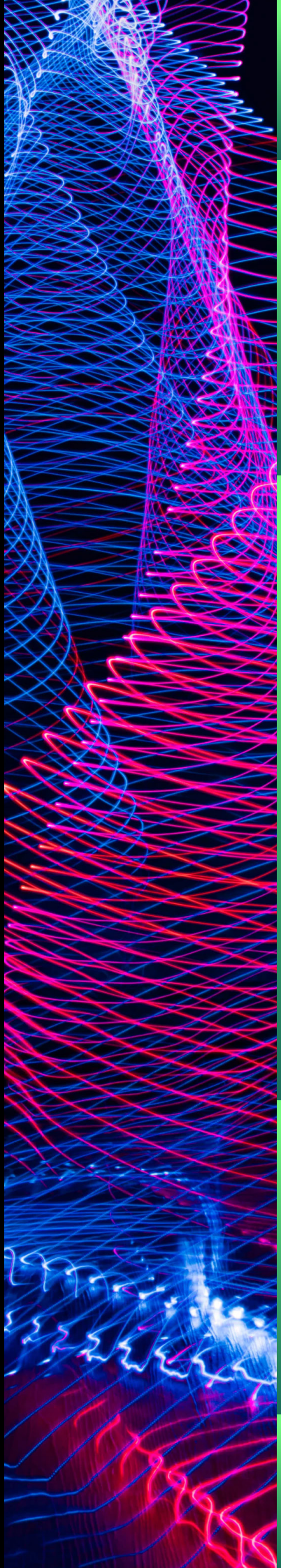
مؤسسة دبي للمستقبل
DUBAI FUTURE FOUNDATION

بالتعاون مع
شرطة دبي
DUBAI POLICE

رقمنة البنية التحتية الحيوية



سيناريوهات المخاطر والقدرة على الصمود في قطاع الخدمات المالية والمصرفية

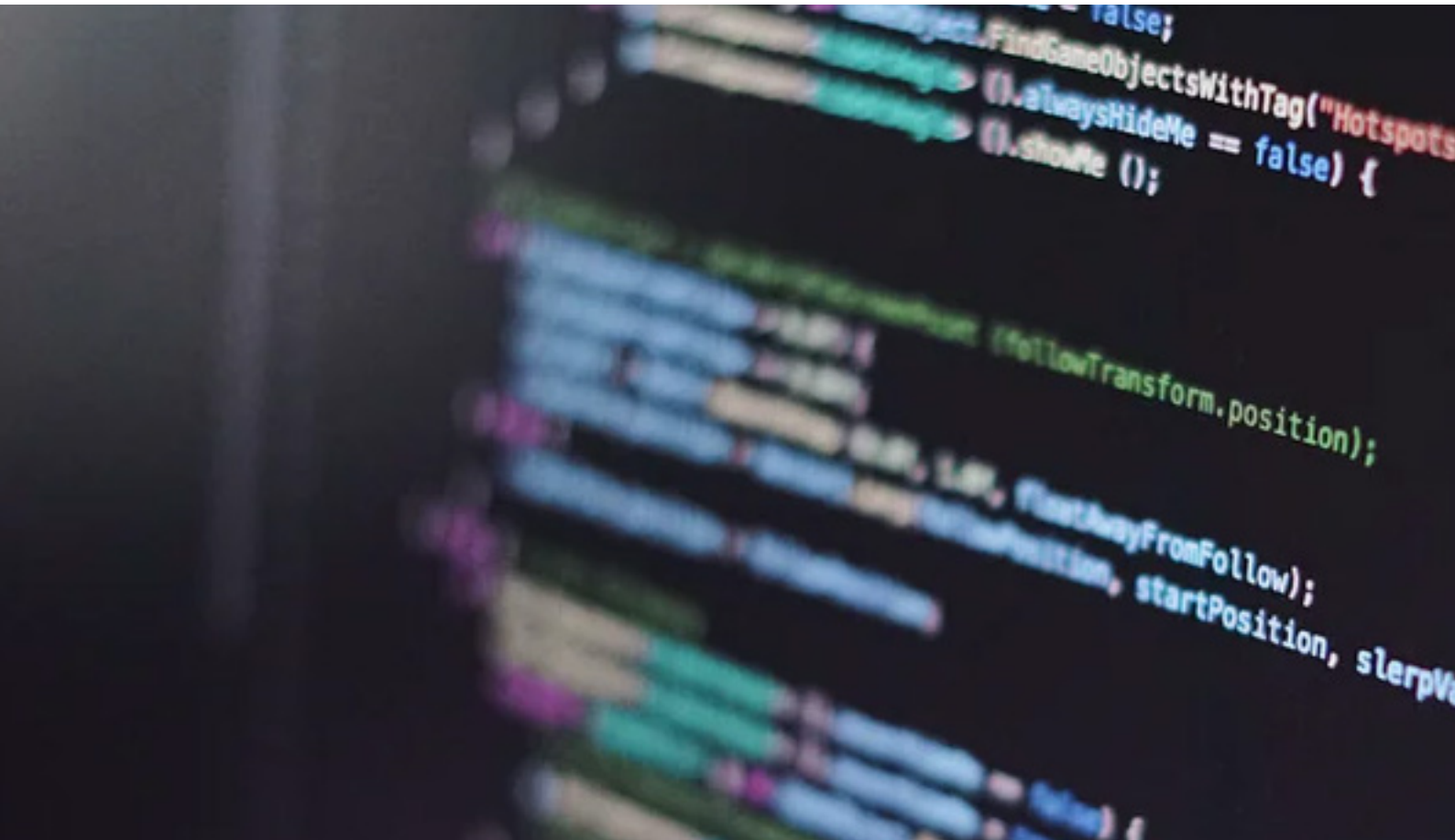
DUBAIFUTURE.AE

ينشر هذا التقرير بموجب ترخيص المشاع الإبداعي باستثناء النصوص أو الشعارات أو الصور التي تملكها جهات أخرى. يُسمح بنسخ محتوى التقرير وتوزيعه على أن تنسبه إلى مصدره الأصلي، وتبيّن إن أجريت عليه أي تغييرات، وتضيف رابطاً إلى الترخيص. يتوفر الترخيص على الرابط التالي
https://creativecommons.org/licenses/by/4.0/deed.ar

يستثني هذا الإشعار أيضًا على وجه التحديد العلامات التجارية لاسم مؤسسة دبي للمستقبل وشعارها من نطاق ترخيص المشاع الإبداعي.

اهتزّت الحكومات وقطاع الأعمال العام الماضي لدى اكتشاف أن برنامج أوريون الشهير الذي طورته شركة سولارويندوز الأمريكية قد تعرض للاختراق. وكان هذا الحدث خطيراً جداً لأن الشركة توفر خدمة مراقبة الشبكة وغيرها من الخدمات الفنية لمئات الآلاف من الهيئات والمؤسسات، منها معظم الشركات الخمسمئة الكبرى المصنفة في قائمة مجلة فورتشن، إضافةً إلى وكالات حكومية من مختلف أنحاء العالم. وأتاح الهجوم للمتسللين الدخول إلى شبكات تلك المؤسسات، ما جعل سرقة معلوماتها السرية أمراً ممكناً. ولم يكن الهجوم بحد ذاته المتسبب بالصدمة الكبرى بقدر ما كانت مدة الشهر التي انقضت قبل اكتشاف حدوثه.

وتعرضت ستة على الأقل من الإدارات الحكومية الأمريكية للاختراق، من بينها الطاقة والتجارة والخزانة والخارجية، بالإضافة إلى شبكات إدارة الأمن القومي النووي. وذكرت وسائل الإعلام أن العشرات من شركات الأمن والتقنية، إلى جانب منظمات غير حكومية خارج الولايات المتحدة، تأثرت أيضاً، وذلك في كل من كندا والمكسيك وبلجيكا وإسبانيا والمملكة المتحدة وإسرائيل ودولة الإمارات العربية المتحدة.



وليست تلك التهديدات أمراً جديداً، إذ يواجه العالم العديد منها باستمرار، وقد تأتي على هيئة كوارث طبيعية كالحرائق المستعرة والفيضانات والأعاصير والأوبئة العالمية، أو تكون من صنع الإنسان كالإرهاب وانقطاع سلاسل الإمداد والتوريد. وتتزايد طبيعة هذه التهديدات وقوتها بصورة متسارعة. لكن حين تؤثر على البنية التحتية الحيوية التي تعتمد عليها رفاهية المجتمعات، فإن ضررها يتفاقم، وخصوصاً عندما يكون قسم كبير من البنية التحتية لمجتمعنا قد انتقل بالفعل -أو ما زال ينتقل- إلى الفضاء الرقمي. ويلعب التخطيط المستقبلي دوراً حيوياً في معالجة المخاطر وتوظيف القدرة على الاستجابة للحوادث التخريبية غير المتوقعة. لذا يتعيّن على المؤسسات أن تتبنى التفكير المستقبلي لتعزيز حالة التأهب ومواجهة نقاط ضعفها وقت حدوث الأزمات.

هذا التقرير جهد مشترك بين مركز استشراف المستقبل ودعم اتخاذ القرار في شرطة دبي، ومؤسسة دبي للمستقبل، ويركز على التهديدات المتزايدة الناشئة عن الجريمة الإلكترونية وانعكاساتها المحتملة على القطاع المالي والمصرفي في إمارة دبي. ويُعد القطاع المالي والمصرفي أحد المكونات الأساسية للبنية التحتية الحيوية في أي مجتمع حديث، ولهذا فهو المحور الذي يركّز عليه هذا التقرير، فيدرس أربعة سيناريوهات مفترضة لحوادث الهجوم السيبراني، واستجابتين محتملتين لها، ويقدم صورة أوسع للمؤسسات الرئيسة في البنية التحتية الحيوية تمكنها من الاستعداد جيداً للمستقبل بهدف صنع واقع مستقبلي آمن قادر على التكيف وتجاوز التحديات. وهذا التقرير هو الحلقة الأولى من سلسلة مؤلفة من ست حلقات تتناول قطاعات مختلفة من ناحية صلتها بالبنية التحتية الحيوية.

ما تعـــريف **البنيـــة التحتيـــة الحيـــوية؟**

تشمل البنية التحتية الحيوية المرافق والخدمات الضرورية اللازمة للحفاظ على سير العمليات المجتمعية ودوران عجلة الاقتصاد، وتُعرّف بأنها «تلك المرافق والخدمات وأنظمة المعلومات بالغة الأهمية للدول لدرجة أن لعجزها أو تعطيلها تأثير مدمر على الأمن القومي والاقتصاد الوطني والصحة والسلامة العامة وأداء الحكومة لوظائفها.»[1] ما يعني أن لها دوراً محورياً في أداء اقتصادنا ورفاهية المجتمع بصورة عامة.

