

القائد السيبراني.. وفرص النجاح في فضاء إلكتروني خطر»





إعداد: هشام مدخنة

تصدرت الخروقات البارزة للأمن السيبراني عناوين الأخبار بكثرة، وتسارعت وتيرتها أكثر في أعقاب جائحة «كوفيد-19».

وفي عام 2020، وفي الفترة ما بين فبراير/ شباط وإبريل/ نيسان وحدها، ازدادت الهجمات التي تستهدف القطاع المالي بنسبة 238%، بالإضافة إلى هجمات «برامج الفدية» التي تضاعفت هي الأخرى تسع مرات

ومع التركيز الشديد على إدارة العوامل البيئية والاجتماعية والحوكمة، بات وضع إطار تنظيمي قوي للأمن السيبراني أكثر أهمية من أي وقت مضى

على المستوى الوطني، يُعد التعاون الفعال بين قادة القطاعين الخاص والعام أمراً أساسياً لضمان مرونة الدولة الإلكترونية. فالأمن السيبراني بمثابة فريق رياضي يحتاج جهود أعضائه بالكامل لتحقيق الفوز، كما أن على شرائح المجتمع المختلفة العمل معاً لضمان فضاء إلكتروني أكثر مرونة وأماناً

ويمكن للحكومات أن تضع مبادرات وطنية لزيادة مستوى الأمان الإلكتروني لمستخدمي الإنترنت لديها. فعلى سبيل المثال، أطلقت سنغافورة في العام الماضي مخططها الرئيسي للفضاء الإلكتروني الأكثر أماناً لتعزيز الأمن السيبراني بين الأفراد، والمجتمعات، والشركات، والمؤسسات. وتهدف الركائز الاستراتيجية الثلاثة للخطة إلى تأمين البنية التحتية الرقمية الأساسية، وحماية أنشطة الفضاء الإلكتروني، وتمكين السكان المتمرسين بهذا الخصوص

ويعد برنامج سنغافورة الحكومي للأمن الإلكتروني جزءاً من مخطط رئيسي أوسع لمساعدة المؤسسات على تحسين وضع أمنها السيبراني. وتشمل بعض المبادرات تطوير مجموعات أدوات الأمن السيبراني، ومنح «علامة الثقة» للمؤسسات ذات الممارسات الرائدة في هذا المجال

دور الصناعة والشركات

يلعب الصانعون الرقميون دورهم المهم أيضاً في التصدي للهجمات الإلكترونية، وبناء عليه تعمل الحكومة في سنغافورة مع رواد الصناعة على زيادة الوعي ودفع تبني الأمن السيبراني بين قطاعات الأعمال. وتشجع الدولة كذلك الشركات على إعطاء الأولوية لممارسات الأمان عن طريق وضع تصور، وتطوير، ونشر، وتوفير، المنتجات والخدمات لرفع مستويات أمان أجهزة (CLS) «الرقمية. ولهذه الغاية، أطلقت سنغافورة مخطط «علامات الأمن السيبراني. إنترنت الأشياء، واعتماد أفضل الممارسات في دمج الأمان في دورات حياة تطوير المنتجات

وهناك أيضاً الكثير من العمل الذي يتعين القيام به على مستوى الشركة نفسها. فبعد ازدياد أعداد الهجمات الإلكترونية أثناء الوباء، إلى جانب المخاطر الأمنية الإضافية للعمل عن بُعد، أُجبرت معظم المؤسسات تقريباً على تسريع خطط التحول الرقمي، وإعطاء الأولوية أكثر لتقنيات الأمان الجديدة

ولاتخاذ قرارات من شأنها دفع استراتيجياتهم إلى الأمام بشكل فعال وآمن، سيعتمد كبار المديرين التنفيذيين ومجالس الإدارات بشكل أكبر على قادة الأمن السيبراني المتمرسين لحفظ أمن مؤسساتهم بالتوازي مع إدارة المخاطر. ولتلبية هذه الاحتياجات، يجب على كبار مسؤولي أمن المعلومات صقل مجموعة من أربع مهارات أساسية للانتقال من مرحلة «خبراء» إلى «قادة» استراتيجيين، وحماية الشركة من شتى المخاطر الإلكترونية المحتملة

