الوسائل والتكنولوجيا التقليدية التي تتبعها من أجل الإجراءات الأمنية، مثل برامج الحماية (Firewalls)، أصبحت غير مُجدية وبدأت تفشل في توفير الأمن في النظام الإلكتروني، وهناك حاجة مُلحة لوجود برامج جديدة ومتكاملة للكشف عن عمليات الاختراق.

وفي الاستبيان السنوي حول أمن المعلومات العالمية (GISS) لعام 2017، والذي أجرته إرنست ويونغ (EY) على 1735 من كبار المسؤولين التنفيذيين لتكنولوجيا المعلومات، وجدنا بأن الغالبية العظمى من المتخصصين في مجال الأمن الإلكتروني لم يعتمدوا بعد على البرامج المدروسة والمتطورة في الكشف عن عمليات الاختراق. وبالمثل، فإنه لم يتم اعتماد تقنيات متقدمة، على نطاق واسع، للكشف عن البرامج الضارة والاختراقات.

الحماية والمرونة التقليدية	الحماية والمرونة الإلكترونية
التركيز على الجوانب الفنية والتقنية للتعافي من الكوارث	اعتماد منهج شمولي لمواجهة التهديدات التخريبية والرد عليها
مُوجهة من قِبل اللوائح والأنظمة الخارجية	مُوجهة من قِبل توقعات العملاء وإنتاج القيمة
مدعومة من قِبل النظم القديمة	مدعومة من قِبَل تقنيات ذكية ومتطورة
تبادل المعرفة مُقتصر داخل الشركة	تبادل المعرفة بشكل سلس بين الشركات والجهات الحكومية
إعداد خطة التعافي من الكوارث داخل حدود المنظمة	إعداد خطة ذات تغطية أوسع تمتد خارج حدود المنظمة لتشتمل على الأشخاص والمجتمع
اعتماد منهج تفاعلي	اعتماد منهج استباقي وفعّال
حدوث معظم الكوارث بسبب أعطال فنية	تحديد ومعالجة الأسباب المؤدية إلى حدوث التعطيل
معظم العمليات يدوية	تشغيل العمليات بشكل آلي ومتكامل
العمل باستمرار على التحسين	الابتكار المستمر وإعادة الهيكلة

استبيان إرنست ويونغ (EY) السنوي حول أمن المعلومات العالمية (GISS)، لعام 2016



تعد النماذج التقليدية للاستمرارية التشغيلية غير قادرة على توفير الحماية الكافية للحكومات التي تحولت إلى النظام الرقمي، ويعود ذلك لمجموعة الأسباب التالية:

- عدم إمكانية استرجاع المعلومات الصادرة عن مصادر متنوعة والتي يصل إليها العديد من المستخدمين. وعدم قدرة تلك النماذج على تحديد أصول البيانات الهامة أو العثور عليها أو تتبع الكيفية التي تتدفق من خلالها عبر الأنظمة الرقمية.
- الافتقار إلى القدرة على التوقع المُسبَق لحدوث اختراق أمني إلكتروني.
- عدم القدرة على التكيف مع المتطلبات المُعقدة التي تختلف باختلاف الموقع.
- عدم القدرة على التعامل مع دمج العديد من أصحاب المصلحة وسلاسل الإمداد المعقدة.

ويتطلب التطور السريع في التهديدات الإلكترونية وجود آلية لاستشعار المخاطر الناشئة ومقاومتها، وهذا لا يمكن تحقيقه إلا من خلال استراتيجية المرونة الإلكترونية.

المرونة الإلكترونية في العصر الرقمي

يمكننا تعريف المرونة بأنها القدرة التنظيمية على استشعار الأحداث المتعلقة بالتهديدات الإلكترونية التخريبية ومقاومتها والرد عليها وضبط العمليات وإعادة تشكيلها في مختلف البيئات التي تتواجد فيها المخاطر، سواء كانت مخاطر متوقعة أو غير متوقعة. وتنشأ المخاطر غير المتوقعة عندما تكون وتيرة التغيرات التكنولوجية والرقمية سريعة للغاية؛ الأمر الذي يُشكل تحدياً جدياً للتنبؤ بالعديد من المخاطر التي تنشأ في المجال الرقمي.

تشتمل المرونة الإلكترونية على كل من الأمن الإلكتروني والمرونة التنظيمية، وتهدف إلى صد الهجمات الإلكترونية المحتملة وضمان البقاء والاستمرارية حتى بعد حدوث أي هجمات.

تطور نماذج المرونة

1 النسخ الاحتياطي للمعلومات والبيانات

نظراً للوعي بالأحداث التخريبية المحتملة ضد الأعمال والشركات وما يتبعها من كوارث؛ فلا بد من إجراء عملية النسخ الاحتياطي للبيانات والمعلومات حتى يُمكن استرجاعها وإعادتها إلى أفضل حالاتها الممكنة بعد وقوع أي هجوم تخريبي.

2 التعافي من الكوارث

يكمن الهدف من عملية التعافي من الكوارث في حماية الأنظمة الفنية أكثر من تقديم الحماية إلى الجوانب التنظيمية أو جوانب الأعمال الأخرى.

3 إدارة الأزمات

لقد تطور هذا المجال، منذ أواخر الثمانينيات وحتى التسعينيات من القرن الماضي، ليأخذ في اعتباره العوامل الخارجية من خلال التركيز على الدروس المستفادة أكثر من إدارة الأزمات. وتختلف منهجية إدارة الكوارث من حيث التركيز المبدئي والداخلي والوقائي والتعامل مع إجراءات الوقاية ومنع الكوارث وإجراءات التعافي منها.

4 إدارة استمرارية الأعمال

لقد تم تطوير طريقة التفكير القائمة على القيم وتركيزها نحو إدارة استمرارية الأعمال، حيث تم توسيع النطاق ليضم كامل المؤسسة أو الشركة، بمن في ذلك الموظفين.

5 المرونة المؤسسية

بعد إلقاء نظرة شاملة وسريعة على العناصر الأساسية والحوكمة والقيادة والكفاءات والقدرات اللازمة للمساعدة في إحداث أثر كبير، توصلنا إلى أربع مراحل لازمة للحد من وقوع المخاطر وتخفيض التكاليف وتحقيق أفضل العائدات، وتتمثل هذه المراحل فيما يلي:

- الاستشعار والتوقع
- الإعداد والتخطيط
- الاستجابة والتعافي
- التعلم والتكيف

وبالتالي، معالجة مواطن الضعف وأوجه القصور المختلفة الخاصة بنموذج المرونة التقليدي.