وتشمل البنية التحتية الحيوية، على سبيل المثال لا الحصر، كلاً من الطاقة وأنظمة المياه والنقل والزراعة والاتصالات والرعاية الصحية والغذاء والتمويل المصرفي وخدمات الطوارئ في كلٍ من القطاعين العام والخاص.[2] وتعرِّف حكومات الدول المختلفة البنية التحتية الحيوية تبعاً لأُطر تلك الدول وأولوياتها الوطنية. ففي دبي، تشمل البنية التحتية الحيوية القطاعات التي نذكرها أدناه مع أهم المؤسسات التي تنتمي لكل قطاع:

خدمات الطوارئ	مؤسسة دبي لخدمات الإسعاف.
قطاع النقل	هيئة الطرق والمواصلات، مطارات دبي، حافلات دبي، تاكسي دبي، مترو دبي، موانئ دبي.

1. Jahier, Khan. (2014). Critical Infrastructure Protection within NATO. Civil-Military Planning and Support Section, Operations Division. Retrieved 17 October 2020, from: http://www.cipre-expo.com/wp-content/uploads/2014/02/Khan-Jahier-NATO-CIPwithin-NATO.pdf
2. Radvanovsky, R. S., & McDougall, A. (2018). Critical infrastructure: homeland security and emergency preparedness. CRC Press.

الشؤون المالية	مركز دبي المالي العالمي، إدارة الشؤون المالية، البنوك، شركات التمويل، البنوك الاستثمارية والتجارية، شركات الصرافة، مصرف الإمارات العربية المتحدة المركزي.
قطاع الطاقة	شركة بترول الإمارات الوطنية «إينوك.»
قطاع الكهرباء والماء	هيئة كهرباء ومياه دبي «ديوا.»
تقنية المعلومات والاتصالات	مدينة دبي الذكية، مدينة دبي للإنترنت، هيئة تنظيم الاتصالات، شركات الاتصالات (دو واتصالات.)
خدمات الرعاية الصحية	المستشفيات، العيادات، الصيدليات، هيئة الصحة بدبي، مدينة دبي الطبية.
السلامة العامة	شرطة دبي، الدفاع المدني - دبي.

وتضيف دول أخرى كالولايات المتحدة، مزيداً من الفئات إلى البنية التحتية الحيوية، كالمرافق التجارية، والتي تضم مجموعة متنوعة من المواقع التي تجذب حشوداً كبيرةً من الناس بغرض التسوق أو العمل أو الترفيه أو السكن.

تسارع رقمنة البنية التحتية الحيـــوية

غيرت التقنية الرقمية مختلف المكونات التي تتشكل منها البُنى التحتية الحيوية للدول، إذ مكنت رقمنة الحوالات والأسهم والتدفقات المالية الأجهزة الذكية المتصلة بالشبكة من تبادل المعلومات مع بعضها عبر منظومات اجتماعية تقنية، ما أتاح للمؤسسات، وخاصة تلك التي تعمل في نطاق البنية التحتية الحيوية، نشر أنظمة اتصالات ذكية تلقائية ذاتية المراقبة قادرة على تحليل المشكلات وتشخيصها دون الحاجة إلى تدخل بشري. وبعبارةٍ أدق، غيرت الرقمنة تصميم البنية التحتية الحيوية بما يدعم المبادئ التالية: [3,4]

الاتصـــال
تتصل الأنظمة والآلات من خلال بنية تحتية تابعة للقطاع العام تستخدم تقنيات مختلفة.

الاســـتمرارية
إمكانية العمل دون أي تدخل بشري، بالإضافة إلى توفير القدر الكافي من الإدارة لإجراء التحديثات بصورة مستمرة بهدف مواكبة معايير الأمان العالية.

الأمـــان
ضرورة توفر معايير الأمان العالية للحماية من الهجمات الإلكترونية.

الحمـــاية
يتعين استخدام الوسائل التقنية لحماية مكونات البنية التحتية الحيوية.

3. https://www.cisa.gov/commercial-facilities-sector.
4. SolidRun. (2020). Digital Transformation in Critical Infrastructure Networks. Retrieved 17 October 2020, from: https://www.solid-run.com/wp-content/uploads/2020/09/whitepaper-digital-transformation-whitepaper.pdf

فوائـد الرقمنـة للبنـية التحـتية الحيـوية تفـوق المخـاطر المحـتملة

أدركت الحكومات في مختلف بقاع العالم سريعاً فوائد الرقمنة والابتكارات القائمة على البيانات في توفير مستوى من الخدمات لمواطنيها قادر على الاستمرار والصمود. ففي دبي، قال صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي «رعاه الله» إن «الاقتصاد الرقمي محفز رئيسي في نمو وتطوير قطاعات اقتصادية جديدة لدينا، وتعزيز تنافسيتنا في السوق العالمي وفي اقتصاد المستقبل» ويوفر التحول الرقمي للبنية التحتية الحيوية الفوائد المهمة التالية: [5,6]

مضاعفات أقل

تقلل رقمنة البنية التحتية الحيوية من تعقيدات توفير أنظمة تقنية المعلومات وإدارتها، إذ توفر طريقة منخفضة التكلفة لتخطيط البنية التحتية لتقنية المعلومات وتخصيصها وتنفيذها وصيانتها.

سير عمل أكفأ

توفر رقمنة البنية التحتية الأساس لرفع كفاءة سير العمل، فعندما يكون لكل مهمة ضمن سير العمل احتياجاتها المستقلة، تتمكن فِرَق العمل من التحكم في كيفية إدارة الخوادم وغيرها من البُنى التحتية. ويقلل ذلك أيضاً الحاجة إلى فِرَق عمل كبيرة تؤدي أعمالاً يدوية كثيرة لتطوير المنتجات، إضافةً إلى خفض تكاليف التوظيف من خلال توفير سبل التواصل (جهاز إلى جهاز) (ونظام إلى نظام)، إذ تُتبادل البيانات عبر أنظمة متعددة قد توجد في أي مكان من البنية التحتية دون أي تدخل بشري.

5. Calsoft Inc. (2020). 5 Key Benefits of Infrastructure Automation. Retrieved 17 October 2020, from: https://blog.calsoftinc.com/2020/05/5-key-benefits-of-infrastructure-automation.html

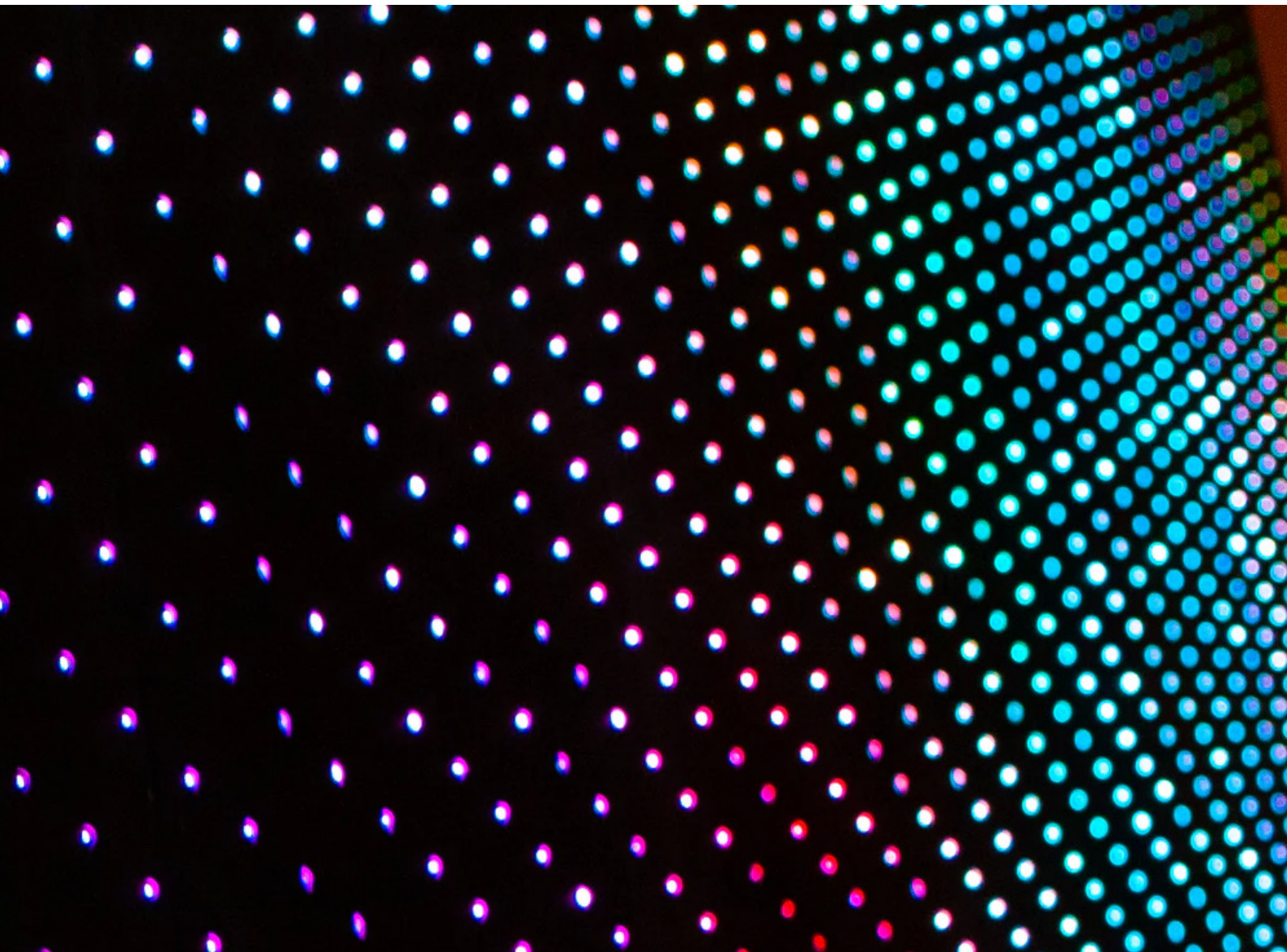
6. SolidRun. (2020). Digital Transformation in Critical Infrastructure Networks. Retrieved 17 October 2020, from: https://www.solid-run.com/wp-content/uploads/2020/09/whitepaper-digital-transformation-whitepaper.pdf

توصيل أسرع

تتحكم أتمتة البنية التحتية في عملية تزويد تقنية المعلومات، ما يقلل من الوقت (والجهد) اللازمين لإعداد أساس البنية، وبذلك تتمكن فِرَق العمل من البدء بتصنيع المنتجات في وقت أبكر وطرحها في السوق بسرعة أكبر، فتنافس بقوة أكبر وتلبي حاجات السوق ومتطلبات العملاء.