اتخاذ موقف استباقي -1

يعني هذا وجود الأساسيات في مكانها الصحيح مثل إدارة الهوية والوصول، وبرامج الحماية من الفيروسات، ورموز التصحيح، وتحكم أمني فعال. ويعني ذلك أيضاً تفعيل المراقبة المستمرة لاكتشاف التهديدات من الجهات الفاعلة الخارجية أو الداخلية من موظفي المؤسسة نفسها

يجب على كبير مسؤولي أمن المعلومات مواكبة مشهد التهديدات المتطور باستمرار، وأن يكون على وعي تام بالانتهاكات في كل من قطاع شركته أو القطاعات الأخرى، مع الأخذ في الاعتبار كيفية تأثير هذه الانتهاكات على المؤسسة، والعمل على تطوير تكتيكات جديدة لمواجهة التهديدات المحتملة. وتتطلب الاستباقية أيضاً الممارسة، لذلك من المهم جداً أن تحافظ المؤسسات ومن خلفها «القائد السيبراني» وفرق الدعم على برامج تدريبية هادفة تنشط الذاكرة باستمرار، للاستجابة بسرعة وفعالية عند حدوث خرق إلكتروني

الاستماع والفهم المطلق -2

لتأسيس أنفسهم كشركاء استراتيجيين، يجب أن يكون قادة الأمن السيبراني مستمعين بارعين. فمن خلال الاستماع والتعرف إلى العمليات التجارية المهمة لمؤسساتهم، سيتمكن كبار مسؤولي أمن المعلومات من حماية تلك البيانات، والمساعدة إذا لزم الأمر في استعادتها. ويحتاج قادة الأمن السيبراني كذلك إلى فهم «أفقي» لتحديد الوظائف الأساسية للمنظمة، والتي تتطلب أكبر قدر من الاهتمام والحماية وإلى فهم «عمودي»، يشمل مبادئ الأمن السيبراني والتدابير اللازمة للتنفيذ، والتي تحمي العمليات التجارية، وتعالج المخاطر، وتوازن في التكاليف. ومع وضع ذلك في الاعتبار، فإن كبير مسؤولي أمن المعلومات بحاجة مجدداً إلى فهم واضح لمدى تعرض مؤسسته للخطر، وما مقدار المخاطر التي ترغب الإدارة في تحملها وهم يوازنون بين أولويات العملاء والشركاء من جهة، والحاجة إلى ضمان أمن العمليات التجارية من جهة ثانية

«ثنائية اللغة» التقنية والاستراتيجية -3

لكي يكونوا سفراء مؤثرين، يجب أن يمتلك مسؤولو أمن المعلومات أكثر من مجرد مهارات تواصل استثنائية، في الواقع، يجب أن يكونوا «ثنائيي اللغة». وهذا يعني أن تكون طليقاً في «اللغة الفنية»، فضلاً عن «اللغة الاستراتيجية» الأوسع لمجلس الإدارة والقيادة العليا.

وبصفته حليفاً وشريكاً مهماً لأصحاب المصلحة الرئيسيين، يجب على كبار مسؤولي أمن المعلومات أيضاً النظر إلى الأمن السيبراني كعنصر تمييز، وخاصة في الصناعات التي تكون فيها الثقة أمراً بالغ الأهمية في علاقات العمل. إذ يعد الأمن الإلكتروني عنصراً مهماً بشكل متزايد في توقعات العملاء، والحفاظ عليه أولوية قصوى، وليس مجرد جانب من جوانب عملية التطوير.

