السلامة الرقمية

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

العدد الأول / الخميس 16 ربيع الأول 1446هـ - 19 سبتمبر 2024م

دلال العقيدي
العالم على أعتاب تطوّرات تكنولوجية وتحوّلات سيبرانية

دولة قطر
تحصل على النقاط الكاملة 100% في المؤشـر الدولي للأمن السيبراني

تغييرات كبيرة
ضمن الإصدار الخامس من المؤشر الدولي للأمن السيبراني

المحتويات

العالم على أعتاب تطوُّرات تكنولوجية وتحوُّلات سيبرانية

دلال العقيدي
مدير إدارة التميز السيبراني الوطني

في سياق التطورات التكنولوجية المتسارعة، والانتشار السريع أُفقياً وعمودياً للفضاء السيبراني، يبدو العالم على أعتاب ثورة تكنولوجية جديدة، مهَّد لها ظهور مفاهيم جديدة، مثل إنترنت الأشياء، والـذكاء الاصطناعي، والذكاء الاصطناعـي التوليدي، وعوالم الميتافيـرس، والتوائم الرقمية، وغيرها من المفاهيم التكنولوجية الحديثة.

هذا الواقـع التكنولوجي يترك آثاره المباشـرة وغير المباشـرة على مختلف جوانب الحياة، بما يشـمل الاقتصاد والثقافـة والمجتمع، وحتى السياسة. كما أن التصاعد المتسارع للتهديدات السـيبرانية وزيادة حدة الخسـائر الناجمة عنها ساهم في جعل الأمن السيبراني ركناً رئيساً من أركان الأمن القومي للدول.

ومن جهة أخـرى، يتَّجه العالـم أجمع بخطواتٍ سـريعةٍ نحو الرقمنة، وهذا مـا يُحتِّم الاهتمام الكافـي بتوفير الأمـن السـيبراني والسلامة الرقمية لمختلف الخدمات الرقمية التي تُقدِّمها الحكومـات، فالخدمات الرقمية غير المدعومة بفضاء سـيبراني آمِن، سـتفقد فاعليتها، وقد تتحوَّل لثغرة أمنية يتسـلل منهـا المهاجمون. كلّ هذه المعطيات تُعزِّز من فكرة أن التطوُّرات التكنولوجيـة التـي سيشـهدها العالـم في السـنوات القادمة سـيكون لها بالـغ الأثر في مختلف جوانب الحياة.

وانطلاقاً من هذا الطـرح، ومن ضرورة الإلمام التـامّ بمختلـف التطـورات والمسـتجدَّات السـيبرانية والتكنولوجية؛ جـاءت فكرة "مجلة المبـادرة الوطنيـة للسلامة الرقميـة"، والتي تهدف لتقصّي المستجدَّات السيبرانية الحديثة، وعَرْضها بأسـلوب مختصر يتناسب مع مستوى وعي الجمهور العام.

وتسـعى الوكالة الوطنية للأمن السيبراني من خلال هـذه المجلة، إلى نقل صـورة دقيقة عن التطورات الدولية السيبرانية، وتحليلها، وتحديد آثارها علـى الفضاء السـيبراني الدولي، وذلك انطلاقـاً من وحدة الفضاء السـيبراني الدولي، واسـتناداً إلى فكرة أن التهديدات السيبرانية لا تعترف بالحدود، بل هي تهديدات تَطال الجميع.

تغييرات كبيرة ضمن
الإصدار الخامس من المؤشر الدولي للأمن السيبراني

دولة قطر تحصل على النقاط الكاملة 100% في المؤشـــر الدولي للأمن السيبراني

في سياق التطورات المستمرة في مجال الأمن السـيبراني؛ صـدر مؤخراً الإصـدار الخامس من المؤشر الدولي للأمن السيبراني، والذي يُعَدّ من الأدوات الأساسية لتقييم وتوجيه إستراتيجيات الأمن السيبراني على مستوى العالم.

ويُعدّ هذا الإصدار الجديد تتويجاً لجهود طويلة الأمد في تحسـين القدرة علـى قياس فعالية التدابير الأمنية وملاءمتها لمواجهة التهديدات المتزايدة والمتطورة في عالم الإنترنت.

التركيز علـى القضايـا الاجتماعية والإنسانية يدخل ضمن تقييم الدول سيبرانياً

أحد أبـرز التغييرات التي طرأت على هذا الإصدار -مقارنـةً بالإصدار السـابق- هو إدخـال معايير تقييـم جديـدة تعكـس التقـدم التكنولوجي والتهديدات الحديثة؛ فقـد تم تعديل منهجية التقييم لتشـمل معايير أكثـر تفصيلاً وملاءمةً للتغيُّرات السريعة في المشهد السيبراني.

ومـن بين هذه التعـديلات، تم التركيز بشـكل أكبر على تقييم القدرات الدفاعية في مواجهة الهجمات السـيبرانية المعقَّـدة، بما في ذلك الهجمـات القائمة علـى الـذكاء الاصطناعي والتعلم الآلي. هذا التغيير يعكس الوعي المتزايد بخطورة التهديـدات المتقدّمـة، ويؤكّد على أهمية التكيُّف السريع مع التقنيات الجديدة[1].

كما أُدْخِلَت تعديلات على نطاق التقييم؛ ليشمل المزيـد من القطاعـات الصناعيـة والحكومية التي لم تكن ممثلةً بشكلٍ كافٍ في الإصدارات السـابقة. فبـدلاً مـن التركيز التقليـدي على القطاعات المالية والتجارية، أصبح المؤشر الآن يتناول تأثير الأمن السـيبراني على البنية التحتية الحيوية، مثل الطاقة والنقل والمرافق العامة. هذا التوسُّـع يعكس الاعتراف المتزايد بأهمية حماية جميع القطاعات الحيوية لضمان استقرار الأنظمة الاقتصادية والاجتماعية.

1. Global Cybersecurity Index 2024, International Telecommunication Union, Published in Switzerland Geneva, 2024, on site: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

ومن التغييرات البارزة الأخرى أيضاً: إدخال معايير جديدة تتعلق بإدارة المخاطر والاستجابة للحوادث؛ فقد تم تحسين معايير تقييم استجابة المؤسسات للحوادث السيبرانية بشكلٍ يتماشى مع الممارسات العالمية الأفضل، مع التركيز على تعزيز القدرة على الكشف المبكّر والتعامل الفعّال مع الحوادث. ويشمل ذلك تقييم مدى فعالية إستراتيجيات الاستجابة للحوادث، وكيفية إدارة الأزمات بشكل يُخفّف من تأثير الهجمات.

