

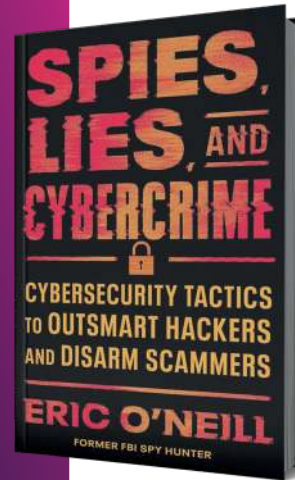
الجواسيس في العصر الرقمي

كيف يستغل المخترقون الخداع والثقة لشن الهجمات الإلكترونية

سلسلة الأمن السيبراني



للكاتب
إريك أونيل



في ثوانٍ...



حين أصبحت حياتنا كلمة سر

لماذا نقرأ كتب الأمن السيبراني؟

كل شيء في حياتنا أصبح متصلاً. مصارفنا، بيوتنا، صور أطفالنا، أسرار شركاتنا، وحتى نبض قلوبنا.

نعيش داخل سحابة كبيرة، نظنها آمنة، حتى تأتي لحظة اختراق واحدة لتذكرنا بأننا مكشوفون أكثر مما نتصور.

الأمن السيبراني لم يعد تخصصاً للمهندسين وخبراء الشبكات، بل أصبح ثقافة عامة، مثل معرفة قواعد المرور. فنحن جميعاً نقود في الطريق السريع للإنترنت، ومن لا يعرف قواعد الحماية، سيكون أول ضحية.

في هذا العدد من سلسلة «كتاب في دقائق» التي تصدر عن مؤسسة محمد بن راشد آل مكتوم للمعرفة، نفتح ملف كتب الأمن السيبراني. كتب لا تعلمك كيف تكتب كوداً، بل كيف تحمي نفسك كخبير.

سنقرأ كيف تُدار الحروب السيبرانية بين الدول، وكيف يُسرق مستقبل كامل بضغطة زر، وكيف يتحول هاتفك الصغير إلى ثغرة تهدد حياتك كلها.

قراءة هذه الكتب اليوم ليست خياراً، بل هي خط الدفاع الأول. لأن أغلى ما تملكه في العصر الرقمي ليس مالك، بل بياناتك.

جمال بن حويرب

المدير التنفيذي

لمؤسسة محمد بن راشد آل مكتوم للمعرفة

تكتشف منظمة إنسانية غير حكومية، ذات يوم، أن مجموعة «لوكبيت» المتخصصة في تطوير برامج الفدية واستخدامها، قد اخترقت أنظمتها حول العالم. سُـُـرقت الملفات، وربما سُـُـرقت بيانات حساسة، وتعطلت العمليات، وأصبحت المنظمة تحت ضغط مهول للتفاوض مع المهاجمين واتخاذ قرار بشأن دفع الفدية. تكشف مثل هذه الحوادث مدى سرعة تحوّل الهجوم الإلكتروني من مشكلة تقنية إلى أزمة مؤسسية تمس القيادة، والتأمين، والاتصالات، والسمعة، واستمرارية الأعمال. فضلاً عما تسببه من ضغط نفسي مهول على المسؤولين والموظفين.

يمكن تشبيه الأمر بفقدان منزل في حريق؛ فقد يدمر الحريق خلال ساعات ما استغرق بناؤه سنوات. وكذلك يستطيع الهجوم الإلكتروني أن يلحق في وقت قصير أضراراً بالغة بأصول رقمية تراكمت على مدى أعوام.

فقد أصبحت البيانات من أ ثمن أصول العصر الرقمي. فمعلومات الهوية الشخصية، وكلمات المرور، ووثائق الشركات، وسجلات العملاء، والمعلومات المالية، والملكية الفكرية، والسجلات الطبية، والمراسلات الخاصة، كلها قد تُسرق ثم تُباع أو تُستغل في الابتزاز أو الاحتيال أو شن هجمات أخرى.

والبيانات المسروقة لا يمكن استعادتها بسهولة مثل الممتلكات المادية. فقد تتمكن من تغيير كلمة مرور مسربة، لكن ماذا تفعل إذا تسرب رقم الضمان الاجتماعي، أو سجل طبي، أو صورة شخصية، أو سر تجاري؟ قد تظل بعض هذه المعلومات متداولة أو قابلة للاستغلال سنوات طويلة بعد وقوع الاختراق.

وتتوقف قدرة المؤسسة على تجاوز الهجوم بأقل قدر ممكن من الخسائر على مجموعة من العوامل، من بينها وجود تغطية تأمينية مناسبة، وجرّد دقيق للأصول والبيانات، ونسخ احتياطية موثوقة. إلى جانب وجود خطة واضحة للاستجابة إلى الحوادث، وتحديد المسؤوليات مسبقاً، ومعرفة الأنظمة والبيانات التي لا يمكن للمؤسسة الاستغناء عنها.



من الهويات المزيفة إلى التزييف العميق

في الواقع، لا تقتصر الجرائم الإلكترونية الحديثة على كونها مواجهة تقنية بين المهاجمين وفرق الأمن السيبراني، إذ يمكن النظر إليها أيضاً بوصفها امتداداً رقمياً للأساليب قديمة في التجسس والخداع. فالأجهزة الاستخباراتية والمجرمون استخدموا تاريخياً أساليب مثل الهويات المزيفة، والمراقبة السرية، ونقاط الالتقاء الآمنة، واستمالة المصادر.

أما اليوم، فقد ظهرت نظائر رقمية لهذه الأساليب، مثل التصيد الاحتيالي، وبرامج الفدية، والتزييف العميق، وسرقة بيانات الاعتماد، والبرمجيات الخبيثة، واستغلال العملات المشفرة في بعض أنماط الجريمة.

وعلى الرغم من أن التكنولوجيا عنصر أساسي في كثير من هذه الهجمات، فإن نجاحها يعتمد بدرجة كبيرة على السلوك البشري. فقد يبدأ الهجوم برسالة تبدو مقنعة، أو شخص مألوف، أو شعور بالإلحاح، أو عرض مغرٍ، أو تحديث برمجي يبدو رسمياً، أو كلمة مرور أعيد استخدامها في أكثر من خدمة.

وغالباً، يكون أقوى أسلحة المجرم هو إقناع الضحية بأن ما تراه حقيقي. فالمهاجم يبحث عن نقطة الضعف، سواء كانت تقنية أو بشرية. وهذا لا يعني التوقف عن استخدام التكنولوجيا، بل استخدامها بقدر أكبر من الوعي والحذر.