أخطاء أقل

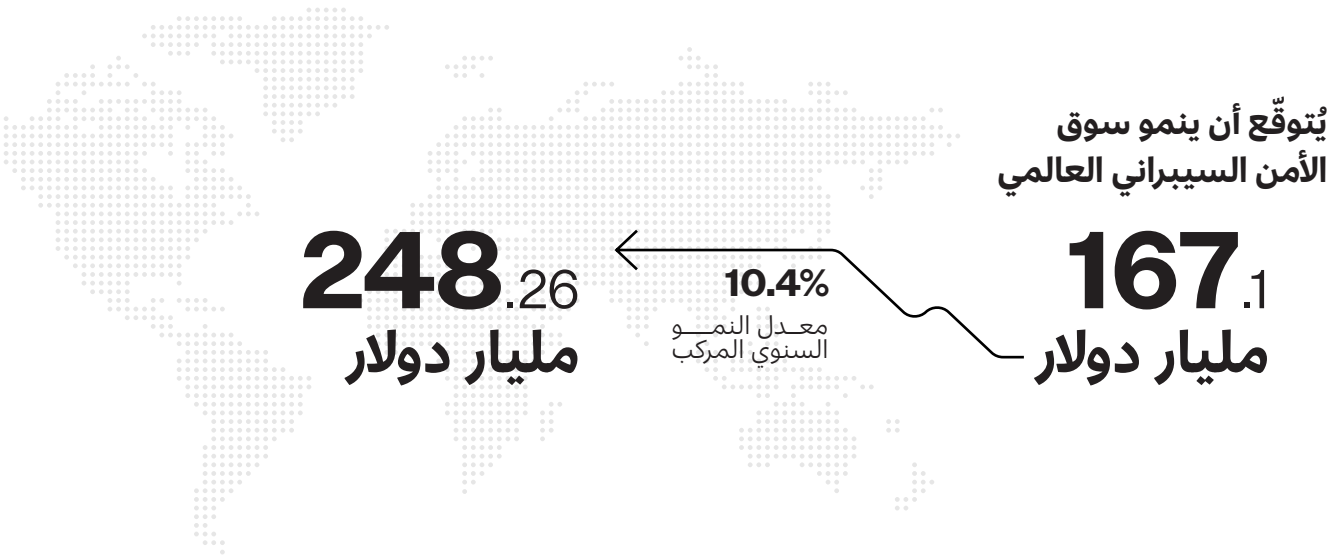
تقلل أتمتة البنية التحتية معدل الخطأ المرتبط بالإدخال اليدوي، إذ تتيح الاستفادة من البنية التحتية تبادل البيانات تلقائياً دون أي تدخل بشري، ما يقلل فرص وقوع الخطأ، ويمكّن فِرَق تقنية المعلومات من التركيز على المهام ذات الأهمية القصوى للمؤسسة.



خفض مخاطر البنية التحتية الحيوية المعتمدة على البيانات

تُعد دبي مدينةً رائدةً على مستوى العالم في استخدام التقنية الحديثة، بهدف تحسين مستوى المعيشة ونوعية الحياة. وأكد صاحب السمو الشيخ محمد بن راشد آل مكتوم نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي «رعاه الله» إن «أولوياتنا القادمة هي تطوير مساهمة الاقتصاد الرقمي في اقتصادنا الوطني، وترسيخ البنية التحتية الذكية في الدولة، وتعزيز الجاهزية الرقمية، وضمان استمرارية الأعمال في حكومة الإمارات تحت أي ظرف.»

وأصبحت العديد من خدمات دبي رقميةً بالفعل، من التقدم للحصول على تأشيرات الإقامة إلى دفع رسوم ركن السيارة، فمعظمها يسهل إنجازه اليوم من خلال الهاتف النقال. لكن رقمنة جوانب البنية التحتية الحيوية كاملة، يزيد مخاطر التخريب السيبراني وتهديداته، ولهذا ينمو سوق منتجات الأمن السيبراني وتزدهر خدماته، إذ يُتوقّع أن ينمو سوق الأمن السيبراني العالمي من 167.1 مليار دولار في العام 2019 إلى 248.26 مليار دولار بحلول العام 2023، محققاً بذلك معدل نمو سنوي مركب نسبته 10.4%. [7]



7. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/#558174da381d

وتنبهت حكومات الدول إلى ذلك أيضاً، إذ خصص الرئيس الأمريكي في ميزانيته للعام 2019 مبلغ 15 مليار دولار للأمن السيبراني، بزيادة قدرها 583.4 مليون دولار (4.1 بالمئة) عن العام 2018، وكان لوزارة الدفاع الحصة الأكبر في تلك الميزانية، إذ أعلنت في العام 2019 عن تخصيص مبلغ 8.5 مليار دولار لتمويل نظم الأمن السيبراني، بزيادة قدرها 340 مليون دولار (4.2 في المئة) عن العام 2018. [8]

مـعالجـة العنـاصر الثـلاثـة للمخـاطر

تنشأ المخاطر من عمل ثلاثة عناصر: التهديدات التي تتعرض لها الأصول، ونقاط ضعف الأصول أمام التهديد، والعواقب. ويعمل الأمن السيبراني على الوقاية من التهديدات، في حين يتولى التأمين مهمة التعافي منها.

ولبناء نظام مرن قادر على الصمود لا بد من الاستعداد لما يجب القيام به عند وقوع التهديدات أو المخاطر. «ويختلف الخطر عن التهديد من ناحية أن التهديد موجه إلى كيان أو أصل أو نظام أو شبكة أو منطقة جغرافية، أما الخطر فلا يكون موجهاً.» [9] وتُعرّف نقطة الضعف بأنها «سمة مادية أو خاصية تشغيلية تجعل الكيان عرضةً للاستغلال أو لخطر معين.» وتُعرّف العواقب بأنها «آثار لحدث أو حادثة أو واقعة.» [10] ولذا فإن المرونة مرتبطة بالحماية ونوعية الاستجابة أثناء الأزمة وبعدها.

8. https://cybersecurityventures.com/cybersecurity-market-report/
9. Department of Homeland Security, 2010.
10. Ibid.

الأبعـاد **الأربعــة** للمرونة

للمرونة أبعاد أربعة حُددت وفق الأبحاث كما يلي: [11]

المرونة التقنية
وتشير إلى قدرة نظام المؤسسة على تأدية مهامه بالشكل الصحيح عند تعرضها لأزمة.

المرونة الاقتصادية
وتشير إلى قدرة الكيان على مواجهة التكاليف الإضافية التي تنشأ عن الأزمة.

المرونة التظيمية
وتشير إلى قدرة مديري الأزمات على اتخاذ قرارات وإجراءات تؤدي إلى تجنب الأزمة أو على الأقل الحد من تأثيرها.

المرونة الاجتماعية
وتشير إلى قدرة المجتمع على تخفيف وطأة الأزمة من خلال مساعدة المستجيبين الأوائل أو تقدم أبنائه للعمل كمتطوعين.

وتلعب أنظمة البيانات والمعلومات الضخمة دوراً رئيساً متصاعداً في كل عنصر من عناصر المرونة الأربعة تلك، ولهذا قد يؤثر فشل النظام بسبب خطأ بشري أو كارثة طبيعية أو عمل تخريبي، على كلٍ منها. ولهذا لا بد من دراسة سيناريوهات الفشل المحتملة والعمل على تجنبها. مثلًا، ما تداعيات تعطل بنية نظام السلامة المدمج في أنظمة بيانات الشرطة والجهات الأمنية؟ وما تداعيات تعطل مولدات الطاقة المخصصة لحالات الطوارئ كما حدث في كارثة فوكوشيما دايتشي النووية في اليابان عام 2011؟ وما تداعيات تعطل قدرة فريق الأزمات والإدارة العليا على الاجتماع والتنسيق بسبب هجوم إلكتروني؟ وما تداعيات عدم جاهزية مديري الأزمات لطبيعة الأزمة كما ثبت في أزمة كوفيد- 19؟

11. Labaka et al. in Technological Forecasting & Social Change 103 (2016) 21–33.

الخدمات المالية والمصرفية إحدى المكونات الأساسية للبنية التحتية الحيوية في دبي

صُنّفت دبي في العام 2019 ثامن أهم مركز مالي قيادي على مستوى العالم (مرتفعةً من المرتبة 15 التي شغلتها في العام 2018)، ومتقدمةً بذلك على جميع مدن مجلس التعاون الخليجي في هذا المجال،[12] وبلغ عدد البنوك المرخصة في البلاد حينها 22 بنكاً. ويعد القطاع المصرفي في دولة الإمارات الأكبر في المنطقة، إذ يضم ما يقرب من ثلث الأصول المصرفية لدول مجلس التعاون الخليجي. ورسخت دبي (والتي تمثل أحد المركزين الماليين الأهم في الدولة) مكانتها كمكون أساسي في نظام الخدمات المالية العالمي بأسواقها النشطة في الداخل والخارج.

ويشير تقرير الآفاق الاقتصادية للعام 2019 الصادر عن دائرة التنمية الاقتصادية إلى أن قطاع البنوك والتأمين وأسواق رؤوس المال والخدمات المالية كان ثالث أكبر مساهم في الناتج المحلي الإجمالي الحقيقي لدبي في العام 2018، إذ أضاف قيمةً بلغت 40.4 مليار درهم بالأسعار الثابتة أو 10.2 في المئة من المجموع الكلي. ويسهم القطاع في دعم الأنشطة الاقتصادية الأخرى بشكلٍ غير مباشر من خلال إطالة أمد استحقاق القروض والتسهيلات الائتمانية.

ويُعد بنك الإمارات دبي الوطني، ومقره دبي، ثاني أكبر بنك في الدولة، والأكبر في إمارة دبي، والثالث على مستوى دول مجلس التعاون الخليجي، بنسبة استحواذ بلغت نحو 20 بالمئة من محفظة القروض الوطنية. وبنك دبي الإسلامي، أكبر مؤسسة مالية متوافقة مع الشريعة الإسلامية في دولة الإمارات، وثاني أكبر بنك إسلامي في العالم. وتضم دبي أيضاً سوقاً محلية لتجارة الأسهم والأوراق المالية، بالإضافة إلى سوق دبي المالي وسوق رأس المال الدولي ناسداك دبي.