فيما يخصّ القياس والتقارير، شهد الإصدار الخامس تحسينات كبيرة في طرق جمع البيانات وتحليلها؛ فقد تم تطوير أدوات تحليلية جديدة تُتيح للمؤسسات تقييم أدائها الأمني بشكل أكثر دقةً وتفصيلاً[1].

الإصدار الخامس من المؤشر الدولي للأمن السيبراني: تحسينات كبيرة في طرق جمع البيانات وتحليلها

وتتضمَّن هذه الأدوات تحسينات في جمع بيانات الأمن السيبراني، وتحليل الاتجاهات والتوقعات المستقبلية، مما يُعزّز من قدرة المؤسسات على التخطيط الإستراتيجي واتخاذ القرارات المبنية على بيانات موثوقة.

من بين التغييرات البارزة التي شهدها هذا الإصدار الجديد في ترتيب الدول في مؤشرات الأمن السيبراني، تم تقسيم الدول إلى خمس مجموعات في التصنيف؛ يضمّ التصنيف الأول الدول الرائدة في مجال الأمن السيبراني.

1. Global Cybersecurity Index 2024, International Telecommunication Union, Published in Switzerland Geneva, 2024, on site: https://www.itu.int/dms_pub/itu-d/opb/hdb/d-hdb-gci.01-2024-pdf-e.pdf

جدير بالذكر أن دولة قطر قد حصلت على مجموع النقاط الكاملة في المؤشر 100%، وذلك على مستوى محاور المؤشـــر الخمسة، وهي: محور التدابير القانونية، والتدابيـــر التنظيمية، وتدابير التعاون، وتدابير بناء القـــدرات، والتدابير الفنية. وحصلت قطر في كلٍّ من هذه التدابير على 20 نقطة من أصـــل 20، وبذلك تكـــون قد حصلت على نقاط المؤشر الكاملة.

هجوم سيبراني

يُوقِف حركة النقل في لندن

هجوم سيبراني على هيئة النقل في لندن يُثير تساؤلات حول مدى أمان الشبكات الحيوية في المدن الكبرى

في واحدةٍ من أبرز قضايا الجريمة السيبرانية التي شهدتها لندن مؤخراً، اعتقلت السلطات شاباً بتهمة خرق شبكة النقل العامة، ما أدّى إلى اضطراب كبير في النظام الذي يعتمد عليه ملايين الركاب يومياً[1].

القضيــة بدأت عندمــا لاحظت هيئة النقل في لندن وجــود أعطال غير مُبرَّرة في نظامها الإلكتروني، ما تسـبَّب في تأخيرات طويلة للقطارات والحافلات، وتجاوزات في جداول التشــغيل. مع تفاقم المشكلة وعدم قدرة الفنيين على تحديد السبب الرئيس في ذلك[2].

ثم اتضح أن الأمر لا يتعلق بعطل تقني عابر، بل هو نتيجة لهجوم سيبراني معقّد.

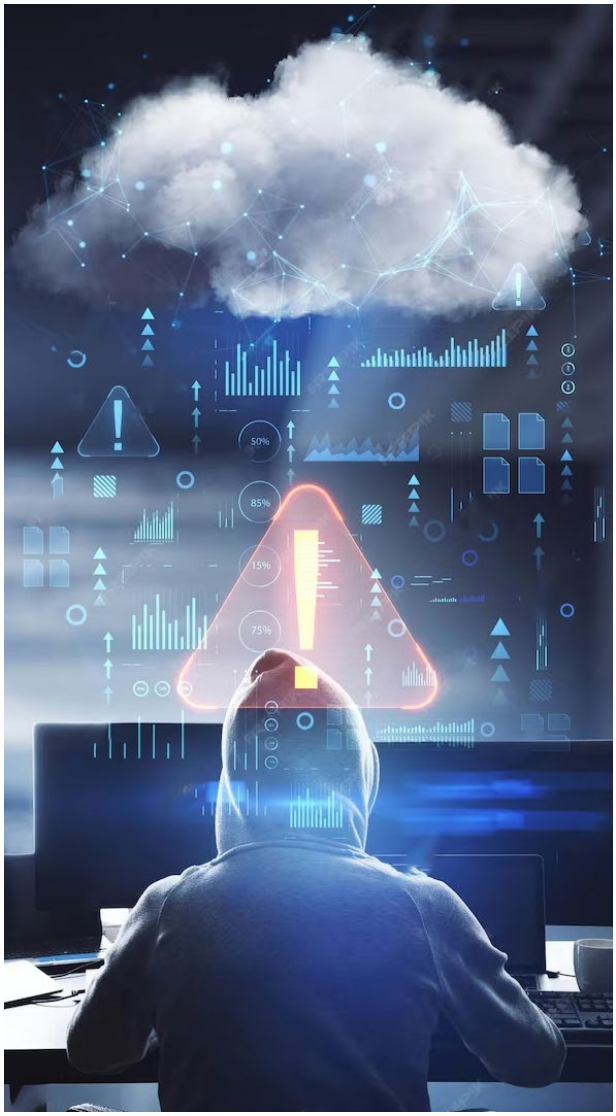
بعد تحقيقات مكثّفة، تمكّنت الشــرطة من تحديد مصدر الهجوم، وتتبُّع الأنشــطة المشــبوهة، وتم تحديد المتّهم وهو شــابّ في أوائل العشــرينيات من عمره. استخدم مهاراته العالية في البرمجة للاختراق والدخول إلى نظام النقل المركزي[3].

الهدف من وراء هذا الهجوم لم يكن واضحاً تماماً في البداية، لكنّ المحقّقين يشيرون إلى احتمال أن الشابّ كان يسعى لإثبات قدراته في مجال الاختراق، وربما لاســتعراض قدراته الســيبرانية. الســلطات لم تستبعد أيضاً احتمال أن تكون دوافعه سياسية أو أيديولوجية.