ويبدأ ذلك بفهم البيانات التي تحتاج إلى الحماية، وتقييد الوصول إليها، والتحقق من الطلبات غير المعتادة، والاستعداد للحوادث قبل وقوعها. لذلك، استعد مسبقاً، ولا تمنح الثقة تلقائياً، وتحقق من الطلبات المهمة، واتخذ قراراتك بهدوء، ولا تسمح للخوف أو الاستعجال بأن يحدد رد فعلك. فهذه الإجراءات أكثر فاعلية من الارتجال بعد وقوع الكارثة.

من هذا المنطلق، سنحاول التفكير بعقلية الجاسوس من خلال ستة مفاهيم رئيسية، ثم ننتقل إلى كيفية اكتشاف الهجمات والتعامل مع المخاطر والاستجابة إلى الحوادث والتعلم منها.

ساحة حرب إلكترونية جديدة

وقد ساعدت خصائص الخصوصية هذه في توفير أدوات مهمة للصحفيين والمدافعين عن الخصوصية وغيرهم، لكنها في الوقت نفسه أوجدت بيئة يمكن استغلالها في الأسواق والمنتديات والأنشطة الإجرامية.

على الجانب الآخر، أصبحت بعض أشكال الجرائم الإلكترونية أكثر تنظيماً، إذ تعمل مجموعات برامج الفدية أحياناً وفق هياكل تشبه الشركات، فتضم مطورين، ومفاوضين، وشركاء، وفرق دعم، وآليات للتسويق والدفع. ويتيح نموذج «برامج الفدية بصفته خدمة» لمجرمين أقل خبرة استخدام أدوات وبنية تحتية طورها آخرون بدلاً من بناء كل شيء بأنفسهم.

كما أصبحت أسواق الجريمة الإلكترونية توفر أنواعاً مختلفة من الأدوات والبيانات المسروقة، مثل بيانات الاعتماد، والمعلومات الشخصية، وبعض البرمجيات الخبيثة، ووسائل الوصول إلى أنظمة مخترقة.

وتوفر العملات المشفرة في بعض الحالات وسيلة دفع عابرة للحدود، وقد تجعل استرداد الأموال أو عكس بعض المعاملات أكثر صعوبة بعد إتمامها.



لم تعد الأدوات والأساليب التي يستخدمها المجرمون الإلكترونيون حكرًا على أجهزة الاستخبارات أو المجموعات ذات القدرات التقنية العالية. فقد أسهمت خدمات الإنترنت المظلم، والعمل عن بعد، وسهولة تداول البيانات المسروقة، وبعض استخدامات العملات المشفرة، والذكاء الاصطناعي، ونموذج الجريمة الإلكترونية بوصفه خدمة في خفض الحواجز أمام تنفيذ هجمات متطورة. ولم يعد المجرم بحاجة بالضرورة إلى امتلاك خبرة تقنية استثنائية، إذ يمكنه شراء أدوات أو استئجارها، أو أنمتة بعض مراحل الهجوم، أو الاستفادة من خدمات جاهزة يقدمها مجرمون آخرون.

لفهم المقصود بالإنترنت المظلم، من المفيد تصور الإنترنت في ثلاث طبقات من باب التوضيح: الطبقة الأولى هي الويب السطحي، أي الجزء من الإنترنت الذي يمكن لمحركات البحث العامة فهرسة جزء كبير من محتواه، والذي يستخدمه معظم الناس يومياً.

الطبقة الثانية هي الويب العميق، ويشمل المحتوى غير المفهرس عادةً في محركات البحث العامة، مثل قواعد البيانات الخاصة، والسجلات الطبية، والحسابات المصرفية، وأنظمة الشركات، والبريد الإلكتروني، والرسائل الخاصة، وغيرها من الموارد التي تتطلب تسجيل دخول أو صلاحية وصول.

أما الطبقة الثالثة فهي الويب المظلم، وهو جزء من الويب العميق يعتمد على تقنيات وشبكات مصممة لإخفاء موقع المستخدم أو الخدمة بدرجة أكبر. ويمكن استخدام هذه التقنيات لأغراض مشروعة تتعلق بالخصوصية وحرية التعبير وحماية المصادر، كما يمكن إساءة استخدامها في أنشطة إجرامية.

ومن أشهر التقنيات المستخدمة في هذا السياق شبكة «تور». وتعتمد على تمرير حركة البيانات عبر عدة مرّجّلات، مع استخدام طبقات متعددة من التشفير، بحيث لا يستطيع مرّجّل واحد بمفرده معرفة هوية المستخدم والوجهة النهائية للاتصال. ولا يعني ذلك إخفاء الهوية بصورة مطلقة؛ فالشبكة توفر طبقة مهمة من الخصوصية، لكنها لا تلغي جميع وسائل التتبع، أو كل أنواع الهجمات.

وتتيح خدمات «تور»، المعروفة باسم خدمات «التوجيه البصلي»، تشغيل خدمات ومواقع لا تكشف عناونها الشبكي بالطريقة المعتادة، كما تُستخدم في تطبيقات مشروعة مثل التواصل الآمن، ومشاركة الملفات، وحماية هوية بعض المستخدمين والصحفيين ومصادرهم.

فكر جاسوس

سنتناول ست مفاهيم أساسية تعرّفنا كيف يفكر الجاسوس:



1. الخداخ: كيف يبدأ الهجوم؟

تقوم نسبة كبيرة من الجرائم الإلكترونية، في جوهرها، على خداع الضحية وكسب ثقتها، ثم استغلال نقطة ضعف لديها للاستيلاء على شيء ذي قيمة، قبل أن تدرك ما يحدث، وتتمكن من احتواء الضرر. وقد تكون الضحية التالية أنت. فكل شخص أو مؤسسة تستخدم التكنولوجيا يمكن أن تصبح هدفاً من الشركات الكبرى والحكومات والمنظمات غير الربحية، إلى الأسر والمتقاعدين والمراهقين. يعتمد المهاجم على قدرته على الخداع والمخادع، سواء كان جاسوساً أو محتالاً أو مجرماً إلكترونياً، يحاول إقناع الهدف بتصديق شيء غير صحيح: أن رسالة بريد إلكتروني ما رسمية وموثوقة، أو أن شخصاً ما جدير بالثقة، أو أن فرصة استثمارية قائمة بالفعل، أو أن تحديثاً برمجياً آمناً، أو أن هناك حالة طارئة تتطلب استجابة فورية.