ومن خلال الانتقال من موقع دفاعي إلى موقع يُمكن الأعمال بشكل استباقي من الابتكار، سيتمكن مسؤولو أمن المعلومات من مساعدة مؤسساتهم على التحول بأمان في هذا العصر الرقمي، كما سيصبحون متنفذين أكثر بين قادة الأعمال والإدارة العليا.

إقامة حوار منظم -4

من المهم أن يجري القادة الرقميون محادثات منتظمة مع رؤساء الأعمال والمديرين التنفيذيين، وبأن تصبح إدارة المخاطر الإلكترونية جزءاً من عملية صنع القرار اليومية. فمن خلال حوار ثنائي الاتجاه، سينظر كبار المديرين التنفيذيين إلى مسؤولي أمن المعلومات على أنهم شركاء أساسيون في الاستراتيجية والأهداف والاحتياجات.

في النهاية، يجب أن يساعد تطوير مجموعات المهارات الأربع هذه مسؤولي الأمن السيبراني على بلورة فهم واضح للقضايا ذات الصلة، وإحساس بديهي في المخاطر المستقبلية، والمساعدة في إضفاء الطابع المؤسسي على قرارات تجنب المخاطر المتخذة على مستوى مجلس الإدارة.

ارتفاع متوسط تكلفة اختراق البيانات إلى 3.56 مليون دولار

العالمية في مجال الحماية الإلكترونية، تقرير التهديدات الإلكترونية لمنتصف عام Acronis «أصدرت شركة «أكرونيس عرضة لمخاطر محددة وذلك (SMBs) 2021، وأطلقت في التقرير تحذيراً بأن الشركات الصغيرة ومتوسطة الحجم بناءً على اتجاهات الهجمات التي تم رصدها في أثناء أول ستة أشهر من العام

وقد كشف التقرير عن أنه في أثناء النصف الأول من عام 2021، تعرّضت 4 من بين 5 مؤسسات إلى اختراق في آلية الأمان الإلكتروني ناشئ عن ثغرة أمنية في النظام البيئي لمُورّد الخدمات التابع لجهة خارجية الذي تتعامل معه. وهذا الأمر يحدث في الوقت الذي ارتفعت فيه تكلفة اختراق البيانات إلى ما يقارب 3.56 مليون دولار أمريكي، مع ازدياد سريع لمتوسط المبالغ المدفوعة مقابل برمجيات الفدية الضارة بنسبة 33% إلى ما يزيد على 100000 دولار أمريكي

وبينما يمثل هذا الأمر ضربة مالية هائلة لأية مؤسسة، فإن هذه المبالغ المالية ستكون بمثابة إعلان الوفاة لمعظم أنه يمثل مصدر قلق هائل في النصف الثاني من عام Acronis الشركات الصغيرة ومتوسطة الحجم، والذي تظن

بينما تؤثر الزيادة في معدل Acronis وأوضح كاندريد ويست، نائب رئيس قسم أبحاث الحماية الإلكترونية في شركة الهجمات على المؤسسات بكافة أحجامها، هناك شيء ما لا يتم الإبلاغ عنه بشكل كافٍ في تغطية اتجاهات التهديدات الإلكترونية الحالية، وهو حجم التأثير الواقع على مجتمع الشركات الصغيرة». «فبخلاف الشركات الأكبر حجماً، لا تمتلك الشركات الصغيرة ومتوسطة الحجم الأموال أو الموارد أو الخبرات في أطقم العمل اللازمة لمواجهة التهديدات القائمة في الوقت الحالي. لهذا السبب، تلجأ هذه الشركات إلى موفري خدمات تكنولوجيا المعلومات – ولكن إذا كان موفرو خدمات تكنولوجيا المعلومات هؤلاء عرضة للخطر فإن تلك الشركات الصغيرة ومتوسطة الحجم تقع تحت «رحمة مرتكبي الهجمات».