12. https://dubaided.gov.ae/ded_files/Files/Reports/rep_2019/DER2019_EN_Report_f4.pdf

وتعود ملكية نحو 90 بالمئة من أصول البنوك في دولة الإمارات إلى مؤسسات مملوكة محلياً، وتدير 38 مؤسسة أجنبية مرخصة معظم النسبة المتبقية. ويعمل عدد أكبر من المؤسسات الأجنبية من خلال مركز دبي المالي العالمي، والذي يمثل المنطقة الحرة للخدمات المالية الخارجية، ويعد أحد من الركائز الأساسية التي تدعم سمعة الإمارة بصفتها مركزاً مالياً إقليمياً. وتضم المنطقة الحرة نحو 100 بنك أجنبي.[13] وفي المقابل ما زال القطاع المالي غير المصرفي صغيراً، إذ يضم نحو 20 شركة تمويل مرخصة من مصرف الإمارات العربية المتحدة المركزي، تمثل ما يقرب من 1.4 بالمئة من أصول النظام المصرفي الإماراتي.

وكحال معظم الاقتصادات المتقدمة، تلعب البنوك دوراً محورياً في حياة الناس. ومن الأنظمة التي يعتمد عليها مصرف الإمارات العربية المتحدة المركزي، نظام تحويل الأموال الإماراتي، ونظام الخصم المباشر الإماراتي، وأهمها، نظام حماية الأجور، وهو نظام إلكتروني لتحويل الرواتب يمكّن الموظفين من الحصول على رواتبهم عن طريق البنوك ومكاتب الصرافة والمؤسسات المالية. وقد يسبب أي انقطاع في هذه الخدمات صعوبات للأفراد والشركات.

13. https://oxfordbusinessgroup.com/overview/forward-bound-increased-profits-and-stable-liquidity-fuel-expansion

ووفقاً للمركز الاتحادي للتنافسية والإحصاء،[14] يستخدم نحو 90 بالمئة من الناس في دولة الإمارات القنوات المصرفية الرقمية، ويستخدم جميعهم (100 بالمئة) أجهزة الصراف الآلي في معاملاتهم المصرفية، ما يدل على مستوىً مرتفع من الاعتماد على الخدمات الرقمية. بالإضافة إلى ذلك، تستخدم نسبة عالية منهم الخدمات المصرفية عبر الهاتف النقال. وتشهد كل من الفروع الرقمية والمحافظ الإلكترونية وغيرها من الخدمات غير التلامسية زيادةً مستمرةً في عدد المستخدمين. وتُعدّ بنوك الإمارات ودبي رائدة في استخدام «الخدمات المصرفية المفتوحة» والتي من خلالها تُتبادل البيانات بين كيانات متعددة غير مرتبطة. ما يتيح إنشاء «المنصات الموحدة» التي تلبي مجموعةً متنوعة من احتياجات العملاء. ويُنظر إلى إدماج الخدمات المتنوعة في منصة واحدة على أنه حجر الزاوية في الخدمات المصرفية الرقمية.[15] وعلى الرغم من أن هذه الابتكارات المعتمدة على البيانات تحسّن جودة تجربة العملاء، فإنها تضاعف المخاطر الأمنية وتزيد حكماً عدد نقاط الضعف التي تستغلها الهجمات الإلكترونية وأعمال التخريب السيبراني المحتملة. (الصندوق 1.)

14. Federal Competitiveness and Statistics Centre
https://fcsa.gov.ae/en-us/Lists/D_Reports/Attachments/16/StatisticsUnlocked3en-v04.pdf
15. https://assets.kpmg/content/dam/kpmg/ae/pdf/uae-banking-perspectives-2020.pdf

سـيناريوهات نقـاط الضعـف: **ما تداعيات حدوث هجوم إلكتروني على النظام المالي والمصرفي؟**

تمثّل الخدمات المالية والمصرفية مكوناً أساسياً للبنية التحتية الحيوية لأي مجتمع، ما يعني أن للهجمات الإلكترونية على النظام المالي والمصرفي أثراً كبيراً على أداء المجتمع بأكمله، فالترابط والتكافل القائمَين بين النظام المصرفي والمؤسسات التجارية والاقتصادية والاجتماعية، يعني أن الهجوم على مؤسسة أو أكثر قد ينتج عنه آثاراً سلبيةً كبيرةً على الصحة أو السلامة العامة أو الأمن الاقتصادي أو القومي.

لذا صُممت الأنظمة التقنية بطريقة تمنع حدوث هذا التأثير المتتالي، ومع هذا، تستمر تلك الهجمات بالحدوث سنوياً.

1

خمسة أنواع من الهجمات الإلكترونية على المؤسسات المالية والمصرفية*

حذف البيانات المهمة
الإضرار بحالة توفر البيانات الحساسة الضرورية لسير أعمال التقاصّ والتسوية والمدفوعات بدقة وفعالية، وذلك من خلال حذف تلك البيانات.

التلاعب بالبيانات المهمة
الإضرار بصحة البيانات الحساسة الضرورية لسير أعمال التقاصّ والتسوية والمدفوعات بدقة وفعالية، وذلك من خلال التلاعب بتلك البيانات.

تعطيل الخدمات الحرجة على نطاق واسع
تعطيل خدمات التقاصّ والتسوية والمدفوعات بالغة الأهمية، في مؤسسات عدة لفترة طويلة من الزمن.

التعاملات الاحتيالية
الشروع في تعاملات احتيالية تستغل البنية التحتية للمدفوعات بالغة الأهمية.

سرقة المعلومات السرية بالغة الأهمية
انتهاك سرية المعلومات المتعلقة بالعمل بالغة الأهمية لاستخدامها في التداول من الداخل أو في أعمال التلاعب بالسوق أو جمع المعلومات الاستخبارية.

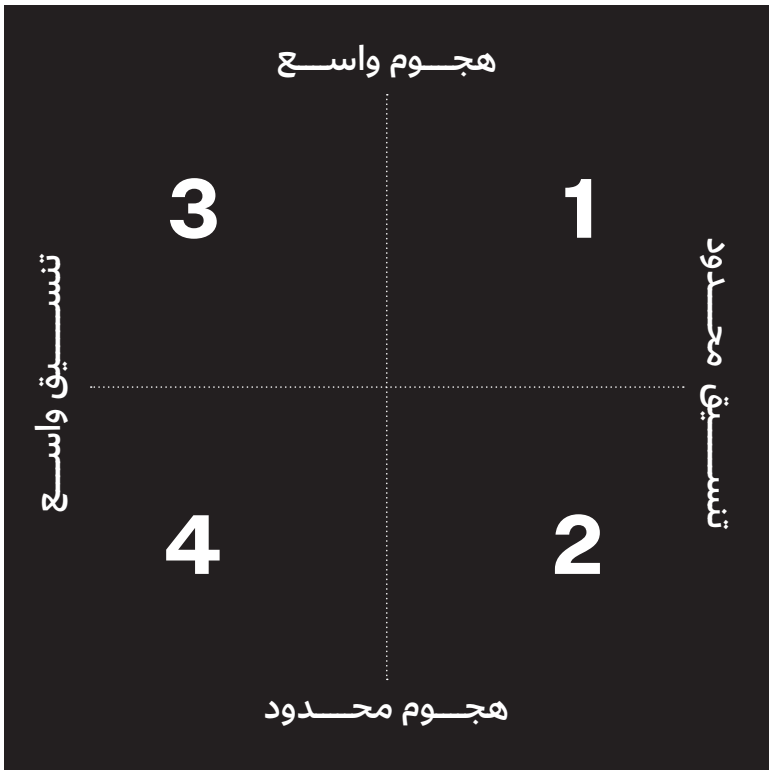
*المصدر: DTCC/OliverWyman, 2016

خيارات الرد

تتراوح الهجمات الإلكترونية من هجمات محدودة تستهدف مؤسسة أو اثنتين إلى هجمات واسعة النطاق تستهدف العديد من المؤسسات بهدف إيقاف النظام برمته. وقد تؤدي الهجمات المحدودة إلى إلحاق أضرار جسيمة بالمؤسسة المستهدفة، في حين تتسبب الهجمات الواسعة بعواقب واسعة النطاق على المنظومة بأكملها.

يحدَّد مدى الضرر من خلال مستوى تنسيق الاستجابة، فقد تمكّن الاستجابة العشوائية لهجوم محدود إحداث ضرر واسع النطاق، في حين تحدّ الاستجابة المدروسة من الضرر الناجم عن هجوم واسع.

في القسم التالي نعرض كلا الاستجابتين ضمن أربعة سيناريوهات.