ينطوي الخداع الناجح غالباً على قدر من الحقيقة. لذلك يبحث المجرمون عن معلومات تخص أهدافهم عبر وسائل التواصل الاجتماعي، والملفات المهنية، ومواقع الشركات، وقواعد البيانات التي تعرضت للتسريب، وغيرها من المصادر المتاحة. وقد تكفي معرفة بعض التفاصيل الأساسية عن الضحية لتسهيل الهجوم، مثل المسمى الوظيفي، وجهة العمل، وخطط السفر، وأسماء أفراد الأسرة، والهوايات، والزملاء، والأحداث الأخيرة، والعلامات التجارية التي يتعامل معها الشخص، أو أسماء كبار المسؤولين في المؤسسة. وتتيح هذه المعلومات للمهاجم صياغة رسائل تصيد موجهة تبدو شخصية ومقنعة.

يشبه ذلك ما كان يحدث في عمليات التجسس التقليدية، حين كان العميل يقضي وقتاً طويلاً في التعرف إلى شخص مستهدف، وفهم دوافعه، وبناء علاقة معه تدريجياً. أما اليوم، فيستطيع المجرم إجراء قدر كبير من هذا الاستطلاع عبر الإنترنت، ثم تنفيذ عملية التلاعب عن طريق البريد الإلكتروني

أو الرسائل النصية أو وسائل التواصل الاجتماعي أو المكالمات الصوتية والمرئية. ونحن نتعامل يومياً مع عدد مهول من الرسائل والتنبيهات والاتصالات الرقمية. ننقر ونرد ونعيد التوجيه بسرعة، ونفترض غالباً أن ما نراه حقيقي. ويمكن لهذه السرعة تحديداً أن تصب في مصلحة المهاجم.

وقد تبدو رسالة تصيد مصممة بعناية وكأنها صادرة عن مدير أو مورد أو زميل أو بنك أو مزود خدمة. وقد يكون هدفها سرقة بيانات الدخول، أو دفع المستخدم إلى تثبيت برنامج خبيث، أو تحويل أموال، أو ببساطة بدء محادثة يمكن استغلالها لاحقاً.

لذلك، عندما تدفعك رسالة ما إلى اتخاذ قرار سريع، توقف قليلاً فالاستعجال من أكثر الأدوات شيوعاً في عمليات الاحتيال والهندسة الاجتماعية.

دقق خصوصاً في تعليمات الدفع غير المتوقعة، وطلبات بيانات الدخول، وإشعارات إعادة تعيين كلمات المرور، والمرفقات غير المألوفة، والرسائل التي تطلب تجاوز الإجراءات المعتادة.

وافحص عنوان المرسل، والنطاق الإلكتروني، ووجهة الرابط، وأسلوب الكتابة، والتوقيت، والإجراء المطلوب، بدلاً من الاعتماد على أي مؤشر منفرد.



2. انتحال الشخصية: كيف يتجاوز المهاجم مشكلة الهوية؟

يسبق لهم مقابلتهم شخصياً، ما قد يسهل انتحال شخصية زميل حقيقي. كما أن السلطة والألفة قد تقللان مستوى الشك.

وقد يمتد الأمر إلى الأفراد والعائلات، إذ يمكن استخدام صوت مستنسخ لمحاكاة أحد أفراد الأسرة، وخلق حالة طوارئ وهمية، أو طلب تحويل مالي عاجل.

وفي مثل هذه الحالات، لا يكفي الاعتماد على المظهر أو الصوت أو البحث عن أخطاء لغوية. فالمحتوى الاصطناعي قد يكون مصمماً بعناية. والدفاع الأفضل هو استخدام أكثر من درجة للتحقق. فلا ينبغي الموافقة على طلب مالي لمجرد أنه جاء من حساب أو شخص يبدو صحيحاً. ويجب أن تعتمد المؤسسات إجراءات تلزم الموظفين بتأكيد الطلبات الحساسة عبر قناة مستقلة، ولا سيما المعاملات المالية الكبيرة أو غير المعتادة. ويمكن للعائلات أيضاً الاتفاق مسبقاً على كلمة أو عبارة خاصة تستخدم للتحقق من هوية أحد أفرادها في حالات الطوارئ غير المعتادة.

وبالمثل، ينبغي أن يكون واضحاً للموظفين أن كبار المسؤولين لا يُفترض أن يكونوا قادرين على تجاوز إجراءات الدفع أو التحقق لمجرد أنهم يشغلون مناصب عليا. فالقاعدة الأساسية هي أن الثقة تأتي بعد التحقق من الهوية، لا من مظهر الشخص أو صوته وحدهما.

يتحدث مدير مالي عبر مكالمة فيديو مع شخص يعتقد أنه الرئيس التنفيذي لشركته. يطلب الرئيس التنفيذي المزعوم تحويل ملايين اليوروهات، فيوافق المدير لأن الصورة والصوت يبدوان حقيقيين. لكن الشخص الذي يظهر أمامه كان شخصية مزيفة أنشأها المهاجمون باستخدام تقنيات الذكاء الاصطناعي، اعتماداً على مواد صوتية ومرئية متاحة للعمامة.

يمثل انتحال الشخصية شكلاً متقدماً من الخداع، إذ يحاول المجرم الظهور في هيئة شخص أو مؤسسة جديدة بالثقة. وهذه ليست فكرة جديدة، لكن الأدوات الرقمية وسّعت نطاقها وجعلت بعض أشكالها أكثر واقعية.

وتزداد المخاطر مع تطور تقنيات الذكاء الاصطناعي التوليدي. فقد أصبحت أدوات استنساخ الصوت قادرة على تقليد أصوات بشرية من عينات صوتية، كما تستطيع تقنيات توليد الصور والفيديو إنشاء محتوى اصطناعي شديد الإقناع في بعض الحالات. ومن السيناريوهات الشائعة أن ينتحل المهاجم شخصية مسؤول تنفيذي رفيع المستوى، أو مؤيد، أو محام، أو موظف في قسم المالية، ثم يطلب تحويل أموال، أو تغيير بيانات مصرفية، أو إرسال وثائق سرية، أو مشاركة بيانات اعتماد.

وفي بيئات العمل التي تعتمد على التواصل عن بُعد، قد يتعامل الموظفون يومياً مع أشخاص لم

3. التسلل: كيف يدخل المهاجم إلى النظام؟

وفي هجمات برامج الفدية، قد لا يشفر المهاجمون الأنظمة فور وصولهم إليها. فقد يقضون وقتاً في إنشاء حسابات، أو رفع مستوى الصلاحيات، أو تعطيل بعض وسائل الحماية، أو استكشاف الشبكة، أو تحديد الأنظمة المهمة، أو سرقة البيانات، ثم يبدأون عملية التشفير أو الابتزاز عندما يصبح تأثيرهم أكبر.