ومن خلال استخدام تقنيات الهندسة الاجتماعية لخداع المستخدمين الغافلين بالضغط على المرفقات أو الروابط الضارة، ارتفع معدل رسائل البريد الإلكتروني بغرض التصيد الاحتيالي بنسبة 62% من الربع الأول إلى الربع الثاني. ويمثل هذا الارتفاع المفاجئ مصدر قلق محددًا بما أنه يتم نشر 94% من البرمجيات الضارة عبر البريد الإلكتروني. مخصص للتصيد الاحتيالي URL بحظر ما يزيد على 393000 عنوان Acronis وفي أثناء الفترة الزمنية نفسها، قامت وضار للعملاء، حيث أدى ذلك إلى منع مرتكبي الهجمات من الوصول إلى بيانات قيّمة وتثبيت البرمجيات الضارة في نظام العميل.

عمليات ترشيح البيانات متواصلة في الزيادة. في عام 2020، تعرّض ما يزيد على 1300 ضحية لبرمجيات الفدية الضارة إلى تسريب بياناتهم بشكل علني بعد وقوع إحدى الهجمات، حيث يسعى مرتكبو الجرائم الإلكترونية إلى زيادة أرباحهم المالية إلى أقصى حد ممكن من الحوادث الناجحة. في أثناء النصف الأول من عام 2021، تم بالفعل نشر ما يزيد على 1100 حالة تسريب للبيانات – وهو ما يعكس حدوث زيادة لهذه العمليات بنسبة 70% للعام الحالي.

لا يزال العاملون عن بُعد، هم الهدف الرئيسي. يتواصل الاعتماد على العاملين عن بُعد في أعقاب وقوع جائحة كوفيد-19. ويستخدم ثلثا العاملين عن بُعد الآن أجهزة العمل لأداء المهام الشخصية ويستخدمون أجهزة المنزل الشخصية لتنفيذ أنشطة الشركة. ونتيجة لذلك، يعمل مرتكبو الهجمات بنشاط على استكشاف العاملين عن بُعد. وقد لاحظت شركة وقوع ما يزيد على ضعف رقم الهجمات الإلكترونية العالمية، مع زيادة بنسبة 300% في شن الهجمات بالقوة Acronis (RDP) المفترقة ضد الأجهزة التي تعمل عن بُعد عبر بروتوكول سطح المكتب البعيد.

مليون دولار قيمة أعلى فدية «ابتزاز إلكتروني» طلبت من شخص واحد 50

ارتفع متوسط خسائر عمليات الابتزاز بواسطة برمجيات الفدية الخبيثة بنسبة 82% منذ عام 2020، حيث بلغ مستوى قياسياً بتسجيله 570 ألف دولار خلال النصف الأول من عام 2021، وذلك نتيجة اتباع قراصنة ومجرمي الإنترنت تكتيكات شديدة العدائية، بهدف إجبار المؤسسات على دفع مبالغ فدية أكبر. وتأتي موجة الارتفاع هذه إثر تنامي متوسط خسائر (عمليات الابتزاز) خلال العام الماضي بنسبة 171%، حيث تخطت عتبة الـ 312 ألف دولار. وتعكس هذه الأرقام، التي جمعتها شركة بالو ألتو نتوركس، الأزمة الحادة التي يعانيها العالم اليوم، والتي باتت تعرف باسم أزمة برمجيات الفدية الخبيثة، وما زالت تتفاقم نتيجة تركيز المؤسسات الإجرامية لجهودها في عمليات الابتزاز بواسطة برمجيات الفدية الخبيثة، التي تعتبر من الأساليب المربحة جداً بالنسبة لهم.

وقد رصدت بالو ألتو نتوركس تفاقم هذه الأزمة، نتيجة متابعة الأخبار العالمية، كما أن الكثير بات يعلم بها بسبب خوضه لتجربة شخصية في هذا الإطار (أي، تعرضه أو شركته لعملية ابتزاز بواسطة برمجيات الفدية الخبيثة)، فقد

استطاعت هجمات برمجيات الفدية الخبيثة منعنا من الوصول إلى أجهزة الكمبيوتر في بيئات العمل، وأدت إلى ارتفاع أسعار اللحوم، وإلى نقص في إمدادات البنزين، وإلى إغلاق أبواب المدارس أمام الطلاب، وإلى تأجيل مواعيد القضايا القانونية والجلسات القضائية، وإلى منع البعض حتى من فحص واختبار المركبات للتأكد من سلامتها، وإلى عدم قدرة بعض المستشفيات على استقبال المرضى.