1. TfL still affected by 'ongoing cyber incident, BBC, September 2024, on site: https://www.bbc.com/news/articles/c4gqg2elkj4o
2. TfL restricts access to online services due to cyber-attack, Gazette&Herald, September 2024, on site: https://www.gazetteherald.co.uk/news/national/24567377.tfl-restricts-access-online-services-due-cyber-attack/
3. Teenager arrested over Transport for London cyber-attack, Burymercury, September 2024, on site: https://www.burymercury.co.uk/news/national/24580847.teenager-arrested-transport-london-cyber-attack/

وأشـــارت التحقيقات إلى أن الشـــابّ تمكّن من الوصول إلى النظام من خلال ثغرة أمنية كانت غير مكتشَفة من قبل، مما أثار قلقاً واسعاً بشأن نقاط الضعف في البنية التحتية السيبرانية للمدينة.

وعلـــى الرغم من أن الســـلطات تمكّنت من اســـتعادة الســـيطرة على النظام بعد ساعات من الاختراق، إلا أن تأثيره كان واضحاً وطويل الأمد.



هجوم ســـيبراني على هيئة النقل البريطانية يستغل ثغرة أمنية كانت غير مُكتَشفة من قبل

تعطّل وســـائل النقل أثّر بشـــكلٍ كبير علـــى حياة الناس اليوميـــة؛ حيث اضطـــرت العديـــد من المحطـــات إلى الإغلاق المؤقّت، وازدحمت الشوارع بالسيارات بسبب تراجع الاعتماد على وســـائل النقـــل العامة. في الوقت ذاته، أثـــارت هذه الحادثة تســـاؤلات حـــول مدى أمان الشـــبكات الحيوية في المدن الكبـــرى، ومدى قدرتها على مواجهة الهجمات السيبرانية المتزايدة.

أول نتائج عملية كرونوس
تظهر بعد قرابة عشر سنوات منذ إطلاقها

بدأت عملية "كرونوس" في أغسطس 2015 كجهد دولي منسَّق لمكافحة الجريمة السيبرانية المنظَّمة، خاصةً تلك التي استهدفت القطاع المالي عبر برمجيات خبيثة مثل "كرونوس".

هذه البرمجية تم تطويرها لسرقة بيانات الحسابات المصرفية عن طريق إصابة الأنظمة البنكية وتحويل الأموال بشكل غير شرعي.

عملية كرونوس لم تقتصر على القبض على المتورطين فحسب، بل شملت أيضاً تفكيك البنية التحتية التي استخدمها المهاجمون

بفضل التعاون الوثيق بين العديد من وكالات تنفيذ القانون العالمية، بما في ذلك الإنتربول واليوروبول، تم تنفيذ سلسلة من المداهمات في دُوَل متعددة أدَّت إلى توقيف أفراد رئيسيين في الشبكة المسؤولة عن الهجمات الإلكترونية[1].

هذه العملية لم تقتصر على القبض على المتورطين فحسب، بل شملت أيضاً تفكيك البنية التحتية التي استخدمها المهاجمون. كما كشفت الحملة عن مدى تعقيد الجريمة السيبرانية الحديثة؛ حيث كانت المجموعات الإجرامية تستفيد من أدوات متطورة وتقنيات تشفير عالية الدقة للتخفي وتجنُّب الرصد. لكن بفضل سنوات من التحقيقات والتنسيق بين الدول، تمكَّنت السلطات من تحقيق تقدمٍ ملموسٍ في تفكيك تلك الشبكات[2].

واحدة من النتائج الرئيسة لعملية "كرونوس" كانت الكشف عن مدى تعرُّض المؤسسات المالية للهجمات الإلكترونية؛ فالبنوك والمنصات المصرفية تُعدّ أهدافاً رئيسةً؛ نظراً لكمية الأموال التي يمكن تحويلها بشكل غير قانوني عبر استغلال الثغرات الأمنية.

1. Hostetler.Stefan, Operation Cronos: The Takedown of LockBit Ransomware Group, Arcticwolf, February 2024, on site: https://arcticwolf.com/resources/blog/operation-cronos-the-takedown-of-lockbit-ransomware-group
2. Owenson.Gareth, How Law Enforcement's Ransomware Strategies Are Evolving, Darkreading, September 2024, on site: https://www.darkreading.com/cybersecurity-operations/how-law-enforcement-ransomware-strategies-are-evolving

عملية كرونوس بمثابة جرس إنذار للمؤسسات الحكومية والخاصة

وقد أظهرت العملية أيضاً أن الجرائم السيبرانية أصبحت أكثر تنظيماً واحترافيةً؛ حيث تعمل شبكات الهجمات السيبرانية بشكل يشبه الشركات التقليدية، مع وجود فِرَق متخصصة في كل جزء من العملية، بدءاً من تطوير البرمجيات الخبيثة، وصولاً إلى تنفيذ الهجمات وتصفية الأموال المسروقة.

تصريحات المسؤولين بعد انتهاء عملية "كرونوس" أشارت إلى أن هذا النوع من العمليات يُعدّ بداية في سلسلة من الجهود لمواجهة الجريمة السيبرانية على مستوى عالمي.

إن الأمن السيبراني أصبح في مقدمة الأولويات الوطنية والدولية؛ حيث تهدّد الهجمات السيبرانية اليوم ليس فقط الأنظمة المالية، بل أيضاً البنى التحتية الحيوية، مثل شبكات الطاقة، والنقل، والاتصالات.

هذه العملية كانت بمثابة جرس إنذار للمؤسسات الحكومية والخاصة بضرورة تكثيف جهود الحماية السيبرانية، وتبنّي تقنيات دفاعية متقدّمة للتصدي لتلك التهديدات المتزايدة.

هجمات سيبرانية

تطال قطاعَي التعليم والمستشفيات في الولايات المتحدة

هجوم سيبراني على المؤسسات التعليمية والصحية في الولايات المتحدة يدفع إلى حالة من الطوارئ القصوى

خلال شهر سبتمبر الجاري، شهدت المؤسسات التعليمية والرعاية الصحية موجةً غير مسبوقة من الهجمات السيبرانية التي أثّرت بشكلٍ عميق على وظائفها الأساسية، وأثارت مخاوف واسعة من تداعياتها.