لذلك، يجب أن تفترض المؤسسة إمكانية حدوث اختراق، وأن تسأل نفسها: كم من الوقت قد يستغرق اكتشافه؟ وإلى أي مدى يستطيع المهاجم التحرك داخل الشبكة؟ وما الأنظمة والبيانات التي يمكنه الوصول إليها؟

ومن التدابير الأساسية، تقليل عدد المسارات التي يمكن استغلالها، وتثبيت التحديثات الأمنية، وحماية الأنظمة والأجهزة المتصلة بالشبكة، واستخدام المصادقة المتعددة العوامل، والتحكم في التطبيقات والصلاحيات.

كما ينبغي تقسيم الشبكات والأنظمة إلى نطاقات منفصلة عندما يكون ذلك مناسباً للحد من قدرة المهاجم على الانتقال من نظام إلى آخر. ويجب كذلك إدارة مخاطر الموردين من خلال تحديد المخاطر الأمنية والتشغيلية والقانونية والمالية المرتبطة بهم، وتقييمها ومراقبتها.

التسلل هو الوصول غير المصرح به إلى نظام أو مؤسسة، ثم محاولة الحفاظ على هذا الوصول واستثماره. ففي التجسس التقليدي، قد يتسلل العميل إلى منشأة أو يستميل شخصاً من داخلها. أما في الجرائم الإلكترونية، فقد يحدث ذلك من خلال برمجيات خبيثة، أو حسابات مختربة، أو أنظمة غير محدثة، أو تنزيلات ضارة، أو بيانات اعتماد مسروقة، أو اختراقات في سلسلة توريد البرمجيات. ومن أبرز الأمثلة على ذلك، اختراق سلسلة توريد برنامج «أوريون». إذ تمكن المهاجمون من إدخال شيفرة خبيثة في نسخ من البرنامج، ثم وصلت النسخ المتضررة إلى بعض العملاء ضمن تحديثات البرنامج المعتادة، ما أتاح للمهاجمين الوصول إلى عدد من المؤسسات المستهدفة، بما في ذلك وكالات حكومية رئيسية ومنظمات أمنية.

يوضح هذا المثال خطورة الثقة في البرمجيات والموردين. فقد تتعرض المؤسسة للاختراق ليس لأن دفاعاتها الداخلية ضعيفة بالضرورة، بل لأن أحد الموردين الذين تعتمد عليهم تعرض للاختراق. وهكذا، لا يقتصر الأمن السيبراني على حماية الأنظمة الداخلية؛ فالمؤسسات تعتمد على مطوري البرامج، ومزودي الخدمات السحابية، والمقاولين، والشركاء، ومقدمي الخدمات الخارجية. وقد يصبح أي اتصال من هذه الاتصالات نقطة دخول محتملة إذا لم تحدث إدارته بصورة مناسبة.

4. الثقة: كيف تتحول العلاقة الإنسانية إلى أداة للهجوم؟

يشمل ذلك استنساخ الصوت وإنشاء مقاطع فيديو مزيفة؛ ما يزيد من قدرة المحتال على بناء قصة تبدو حقيقية.

لذلك، لا تثق بوعود بعوائد استثنائية، أو فرص استثمارية غير متوقعة، أو استثمارات «سرية»، أو طلبات مالية عاجلة من شخص تربطك به علاقة عاطفية، خصوصاً عندما تنتقل العلاقة بسرعة إلى المال.

وتوقف واسأل نفسك: هل يبدو هذا العرض جيداً إلى درجة يصعب تصديقها؟ حيث يساعد هذا السؤال البسيط في كسر حالة الاستعجال التي يحاول المحتال خلقها.

كذلك، تحقق من وجود الشركات المزعومة وتسجيلها لدى الجهات التنظيمية المختصة، واستخدم بيانات الاتصال المستقلة عن تلك التي يقدمها لك الشخص نفسه، ويمكنك استخدام البحث العكسي عن الصور عند الشك في هوية شخص أو صورة.

ولا تتردد في استشارة شخص تثق به. فالمحتال يفضل أن تبقى العلاقة سرية، لأن عزل الضحية عن آراء الآخرين يزيد فرص نجاحه.

تعتمد عمليات الاحتيال القائمة على الثقة على العلاقات والإقناع أكثر من اعتمادها على اختراق تقني مباشر. فقد يبني المهاجم علاقة مع الضحية على مدى فترة من الزمن، ثم يقنعها باتخاذ إجراء طوعي، مثل استثمار المال أو تحويله إلى شخص تدعي أنها تربطها به علاقة عاطفية، أو مشاركة معلومات حساسة، أو المساعدة في حل حالة طوارئ غير حقيقية.

إذ يستغل المحتال احتياجات بشرية طبيعية، مثل الحب، والانتماء، والأمان المالي، والتقدير، والخوف من تفويت الفرص، والرغبة في مساعدة الآخرين. وقد تؤدي عمليات الاحتيال الاستثماري عبر الإنترنت إلى خسائر كبيرة. فقد ينشئ المجرم مواقع إلكترونية مقنعة، وواجهات مزيفة تعرض أرباحاً وهمية، وهويات مزيفة، وعلاقات طويلة الأمد مع الضحية. وقد يسمح لها في البداية بسحب مبالغ محدودة لإقناعها بأن الاستثمار حقيقي، ثم يدفعها إلى إيداع مبالغ أكبر.

ومع تطور الذكاء الاصطناعي، أصبح إنتاج رسائل مقنعة، وتقليد أساليب التواصل الاحترافية، وإنشاء هويات ومحتويات اصطناعية أكثر سهولة. وقد



5. الاستغلال: كيف يستثمر المهاجم نقطة الضعف؟

الإلكتروني، الذي قد يستهدف المراهقين والشباب عبر وسائل التواصل الاجتماعي. فقد ينتحل المجرم شخصية شخص في العمر نفسه، ويبدأ محادثة، ثم يقنع الضحية بإرسال صورة حميمة قبل تهديدها بنشرها ما لم تدفع المال.

ويعتمد المعتدي هنا على الخوف والعار والتهديد بالعواقب الاجتماعية. وهذا يوضح أن الجرائم الإلكترونية قد تترك أثراً نفسياً واجتماعية عميقة تتجاوز الخسائر المالية كثيراً.

الاستغلال هو استخدام نقطة ضعف بعد اكتشافها لتحقيق هدف المهاجم. وقد تكون نقطة الضعف تقنية، مثل خلل في برنامج، أو كلمة مرور ضعيفة، أو شبكة لا سلكية غير آمنة، أو جهاز لم يحصل على تحديث أمني. لكنها قد تكون بشرية أيضاً.

فقد يستغل المهاجم الوحدة، أو الإحراج، أو الطمع، أو الخوف، أو الرغبة في إرضاء صاحب سلطة، أو قلة الخبرة، أو الرغبة في إبقاء أمر ما سرياً. ومن الأمثلة الخطرة على ذلك الابتزاز الجنسي

6. التدمير: ماذا يحدث بعد نجاح الهجوم؟

يتمثل التدمير في قدرة المهاجم على تعطيل الأنظمة أو البيانات، أو تشفيرها، أو حذفها، أو إتلافها، أو كشفها.