إن مواجهة المخاطر الوطنية والقطاعية والترويج لمرونة المؤسسات والشركات والأفراد من شأنها جميعاً أن تساهم في تعزيز الأمن الوطني.

ويُمكن تحقيق الأمن الوطني والقطاعي من خلال توسيع الحوافز والمكافآت الحكومية من أجل مواجهة المخاطر الوطنية والقطاعية وتحقيق مرونة للشركات والمؤسسات والمجتمعات والأفراد ككل. وتعتبر المرونة الإلكترونية عنصراً حاسماً في تطور الحكومات الرقمية ضمن إطار نموذج المرونة الوطنية والقطاعية.

وهناك تساؤل رئيسي يتمثل في كيفية تمكّن المؤسسات أو الشركات من تحقيق استدامة ومرونة في العمليات التشغيلية التي تجري في النظام الإلكتروني، وذلك لأن على تلك الشركات اتخاذ القرار بشأن كيفية تحقيق نتائج أعمالها ضمن إطار هذا النظام الذي -في وجوده- لا يمكن افتراض البقاء الفردي في العالم الرقمي.

وسيكون لوجود استراتيجية فعالة للمرونة الإلكترونية نتائج مهمة على التكاليف الخاصة بالحكومة والقطاع الخاص، وقد تصبح المؤسسات والشركات مترددة في الالتزام بالمزيد من النظم واللوائح القانونية، ولكن هناك اتفاق بين العديد من المؤسسات والشركات التي تحتاج إلى مضاعفة الإشراف والرقابة الحكومية، لا سيّما عند وجود نظام إلكتروني أكثر أمناً وسلامة يؤدي إلى انخفاض التكاليف على المدى الطويل.

ويُمكن للحكومة أن تمد يد العون من خلال ضمان وجود بيئة تنافسية أقوى للشركات التي تقدم خدمات الأمن الإلكتروني، وذلك من خلال تصميم وإعداد سياسات تعليمية لتعزيز وجود المتخصصين في المجال الإلكتروني.

تستطيع الحكومات التركيز أكثر على إعداد استراتيجية قوية للمرونة الإلكترونية عند افتراض أنه يتم تمويل المبادرات والمشاريع الإلكترونية بشكل كاف، وهذا يعني تطوير القدرة على الاستشعار والمقاومة وجعلها جزءاً من آليات ما قبل وقوع الحوادث التخريبية وبذلك تمكين الشركات والمؤسسات من الكشف عن المخاطر الحديثة. وتحتاج الحكومات من أجل معالجة الهجمات الإلكترونية وتحقيق المرونة الإلكترونية إلى وضع إطار عمل وتسهيل إنشاء نظام إلكتروني آمن يشتمل على البنية التحتية الأساسية ودعم مرونة القطاعات. وقد يتضمن ذلك وضع إطار عمل وطني لإدارة المخاطر الإلكترونية وبرامج وطنية لمعرفة نقاط الضعف والمجالات الأكثر عُرضة للهجوم الإلكتروني والتعاون القطاعي ووجود آليات لتبادل المعلومات المتعلقة بالتهديدات الإلكترونية.

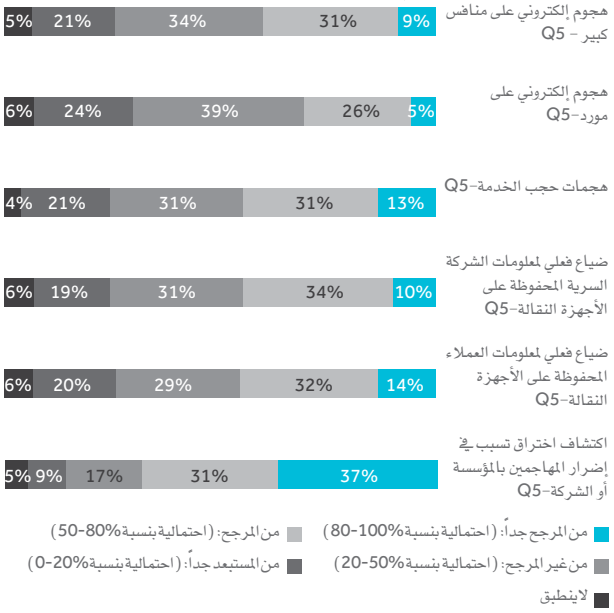
وقد قامت بعض المنظمات بتحسين قدراتها الاستشعارية بصورة كبيرة في السنوات القليلة الماضية، حيث استخدمت المعلومات المتوفرة عن التهديدات الإلكترونية من أجل التنبؤ بالهجمات الإلكترونية القادمة، كما اعتمدت على استخدام آليات وأجهزة مراقبة مستمرة (مثل مراكز العمليات الأمنية) وتحديد وإدارة نقاط الضعف والمجالات الأكثر عُرضة للتهديدات الإلكترونية، إضافةً إلى استخدام وسائل حماية فعّالة.

ووفقاً لاستبيان إرنست ويونغ (EY) السنوي حول أمن المعلومات العالمية (GISS) لعام 2016، فقد ظهر بأن المؤسسات والشركات أصبحت تتمتع بمزيد من الثقة في قدرتها على التنبؤ بالهجمات الإلكترونية القوية والكشف عنها، حيث أظهر الاستبيان أن 50% ممن أُجري عليهم الاستبيان يعتقدون بأنه من المحتمل أن يكونوا قادرين على فعل ذلك؛ وهو أعلى مستوى ثقة شهدناه منذ عام 2013. وبالرغم من ذلك، إلا أنه يبدو واضحاً بأن العديد من الشركات والمؤسسات لم تقم بإنشاء هياكل وإجراءات أساسية لاستشعار ومقاومة الهجمات الإلكترونية. فقد أوضح 44% ممن أُجري عليهم الاستبيان بأنهم لا يملكون مراكزاً للعمليات الأمنية، بينما أوضح 64% بأنهم لا يملكون برامجاً رسمية للمعلومات المتعلقة بالتهديدات الإلكترونية. بالإضافة إلى ذلك، فقد أوضح 55% بأنهم لا يملكون القدرة على تحديد نقاط الضعف والمجالات الأكثر عُرضة للهجمات الإلكترونية.