كانت الهجمات التي طالت المدارس والمستشفيات متزامنةً، مع تزايد التهديدات السيبرانية التي تجتاح العالم السيبراني؛ مما دفَع هذه المؤسسات إلى إعلان حالة من الطوارئ القصوى، وفَرَض عليها اتخاذ تدابير عاجلة لحماية بياناتها وحفظ سلامة واستمرار خدماتها.

بدأت الأحداث بسلسلة من البرمجيات الخبيثة التي استهدفت الأنظمة التعليمية، كان الهدف منها تعطيل الأنظمة الدراسية، وإحداث الفوضى في العمليات التعليمية، مما يعكس أساليب جديدة لابتزاز المال والتلاعب بالبيانات.

الهجوم الذي طال العديد من المدارس تسبَّب في انتشار فيروس تشفير البيانات؛ حيث قام المهاجمون بتشفير ملفات مهمَّة تتعلق بالطلبة والمعلمين، مما أعاق قدرة المدارس على إجراء المحاضرات وتنظيم الأنشطة الدراسية[1].

كما تعرَّضت المعلومات الشخصية للمعلمين والطلبة في العديد من الحالات للتسريب، مما عرَّضهم لمخاطر إضافية مثل الاحتيال وسرقة الهوية. هذا الهجوم لم يُؤثّر فقط على الانتظام الطبيعي للعملية التعليمية، بل ألحق أيضاً أضراراً نفسية بالطلبة وأُسَرهم.

في ذات الوقت، تعرَّضت المستشفيات لهجمات سيبرانية مماثلة؛ حيث تم استهداف أنظمة إدارة المرضى والبيانات الطبية. ومع تعطل الأنظمة، واجهت المستشفيات صعوبة في الوصول إلى سجلات المرضى، مما أعاق قدرتها على تقديم الرعاية الصحية بشكلٍ فعَّال[2].

وفي بعض الحالات، تعطّلت عمليات الجراحة العاجلة والإجراءات الطبية الحيوية؛ بسبب عدم القدرة على الوصول إلى البيانات الطبية اللازمة، مما أدَّى إلى تأخير شديد في تقديم العلاج.

هذا النوع من الهجمات نتج عنه عواقب وخيمة؛ حيث تعرَّضت حياة المرضى للخطر؛ بسبب عدم القدرة على متابعة حالتهم الطبية بشكلٍ مستمر.

أثارت هذه الهجمات ردود فِعْل قوية مِن قِبَل الشركات والمؤسسات؛ حيث تم استنفار فِرَق خاصة للتحقيق في الهجمات، وتحديد مصدرها، وتحديد آليات التصدي لها.

وكانت هناك دعوات ملحَّة لتعزيز تدابير الأمن السيبراني وتطوير إستراتيجيات وقائية جديدة للتصدي لهذه الهجمات المتطورة، وقد تجسَّدت هذه الدعوات في تعزيز التعاون بين الدول وتبادل المعلومات حول التهديدات السيبرانية.

تعكس هذه الهجمات الواقع المتزايد لمخاطر الأمن السيبراني، وتُبْرز الحاجة الملحَّة لمواجهة هذه التهديدات بأساليب مبتكَرة ومستدامة. وتظل المؤسسات التعليمية والصحية في صميم المجتمع؛ ولذا فإن حمايتها من الهجمات السيبرانية ليست فقط مسألة تقنية، بل مسؤولية اجتماعية تعكس مدى الاهتمام بسلامة وأمن المعلومات وحماية الخدمات الحيوية التي يعتمد عليها الجميع.

1. Lyons, Jessica. Cyber crooks shut down UK, US schools, thousands of kids affected, The Register, September 2024, on site: https://www.theregister.com/2024/09/11/uk_us_school_ransomware
2. Alder, Steve. Healthcare Data Breach Statistics, Hipaa Journal, August 2024, on site: https://www.hipaajournal.com/healthcare-data-breach-statistics/

مؤتمر BSides Bloomington 2024

يُشْرِك المجتمع المدني في جهود الأمن السيبراني

مؤتمر BSides Bloomington 2024

يتفرَّد بتركيزه على إشراك المجتمع المحلّي في محادثات حول الأمن السيبراني؛ حيث يتميَّز هذا الحدث بطابعه المجتمعي

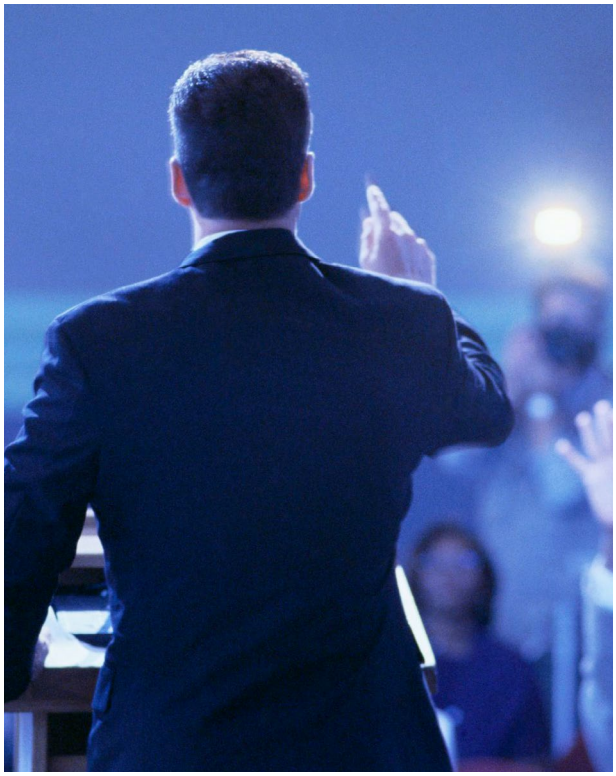
مؤتمر BSides Bloomington 2024 يُعدّ واحداً من الفعاليات المميزة ضمن سلسلة مؤتمرات (BSides) التي تحظى بشعبية عالمية في مجتمع الأمن السيبراني.

يُعقَد هذا المؤتمر في مدينة بلومنغتون بولاية إنديانا بالولايات المتحدة، وهو منصّة تُتيح للمحترفين والمهتمين بمجال أمن المعلومات فرصة للتعلُّم والتفاعل والمشاركة في بيئة داعمة ومُحفِّزة. يتميز هذا الحدث بطابعه المجتمعي؛ حيث ينظّم بالكامل مِن قِبَل متطوعين، ويهدف إلى تعزيز التعاون بين مختلف المتخصصين في المجال[1].