ومن أوضح الأمثلة: برامج الفدية، إذ قد يشفر المهاجمون الملفات، ويسرقون نسخاً من البيانات، ويهددون بنشرها، ويعطلون العمليات، ثم يستخدمون هذه الأضرار لضغط الضحية، ودفعها إلى التفاوض، أو دفع الفدية.

وتكشف هذه الهجمات عن حجم الضرر الذي يمكن أن يحدث حتى إذا أمكن استعادة البيانات لاحقاً. فقد تتوقف الأعمال، ويفقد الموظفون إمكانية الوصول إلى الأنظمة، وتضطر الإدارة إلى اتخاذ قرارات صعبة في ظل نقص المعلومات.

وقد تستعين المؤسسة بالمحامين وشركات التأمين والمحققين وخبراء الأمن السيبراني ومستشاري الاتصالات، بينما تتزايد المخاوف بشأن السمعة والالتزامات القانونية وحجم البيانات التي ربما سُرقَت. ويصبح الأمر أكثر خطورة عندما يستهدف الهجوم بنية تحتية حيوية، فالطاقة والمياه والنقل والرعاية الصحية والاتصالات والأنظمة المالية والخدمات الحكومية، وغيرها من القطاعات الأساسية تعتمد بدرجات متفاوتة على أنظمة رقمية، وقد يؤدي تعطيلها إلى آثار تتجاوز المؤسسة المستهدفة.

فلا يستطيع المستشفى ببساطة إيقاف أنظمتهم، ولا يمكن لشبكات الكهرباء والمياه والنقل أن تتعامل مع الانقطاع كما لو كان عطلاً عادياً. وكلما زادت أهمية الخدمة، ارتفعت قيمة تعطيلها بالنسبة إلى المهاجمين الذين يسعون إلى إحداث أكبر قدر ممكن من التأثير.

ويمكن للذكاء الاصطناعي أن يساعد المهاجمين في بعض مراحل الاستطلاع، وأتمتة بعض المهام، وإنشاء محتوى احتيالي أكثر إقناعاً، وتحسين أساليب انتحال الشخصية. وفي الوقت نفسه، يمكن استخدام التكنولوجيا نفسها لأغراض دفاعية، مثل تحليل البيانات، واكتشاف الأنماط، والتهديدات. كما تثير الحوسبة الكمومية اهتماماً متزايداً في مجال التشفير. ما يشير إلى احتمال جمع مهاجم بيانات مشفرة اليوم على أمل فك تشفيرها مستقبلاً، إذا أصبحت قدرات الحوسبة والتشفير المتاحة له أكثر تقدماً.

لذلك، ينبغي للمؤسسات ألا تبني خططها على افتراض أن كل دفاع سينجح دائماً، بل أن تستعد أيضاً لاحتمال اختراق بعض الأنظمة، وأن تحدد مسبقاً كيفية استمرار العمليات والتعافي والتواصل واتخاذ القرارات تحت الضغط.

كيف تصطاد الجواسيس؟

بعد أن تعرفنا إلى طريقة تفكير الجواسيس، ننتقل الآن إلى كيفية اكتشاف أساليبهم والتصدي لها.

الاستعداد

يبدأ الاستعداد بفهم البيانات والأصول الأكثر أهمية للمؤسسة. وهناك ثلاثة أسئلة أساسية ينبغي أن تعرف المؤسسة إجاباتها: ما الأصول والبيانات الحيوية؟ أين توجد؟ ومن يمكنه الوصول إليها؟ فلا يمكن حماية ما لا نعرف وجوده.

لذلك، ينبغي جرد البيانات والأصول الحيوية وتصنيفها، وعزل المعلومات الشديدة الحساسية قدر الإمكان، بدلاً من توزيعها على أنظمة متعددة دون رقابة واضحة.

كما يجب ألا يحصل المستخدمون إلا على الصلاحيات التي يحتاجون إليها لأداء مهامهم، مع تقييد الصلاحيات الإدارية ومراجعتها دورياً.

ولا ينبغي الاعتماد على أداة واحدة لحماية المؤسسة، بل على منظومة من الضوابط بحسب طبيعة المؤسسة ومخاطرها، وتشمل حماية الشبكات والأجهزة، والمصادقة المتعددة العوامل، وإدارة الصلاحيات، والنسخ الاحتياطية، ومراقبة الأنظمة، والتحديثات الأمنية، وخطة واضحة للاستجابة إلى الحوادث.

ويمكن للتأمين السيبراني أن يخفف بعض الخسائر المالية المرتبطة بالحوادث، لكنه ليس بديلاً عن

الأمن السيبراني. وقد ترتبط التغطية التأمينية بشروط وضوابط أمنية محددة، لذلك ينبغي أن تتوافق التغطية مع طبيعة المخاطر الفعلية التي تواجهها المؤسسة.

وقد وضع «المعهد الوطني للمعايير والتقنية» في الولايات المتحدة إطار الأمن السيبراني لمساعدة المؤسسات في إدارة مخاطر الأمن السيبراني. ويتضمن الإطار ست وظائف رئيسية: الحوكمة، والتعريف، والحماية، والكشف، والاستجابة، والتعافي. ويؤكد الإطار أن إدارة الأمن السيبراني عملية مستمرة لإدارة المخاطر وليست مشروعاً تقنياً ينتهي بمجرد تطبيق مجموعة من الأدوات.

ويمكن للأفراد تطبيق المبادئ نفسها على نطاق أصغر: تحديد الحسابات المهمة، واستخدام كلمات مرور فريدة، وتفعيل المصادقة المتعددة العوامل، والاحتفاظ بنسخ احتياطية من الملفات المهمة، وتأمين الشبكات المنزلية، وتحديث الأجهزة والبرامج، وتقليل المعلومات الشخصية المنشورة علناً، ووضع طريقة واضحة للتحقق من الطلبات المالية أو العائلية غير المعتادة.

التقييم

ويحتاج الأفراد بدورهم إلى تقييم وضعهم الأمني باستمرار. فقد تتغير إعدادات الخصوصية، أو تظل حسابات قديمة نشطة، أو تظهر بيانات اعتماد في قواعد بيانات ناتجة عن اختراقات سابقة، أو يطلب تطبيق جديد صلاحيات لا يحتاج إليها فعلاً. كما ينبغي توخي الحذر عند استخدام شبكات لا سلكية عامة غير موثوقة، وتجنب مشاركة البيانات الحساسة عبر اتصالات غير آمنة، وإيقاف مشاركة الموارد غير الضرورية، وحذف الشبكات العامة المحفوظة من الأجهزة عندما لا تعود هناك حاجة إليها. وعندما يبدو عرض أو رسالة أو علاقة أو طلب ما غير طبيعي، توقف قبل اتخاذ أي إجراء. واسأل نفسك: هل توجد مؤشرات على خداع، أو انتحال شخصية، أو وصول غير مصرح به، أو استغلال، أو ضغط متعمد؟ إذا كانت الإجابة نعم، فالخطوة التالية هي التحقق.