وهناك دليل آخر على عدم الاستعداد للمرونة الإلكترونية؛ فقد أوضح 62% ممن شملهم الاستبيان ذاته من المؤسسات بأنهم لم يقوموا بزيادة إنفاقهم على الأمن الالكتروني لولا تعرضهم إلى اختراقات أمنية وإن لم تُلحق بهم أي أضرار.

وتكمن المشكلة في أن مرتكبي الجرائم الإلكترونية كثيراً ما يقوموا بعد حدوث الاختراق بإجراء »هجمات اختبارية« أو »خامدة«، أو أن يقوموا بإجراء اختراق آخر كوسيلة تضليلية؛ لذلك فإنه يتعين على المنظمات افتراض أن الأضرار ستحدث في كل الأوقات طالما أن هناك هجمات إلكترونية، وإن لم يتم العثور عليها فإنه ينبغي على هذه المنظمات النظر إلى امكانية أن هذه الأضرار قد حدثت بالفعل ولكنها لم تظهر بعد.

"ما هي احتمالية أن يُشجع أي من الأحداث التالية مؤسستكم أو شركتكم على زيادة ميزانيتها الخاصة بأمن المعلومات خلال الأشهر الـ 12 المُقبلة؟"



دور القيادة

يعتبر دور كل من القيادة التنفيذية والدعم والإسناد دوراً حاسماً فيما يتعلق بالمرونة الإلكترونية الفعالة. وعلى عكس أنشطة "الاستشعار" و"المقاومة" التقليدية التي يُمكن اعتبارها بأنها مجال عمل خاص بمدير إدارة أمن المعلومات أو من يعادله في المنصب في مرحلة "التفاعل" والاستجابة، فإن المرونة الإلكترونية تتطلب وجود غيره من كبار المسؤولين التنفيذيين في القيادة الفعالة والقيام بدور أكثر نشاطاً. وقد أظهر استبيان إرنست ويونغ (EY) السنوي حول أمن المعلومات العالمية (GISS)، في عام 2013، بأن الثلث ممن أُجري عليهم الاستبيان تقريباً قد ذكروا بأن هناك نقص في الوعي التنفيذي والدعم لاستراتيجية الأمن الإلكتروني. وهذا يُشير إلى أن المؤسسات والشركات لا تعمل بشكل كاف لضمان قيام كبار المسؤولين التنفيذيين بدورهم في قيادة وتحقيق المرونة الإلكترونية.

تأمين النظام الإلكتروني

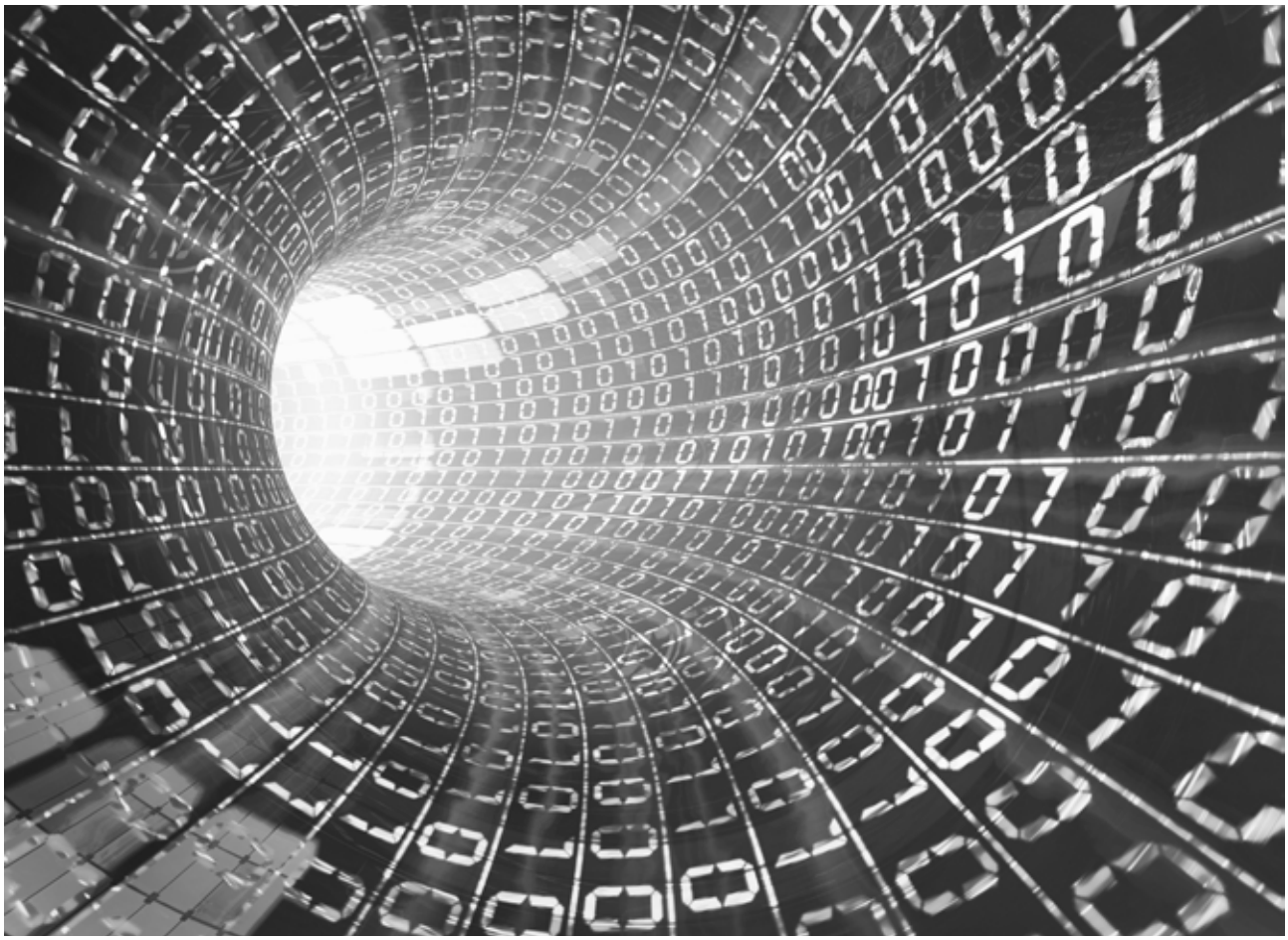
إن الهجمات الإلكترونية في البيئة السائدة هذه الأيام والتي تحدث ضد الأنظمة الإلكترونية الخاصة بالمورّدين والعملاء والجهات الحكومية من شأنها التأثير على المؤسسة أو الشركة نفسها، الأمر مما يشكل مجالاً رحباً للمخاطر التي غالباً ما يتم إهمالها والتغاضي عنها، وذلك كما أظهر استبيان ارنست ويونغ المذكور. فقد أوضح 68% ممن أُجري عليهم الاستبيان أنهم لن يقوموا بزيادة الإنفاق على أمن المعلومات حتى وإن حدثت هجمات إلكترونية ضد أحد الموردين. وبشكل مماثل، فقد أوضح 58% بأنهم لن يزيدوا إنفاقهم على أمن المعلومات ما لم تحدث هجمات إلكترونية كبيرة ضد أحد المنافسين الكبار. وما زال مرتكبي الهجمات الإلكترونية يفضلون مهاجمة المؤسسات والشركات التي يشابه بعضها بعضاً وذلك باستخدام أساليب وتقنيات كانوا قد تعلموها من خلال تجاربهم الماضية خلال إجراء الهجمات الإلكترونية.