أهم ما يميز BSides Bloomington هو أنه ليس مجرد مؤتمر تقني، بل هو تجربة تفاعلية تُشجّع المشاركين على تقديم عروضهم وأفكارهم، والمساهمة بشكلٍ مباشر في الحوارات والنقاشات.

الموضوعات التي تتناولها الجلسات تشمل أحدث الابتكارات في حماية الشبكات، وتأمين البنية التحتية الحيوية التي أصبحت هدفاً رئيساً للتهديدات السيبرانية، وكذلك الأبحاث المتقدّمة حول الأمن السحابي، وتأمين التطبيقات، والتهديدات المتزايدة التي تُواجهها الشركات والمؤسسات.

يتفرَّد المؤتمر بتركيزه على إشراك المجتمع المحلي في محادثات حول الأمن السيبراني، وإتاحة الفرصة لكلٍّ من الهواة والمحترفين لعَرْض أبحاثهم، والمشاركة في نقاشات حيوية حول أحدث التوجُّهات في عالَم الأمن السيبراني.



لا تقتصر قيمة BSides Bloomington على الجوانب التقنية فقط، بل تشمل أيضاً جوانب تعليمية وتوعوية تُسهم في توسيع الفهم حول التحديات السيبرانية، وكيفية مواجهتها بطرق إبداعية وفعَّالة.

يمكن القول: إن BSides Bloomington يمثل نقطة التقاء مهمة لمجتمع الأمن السيبراني، فهو لا يهدف فقط إلى تبادل المعرفة، بل يسعى أيضاً إلى بناء مجتمع مترابط، يُمكِّن أفراده من التعاون بشكلٍ مستمر لمواجهة التهديدات السيبرانية المتزايدة في العصر السيبراني.

هذه الفعالية تُمثّل فرصة ثمينة لكلّ مَن يسعى إلى تطوير مهاراته في مجال الأمن السيبراني، وتوسيع شبكة علاقاته المهنية، والتعلم من خبراء المجال في بيئة تفاعلية ومفتوحة.

1. https://bsidesbloomington.org/schedule

تصاعُد الهجمات السيبرانية
على قطاع الطاقة في أوروبا والولايات المتحدة

خلال شهر أغسطس الماضي، شهد قطاع الطاقة في أوروبا تصاعداً ملحوظاً في الهجمات السيبرانية، وهو ما أثار قلقاً واسعاً بين الحكومات والشركات. هذه الهجمات استهدفت البنية التحتية الحيوية للطاقة مثل أنظمة الكهرباء والغاز، مما أدّى إلى تعطيل بعض الأنظمة بشكلٍ مُؤقّت، وتهديد سلامة إمدادات الطاقة.

الهجمات السيبرانية على قطاع الطاقة في أوروبا ليست ظاهرةً جديدةً، لكنّها أصبحت أكثر تعقيداً وتنسيقاً في الآونة الأخيرة. أحد الأسباب الرئيسة وراء هذا التصاعد هو الاعتماد المتزايد على التكنولوجيا والأنظمة السيبرانية في إدارة شبكات الطاقة، مما يزيد من فرص الاستهداف. ومن بين التكتيكات التي تم استخدامها في هذه الهجمات هي برمجيات الفدية (Ransomware) التي تعمل على تشفير بيانات الأنظمة، وطلب فدية مالية مقابل فك التشفير. في بعض الحالات، تم استهداف شركات الطاقة الكبرى بهدف تعطيل الإنتاج والتسبُّب في خسائر مالية كبيرة[1].

1. Critical infrastructure faces 30 percent surge in cyber-attacks, Industrial Cyber, August 2024, on site: https://industrialcyber.co/critical-infrastructure/critical-infrastructure-faces-30-percent-surge-in-cyber-attacks-knowbe4-report-highlights/

أوروبا والولايات المتحدة تتعرَّضان لهجمات سيبرانية استهدفت البنية التحتية الحيوية للطاقة مثل أنظمة الكهرباء والغاز

الهجمات الأخيرة تميَّزت باستخدام برمجيات ضارَّة متقدمة مثل Sandworm وSnake، وهي أدوات اختراق معروفة بفعاليتها في استهداف البنية التحتية الحيوية. إضافةً إلى ذلك، كانت هناك محاولات متزايدة لتدمير البنية التحتية الفيزيائية من خلال الهجمات السيبرانية، مثل تعطيل الأنظمة التي تتحكَّم في تشغيل المحطات الكهربائية، وهو ما قد يُؤدّي إلى انقطاع التيار الكهربائي على نطاقٍ واسعٍ.

تصاعُد الهجمات السيبرانية على قطاع الطاقة وهجمات الفدية يُشكّل تحدياً كبيراً للمجتمعات الحديثة، ويستدعي اتخاذ تدابير أمنية أكثر شمولاً.

كما تم الإبلاغ عن هجمات فدية واسعة النطاق استهدفت الشركات الكبرى والمرافق الحكومية في الولايات المتحدة وأوروبا. إحدى أبرز الهجمات كانت على مؤسسة مالية كبرى في أوروبا؛ حيث تم تشفير أنظمتها، وطالَب المهاجمون بفدية تُقدَّر بملايين الدولارات.

كانت الهجمات تتميَّز بتكتيكات جديدة مثل "الفدية المزدوجة" (Double Extortion)؛ حيث لا يقوم المهاجمون بتشفير البيانات فقط، بل يُهدّدون بنشر المعلومات الحساسة إذا لم يتم دفع الفدية. هذا النوع من الهجمات يضع ضغطاً مضاعفاً على الضحايا، الذين لا يواجهون فقط خسارة بياناتهم، ولكن أيضاً خطر تسرُّب معلوماتهم السرية.

يمكن تفسير هذا التصاعد في هجمات الفدية والهجمات السيبرانية على البنية التحتية الحيوية بعدة عوامل:

أولاً: الاعتماد المتزايد على التكنولوجيا السيبرانية والتواصل عبر الإنترنت في إدارة الشبكات الحيوية، مثل الكهرباء والطاقة، زاد من نقاط الضعف.

ثانياً: جماعات القراصنة المدعومة من دول أصبحت أكثر تطوراً واستخداماً للتكنولوجيا المتقدمة في شنّ هجماتها.