تنسيق محدود في ظل سيناريوهين: **هجمات واسعة النطاق وأخرى محدودة**

تنسيق محدود في ظل سيناريوهين

هجمات واسعة النطاق وأخرى محدودة

1

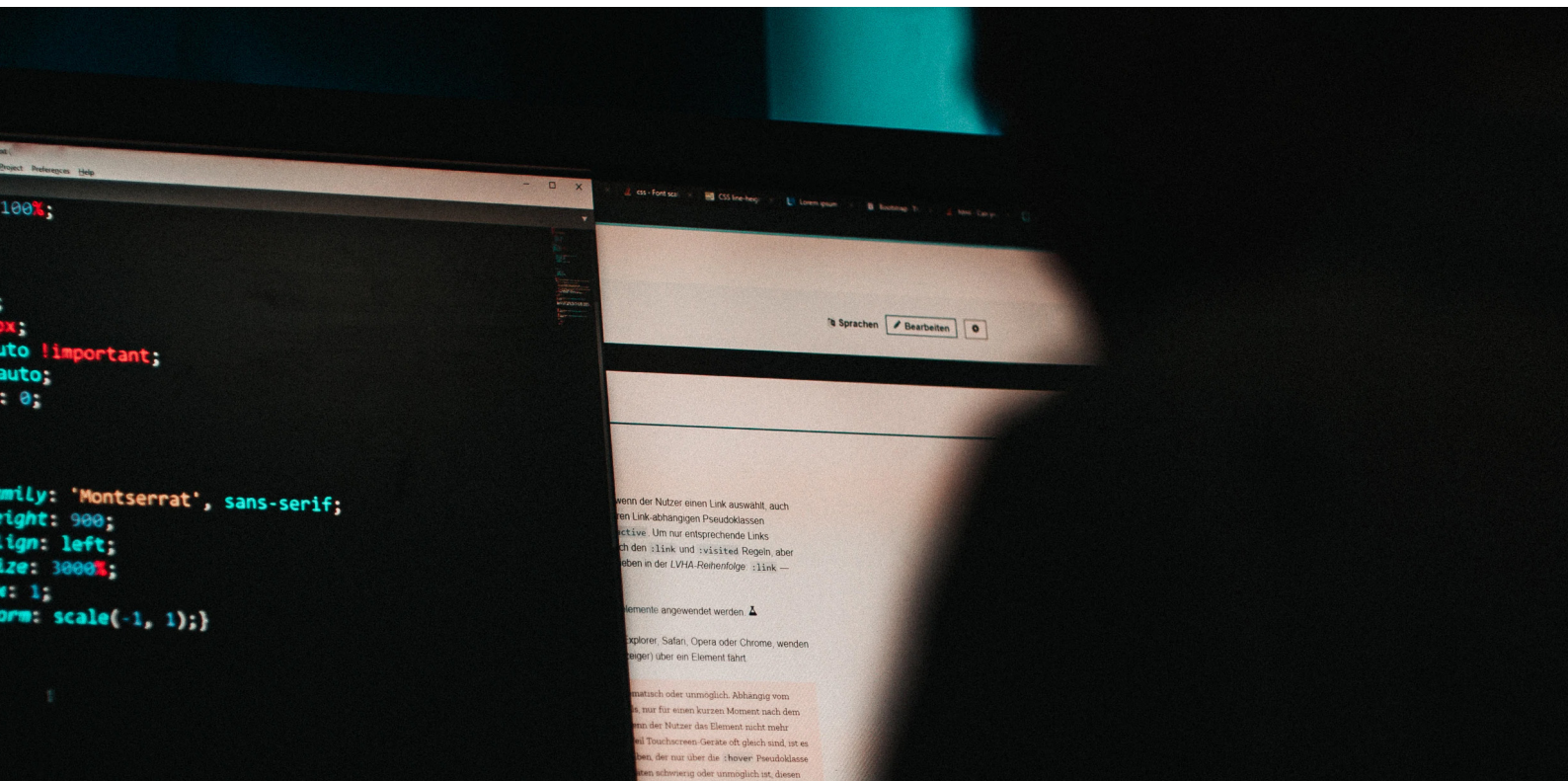
في هذا السيناريو، حدث هجوم واسع النطاق على النظام المالي والمصرفي أدى إلى توقف أغلب الأعمال، ومع هذا، لم يُواجه الهجوم بادئ الأمر إلا برد ضعيف التنظيم نتيجة عدم الاستعداد والجاهزية ضمن المؤسسات على جميع المستويات، إذ ليس لديها وسائل الإنذار المبكر، مع انخفاض مستوى التدريب والتنسيق بينها، فليس لديها إجراءات منسقة واضحة لما يجب عمله، ولا تعرف كيف ترد على هذا النوع من التهديدات، ومعلوماتها فقيرة عن تصميم أنظمتها الأمنية وبنيتها، وتنقصها المعرفة بالجهات الحكومية التي ينبغي الاتصال بها والتنسيق معها، وإدراكها ضعيف لمدى التهديد وطبيعة الخطر وحجم الخسارة المحتمل.

على المستوى التنظيمي، قلة قليلة من المؤسسات تملك استراتيجية عملية لكيفية الرد على هذه النوعية من الهجمات، إذ كانت المؤسسات تفتقر عموماً إلى وحدات التنسيق المسؤولة عن القضايا الأمنية، بالإضافة إلى غياب أنظمة المراقبة والتنفيذ لديها. وتسبب عدم كفاية الإرشادات وضعف فعالية أطر العمل الناظمة، بوقوع المعلومات والبيانات في معظم المؤسسات تحت خطر التهديدات الأمنية.

وفي هذا السيناريو، تسبب الهجوم المفترض وعواقبه بضرر واسع على سمعة المؤسسات المستهدفة في البلاد لأمد طويل، ما أثار قلق الناس من أن الإدارات العليا لتلك المؤسسات غير قادرة على ضمان مستوى كافٍ لأمن البيانات. ولا ريب أن مخاوف الناس في هذه الحالة مبررة، إذ أن هجمات مماثلة قد تتكرر، وقد يضطرون إلى مواجهة انقطاعات متكررة في سير العمل.

من الناحية الاقتصادية، أدى التنسيق الضعيف والمحدود إلى إطالة أمد التعافي. وركزت البنوك الأكبر حجماً على تعافيها بالتنسيق ما أمكنها مع البنوك الكبيرة الأخرى، أما البنوك الأصغر فكان الخطر عليها أكبر، ونظراً لأن العديد منها تمارس أعمالها في الإمارات الأصغر، فإن التداعيات الاقتصادية للهجوم الإلكتروني على النظام المصرفي كانت أكثر حدةً على تلك الإمارات، فتوقفت فيها مدفوعات الرواتب والمعاشات التقاعدية ومدفوعات العقود العامة. وأدى عدم التنسيق على جميع المستويات إلى غياب مصدر واحد للمعلومات عن الحادث، ما ترك الساحة لانتشار الشائعات بين العملاء، وشهدت بعض البنوك تهافت عملائها على سحب إيداعاتهم، مدفوعين بالقلق على أمان أموالهم وقدرتهم على الوصول إليها. ويبقى الوقت الذي يتطلبه التعافي مجهول ويتفاقم الضرر الاقتصادي الناتج كل ساعة.

على المستوى المجتمعي، انتشرت الشائعات والمخاوف من فقدان الوظائف، وإساءة استخدام الأموال، وارتجاع المدفوعات، وفقدان أهم المعلومات التجارية. ودفع ارتفاع مستوى التوتر والقلق في المجتمع من تمكنوا من الوصول إلى حساباتهم المصرفية إلى سحب أموالهم وتحويلها إلى خارج البلاد عبر وسائل بديلة. وازدادت حوادث العنف في البنوك وشركات تحويل الأموال، إضافةً إلى الإضرابات العمالية، وحتى العنف المنزلي، وباتت أقسام الشرطة غارقة بطلبات التدخل والمساعدة.



تنسيق محدود في ظل سيناريوهين

هجمات واسعة النطاق وأخرى محدودة

2

في السيناريو الثاني، استهدف هجوم محدود مؤسسة أو اثنتين من المؤسسات المالية في دبي. ولأن الهجوم موجه إلى عدد محدود من المؤسسات، ساد شعور عام بين البنوك وغيرها من المؤسسات في الإمارة بأن «هذا لن يحدث لنا.» واعتُبر أن الهجوم ناتج عن ثغرات محددة في المؤسسات المستهدفة ولا داعٍ إلى أن تقلق المؤسسات الأخرى بشأنه.

وأجبر الهجوم المحدود المؤسسات المستهدفة على التكيف وتعلم الدرس والاستعداد بشكل أفضل للمستقبل. لكن هذا حدث بصورة فردية مستقلة، ما جعل الدروس المستفادة من الهجوم مقتصراً عليهم دون مشاركته مع المؤسسات الأخرى. ولأن الاستجابة كانت محدودة التنسيق، فإن فرصة التحضير لاستجابة أوسع وتنسيق أعلى بين الأهداف المحتملة الأخرى في الإمارة كانت محدودةً أيضاً، ما أدى إلى الحد من التعلم التقني والتنظيمي في المؤسسات التي تُعد جزءاً أساسياً من منظومة البنية التحتية الحيوية.

ومع هذا، فقد أدى الهجوم المحدود إلى ترك الآلاف من الأفراد والشركات خارج الخدمة دون مكان يلجؤون إليه سوى البنوك، ولأن البنوك كانت تسعى جاهدةً لإحصاء الأضرار وإعادة الخدمة، فلم يكن لديها فائض من الموارد يكفي لتلبية الاحتياجات الملحة للعملاء المتضررين. وكشَف التنسيق المحدود أيضاً أن المؤسسات الاجتماعية والحكومية لم تكن على درجة كافية من الجاهزية للإسراع في مد يد العون، إذ أدى شح المعلومات عن عمق الهجوم واتساعه إلى إعاقة قدرتها على تقديم الدعم الفعال عند الحاجة.

وعلى الرغم من أن الهجوم كان على نطاقٍ محدود، فقد ولّد إحساساً بالقلق وعدم الأمان بين المتضررين منه مباشرةً أو غير مباشرة، داخل البلاد وخارجها. واضطر العملاء الذين لم يتمكنوا من دفع الفواتير أو إكمال المعاملات المالية الضرورية إلى تبرير تقصيرهم بشكل فردي ومواجهة عقوبات محتملة، ما أدى إلى خفض الثقة في أمن النظام المصرفي، إذ لاحظ العملاء أن مسؤولية الأمن تقع على عاتق كل مؤسسة مصرفية وحدها، وولّد انطباعاً بأن بعض البنوك والمؤسسات المالية أفضل استعدادا وحنكة في التعامل مع الهجمات الإلكترونية المتزايدة. وأدت هذه الانطباعات إلى منافسة غير مفيدة بين المؤسسات المالية مبنية على الحصانة المفترضة ضد المخاطر الإلكترونية، ما رفع مستوى الاستثمار في تقنيات الأمن السيبراني إلى مستويات تجاوزت الحدود الفعّالة المثلى.

وبشكل عام، أدت الاستجابة غير المنسقة إلى اضطرار كل مؤسسة إلى دفع فاتورة أمنها بمفردها، ما زاد تكاليف الأمان على كل منها مقابل كفاءة أمنية أخفض، الأمر الذي يتناقض مع سيناريو التنسيق الواسع بين المؤسسات ضمن منظومة البنية التحتية الحيوية حيث تبقى الكفاءة الأمنية عالية وتُوزَّع تكاليف الأمن بين الجميع.

تنسيق واسع في ظل سيناريوهين

هجمات واسعة النطاق وأخرى محدودة

3

في السيناريو الثالث، يتعرض النظام المالي والمصرفي لهجوم إلكتروني. يُكتشف الهجوم بسرعة بسبب وجود نظام تنبيه مركزي في وحدة الكشف والتصدي التابعة للأمن السيبراني في دبي، فهي تراقب التهديدات الإلكترونية باستمرار وتكشف عنها. وفي هذا السيناريو يفترض أن معظم المؤسسات الرئيسة المكونة للبنية التحتية الحيوية أصبحت مدربة على هذا النوع من الهجمات، وتمتلك حلولا تقنية متقدمة قادرة على توقع بالتهديدات بتحليل البيانات، وتتبع ومراقبة كل من وسائل التواصل الاجتماعي، والمحادثات الجماعية عبر الإنترنت، والاضطرابات السياسية، ومحادثات الشبكات العميقة والمظلمة. ويوجد في هذا السيناريو فريق طوارئ يعمل بين المؤسسات ويعرف بالضبط الخطوات التي يجب اتخاذها. إضافةً إلى توفر مستوىً عالٍ من الوعي لدى جميع الأطراف المعنية، ليس على مستوى الإدارة العليا فحسب بل على جميع مستويات المؤسسة، ما يُشعر الموظفين بالكفاءة والثقة بقدرة مؤسساتهم على منع مثل هذه الهجمات من الاستمرار لفترة طويلة وإلحاق الضرر بالاقتصاد.