الأثر المترتب على انترنت الأشياء

إن ظهور إنترنت الأشياء "Internet of Things" والنمو السريع في عدد الأجهزة المرتبطة به سيشكل تحدياً لقدرات استشعار المخاطر لدى المؤسسات والشركات؛ فسيصبح من الصعب تحديد وتتبع حركة البيانات المشبوهة في الشبكات العاملة وتحديد هوية الأشخاص الذين يقومون بالدخول إلى هذه البيانات، وهذا بدوره سيشكل صعوبة أكثر أمام تحديد أي جزء من البيئة الإلكترونية سيؤثر على المؤسسة أو الشركة وما الأجزاء التي لن تؤثر عليها.

وستصبح الأجهزة في المستقبل قادرة على العمل مع بعضها البعض في الوقت نفسه، وذلك للتنبؤ بالهجمات الإلكترونية ومنعها والحد من انتشار هذه الهجمات على امتداد الأجهزة المشاركة، وتقليل الآثار المترتبة عليها وإعادة الأمور إلى ما كانت عليه قبل حدوث الهجمات. ولا بد من وجود القدرات الأمنية في الأجهزة الإلكترونية لتكون قادرة على ممارسة الأنشطة الوقائية والدفاعية وبالتنسيق مع بعضها البعض ومع مجموعة واسعة من الأجهزة الأخرى.

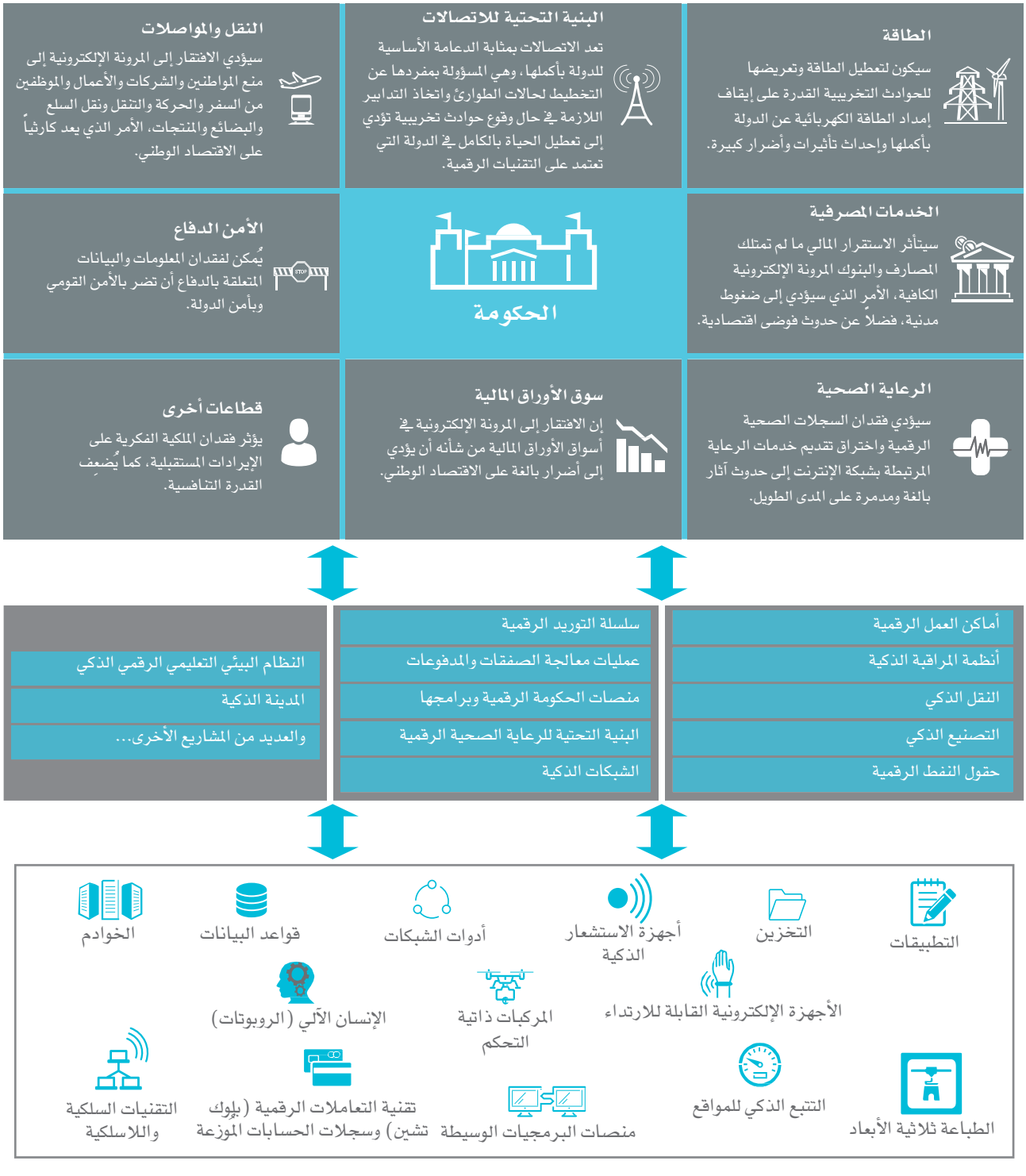
وفي سياق النظام الإلكتروني، سيعتمد مدراء النظام على تطبيقات الحاسوب التي تقوم بالكشف عن نقاط الضعف الأمنية المعروفة والمجالات الأكثر عُرضة للهجوم، والإبلاغ عنها بصورة تلقائية في الشبكات الإلكترونية العاملة. وفي بعض الحالات، يقوم المسئولين بإصلاح مركز الضعف وأوجه القصور الأمنية التي يتم الكشف عنها وذلك بصورة تلقائية أيضاً.