صاحبه، وإنما استخدم وسائل تحقق مستقلة، مثل أدوات كشف الذكاء الاصطناعي الموثوقة عند الحاجة. وينبغي للمؤسسات الاحتفاظ بالأدلة وتوثيق الحوادث. فقد تساعد لقطات الشاشة، والسجلات، والرسائل، والطابع الزمني، والملفات المشبوهة، وغيرها من الأدلة الرقمية، في إعادة بناء ما حدث. كما يجب أن يعرف الموظفون متى وكيف يرفعون المخاوف إلى المسؤولين. فثقافة معاقبة الموظف الذي يبلغ عن خطأ قد تزيد الضرر، لأنها تشجع على إخفاء الحوادث بدلاً من الإبلاغ عنها. والسرعة مهمة، فقد يواصل المهاجم سرقة البيانات، أو تغيير الأنظمة، أو حذف الأدلة، بينما لا تزال المؤسسة تناقش كيفية التصرف. والهدف من التحقيق في الساعات الأولى ليس إنتاج تقرير أكاديمي كامل، بل جمع معلومات موثوقة بما يكفي لاحتواء التهديد واتخاذ القرار التالي.

قدرة المؤسسة على استعادة الأنظمة من النسخ الاحتياطية، وما إذا كانت بيانات حساسة قد سُرقَت، وحجم التعطيل التشغيلي، والمتطلبات والقيود القانونية، وتأثير الحادث في السلامة العامة، والتغطية التأمينية، والمخاطر المتعلقة بالسمعة، وما يمكن التحقق منه بشأن هوية المهاجم وتهديداته. والدرس الأهم هو ألا تسمح للمهاجم بأن يتخذ القرار نيابةً عنك. فالمجرمون يمارسون الضغط عمداً لأن الخوف، والإحراج، والعزلة، والاستعجال، قد تدفع الأشخاص إلى اتخاذ قرارات أسوأ. أما الاستعداد فيمنحك خيارات، والتقييم يوضح الوضع، والتحقيق يوفر السياق، والقرار المبني على هذه المعلومات يتيح لك التصرف بوعي بدلاً من الاستجابة بدافع الذعر.

لا توجد خطة أمنية تظل فعالة إلى الأبد. فالتكنولوجيا تتغير، والمؤسسات تندمج، والموظفون ينضمون ويغادرون، والموردون يتغيرون، والمتطلبات التنظيمية تتطور، والمهاجمون يبتكرون أساليب جديدة. لذلك، يجب أن يكون تقييم الوضع الأمني عملية مستمرة للتحقق من أن الضوابط الحالية لا تزال مناسبة للمخاطر القائمة. وقد يشمل ذلك تقييمات للتهديدات الأمنية، واختبارات اختراق مناسبة، وعمليات تدقيق، ومراقبة للتهديدات، ومراجعة دورية للصلاحيات. كما ينبغي إلغاء وصول الموظفين والموردين والاستشاريين فور انتهاء الحاجة إليه. ويجب أيضاً مراجعة اتصالات الأطراف الخارجية، وتقييم الأنظمة والخدمات الجديدة قبل دمجها في البيئة المؤسسية. أما العمل عن بُعد، فينبغي النظر إليه بوصفه توسعاً في سطح الهجوم، وليس مجرد وسيلة لزيادة الإنتاجية. فكل جهاز وحساب واتصال عن بعد قد يضيف نقطة تحتاج إلى الحماية.

التحقق

ينقل التحقق الشخص من مرحلة الشك إلى فهم ما يحدث. ولا تحتاج إلى أن تكون محققاً في مكتب التحقيقات الفيدرالي أو خبيراً في الأمن السيبراني لاكتشاف كثير من المؤشرات الأساسية. ما تحتاج إليه هو الفضول، ودقة الملاحظة، والاستعداد للتحقق بصورة مستقلة. فعند الاشتباه في انتحال شخصية، تحقق من نطاق المرسل، وتواصل مع الشخص عبر قناة معروفة ومستقلة، وتحقق من تعليمات الدفع من خلال مصدر آخر. وفي حالة عروض الاستثمار، تحقق من وجود الشركة، ومن تسجيلها لدى الجهة التنظيمية المختصة. وفي حالات الاحتيال العاطفي، افحص تاريخ الحساب، وابحث عكسياً عن الصور عند الحاجة. أما عند الاشتباه في محتوى اصطناعي أو تزييف عميق، فلا تعتمد على المحتوى نفسه لإثبات هوية

اتخاذ القرار

بعد اتخاذ القرار أصعب مراحل التعامل مع الحادث غالباً، لأنه يحدث تحت ضغط وفي ظل معلومات ناقصة. فالخطط مهمة، لكن الحوادث نادراً ما تسير تماماً وفق السيناريو المتوقع. لذلك، يحتاج القادة إلى استخدام المعلومات المتاحة من الاستعداد، والتقييم، والتحقيق، لاتخاذ قرارات مناسبة في الوقت المناسب. وتُعد مسألة دفع الفدية في هجمات برامج الفدية من أكثر القرارات تعقيداً. فدفع الفدية لا يضمن استعادة البيانات أو عدم تسريبها، كما أن دفع الأموال للمجرمين قد يشجع استمرار نموذج الجريمة. وفي المقابل، قد تواجه المؤسسة ظروفاً تشغيلية وقانونية وإنسانية تجعل القرار أكثر تعقيداً. ومن العوامل التي ينبغي وضعها في الاعتبار:

من التجسس التقليدي إلى نظيره الرقمي



التكنولوجيا عنصر أساسي في هذه الهجمات، لكن نجاحها يبقى معتمداً في الأساس على السلوك الإنساني.

عقلية صائد الجواسيس

وفيما يخص الأفراد والعائلات، يمكن تطبيق المبادئ نفسها على نطاق أصغر. وذلك عبر تقليل المعلومات الشخصية المنشورة للعامة، واستخدام كلمات مرور قوية وفريدة، وتفعيل المصادقة المتعددة العوامل.

بجانب الحفاظ على تحديث البرامج والأجهزة، والاحتفاظ بنسخ احتياطية من البيانات المهمة. والتحقق من الطلبات غير المتوقعة، واستخدام قناة اتصال منفصلة للتأكد من هوية الأشخاص عند إجراء معاملات حساسة.