وتعلن الحكومة عن تفعيل إجراءات الطوارئ. وتقدَّم الضمانات من أعلى مستويات القيادة، خاصةً بما يتعلق بسلامة الأموال وتوفر السلع والخدمات الأساسية.

ويجري التنسيق بين جميع البنوك والمُلّاك والمعنيين، وكذلك المصرف المركزي، والهيئات الحكومية المعنية، وكبار تجار التجزئة، ومكاتب الائتمان، ووحدة شرطة الجرائم الإلكترونية، وسلاسل محلات البقالة الرئيسة ومحطات الوقود، بالإضافة إلى الخدمات الطبية. وبموجب إجراءات الطوارئ، تعمل بطاقة الهوية الإماراتية كبطاقة دفع مؤقتة لشراء السلع والخدمات الأساسية (بحدود عليا ثابتة).

ويبدأ العمل بشبكة جرى التحقق من فعاليتها مسبقاً، تعتمد مبدأ نقاط الشراء في محلات البقالة ومحطات الوقود. وتعلن شركات التأمين عن استعدادها للتمويل الفوري الطارئ. وتؤدي أنظمة النسخ الاحتياطي عملها في البنوك والمؤسسات الرئيسة الأخرى قبل انتشار أي حالة ذعر.

يضمن هذا المستوى الواسع من التنسيق بين الشركات والمؤسسات الحكومية والمجتمعية استمرار الأعمال التجارية الأساسية والحياة اليومية دون انقطاع.

وتُجهَّز الخطة المعدّة مسبقاً لكيفية التعامل مع الموقف، وتدخل حيز التنفيذ بطريقة عالية التنسيق. والنتيجة، تناغم الاستجابة على كافة المستويات وفي جميع القطاعات.

تنسيق محدود في ظل سيناريوهين

هجمات واسعة النطاق وأخرى محدودة

4

السيناريو الرابع شبيه بالسيناريو الثاني، إذ ضرب هجوم محدود 1 إلى 3 مؤسسات مالية في إمارة دبي، إلا أن الجانب المختلف هذه المرة أن الاستجابة واسعة ومنسقة، فقد رفعت وحدة الكشف والتصدي التابعة للأمن السيبراني في شرطة دبي مستوى التنبيه على الفور إلى اللون الأحمر لإعلام جميع مؤسسات منظومة البنية التحتية الحيوية في دبي بالحاجة إلى تفعيل إجراءات الطوارئ. وتتألف منظومة البنية التحتية الحيوية من المؤسسات الرئيسة التي تقدم الخدمات الأساسية في الإمارة، وتشمل الرعاية الصحية، وخدمات الرعاية الاجتماعية، وإمدادات الطاقة والمياه، والنقل، والإمدادات الغذائية، والخدمات المالية والمصرفية. وأنشأت شرطة دبي منصة «الطوق الأمني» الممتدة عبر جميع المؤسسات الأعضاء في المنصة، وخصصت كل مؤسسة وحدةً تعمل بدوام كامل كنقطة تنسيق ومراقبة واتصال مع الشرطة.

وما إن أطلقت المؤسسة المتضررة إنذار الخطر، صدر تنبيه إلى جميع المؤسسات الأعضاء لتفعيل خطط الطوارئ الخاصة بها، وشملت مجموعةً من الإجراءات منها الاتصال الفوري بالعملاء والشركاء وتفعيل الخطط الاحتياطية لدعم العملاء المعرضين للخطر.

وجرت مشاركة المعلومات حول طبيعة التهديد، وحشد الخبراء الفنيين عبر منصة «الطوق الأمني» بسرعة لتقديم المساعدة التقنية. وتقاسمت الأطراف المعنية كلاً من التكاليف والمعلومات المتعلقة بالحادث. وشعر العملاء بالارتياح لأن الوضع تحت السيطرة وأن جميع الأطراف المعنية وقفت معاً لصد الهجوم ولم تُترك المؤسسات الضعيفة وحدها في مواجهته. وبفضل الإنذار الواسع بشأن الهجوم شعر عملاء المؤسسات المالية المستهدفة بأن جميع المؤسسات المهمة العامة والخاصة والتي لديها معاملات مالية معها على علم بالوضع وأبلغتهم بالإجراءات المؤقتة المتخذة لمعالجته حتى استعادة الخدمة بالكامل، ما عزز الثقة بالنظام. ووُزعت تكاليف الإجراءات الأمنية والتعافي من الأضرار على مختلف الأطراف المعنية في المجال وتقاسم الجميع الخبرات والمعلومات المكتسبة من هذه التجربة.

كيفية تحسين مستوى الاستعداد؟

الثغرات التقنية

يتمثل البعد التقني للمخاطر في قدرة الأنظمة المادية على التأقلم والأداء الجيد في ظل الأزمات والاستمرار في تأدية وظائفها الرئيسة.[16] لذا يدور الاستعداد التقني حول ثلاثة محاور رئيسة هي: الوقاية والكشف والتعافي.

وعلى المؤسسات أن تكون على دراية عند حدوث هجوم إلكتروني أو اكتشاف ثغرة أمنية. وللوقاية من خلال الاعتراض والتصدي أهمية خاصة، فإن نجح اعتراض الهجوم ومنعه في الوقت المناسب، فلا حاجة بعد ذلك إلى بذل مزيدٍ من الجهود باستثناء تبادل المعلومات المتعلقة بالهجوم مع السلطات المختصة والمؤسسات الأخرى ضمن المجال.

16. Ionuţ A. (2018). Improving The Level of Critical Infrastructure Protection by Developing Resilience. Land Forces Academy Review. 23. 237-243. 10.2478/raft-2018-0028.

وإن لم يحدث الكشف والاعتراض في الوقت المناسب، فعلى الأنظمة التقنية أن تكون مصممة بطريقة تمكنها من الاستجابة سريعاً لتخفف الأضرار، فالاستجابة يجب أن تركز على تخفيف أثر الهجوم من ناحيتي التوقيت والانتشار.

ولا بد أيضاً من تصميم النظام التقني بما يسرع مدة التعافي، مع ضرورة تحقيق توازن بين الاسترجاع السريع للخدمة والاسترجاع الآمن لها. ولا بأس من جعل العمليات البديلة والتطبيقات الاحتياطية ومراكز البيانات المتنوعة جغرافياً جزءاً من استراتيجية التعافي.

لا يمكن الوصول إلى حالة الصمود التقني إلا من خلال تنسيق واسع بين المؤسسات المترابطة، فقد يقوَّض التعافي السريع في بعض المؤسسات بسبب بطء التعافي في مؤسسات أخرى. وتدعو الحاجة في المؤسسات إلى شراء أنظمة توقع متقدمة قادرة على التحذير من حدوث التهديدات من خلال تحليل البيانات، وتتبع وسائل التواصل الاجتماعي ومراقبتها. فضلاً عن الحاجة إلى توظيف أصحاب المهارات اللازمة لتشغيل تلك الأنظمة والتعديل عليها، لتحقيق مستوىً عالٍ من الجاهزية ضد الهجمات الإلكترونية الوشيكة.

ما دور البنوك؟

أمام البنوك طرائق كثيرة لإنشاء بيئة رقمية أكثر أماناً، والتمكن من مجابهة التهديدات السيبرانية المحتملة.

تقييـم الأمـن السحـابي

راجع البنية الأساسية لسحابتك بصورة منتظمة وتأكد من أنها محدّثة. وقيّم مستوى الأمان الحالي لسحابتك مقارنةً بمستويات الأمان المعيارية ومعايير الأداء والامتثال المثلى.

مراقبة الأمن السحابي

استخدم أداةً لإدارة الثغرات الأمنية تساعدك على اكتشاف التهديدات تلقائياً والوقاية منها قبل وقوعها.

وضع سـياسـات صارمة لإدارة الوصـول

من خلال منح أذونات الدخول للموظفين الذين يحتاجون إليها فحسب، فإنك تضمن أن مؤسستك محمية جيداً من الداخل، خاصةً إن كنت توظف متعاقدين أو موظفين بدوام جزئي.

وضع خطـة تعافي من الكـوارث

يقي وجود خطة من فقدان البيانات ويتيح لك تقليل وقت التعطل عن العمل بعد حدوث انقطاع، ولا ينجح ذلك إلا إن أجريت النسخ الاحتياطي لبياناتك بتكرار منتظم.

تشـــفير البيـــانات

يضمن تشفير بياناتك وحماية مفاتيح التشفير، توفير الحماية المستمرة لأصولك الرقمية الحساسة حتى إن تعرّض نظام تقنية المعلومات لديك لهجوم شديد.

الثغـرات التنظيـمية

يتمثل البعد التنظيمي للمخاطر في قدرة المؤسسات على التنبؤ بالاضطرابات غير المتوقعة والاستعداد لها والتفاعل والتكيف معها.[17] ومع استمرار تحول المؤسسات إلى النظام الرقمي، واستخدامها لتقنيات الخدمات السحابية والذكاء الاصطناعي وإنترنت الأشياء وغيرها، فإنها تصبح عرضةً لمخاطر وثغرات جديدة.

ومن الجوانب المهمة للاستعداد التنظيمي زيادة الوعي بين الموظفين عن كيفية حدوث الهجمات الإلكترونية والتأثير الذي تحدثه. ولا يتم ذلك بفعالية عالية إلا إن كان الأمن السيبراني من الوظائف المدمجة في المؤسسة، والتي تعمل بالتنسيق مع مثيلاتها في المؤسسات الأخرى. وتحتاج المؤسسات إلى اعتماد إطار عمل ناظم لشؤون الأمن السيبراني يحدد القوانين والسياسات والخطوات ويقدم الإرشادات للمؤسسات عن كيفية إدارة البيانات وحمايتها والاستجابة للمخاطر وأعمال التخريب.

وكما أن سلوك فردٍ واحد قد يتسبب بتقويض أمن مؤسسة بأكملها، قد تقوض مؤسسة واحدة أمن القطاع برمته. ولا يكون الوعي فعالاً إلا عند تطبيقه على مستوى القطاع بأكمله ومقترناً بالتنسيق والقوانين المنظمة.

17. Denyer, D. (2017). Organizational Resilience: A summary of academic evidence, business insights and new thinking. BSI and Cranfield School of Management.

وينبغي للقوانين والتشريعات أن تربط البروتوكولات والممارسات معاً في المؤسسات وعلى مستوى الدولة. ولأن العمليات الرقمية تتسم بأنها عابرة للحدود، على المؤسسات أن تكون واعيةً بالمخاطر الأمنية التي قد تتعرض لها جراء تعاملها مع سلاسل الإمداد العابرة للحدود.