إنشاء نظام إلكتروني مرن

كلما تطورت التهديدات الإلكترونية وازدادت؛ سترى الحكومات بأن الطرق والأساليب التقليدية لأمن المعلومات ستُثْبِت بصورة متزايدة أنها غير كافية للقيام بمهمة حماية المنظمات، كما أن المنظمات الفردية ستحتاج إلى إنشاء خط الأساس لأمن المعلومات والبيانات لديها، ولكنها ستدرك حينها بأنها لا تستطيع تحقيق الأمن التام من خلال اعتمادها على نفسها فقط.

لذلك، ستلجأ هذه المنظمات إلى العمل مع شركاء موثوقين يمكن الاعتماد عليهم لحماية الأنظمة الإلكترونية. ويعد النظام الإلكتروني المرن واحداً من الأنظمة الموثوقة في حماية النظم والمعلومات والتي تعمل هذه المنظمات من خلاله.



وينبغي على المؤسسات والشركات، من أجل القيام بذلك، النظر إلى المحيط الخارجي لتقييم أثر الهجمات الإلكترونية التي تحدث ضد الشركاء أو الموردين أو الوكلاء أو الأطراف المعنية الأخرى. كما ينبغي أن يتم تشجيع المواطنين من ذوي الاختصاص في المجال الإلكتروني على التعاون مع الأطراف الأخرى من أجل تطوير أنظمة إلكترونية آمنة ومرنة، وذلك من خلال التفاعل معهم وتبادل المعلومات، ولكن مثل هذا التعاون يتطلب التزاماً راسخاً بالمرونة الإلكترونية وتعزيز السلوكيات السليمة في مجالات قيادة المرونة الإلكترونية والشراكات الخاصة بها والاستعداد للتغيير، كما يتطلب ذلك التزاماً راسخاً من الأفراد والقادة لتحقيق هذه الأهداف.

وتقوم الحكومات والمنظمات الكبرى بوضع أطر عامة للسياسات والممارسات الخاصة بتطوير الأنظمة الإلكترونية المرنة. وتتسم فكرة التعاون مع الشركاء بالبطء الشديد نظراً لصعوبة تنفيذها. ويجب على المنظمات في الوقت نفسه أن تضمن بأنها تقوم بتطوير قدراتها في أمن المعلومات بشكل يُمكنها من معالجة المخاطر المحيطة بها.

الخصائص الرئيسية للمؤسسات ذات المجال الإلكتروني المرن

فهم طبيعة عمل المنظمة بأكملها: تتطلب المرونة الإلكترونية حلاً شاملاً يغطي المنظمة بأكملها، لأن أنصاف الحلول لا تُجدي نفعاً. وهذا يبدأ بالفهم العميق للبيئة التشغيلية داخل المنظمة لمعرفة مهام سير العمل التي يجب الحفاظ عليها لتتمكن المنظمة من الاستمرار في عملها في حالة حدوث هجمات إلكترونية، والحفاظ على الموظفين والأصول الرئيسية في الوقت نفسه.

فهم النظام الإلكتروني: لا بد من تخطيط وتقييم العلاقات الخارجية للمنظمة على امتداد النظام الإلكتروني وتحديد المخاطر حيثما وجدت، وإجراء تقييم للمخاطر التي تدور حول دور المؤسسة في النظام الإلكتروني، بالإضافة إلى تحديد العوامل المؤثرة على مدى سيطرة المنظمة على نظامها الإلكتروني.

تحديد الأصول الأكثر أهمية: تقوم معظم المؤسسات بالإفراط في حماية بعض الأصول، بينما تهمل أصولاً أخرى. وقد أظهر استبيان ارنست ويونغ أن أكثر من نصف من أُجرِيَ عليهم الاستبيان قد صنفوا المعلومات الشخصية للعملاء معروفي الهوية كمعلومات مهمة في المؤسسة وذات قيمة أكبر لمرتكبي الجرائم الإلكترونية، بينما صُنّفَت الملكية الفكرية لبراءات الاختراع أنها ذات القيمة الأكبر من قِبَل 11% فقط.

تحديد مسببات المخاطر

يُمكن للجهات المسؤولة عن الأمن الإلكتروني أن تحقق نجاحاً محدوداً في حال عدم امتلاكها لرؤية شاملة حول بيئة المخاطر والتهديدات الإلكترونية، وهذا يتطلب منها التعاون مع الجهات الأخرى في النظام الإلكتروني.

إدارة العنصر البشري

يجب أن يكون الأفراد، في حال التعرض للهجمات الإلكترونية، على استعداد كاف ودراية بكيفية التعامل مع هذه الهجمات والتكيف معها، وهذا يتطلب إجراء اتصالات واضحة داخل وخارج المؤسسة، كما يجب على المدراء والقادة في الوقت نفسه وضع نموذج قوي لكيفية التعامل مع هذه الأزمات عند حدوثها.

نشر ثقافة الاستعداد للتغيير

ستقلل الاستجابة السريعة للهجمات الإلكترونية من إمكانية حدوث أثار ملموسة على المدى الطويل؛ فالمؤسسات التي تستجيب بصورة سريعة يكون لديها خطة قوية جداً لإدارة الأزمات والتدريب عليها وامتلاك القدرة على الاستعانة بالموارد في كافة أقسامها. وتستطيع المنظمات من خلال تمارين المحاكاة أن تختبر وتجرّب الخطط الحالية لإدارة الأزمات وتطبيق الممارسات الجارية وحصر المخاطر المحيطة بها، وذلك لضمان أنها تتوافق بالكامل مع استراتيجية المؤسسة وقدرتها على تحمل المخاطر.