ثالثاً: الأرباح المحتمَلة من هذه الهجمات تجعلها جذّابة للمجرمين، خاصةً مع تطوّر العملات السيبرانية التي تجعل تتبُّع الأموال المدفوعة في الفدية أمراً صعباً[1].

1. The New Energy Frontier: Tackling Cyber Threats in Europe's Renewable Energy Systems, The European Business Review, September 2024, on site: https://www.europeanbusinessreview.com/the-new-energy-frontier-tackling-cyber-threats-in-europes-renewable-energy-systems

Oracleg IBM تُطلقان أنظمة تشفير جديدة

في الأشهر الأخيرة، تم إطلاق مجموعة جديدة من أدوات التشفير التي تهدف إلى تعزيز أمان البيانات في البيئات السيبرانية المختلفة. تأتي هذه الابتكارات في وقتٍ تتزايد فيه التهديدات السيبرانية وتتعقّد الهجمات، مما يضع الشركات والمؤسسات أمام تحديات كبيرة لحماية بياناتها.

وفي ظل التطور التكنولوجي المستمر، يُعدّ تحسين وسائل التشفير واحداً من أهم السُّبل التي يمكن الاعتماد عليها لضمان سرية البيانات ومنع اختراقها.

أحد أبرز التطورات التي حدثت في مجال التشفير هي إطلاق أدوات تعتمد على الحوسبة الكمومية. وقدَّمت شركتا IBM & Google حلولًا جديدة تعتمد على تشفير ما بعد الكم، والذي يُعتبر جزءاً من الجهود الرامية إلى تأمين الأنظمة في عصر الحوسبة الكمومية[1].

تطوير أدوات التشفير من أهم تقنيات ضمان سرية البيانات

هذه التقنيات تعتمد على خوارزميات جديدة لا يمكن فكّ تشفيرها باستخدام أجهزة الحوسبة التقليدية أو الكمومية، وهو ما يُمثِّل تقدُّماً كبيراً في هذا المجال.

الحوسبة الكمومية لديها القدرة على كَسْر أنظمة التشفير التقليدية بسرعة كبيرة بفضل قدراتها الحسابية الهائلة، ولهذا السبب كان هناك ضغط كبير على تطوير أدوات تشفير قوية قادرة على الصمود أمام هذه التقنية المستقبلية.

1. Korolov, Maria. IBM, Microsoft and Boeing mark advances in quantum computing, Network World, September 2024. On site: https://www.networkworld.com/article/3523669/ibm-microsoft-and-boeing-mark-advances-in-quantum-computing.html

ومن بين هذه الأدوات، تم تطوير خوارزميات جديدة مثل CRYSTALS-Kyber، CRYSTALS-Dilithium، المعتَمَدتين مِن قِبَل معهد المعايير والتكنولوجيا الوطنية (NIST) كجزء من مبادرة لتطوير أنظمة تشفير مقاومة للحوسبة الكمومية.

التشفير السحابي المتقدّم

بالتوازي مع تطورات الحوسبة الكمومية؛ أطلقت شركات أخرى مثل Microsoft، Oracle أدوات تشفير جديدة مخصَّصة لحماية البيانات في البيئات السحابية.

IBM و Google تقدّمان حلولاً جديدة تعتمد على تشفير ما بعد الكم

ولكن مع ازدياد الاعتماد على الحوسبة السحابية لتخزين البيانات وإدارتها؛ ظهرت الحاجة لتقنيات تشفير متقدّمة تحمي البيانات أثناء نَقْلها وتخزينها في السحابة.

أدوات التشفير السحابي مثل Azure Confidential Computing من Microsoft تعتمد على استخدام أدوات لتأمين البيانات وهي في حالة استخدام، وليس فقط أثناء النقل أو التخزين.

هذه الأدوات تُتيح معالجة البيانات في بيئة معزولة وآمِنَة، مما يُقلّل من مخاطر التهديدات السيبرانية التي قد تَستهدف الأنظمة السحابية.

علاوةً على ذلك، قدَّمت Oracle تقنيات جديدة في التشفير الشفاف؛ حيث يمكن للمستخدمين تشفير بياناتهم دون الحاجة إلى القلق بشأن فقدان الأداء أو القدرة على الوصول السريع إلى البيانات.

IBM و Google تطلقان أداة TLS 1.3 وهي نسخة محسَّنة من بروتوكول الأمان المستخدم في معظم التبادلات على الإنترنت

في مجال حماية الاتصالات، تم إطلاق أدوات جديدة تهدف إلى تأمين القنوات المستخدَمة في نقل المعلومات بين الأجهزة. إحدى هذه الأدوات هي TLS 1.3، وهي نسخة محسَّنة من بروتوكول الأمان المستخدَم في معظم التبادلات على الإنترنت.

تُقدّم هذه النسخة تحسينات كبيرة في سرعة وأمان الاتصالات، وتُوفّر ميزات إضافية لحماية البيانات المتبادَلة، مثل مفاتيح التشفير الأكثر تعقيداً والآليات الجديدة للتفاوض على أمان الاتصال[1].

إلى جانب حماية الأنظمة الكبيرة مثل البنوك والمؤسسات الحكومية؛ يمكن لهذه الأدوات الجديدة أن تكون حلاً مناسباً لمجالات حساسة مثل الرعاية الصحية والمالية. على سبيل المثال، يمكن لمستشفيات تعتمد على التقنيات السحابية أن تَستخدم تشفير البيانات المحسّنة لضمان أمان السجلات الطبية للمرضى. كما يمكن للبنوك والمؤسسات المالية استخدام تشفير متقدّم لحماية بيانات العملاء والمعاملات السيبرانية.

يُمثّل إطلاق هذه الأدوات مرحلةً جديدةً في حماية البيانات الحساسة؛ حيث تسعى الشركات إلى البقاء متقدّمة بخطوة على المهاجمين السيبرانيين، وضمان حماية أنظمتها بأحدث تقنيات الأمان.