ما دور المؤسسات؟

توظيف مواهب جديدة

يرتبط مجال الأمن السيبراني ارتباطاً وثيقاً بتوفر أصحاب المواهب والخبرات. وتحتاج المؤسسات العاملة في نطاق البنية التحتية الحيوية إلى البحث بذكاء عن أصحاب المواهب في مجال الأمن السيبراني، وقد يتجه المعنيون في البنية التحتية إلى «المرافق الإلكترونية» على سبيل المثال، وهي مجموعات تعمل لصالح المجال، تجمع المعلومات والموارد لتحسين فعالية الأمن السيبراني لأعضائها.

تشكيل فريق استجابة سيبراني

تُعد الساعات الأولى بعد اكتشاف هجوم إلكتروني الأكثر أهميةً وفعاليةً في تقليل الخسائر، وتزداد أهميتها في حالة الهجمات الموجهة إلى البنية التحتية حين يكون فقدان الأرواح تأثيراً جانبياً محتملاً من الدرجة الثانية أو الثالثة. لذا، يعد اختيار فريق الاستجابة وتدريبه قبل وقوع الحادث أمراً أساسياً.

تغيير العقلية السائدة في المؤسسات

لبدء التحول في العقلية ونمط التفكير، على المؤسسات أن تطور تصوراً لما سيبدو عليه مشهد الهجوم السيبراني من وجهة نظرها، ولطالما كانت ألعاب الحرب السيبرانية وتدريبات المحاكاة النظرية عنصراً أساسياً في تطوير هذا التصور ضمن الشركات، ويُرجَّح أن تكون تلك الإجراءات فعالةً أيضاً للبنية التحتية، إذ تحاكي سيناريوهات التدريب الفعالة سلوكيات مهاجمي العالم الحقيقي بهدف فرض سلسلة من القرارات الصعبة على الفريق، ما يخلق العديد من فرص التعلم (والتي قد تكون مؤلمةً في بعض الأحيان).

وتوفر اللائحة الأوروبية العامة لحماية البيانات نقطة انطلاق جيدة لإدارة البيانات عبر الحدود، ولكن ينبغي استكمالها باللوائح الوطنية المناسبة أيضاً. فالتشريع في نهاية المطاف يمثل أساساً للامتثال ووضع الأمن في مكانة بارزة على جدول أعمال الإدارات العليا.

على مستوى المؤسسات الفردية. تحتاج الإدارات إلى إدراك حجم الخسائر المالية المدمرة المحتملة التي قد تنجم عن هجوم إلكتروني، وتحديد الخدمات الأكثر أهميةً، وتطوير استراتيجية للحماية وأخرى لتخفيف العواقب والأضرار، وكي تطبق هذه الاستراتيجية بكفاءة عالية، تحتاج المؤسسات إلى تمتين الشراكات مع المساهمين والمعنيين الرئيسين بحيث تتمحور حول التنسيق الأمني وإدارة المخاطر. وعلى الإدارة أن تكون على دراية تامة بالحدود الممتدة لهيكلها الأمني قبل أن تشرع بعقد شراكات ضمن منظومتها التجارية والتقنية مع مؤسسات مساهمة يحتمل أن تكون عرضةً للخطر.

وعلى المؤسسات أيضاً أن تجتمع لتبادل الخبرات. الأمر الذي يقلل احتمالية تكرار الهجمات مستقبلاً نتيجة زيادة الوعي بمختلف أشكال نقاط الضعف.

الثغــرات الاقتصـــادية

يتمثل البعد الاقتصادي للمخاطر في قدرة الاقتصاد على التكيف والتعافي وإعادة البناء وتقليل الأثر السلبي الإجمالي على الرفاهية الاجتماعية، وكلما طال انقطاع الخدمات، زاد التأثير على الاقتصاد. ومن الجوانب المهمة في هذا السياق إدارة المخاوف، فلعامة الناس وأصحاب الأعمال مخاوف مبررة مرتبطة بالمدة المحتملة لانقطاع الخدمات وسلامة أموالهم.

لذا فلا بُد من وجود استجابة واسعة التنسيق عالية المستوى من الهيئات الحكومية الرئيسة وكبار اللاعبين الاقتصاديين، كالمصرف المركزي وكبار أصحاب الأعمال. وظهر هذا المستوى العالي من التنسيق الفعال لمواجهة أزمة وطنية، في أداء حكومة دولة الإمارات العربية المتحدة خلال ذروة أزمة كوفيد- 19.

لكن هجوماً إلكترونياً على النظام المصرفي قد يتسبب بأزمةٍ أكثر حدةً خلال فترة زمنية أقصر، فمع توقف المدفوعات الإلكترونية، وأجهزة الصراف الآلي، والمدفوعات في المتاجر، والحوالات بين البنوك محلياً ودولياً، سيكون التأثير الاقتصادي حاداً. وفي هذه الحالة، على إدارة المخاوف أن تطمئن الجمهور بشأن توفر السلع والخدمات الأساسية، بصورة استباقية مع بداية أي أزمة من هذا النوع.

وبإمكان تحالف واسع من الهيئات الحكومية الرئيسة وكبار اللاعبين الاقتصاديين، مبني مثلاً على لجنة كوفيد- 19، إعداد خطة طوارئ مشتركة وخطة استجابة وتبليغهما عامة الناس، حينها سيكون الجمهور وجميع الأطراف الفاعلة المعنية مطمئنين إلى أن الأزمة تحت السيطرة. وسيكون الحصول على ضمان من أعلى مستويات القيادة، خاصةً فيما يتعلق بسلامة الأموال وتوفر السلع والخدمات الأساسية، أمراً بالغ الأهمية.

وإضافةً إلى تفعيل صناديق الطوارئ وآليات توزيع الأموال، فعامة الناس والشركات الصغيرة بحاجة إلى المال لشراء السلع والخدمات الأساسية، كالوقود والخدمات الطبية.

ويتعين كذلك وضع قائمة محددة مسبقاً بالتعاملات التي يُحتمل أن تكون عرضةً للخطر، تسمح لفريق الاستجابة الطارئة بالتدخل الفوري لتقليل وقت الانقطاع إلى حده الأدنى، وتُستخلص هذه القائمة من تمارين اختبار الإجهاد المنفذة لتحديد مدى الضعف الذي تتسم به قائمة أنظمة المدفوعات الأساسية المحددة مسبقاً (كالمستشفيات والشرطة والدفاع المدني وغيرها.)

ويتعيّن على هيكل إدارة الأزمات أن يكون واضحاً ومرئياً كما كان حاله أثناء استجابة كوفيد- 19، إذ يجب أن تكون الاستجابة قوية ومطمئنة، وأن تُبلّغ المعلومات من خلال قنوات رسمية وجهات معنية تعلم بالضبط ما عليها فعله وفقاً للخطة.

على الصعيد الاقتصادي، يعد طول زمن الانقطاع عاملاً رئيساً، فكلما طال الهجوم، كان الضرر الذي يُلحقه بالاقتصاد وسمعته على المدى الطويل أكبر. ولطريقة إدارة الأزمة تأثير طويل الأمد على سمعة المؤسسات العامة والاقتصادية التي تدير اقتصاد دبي. ولأن الثقة عكس الخوف، فإن إدارة المخاوف عنصر أساسي في الحفاظ على الثقة في اقتصاد دبي على المديين القصير والطويل.

الثغـــرات الاجتمـــاعية

نقاط الضعف الاجتماعية هي المخاطر التي قد تؤثر على قدرة المجتمعات على التعامل الفعال مع التهديدات والتحديات الطارئة والتكيف معها. ويُقيَّم أسلوب تعامل المجتمع مع الأزمة إلى حد كبير من خلال طريقته في تخفيف الأثر السلبي على شرائحه الأكثر عرضةً للخطر.

وعلى الهيئات الحكومية الرئيسة ومؤسسات القطاع الاجتماعي وشرطة دبي أن تعمل معاً لوضع خطة استباقية للتخفيف من أثر هجوم إلكتروني واسع النطاق على الفئات الأكثر عرضةً للخطر في المجتمع، تبدأ من التوعية الوقائية. وكما هو الحال مع جوانب الصمود الأخرى التي نوقشت سابقاً، فإن لاستمرارية الخدمة وإدارة المخاوف أهميةً قصوى.

ويتعيّن تجهيز قائمة محددة مسبقاً من الشرائح المجتمعية ذات الاحتياجات الأكثر إلحاحاً، والتي لا تحتمل إلا الحد الأدنى من انقطاع السلع والخدمات. إضافةً إلى وضع خطة احتياطية واسعة النطاق وإبلاغها لجميع الجهات الرئيسة المستجيبة لحالات الطوارئ، والتي تشمل بعض مؤسسات القطاع الخاص كشركات الخدمات اللوجستية والعيادات الخاصة ومحطات الوقود ومحلات البقالة. فمثلاً يُمنح أشخاص من مهن معينة إمكانية الوصول إلى السلع والخدمات عبر نقاط توزيع مخصصة دون الحاجة إلى سداد أي مدفوعات.

وتقدّم شركات التأمين ضمانات تلقائية للمدفوعات غير الإلكترونية التي تعتمد على إظهار بطاقة مصرفية بلاستيكية وبطاقة الهوية الشخصية فحسب، ويتعيّن تحديد تسهيلات الدفع البديلة المؤقتة هذه والاتفاق عليها مسبقاً قبل حدوث الأزمة، وذلك لتحقيق أعلى مستويات الضمان وتقليل المخاوف الناشئة عن مصاعب لا مبرر لها.

ويتطلب التنسيق واسع النطاق في مكان عالمي مثل دبي ودولة الإمارات العربية المتحدة التعاون مع النوادي الإثنية والقبلية ومجالس الأحياء والمجالس العائلية، إضافةً إلى المجالس المهنية، والتشارك معها. ويلعب كبار أصحاب الأعمال دوراً مهماً أيضاً في تنسيق الاستجابة بين الهيئات الحكومية والبنوك وكبرى شركات تجارة التجزئة وموظفيها.

ولا بد أيضاً من إدارة الوعي على مستوى المجتمع المحلي، خاصةً لدى الأطفال وأهاليهم، وبمختلف اللغات. ولا تقتصر أهمية مركزية الاستجابة واتساقها على منع الخوف والقلق غير الضروريين فحسب، بل منع عمليات الاحتيال والأنشطة الإجرامية أيضاً التي قد تسعى إلى الاستفادة من الموقف.