وضع خطة عمل لإنشاء نظام إلكتروني مرن

ينبغي على الحكومات مواكبة التغييرات التكنولوجية المتسارعة بينما تقوم بالاستعداد لدخول العصر الرقمي، وهذا سيساعدها على تبني وتأمين هيكل تنظيمي يتسم بالمرونة التي تمكنه من التكيف مع أعطال النظام وإمكانية التشغيل البيني والانفتاح الرقمي من البداية إلى النهاية.

ويجب تعزيز التصميمات والحلول المتقدمة من أجل تبادل الدروس المستفادة وتبني المعايير المتعارف عليها، كما يجب تبني أسلوب عمل متناسق من أجل تحسين المحتوى والمعلومات والبيانات التي يتم عرضها عبر مختلف القنوات. وهذا من شأنه أن يضمن الخصوصية والسرية في العصر الرقمي المتعرض للمخاطر. ويجب كذلك تطبيق نموذج محدد للخدمات في جميع الإدارات والوزارات والأعضاء ذوي الصلة.

سمات المرونة الرئيسية للحكومة الإلكترونية

قيادة المرونة

- الالتزام المثالي القائم على التنفيذ من أجل تأسيس الحكومة الإلكترونية المرنة.
- التشاور بشأن أنماط الحوكمة غير الاعتيادية والمساعدة على اتخاذ القرارات بصورة سريعة وحاسمة وعادلة عند حدوث الهجمات الإلكترونية.

ثقافة المرونة

- دعم تطبيق منهج "one-in, all-in approach" في كافة أنحاء الحكومة وتشجيع سلوكيات المرونة الإلكترونية من أجل التعاون والحذر وروح المبادرة والاستعداد للتعلم من الفشل والأحداث التخريبية، إن وُجدت.

الشبكات المرنة

- دعم وتقوية العلاقات القائمة على الثقة مع الأطراف الأخرى (بما في ذلك شركاء الأعمال والمواطنين والجهات المعنية الأخرى) لزيادة القدرة على الصمود في وجه المخاطر والتهديدات الإلكترونية وتسريع التعافي منها.

الاستعداد للتغيير المرن

- استعداد الإدارات المدعمة بالتدريب والأدوات والوسائل والتقنيات التي تساعد على الكشف السريع عن المخاطر والتهديدات الإلكترونية والتعامل والتكيف معها في سياق أمني متغير على الدوام.

تحتاج الحكومات إلى تتبع وتقييم سمات المرونة الإلكترونية في كافة الفروع التنفيذية؛ فهذه السمات ستظهر كيف أن المؤسسات والشركات تتمتع بمرونة في قدرتها على التنبؤ بالتهديدات الإلكترونية لأمن المعلومات. كما أن هذه الحكومات والشركات والمؤسسات تحتاج إلى إدارة المخاطر ذات الأثر الكبير والاحتمالية المنخفضة والحصول على نتائج مثالية في البيئة الرقمية، وهذا يمكن تحقيقه فقط من خلال اتباع نهج شامل للمكونات والحوكمة والقدرات القيادية المطلوبة لإدارة هذه الأنواع من المخاطر. وتضمن المرونة الإلكترونية وجود قدرة مستمرة للتكيف مع التغييرات التي تجري في الأعمال والبيئة الخارجية.

يتكون مخطط المرونة الإلكترونية من العناصر الخمسة التالية:

1. اتباع نهج شامل

ينبغي على أصحاب القرار في الحكومة وعلى جميع المستويات السعي إلى تثقيف أنفسهم حول موضوع التهديدات الإلكترونية. فلم يعد بإمكان أصحاب القرار افتراض أن المشتريات الخاصة بتقنية أمن المعلومات أو أحد برامجها ستعالج هذا التحدي. ويتطلب ازدياد التعقيد في التهديدات والهجمات الإلكترونية منهجاً أكثر شمولية من أجل الحماية منها. ويجب أن تركز استراتيجية المرونة الإلكترونية على السلوكيات الخاصة بجميع الأطراف المعنية، وليس فقط على فرق أمن المعلومات.

وتبدأ الجهات الحكومية حالياً في وضع أطر عمل وطنية تهدف إلى توفير أساس قانوني يقوم عليه تنفيذ النظام الإلكتروني المرن. وعلى المستوى التنظيمي؛ فلا بد من المضي خطوة إلى الأمام من أجل إلزام الجهات الحكومية باستخدم العمليات الإلكترونية المرنة في إطار النظام الإلكتروني والالتزام كذلك بالشفافية والوضوح. وستساعد أدوات الحوكمة والمخاطر والامتثال القانوني في الكشف عن نقاط الضعف والمجالات الأكثر عُرضة للتهديدات الالكترونية.

2. الاستفادة من الشبكات الإلكترونية المرنة

تستطيع الحكومات، من خلال المعلومات الموحدة والمترابطة وذات المرجعية الواحدة في جميع الأنظمة، من أن تضع خط الأساس للسلوكيات الطبيعية في الأنظمة والشبكات الإلكترونية، كما يمكنها أيضاً دمج هذه المعلومات والكشف عن حالات التسلل الإلكتروني والتعامل مع التكنولوجيا لتحديد الأنشطة الإلكترونية المشبوهة وغير الطبيعية. كما يُمكن للحكومات أيضاً الاستفادة من العمليات التشغيلية الآلية لمساعدتها في الكشف عن الهجمات الإلكترونية في الوقت المناسب وتمكينها من التعامل بشكل مُسبَق مع التهديدات الأمنية لإلكترونية. ويُمكن أيضاً لخدمات المعلومات الإلكترونية القائمة على تقنية الحوسبة الرقمية أن تُساعد في الكشف المبكر عن التهديدات الإلكترونية المستمرة وتوظيف الأفراد المؤهلين والمدربين من أجل العمل كأدوات استشعار بشرية لكشف ومواجهة هذه التهديدات.