1. How to migrate to TLS, Microsoft, September 2024, on site: https://learn.microsoft.com/en-us/azure/service-fabric/how-to-migrate-transport-layer-security

الاتحاد الأوروبي يُصْدِر تشريعات سيبرانية جديدة

الاتحاد الأوروبـــي يرد على تصاعُـــد الهجمات بإصدار تشـــريعات سيبرانية صارمة

فـــي إطار الجهود المتزايـــدة لحماية الفضاء الســـيبراني والتصدّي للتهديدات الســـيبرانية؛ أعلن الاتحاد الأوروبي عن إصدار مجموعة من التشـــريعات الجديدة في مجال الأمن الســـيبراني خلال شهر سبتمبر الجاري.

هذه الخطوة جاءت ردّاً مباشـــراً على تصاعُد الهجمات الســـيبرانية التي استهدفت بشكلٍ متزايد البنية التحتية الحيوية، والمؤسسات الحكومية، والشركات الكبرى في جميع أنحاء أوروبا.

تهدف هذه التشريعات إلى تعزيز الأمن السيبراني، وتنسيق الجهود بين الدول الأعضاء؛ لمواجهة التحديات المتزايدة التي تَفرضها الهجمات السيبرانية المتطورة.

هذا وقد شـــهدت أوروبا ارتفاعاً ملحوظاً في حجم وتعقيد الهجمات الســـيبرانية في الســـنوات الأخيرة، مما أثَّر بشـــكلٍ كبيرٍ علـــى البنية التحتية الحيوية، مثل قطـــاع الطاقة والنقل والخدمات المالية.

التشريعات الأوروبية الجديدة تُحفّز الابتكار في الأمن السيبراني

آثار هذه الهجمات لا تقتصر على الأضرار المالية أو التقنيــة، بــل تــؤدّي إلى تعطيــل الأنظمة الحكومية والشــركات الحيوية، مما يضع القارة أمــام مخاطــر اقتصادية وأمنيــة خطيرة. ومع الاعتماد المتزايد على التكنولوجيا الســيبرانية فــي القطاعات الحيويــة، ازدادت الحاجة لتعزيز الأمن السيبراني بشكلٍ كبير.

الهجمــات الســيبرانية أصبحــت أكثــر تعقيداً وتنظيمــاً، ممــا دفَع الاتحــاد الأوروبي لاتخاذ إجراءات صارمة لتأمين الأنظمة السيبرانية.

تشــريعات الأمن الســيبراني الجديدة التي تم الإعلان عنهــا تُركِّــز علــى رفع معاييــر الأمان الســيبراني للمؤسســات؛ حيث تُلزم الشركات الكبرى بتحســين أنظمتها الأمنية واتباع معايير صارمة لحماية البيانات والشبكات. كما أنها تعزّز التعــاون بين الــدول الأعضاء؛ مــن خلال تبادل المعلومات، والتنســيق لمواجهــة التهديدات الســيبرانية المشــتركة، مع إنشــاء مراكز أمن ســيبراني إقليميــة لتنســيق الجهــود وتبادل الخبرات.

التشــريعات تشــمل أيضاً فرض عقوبات مالية كبيرة على المؤسسات التي تفشل في الالتزام بالمعايير الجديدة؛ بهــدف تحفيزها على اتخاذ التدابير الأمنية اللازمة.

بجانب ذلك، تُركّز التشــريعات على حماية البنية التحتيــة الحيوية، مثل أنظمــة الطاقة والمياه والاتصالات، مع تخصيص موارد إضافية لضمان أمان هذه القطاعات. كما تشــجّع التشــريعات الجديــدة علــى الابتــكار فــي مجــال الأمــن الســيبراني؛ من خلال تمويل الأبحاث والتطوير في هذا المجــال، بما في ذلك تطبيقات الذكاء الاصطناعي والأمــن الكمومي، لتطوير أدوات جديدة أكثر فعالية في حماية الأنظمة[1].

إصــدار هذه التشــريعات من المتوقّــع أن يؤثّر بشــكل كبيــر علــى كيفيــة تعامل الشــركات والحكومات مــع الأمن الســيبراني في أوروبا؛ حيث سيزيد الإنفاق على تقنيات الأمان لتحسين البنية التحتية. كما أن التعاون المتزايد بين الدول الأعضاء سيعزّز من قدرة الاتحاد الأوروبي على التصدّي للهجمات الســيبرانية؛ مما يُسهم في حمايــة البيانات الحيوية ويُعــزِّز الثقة بالأنظمة السيبرانية.

جديــر بالذكــر أن ردود الفعل على التشــريعات الجديدة كانت إيجابية بشــكلٍ عام؛ حيث رحَّبت بها الشــركات والخبــراء كخطــوة ضرورية في ظل التهديــدات المتزايدة. من جانبها أشــادت المنظمــات الحقوقية بالتشــريعات الجديدة؛ لتركيزها على حماية البيانات الشخصية.

ورغــم كل ذلك، هنــاك انتقادات تشــير إلى أن زيادة العقوبات قد تُشــكّل عبئاً على الشركات الصغيرة والمتوســطة التي قد تُواجه صعوبات في تمويل تقنيات الأمان المتقدمة.

1. Data Act explained, European Commission, September 2024, on site: https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained

الذكاء الاصطناعي في مواجهة «التّهديدات السّيبرانيّة»

شــهد مجال الذكاء الاصطناعي تطوّرات كبيرة في السنوات الأخيرة، وأصبح يلعب دوراً حاسماً في مكافحة التهديدات الســيبرانية التي تتزايد بشكلٍ مستمرّ.

ومــع ازديــاد تعقيــد الهجمــات الســيبرانية وتنوّع الأســاليب التــي يســتخدمها القراصنة والمخترقــون؛ أصبــح الــذكاء الاصطناعــي أداة أساســية للمســاعدة في التصــدّي لهذه التهديدات.

الذكاء الاصطناعي يُتيح اكتشــاف الهجمات الســيبرانية قبل حدوثها أو في مراحلها المبكّرة

يعتمــد الــذكاء الاصطناعي في هــذا المجال علــى تقنيــات تعلُّم الآلــة والتحليــل التنبؤي؛ للتعرُّف على الأنماط غير العادية أو المشبوهة فــي الأنظمة الســيبرانية؛ مما يُتيح اكتشــاف الهجمات قبل حدوثها أو في مراحلها المبكرة.

أحد التطورات المهمَّة هو استخدام خوارزميات التَّعلُّم العميق لتحليل كميات هائلة من البيانات بســرعة وفعالية. هذه الخوارزميات قادرة على التعلُّم من الهجمات السابقة، وتحديث قدراتها باستمرار لمواجهة التهديدات الجديدة.