يعتبر صعود موجة هجمات «كوادروبل إكتورشن» أو «الابتزاز الرباعي» من التوجهات العالمية المقلقة التي أشار إليها خبراء بالو ألتو نتوركس، وذلك في خضم معالجتهم للعشرات من حالات الابتزاز ببرمجيات الفدية الخبيثة خلال النصف الأول من عام 2021، حيث باتت الجهات المشغلة ببرمجيات الفدية الخبيثة تستعين الآن بأربع تقنيات متطورة: للضغط على الضحايا، وحثهم على دفع المبالغ المطلوبة

التشفير: أصبح الضحايا يدفعون المال لقاء استعادة إمكانية الوصول إلى بياناتهم المشفرة، وإلى أنظمة الكمبيوتر المخترقة، التي تتوقف عن العمل، لأن ملفات المفاتيح فيها مشفرة

سرقة البيانات: يقوم قراصنة الإنترنت بنشر المعلومات المهمة والحساسة في حال تم رفض دفع الفدية لهم. (انتشر هذا). (التوجه على أرض الواقع خلال عام 2020

وذلك بهدف DoS تستعين عصابات برمجيات الفدية الخبيثة بهجمات الحرمان من الخدمة: DoS الحرمان من الخدمة إغلاق المواقع العامة للضحايا

الإساءة وتشويه السمعة: عادة ما يتواصل قراصنة الإنترنت مع العملاء، وشركاء الأعمال، والموظفين، ووسائل الإعلام لإخبارهم، بأنه تم اختراق شبكة وأنظمة المؤسسات التي يعملون لصالحها

ورغم أنه من النادر وقوع إحدى المؤسسات ضحية هذه التقنيات في آن واحد، إلا هذا العام شهد وبوتيرة متنامية لجوء عصابات برمجيات الفدية الخبيثة لاستعمال أساليب وطرق إضافية عند رفض الضحايا الدفع لهم، وذلك بعد قيامهم بتشفير وسرقة البيانات

وقد أشار «تقرير تهديدات برمجيات الفدية الخبيثة» الصادر عن بالو ألتو نتوركس للعام 2021، والذي غطى توجهات العالم 2020، إلى عمليات الابتزاز المزدوجة باعتبارها إحدى الممارسات الصاعدة، حيث أظهرت عمليات المراقبة والمتابعة الأخيرة للجهات المهاجمة مضاعفتها لعدد مرات استخدام تقنيات الابتزاز «كوادروبل إكتورشن»، أو ما يعرف بـ «الابتزاز الرباعي». وفي ظل اعتمادها وتبنيها لطرق وأساليب الابتزاز الجديدة هذه، أضحت عصابات برمجيات الفدية الخبيثة أكثر جشعاً. فمن بين عشرات الحالات التي دأب على مراجعتها خبراء بالو ألتو نتوركس خلال النصف الأول من عام 2021، سجّل متوسط الفدية المطلوبة ما قيمته 5.3 مليون دولار، أي ما يمثل ارتفاعاً بنسبة 518% عن المتوسط الذي سجّل في عام 2020، الذي بلغ حينها 847,000 دولار 518% عن المتوسط الذي سجّل في

أما أعلى قيمة لفدية تم طلبها من ضحية واحدة، وتم رصدها من قبل خبراء بالو ألتو نتوركس، فقد بلغت 50 مليون دولار، وذلك خلال النصف الأول من عام 2021، مرتفعة بذلك عن فدية بقيمة 30 مليون دولار سجلت العام الماضي