3. القدرة على الاستعداد للتغيير

تحتاج الحكومات إلى أساليب وتقنيات وآليات تساعدها في التعامل بشكل سريع وذكي مع التهديدات المتنامية والهجمات الإلكترونية لأمن المعلومات، ويتضمن ذلك ما يلي:

- فرض حماية على المعلومات والبيانات اللامركزية أو بالقرب منها بشكل وثيق قدر الإمكان، مثل حلول وبرامج إدارة حقوق المعلومات، حيث يتم فرض ضوابط أمنية داخل ملفات البيانات نفسها.
- استخدام آليات وأدوات لامركزية وقابلة للتكيف للكشف عن التسلل الإلكتروني والتعامل معه، وأن تكون مُدمجة في الأجهزة والشبكات العاملة.
- تحقيق المرونة الإلكترونية للنظام ككل في الأجهزة والشبكات العاملة وتمكينها من العودة إلى "الوضع الآمن" عندما تصبح هدفاً لهجمات إلكترونية متقدمة.
- إمكانية الاتصالات الآلية بين الأجهزة والشبكات العاملة وتمكينها من الرد بشكل مبرمج مع السلوكيات المشبوهة أو المشكوك في أمرها.
- استخدام أجهزة استشعار للكشف عن الهجمات الإلكترونية، بحيث ترسل تنبيهات آلية لمراكز العمليات الأمنية، ويمكنها المشاركة مع فرق عمل الطوارئ الإلكترونية الحكومية وشركات المعلومات وجهات تنفيذ القانون.

القيمة الناتجة عن المرونة الإلكترونية

تظهر الفائدة الكبرى والحقيقية من النظام الإلكتروني المرن عند التعرض للمخاطر وحدوث هجمات إلكترونية، وذلك بسبب قدرته على التعافي منها وتجاوزها والرجوع إلى الوضع التشغيلي الأول، وذلك لأن هناك مراقبة وسيطرة في النظام والشبكة يمكنهما من التعامل بشكل سريع مع التهديدات والمخاطر الإلكترونية.

وفي حالة حدوث الهجمات الإلكترونية فإن النظام الإلكتروني الحكومي المرن يستطيع الاستمرار في إجراء المهام الكبرى، والحفاظ على سرية المعلومات وسلامتها وضمان بقائها في نفس الوقت. وفي حال تعرض النظام لمخاطر إلكترونية، فيمكنه الاستمرار في معالجة البيانات كذلك.

1 تجسيد الشعور بالقدرة على مواكبة العمل عند حدوث الأزمات

يساعد ذلك على وضع حلول شاملة للدولة ضمن جهودها المبذولة لتوفير واختبار وتحسين القدرات على مواكبة العمل في حال حدوث هجمات إلكترونية أو حوادث تخريبية.

2 توفير فرص التحسين والتطوير

يساعد ذلك على مواصلة تطبيق الأسلوب المتبع من الدولة في سبيل التجريب والتحسين والتطوير بصورة مستمرة للبدء في تنفيذ آلية المرونة الإلكترونية.

3 المساعدة في تحديد مواطن الضعف أو المخاطر

العمل على تطوير منهج "one-in، all-in approach" وتبني ثقافة الاستعداد للتغيير في جميع الجهات الحكومية؛ لمساعدتها في تحديد مواطن الضعف وأوجه القصور في برنامج المرونة الإلكترونية الخاص بها.

4 القدرة على الاستمرارية بشكل سلس

الاستفادة من الموارد البشرية والإجراءات والفرص التكنولوجية لإعادة تشكيل البيئة الإلكترونية والاستقرار والنمو المستقبلي بعد تكرار حدوث الهجمات الإلكترونية.

5 التغطية الأوسع للمرونة الإلكترونية

تجمع المرونة الإلكترونية بين عدة مجالات، بما فيها تقييم المخاطر وأفضل الممارسات التقنية وإدارة المعرفة وإدارة المخاطر وتنسيق الأدوار لكافة الإدارات والأقسام.

التوصيات

ستصبح الحكومات من خلال الأنشطة والمبادرات والسياسات الاستراتيجية قادرة على وضع الأساس للتحول الوطني الرقمي بطريقة آمنة وأسلوب مرن. وقد تم وضع التوصيات الواردة أدناه لتقديم النصح والإرشاد حول التوجه السياسي العام، فالأنشطة والأعمال التي تقوم بها كل حكومة من الحكومات ستعتمد على ظروف وأوضاع محددة.

ويجب على الحكومات الاهتمام بالتخطيط للربط بين الاستراتيجية الوطنية الرقمية والأهداف الأمنية الإلكترونية الخاصة بها؛ حيث أن هناك غرض واضح وهو بناء نظام إلكتروني مرن.

ويتمثل الجانب الرئيسي في القوى العاملة في المجال الرقمي، حيث أنها لا تقوم بتطوير وتحسين آفاق التوظيف في الدولة، ولكنها أيضاً تشكل ثقافة المرونة الإلكترونية في هذا المجال الرقمي.

ويجب عند تطبيق المرونة الإلكترونية الأخذ بعين الاعتبار المسائل القانونية والخصوصية والسرية على المستويين الوطني والدولي، كما ينبغي على كل حكومة أن تهدف إلى تحقيق التوازن السليم بين كثرة وقلة اللوائح والأنظمة في الوقت نفسه، على المستويين الوطني والدولي كذلك. كما ينبغي النظر في أطر العمل العالمية لتمكين الدولة من المشاركة في المؤسسات الدولية المُشارِكة في عمليات الأمن الإلكتروني.

ويتعيّن على الحكومات كذلك وضع إطار عمل للمساعدة في تحديد الأصول الرئيسية ومعايير حماية هذه الأصول (بطريقة مماثلة لتحديد الأصول الهامّة في البنية التحتية الوطنية)، وسيساعد هذا على تحديد الموارد وتوزيعها بشكل صحيح حسب الأولويات الأكثر إلحاحاً.

ويجب على الحكومات اتخاذ القرار بشأن مستوى المراقبة الإلكترونية التي ستقدمها وإلى أي الجهات ستقوم بتقديمها، ومن ثم وضع المعايير الخاصة بالمراقبة الإلكترونية لتلك الأصول غير المشمولة. وستوفر المراقبة الإلكترونية نظاماً يقوم بالكشف عن الهجمات الإلكترونية بشكل واضح، وبالتالي تسريع الرد عليها والتعامل معها والتعافي منها، فضلاً عن تعديل خطط المرونة الإلكترونية حيثما اقتضى الأمر.

ويجب أيضاً وضع إطار عام للمؤسسات والشركات بهدف التعاون فيما بينها على تبادل المعلومات حول التهديدات الإلكترونية، كما يجب أن تكون هناك برامج ومنصات إلكترونية لتوفير المعلومات حول مصادر هذه التهديدات؛ ليتم تبادلها بشكل فوري وسريع. ويُتيح ذلك فرصة القيام بمزيد من أنشطة التعامل الاستباقي مع هذه التهديدات وليس مجرد المراقبة الإلكترونية، كما يساعد على رفع الوعي بضرورة الحاجة إلى تفعيل خطط المرونة الإلكترونية.