إضافة إلى ضرورة تعليم الأطفال أن الأشخاص الذين يتواصلون معهم عبر الإنترنت قد لا يكونون من يدعون أنهم كذلك. وإذا حدثت مشكلة، يجب الاحتفاظ بالأدلة وطلب المساعدة مبكراً بدلاً من السماح للخجل أو الخوف بعزل الضحية.

يشير كل ذلك إلى أن الأمن السيبراني يشبه سباق تسلح مستمر؛ فالمهاجمون يغيرون أساليبهم باستمرار، وعندما تصبح إحدى التقنيات أقل فاعلية تظهر تقنيات أخرى.

وقد يجعل الذكاء الاصطناعي بعض أشكال انتحال الشخصية والأتمتة أكثر إقناعاً، كما قد تستمر نماذج الخدمات الإجرامية في خفض الحاجز التقني أمام المهاجمين.

لذلك، لا يمكن للمدافعين الاعتماد على قائمة ثابتة من التهديدات. ما يحتاجون إليه هو مجموعة من العادات والضوابط القادرة على التكيف مع تغير التهديدات.

توضح الأساليب السابقة كيف يحوّل المهاجم المعلومات وعلم النفس البشري إلى أدوات للهجوم، وكيف يمكن للضحية أن تستجيب من خلال حماية أصولها، واكتشاف السلوك غير المعتاد، والتحقق من الشكوك، واتخاذ الإجراءات المناسبة. والتحول الأهم هو الانتقال من الدفاع السلبي إلى الوعي النشط بالتهديدات. ولا يعني ذلك أن يصبح كل مستخدم متوجساً من كل شيء، أو أن تتحول كل شركة إلى وكالة استخبارات. بل يعني فهم حقيقة أساسية: الثقة بالبيئة الرقمية لا ينبغي أن تقوم على الألفة وحدها.

فقد يمكن إنشاء صورة اصطناعية، واستنساخ صوت، وتغيير نطاق بريد إلكتروني بحرف واحد، ونسخ موقع إلكتروني شرعي، واختراق مورد برمجي موثوق، أو الاستيلاء على حساب موظف حقيقي. وبالنسبة إلى الشركات، يعني هذا أن الأمن السيبراني مسؤولية قيادية لا تقع على عاتق قسم تقنية المعلومات وحده. فعلى الإدارة المالية فهم أساليب الاحتيال في المدفوعات. وعلى الموارد البشرية إدارة صلاحيات الوصول عند انضمام الموظفين ومغادرتهم. وعلى الفرق القانونية فهم الالتزامات المتعلقة بالبيانات. وعلى المديرين التنفيذيين الالتزام بإجراءات التحقق نفسها المفروضة على الآخرين.

ويحتاج مجلس الإدارة إلى فهم المخاطر التشغيلية ومخاطر السمعة، كما يجب أن يكون الموردون جزءاً من تقييم المخاطر. ويحتاج الموظفون إلى تدريب دوري يعتمد على سيناريوهات واقعية، بدلاً من الاكتفاء بتدريب سنوي شكلي على الامتثال.



أدوات عملية للأمن السيبراني

فيما يلي مجموعة من العادات العملية التي يمكن للمؤسسات والأفراد تطبيقها:

أولاً: افترض أن كلمات المرور قد تتعرض للكشف.

إعادة استخدام كلمة المرور تحول اختراق حساب واحد إلى بوابة محتملة لاختراق حسابات أخرى، لأن المهاجمين قد يجربون بيانات الاعتماد المسروقة على خدمات متعددة. لذلك، تقلل كلمات المرور الفريدة، ومديرو كلمات المرور، والمصادقة المتعددة العوامل قيمة بيانات الاعتماد المسروقة، وتجعل الاستيلاء على الحسابات أكثر صعوبة.

ثانياً: احمِ البيانات وفقاً لقيمتها.

لا ينبغي معاملة جميع الملفات والمستخدمين بالطريقة نفسها. يجب تصنيف المعلومات الحساسة وتقييد الوصول إليها، كما ينبغي إخضاع حسابات المسؤولين لضوابط أكثر صرامة من حسابات المستخدمين العاديين. ولا ينبغي أن يحتفظ الموظفون السابقون أو المتقاعدون الخارجيون بإمكانية الوصول بعد انتهاء الحاجة إليها. فالمؤسسة التي لا تعرف من يستطيع الوصول إلى أهم معلوماتها لا تستطيع ادعاء أنها تسيطر عليها.

ثالثاً: صمّم النسخ الاحتياطية من أجل الاستعادة الفعلية.

لا ينبغي إنشاء النسخ الاحتياطية لمجرد استيفاء مطلب إداري. فقد تحاول مجموعات برامج الفدية الوصول إلى النسخ الاحتياطية المتصلة بالشبكة وتشفيرها أو حذفها قبل تفعيل الابتزاز. لذلك تحتاج المؤسسات إلى نسخ احتياطية مناسبة، ومعزولة عند الحاجة، ومحمية، والأهم من ذلك مختبرة بصورة دورية للتأكد من إمكانية استعادتها. فالنسخة الاحتياطية التي لم تُختبر قد تمنح المؤسسة شعوراً زائفاً بالأمان في اللحظة التي تكون فيها في أمس الحاجة إليها.

رابعاً: حدّث الأنظمة باستمرار.

قد يبحث المهاجمون عن الثغرات المعروفة في أنظمة التشغيل، والتطبيقات، وأجهزة الشبكات، والخدمات المتصلة بالإنترنت. ويمنح تأخير التحديثات المهاجمين وقتاً إضافياً لاستغلال ثغرات قد تكون لها إصلاحات متاحة بالفعل. وينطبق الأمر نفسه على الأجهزة الشخصية، والهواتف وأجهزة الكمبيوتر والمتصفحات والتطبيقات تحتاج جميعها إلى تحديثات أمنية منتظمة.

خامساً: اجعل التحقق جزءاً من الإجراءات التجارية.

لا ينبغي أن يعتمد التحقق على الاجتهاد الشخصي عندما تكون المعاملة حساسة. فالمدفوعات الكبيرة، وتغيير الحسابات المصرفية، وإعادة تعيين كلمات المرور، وطلبات البيانات السرية، والتعليمات غير المعتادة من كبار المسؤولين، يجب أن تخضع جميعها إلى وسيلة مستقلة للتأكد من صحتها. وقد تكون مكالمة هاتفية إلى رقم معروف مسبقاً، أو مسار موافقة منفصل، أو عبارة متفق عليها مسبقاً، كافية لقطع الطريق على بعض محاولات انتحال الشخصية. وتزداد أهمية هذه الإجراءات في ظل انتشار تقنيات التزييف العميق، التي تجعل الاعتماد على الصوت أو الفيديو وحدهما أقل ملاءمة للتحقق من الهوية.