التقـدم نحـو المستقبل

يتزايد تحول الاقتصاد والبنية التحتية الحيوية في دبي إلى الرقمنة. ومع استمرار الشركات ومقدمي الخدمات العامة في دبي في بناء الإمكانات اللازمة للاستفادة من التقنيات الرقمية، ستستمر مخاطر الجريمة الإلكترونية بالنمو والتضخم. ولا تختلف طبيعة التهديد السيبراني عن طبيعة الوباء، فقد يتحول الهجوم الإلكتروني على مؤسسة واحدة بسرعة إلى هجوم على جميع المؤسسات. وكحال الأوبئة، لا بد من إدارة المخاطر السيبرانية بشكلٍ جماعي من خلال التخطيط الواسع والعمل المنسق، ولا ينبغي أن يقع عبء تلك المهمة على عاتق الحكومة بمفردها ولا مؤسسات القطاع الخاص وحدها. إنما المطلوب إطار عمل واسع منسق يشمل جميع القطاعات المعنية، ونذكر هنا بعض العناصر المهمة لهذا الإطار.

نداء إلى العمل!

يمثل الهجوم على مؤسسة مالية واحدة هجوماً على البنية التحتية الحيوية في دبي. وسواء كان الهجوم محدوداً أو واسعاً، فالاستجابة يجب أن تكون واسعة ومنسقة.

على المستوى الحكومي

يتعيّن تشكيل وحدة حكومية رفيعة المستوى مكلفة بالحفاظ على استجابة منسقة واسعة النطاق تشمل جميع الهيئات الحكومية الرئيسة وكبار اللاعبين الاقتصاديين، كالمصرف المركزي وكبار أصحاب الأعمال.

يتعيّن منح الضمانات لعامة الناس من أعلى مستويات القيادة، وطمأنتهم بشأن توفر السلع والخدمات الأساسية وسلامة الأموال والبيانات الشخصية.

يتعيّن إنشاء قائمة محددة مسبقاً بالمجموعات المعرضة للخطر للسماح باستجابة فورية وفعالة في حالات الطوارئ.

على هيكل إدارة الأزمات أن يكون واضحاً ومعروفاً قبل حدوث أي أزمة وعليه أن يكون حاضراً خلال فترة التعافي.

يتعيّن تبليغ المعلومات وإتاحتها عبر قنوات رسمية معروفة.

تمثل شرطة دبي الجهة الأنسب لتنسيق الخطط وضمان تنفيذها عبر جميع المؤسسات الرئيسة المكونة للبنية التحتية الحيوية.

على الحكومة التأكد من أن البروتوكولات والممارسات الأمنية في المؤسسات الرئيسة الواقعة ضمن نطاق البنية التحتية الحيوية مرتبطة ببعضها في مختلف القطاعات وعلى مستوى الدولة.

على مستوى المؤسسات الرئيسة الواقعة ضمن نطاق البنية التحتية الحيوية

على مقدمي السلع والخدمات الأساسية الاتفاق على خطط طوارئ احتياطية على مستوى إمارة دبي تضمن أقل مستوى من انقطاع الخدمات، وأقصى قدر من ضمان الوصول إلى السلع والخدمات الأساسية.

على المؤسسات أن تنبه بعضها بعضاً حال وقوع هجوم إلكتروني أو اكتشاف ثغرة أمنية.

على المؤسسات أن ترفع مستوى الوعي بين الموظفين عن كيفية حدوث الهجمات الإلكترونية وتأثيرها.

على المؤسسات تطوير إطار عمل ناظم لشؤون الأمن السيبراني على مستوى إمارة دبي، يحدد القوانين والسياسات والخطوات ويقدم الإرشادات للمؤسسات عن كيفية إدارة البيانات وحمايتها والاستجابة للمخاطر وأعمال التخريب.

على الإدارات العليا في مختلف المؤسسات المكونة لمنظومة البنية التحتية الحيوية تطوير واعتماد استراتيجيات شاملة متعلقة بشؤون الأمن السيبراني واعتمادها.

على المؤسسات بناء شراكات مع المساهمين والمعنيين الرئيسيين تتمحور حول التنسيق الأمني وإدارة المخاطر، وتتمثل بعض أهدافها في تقليل احتمال تكرار الهجمات مستقبلاً وتخفيض تكلفة تبعاتها المادية.

على المستوى التقني

يجب أن تُصمم الأنظمة التقنية بطريقةٍ تتيح الاستجابة الفورية وسرعة التعافي.

يجب أن يسمح التصميم التقني بتنسيق أمني واسع النطاق بين المؤسسات المترابطة.

على المؤسسات شراء أنظمة تنبؤ متقدمة قادرة عل توقع أنواع التهديدات وتوقع حدوثها من خلال تحليل البيانات، وتتبع وسائل التواصل الاجتماعي ومراقبتها.

على المؤسسات توظيف أصحاب المهارات اللازمة لتشغيل الأنظمة التقنية وتحديثها، لتحقيق مستوىً عالٍ من الجاهزية ضد الهجمات الإلكترونية الوشيكة.

على المؤسسات وضع تصور للمخاطر الأمنية واحتمال التعرض لها جراء تعاملها مع سلاسل الإمداد العابرة للحدود.

الـمؤلفـــون

الدكتور سامي محروم
مؤسسة دبي للمستقبل

فاطمة راشد العليلي
شرطـة دبـي

آمنه علي البوم
شرطـة دبـي

الشيخة ميرة أحمد المعلا
شرطـة دبـي

جاسم محمد الشمري
شرطـة دبـي

المشاركون في التأليف

العميد الدكتور عبد اللّه عبد الرحمن بن سلطان
شرطـة دبـي

النقيب محمد أحمد المهيري
شرطـة دبـي

الدكتور حسام نبيل الشنراقي
شرطـة دبـي

سمية عبدالرحمن بن سلطان
شرطـة دبـي

الدكتور باتريك نوك
مؤسسة دبي للمستقبل

الجهات المشاركة في الورشة الأولى

مصرف الإمارات العربية المتحدة المركزي

هيئة تنمية المجتمع

بلدية دبي

اقتصادية دبي: دائرة التنمية الاقتصادية

معهد المجتمع الرقمي (المدرسة الأوروبية للإدارة والتكنولوجيا، برلين)

غرفة دبي

دائرة الموارد البشرية لحكومة دبي

هيئة كهرباء ومياه دبي

هيئة الصحة بدبي

شرطة دبي

مؤسسة دبي للمستقبل

مركز دبي المالي العالمي

المجلس التنفيذي

بنك الإمارات دبي الوطني

وزارة الداخلية

هيئة الطرق والمواصلات

دبي الذكية

Future Foresight
& Decision Making
Support
Center

استشراف المستقبل
ودعـــم اتخـــاذ
الـقـــرار
مركز

نبذة عن مركز استشراف المستقبل ودعم اتخاذ القرار في شرطة دبي

أنشئ المركز في سبتمبر من عام 1988م تحت مسمى مركز البحوث والدراسات، وفي الثالث من مايو عام 2001م بناءً على الرؤية الثاقبة والتوجيهات الحكيمة من صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة، رئيس مجلس الوزراء، حاكم دبي، تم تحويله إلى مركز لدعم اتخاذ القرار، وفي سبتمبر من عام 2016م، أمر القائد العام بتحويلة إلى مركز استشراف المستقبل ودعم اتخاذ القرار.

ويضم المركز ستة إدارات رئيسية هي علوم المستقبل، نظم دعم اتخاذ القرار، الإحصاء، الشؤون الإدارية، دعم وتطوير السياسات الأمنية.

وللمركز أنشطة متعددة وإصدارات علمية مميزة بلغت أكثر من 1000 إصداراً العديد منها يتم تدريسه في الكليات والمعاهد الشرطية، فضلاً عن أن كثيراً من الباحثين والدارسين للدكتوراه والماجستير في مختلف أنحاء العالم العربي يتخذون من إصدارات المركز مرجعية مهمة لإعداد الدراسات والبحوث المختلفة.
ويمتاز المركز بخبرائه المتخصصين في مجالات دقيقة مثل الإنذار المبكر والتنبؤ الأمني وبحوث العمليات والمؤشرات الكمية والحسابات الأمنية والأنظمة التخطيطية والإحصاء.

وللمركز إنجازات عديدة في مجال استحداث وتطوير المناهج الأمنية بالإضافة إلى أنه يواصل دائماً دعم الجهود الأمنية الرامية إلى مساندة الأهداف الإستراتيجية الخاصة بشرطة دبي حيث قام المركز بتوجيه إمكاناته وتسخير مدخلاته للمساهمة الفاعلة في بلوغ هذه الأهداف، ساعياً نحو المشاركة في تحقيق جميع أهداف الخطة الإستراتيجية لشرطة دبي دون استثناء. وقد كان لمرونة عمل المركز وتعدد تخصصات العاملين به الدور الحاسم فيما حققه المركز من إنجازات على كافة مرتكزات الخطة وجميع أهدافها بلا استثناء.

مؤسـسة دبي للمســـــتقبل
DUBAI FUTURE FOUNDATION

نبذة عن مؤسسة دبي للمستقبـــل

مؤسسة دبي للمستقبل أطلقها صاحب السمو الشيخ محمد بن راشد آل مكتوم، نائب رئيس الدولة رئيس مجلس الوزراء حاكم دبي «رعاه الله» في عام 2016 لتسهم في مسيرة استشراف وتصميم وتنفيذ المستقبل في دبي.

تتعاون المؤسسة مع مختلف الجهات الحكومية والخاصة في دبي ودولة الإمارات والعالم بهدف مواكبة التغيرات المتسارعة في مختلف القطاعات الاستراتيجية والاستعداد لها عبر تبني التقنيات الحديثة مثل الذكاء الاصطناعي والروبوتات والطباعة ثلاثية الأبعاد والبلوك تشين وإنترنت الأشياء وغيرها من أدوات الثورة الصناعية الرابعة.

تشرف مؤسسة دبي للمستقبل على العديد من المشاريع والمبادرات الرائدة مثل متحف المستقبل ومنطقة 2071 ومركز الثورة الصناعية الرابعة ومسرعات دبي المستقبل ومليون مبرمج عربي ومرصد المستقبل وغيرها الكثير من المبادرات المعرفية ومراكز تصميم المستقبل.

تهدف المؤسسة من خلال هذه المبادرات إلى إعداد أجيال الغد من الكوادر الوطنية لمتطلبات المستقبل وتمكينهم بالمهارات الضرورية للمساهمة في مسيرة التنمية المستدامة في الدولة.

وتسهم المؤسسة بتعزيز مكانة دبي كوجهة عالمية لأفضل العقول وحاصنة لأصحاب الابتكارات الواعدة والشركات الناشئة والمؤسسات العالمية للعمل على إيجاد حلول مبتكرة وتطبيقها على أرض الواقع.

dubaifuture.ae research@dubaifuture.gov.ae @dubaifuture

مؤسسة دبي للمستقبل
DUBAI FUTURE FOUNDATION

DUBAIFUTURE.AE