علــى ســبيل المثــال، يمكــن لأنظمــة الذكاء الاصطناعي التعرُّف على الهجمات التي تعتمد علــى التصيــد الإلكتروني؛ حيث تقــوم بتحليل الرســائل الإلكترونية والأنشــطة عبر الشــبكة لاكتشــاف العناصر المشبوهة، أو التي تتطابق مــع أنماط الاحتيــال المعروفة. وهذا يســاعد الشركات والمؤسسات على مواجهة تهديدات مثل هجمات الفدية والهجمات التي تستهدف البيانات الحساسة.

أيضــاً، بــدأت بعــض الحلــول المتقدمــة في استخدام الذكاء الاصطناعي لرصد السلوكيات غير المعتادة في الشــبكات؛ مــن خلال مراقبة نشاط المستخدمين والتطبيقات[1].

1. Basit, A., Zafar, M., Liu, X. et al. A comprehensive survey of AI-enabled phishing attacks detection techniques. Telecommand Syst, October 2021. on site: https://doi.org/10.1007/s11235-020-00733-2

ويمكــن للأنظمــة التعــرُّف علــى أيّ تغييرات مفاجئة أو غيــر متوقعة في ســلوك البيانات، والتي قد تشــير إلى وجود هجوم سيبراني. هذا النوع من التحليل الســلوكي مفيد بشكل خاص في البيئات التي تتعامل مع بيانات حساســة أو أنظمة حرجة، مثــل القطاعات المالية والصحية والبنية التحتية الحيوية.

نقلة نوعية في الأمن الســيبراني تُنتج أدوات متقدّمــة تعتمد على الذكاء الاصطناعي

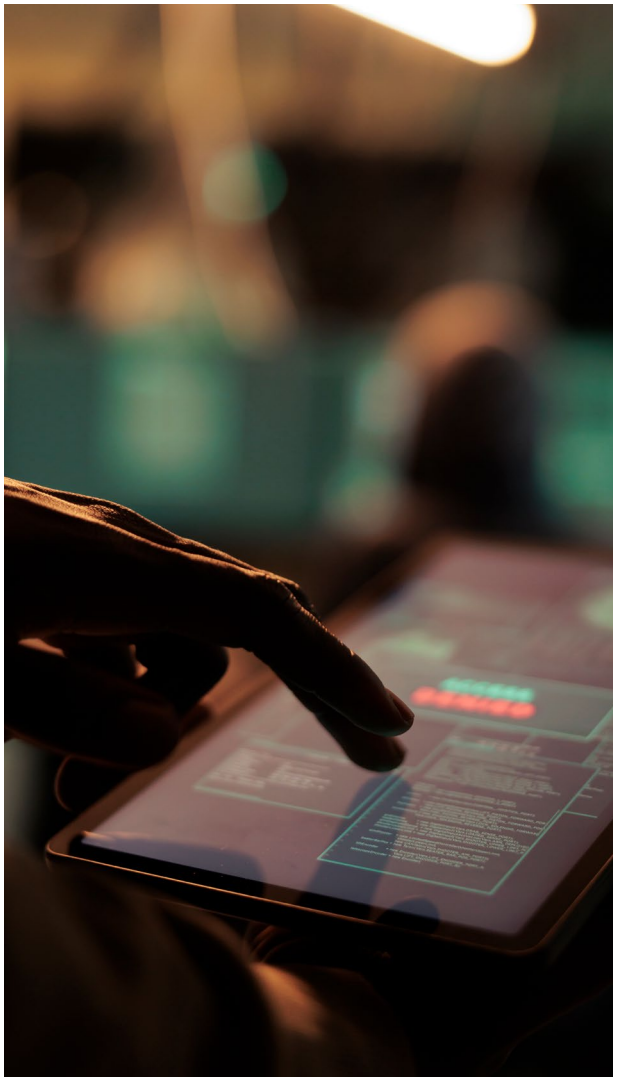
في نفس الوقت، ظهرت أدوات متقدّمة تعتمد على الذكاء الاصطناعي لتطوير تقنيات الحماية الذاتية؛ حيث تســتطيع الأنظمــة التفاعل مع الهجمات بشــكلٍ فوريّ، وإجراء تعديلات على إعدادات الأمان دون الحاجة إلى تدخُّل بشريّ. هذه التقنية تُعدّ نقلةً نوعيةً؛ لأنها تُتيح للأدوات السيبرانية التعامل مع التهديدات بسرعةٍ تفوق قدرات البشــر، مما يقلّل من الأضرار المحتملة.

بفضل هذه التطورات، أصبحت الشركات قادرةً علــى تبنّــي إســتراتيجيات أمان ســيبراني أكثر شمولية وتفاعلية؛ حيث تتطوَّر الحلول باستمرار لمواكبة الهجمات المتزايدة تعقيداً.

أيضــاً، يُعدّ اســتخدام الــذكاء الاصطناعي في تحليــل التهديدات الســيبرانية المعقَّدة تطوراً جوهريــاً فــي هــذا المجــال. وأنظمــة الذكاء الاصطناعــي قادرة على جمــع وتحليل كميات هائلة من المعلومــات من مصادر متعددة، بما في ذلك الإنترنــت المظلم؛ لتوفير نظرة أعمق حول النشــاطات الإجرامية التي قد تســتهدف المؤسســات، وهذا يُسهم في تعزيز الدفاعات الســيبرانية، وتحديد الثغرات قبل أن يســتغلها المهاجمون[1].

علاوةً على ذلك، تُوفّر تقنيات الذكاء الاصطناعي القدرة على تطوير نماذج تنبؤية تُحلّل الاتجاهات السيبرانية المستقبلية، ممَّا يساعد المؤسسات على اتخاذ تدابير وقائية قبل حدوث الهجمات.

1. Why Is Artificial Intelligence (AI) Important In Cybersecurity?, Fortinet, on site: https://www.fortinet.com/resources/cyberglossary/artificial-intelligence-in-cybersecurity



للتواصل مع إدارة التميُّز السيبراني الوطني

00974 404 663 79
00974 404 663 63
https://www.ncsa.gov.qa/
cyberexcellence@ncsa.gov.qa