ومن الضروري وجود معايير شاملة خاصة بأمن معلومات المؤسسات والشركات وقدرات تحليلية ورموز تشفير خاصة بها وكذلك الالتزام بشروط الدخول الإلكتروني، كما يجب على المؤسسات الحكومية أن تبدأ بتبني هذه الأمور ونشرها.

ويتعيّن على الحكومة أيضاً أن تركز بشكل أكبر على ضمان قيام المؤسسات والشركات بتطوير استراتيجيات مناسبة للمخاطر، تتضمن تحديد القدرة على تحمل المخاطر وكيفية التعامل مع التهديدات الإلكترونية. وتحتاج الإجراءات التشغيلية إلى أن تكون آمنة وسليمة بقدر الإمكان، وذلك من خلال الضوابط الداخلية والخارجية والخدمات والبرامج والمنصات الإلكترونية بهدف ضمان حماية العملاء والأصول واستمرارية الخدمات ذات القيمة المرتفعة.

الخاتمة

تواجه الحكومات تحدياً غير مسبوق لا يمكن التغلب عليه إلا من خلال توفير نظام إلكتروني مرن وآمن للأفراد والشركات والمؤسسات على حد سواء. ورغم ذلك فإن الصعوبات لا ينبغي أن تحول دون وجود مثل هذا النظام. ولا بد من اتخاذ خطوات حاسمة في أسرع وقت ممكن لأن التهديدات الإلكترونية في نمو مستمر، إلى جانب التطور السريع في المجالات الرقمية في معظم الدول.

ويتطلب الأساس الخاص بالمرونة الإلكترونية من الحكومات تخطي الحواجز التقليدية وتأسيس شراكات قوية مع القطاع الخاص، وذلك أيضا من أجل تعزيز ثقافة المرونة الإلكترونية. وتعد عملية إنشاء نظام للمرونة الإلكترونية عمليةً معقدة وصعبة وذات تخصصات متعددة لكل دولة، حيث تختلف متطلبات كل دولة بحسب الأوضاع الاجتماعية والقانونية والاقتصادية السائدة فيها.

لقد قمنا في هذا التقرير بتحديد بعض المشكلات والمسائل التي ستواجهها الحكومات، كما تم التطرق إلى أهم التوصيات حول كيفية بناء نظام إلكتروني مرن للدولة. ويكمن الهدف من ذلك في عرض مجموعة من الأدوات والآليات القابلة للتكيف مع التغييرات السريعة في العالم الرقمي. ونأمل أن يساعد ذلك الحكومات في الحصول على إطار عمل عام ومتماسك للتعامل مع التحديات الإلكترونية غير المتوقعة التي ربما تواجهها في المستقبل.

المراجع والمصادر

- 1"التكنولوجيا والقوى العاملة: مقارنة بين ثورة المعلومات والثورة الصناعية" ماثياس هومبيرت، جامعة كاليفورنيا، بيركيلي.
- يمكن الرجوع إلى أوراق عمل خاصة بإرنست ويونغ (EY) حول القيادة الفكرية كما يلي:
- "استبيان إرنست ويونغ (EY) حول أمن المعلومات العالمية 2013 – 2016" أو "GISS" وهو استبيان سنوي عالمي تقوم به إرنست ويونغ منذ 19 عاماً، ويغطي موضوعات حول الأمن الإلكتروني وآفاق التهديدات الإلكترونية وموضوعات جديدة ذات صلة في المجال نفسه. وقد تم إطلاق اسم "الطريق نحو المرونة الإلكترونية: الاستشعار – المواجهة– الاستجابة" على استبيان ارنست ويونغ حول أمن المعلومات العالمية «GISS» لعام 2016.
- "عوامل التغيير: كيف يمكن لحكومات "CTOs" قيادة التحول الرقمي" آراء وأفكار القطاع الحكومي والعام.
- "تجنب ضياع الجيل: رواد الأعمال الشباب يحددون خمسة أمور واجبة للعمل" أحد مؤلفات قمة تحالف رواد الأعمال الشباب في دول العشرين حول المرونة الإلكترونية.
- "كيف تقترب دول مجلس التعاون الخليجي من إغلاق الفجوة في المهارات؟" اختبار التحديات والفرص للحكومات لمعالجة الاتساع المتنامي في فجوة المهارات.
- "المواطن اليوم: توفير المستقبل الرقمي" كيف يقوم صناع السياسة في العالم باستخدام التكنولوجيا لتعزيز الخدمات العامة."
- "تصور المستقبل الرقمي" كيف تقوم التقنيات الرقمية بتحول الشركات في المجالات المهنية والصناعية.
- "هل تخلق التقنية الرقمية أزمة قدرات في القوى العاملة؟" تحديات جديدة في مجال القوى العاملة.
- "تقنية The Power of Three for Smarter، المزيد من مدن المرونة الإلكترونية"
- تحقيق المرونة الإلكترونية في النظام الإلكتروني"
- "المرونة الإلكترونية لسلسلة التوريد"
- "تقنيات إرنست ويونغ (EY) للمرونة الإلكترونية في العمليات التشغيلية"
- "المواطن اليوم: تعزيز الخدمات العامة من خلال التكنولوجيا"
- "استخدام الروبوتات لعمليات جعل الوظائف المالية تتم بشكل آلي في المستقبل"
- "في المستقبل عندما تكون البيانات متوفرة في كل مكان، من سيقوم بحفظها بعيداً عن الأيدي الخطأ؟"

المؤلفون

رداد أيوب

شريك مسؤول، إرنست ويونغ

رئيس قسم استشارات المرونة الإلكترونية،

أوروبا والشرق الأوسط والهند وأفريقيا (EMEIA)

البريد الإلكتروني: Raddad.Ayoub@ae.ey.com

كلينتون م فيرث

شريك مسؤول، إرنست ويونغ

رئيس قسم استشارات الأمن الإلكتروني،

منطقة الشرق الأوسط وشمال أفريقيا

البريد الإلكتروني: Clinton.Firth@ae.ey.com

محمد نياز

شريك مسؤول، إرنست ويونغ

رئيس قسم استشارات مخاطر تكنولوجيا المعلومات والمرونة الإلكترونية المؤسسية،

منطقة الشرق الأوسط وشمال أفريقيا

البريد الإلكتروني: Mohamed.Nayaz@om.ey.com