سادساً: تعامل مع وسائل التواصل الاجتماعي بوصفها مصدراً للمعلومات التي قد يستفيد منها المهاجم.

قد تكشف المنشورات العامة عن جداول السفر، والعلاقات الأسرية، والمسؤوليات الوظيفية، والموردين، والمديرين التنفيذييين، والهوايات، والروتين اليومي. وقد لا يبدو أي تفصيل منها خطراً بمفرده، لكن المجرمين يستطيعون جمع هذه التفاصيل وبناء قصة مقنعة انطلاقاً منها. فكلما قلّ ما تكشفه للعامة دون حاجة، قلّ السياق الذي يستطيع المهاجم استخدامه لبناء عملية خداع شخصية.

وأخيراً: أبلغ عن الخطأ فور وقوعه.

إذا نقرت رابطاً خبيثاً أو استجبت لرسالة مشبوهة، فلا تحاول إخفاء الأمر خوفاً من اللوم. إذ قد تكون سرعة الإبلاغ عاملاً حاسماً في الحد من الضرر. وبعد وقوع الحادث، يجب على المؤسسة توثيق ما حدث، وتحديد الضوابط التي فشلت، وتحسين الإجراءات لمنع تكرار السيناريو نفسه. ولا يعني ما سبق أن الهدف هو بناء نظام لا يتعرض للهجوم مطلقاً، فلا توجد منظومة أمنية واقعية تضمن ذلك. وإنما الهدف هو جعل الهجمات أصعب تنفيذاً، وأسهل اكتشافاً، وأقل ضرراً عند وقوعها، وأقل احتمالاً للنجاح بالطريقة نفسها مرة أخرى.

طبقات الإنترنت الثلاث

ساحة حرب إلكترونية جديدة

الويب السطحي

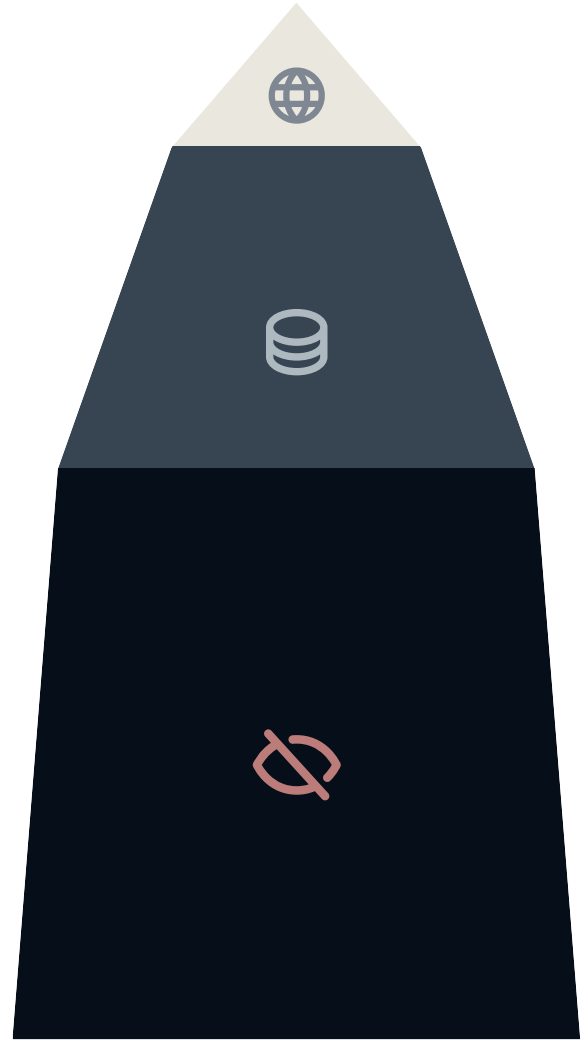
ما تفهرسه محركات البحث العامة،
يستخدمه معظم الناس يومياً.

الويب العميق

يتطلب تسجيل دخول أو صلاحية وصول،
الطبقة الأكبر حجماً.

الويب المظلم

شبكات مصممة لإخفاء موقع المستخدم
أو الخدمة بدرجة أكبر.



إساءة استخدام

أسواق ومنتجات الجريمة الإلكترونية



استخدام مشروع

تصفح وفهرسة للشبكة



التوجيه البصلي، شبكة «تور»

طبقات تشفير متعددة تُخفي مسار البيانات، دون إخفاء الهوية بصفة مطلقة.



خلاصة القول

من يسيطر على المعلومات والثقة والوقت والقرارات يمتلك قدراً كبيراً من القوة. وينجح مجرمو الإنترنت عندما يتمكنون من السيطرة على الموقف: يختارون الرسالة، ويخلقون شعوراً بالإلحاح، ويحددون الرواية التي تبدو للضحية حقيقية، ثم يدفعونها إلى رد فعل سريع.

أما عقلية صائد الجواسيس فتعيد هذه السيطرة إلى الطرف الآخر. فالتفكير كجاسوس يعني أن تسأل كيف يمكن للمهاجم استغلال المعلومات المعروفة عنك.

هل يمكن للمعلومات المنشورة للعمامة أن تساعد في انتحال شخصيتك؟ هل يمكن لكلمة مرور مسربة أن تفتح حسابات أخرى؟ هل يمكن لمورد خارجي أن يصبح مدخلاً إلى شبكتك؟ هل يمكن ضغط موظف مالي لتجاوز إجراءات التحقق؟ هل يمكن التلاعب بمراهق من خلال الخوف أو الخزي؟ وهل تستطيع مؤسستك الاستمرار في العمل إذا تعطلت أنظمتها الأساسية غداً؟

فالتصرف كصائد جواسيس يعني طرح هذه الأسئلة قبل وقوع الهجوم.

لذا، استعد من خلال تحديد البيانات الحساسة، وتقييد الوصول إليها، وتطبيق طبقات متعددة من الحماية، وإنشاء نسخ احتياطية قابلة للاستعادة، ووضع خطة واضحة للاستجابة للحوادث.

وقيم وضعك باستمرار مع تغير التكنولوجيا والأفراد والموردين والمخاطر. وتحقق من كل ما يخرج عن النمط المعتاد. واتخذ قراراً سريعاً عندما تتوافر أدلة كافية على وجود تهديد، لكن اتخذ القرار انطلاقاً من الاستعداد والمعرفة، لا من الذعر.

لا تهدف هذه المقاربة إلى نشر التشاؤم أو الخوف، بل إلى منح الأفراد والمؤسسات قدراً أكبر من القدرة على التصرف.

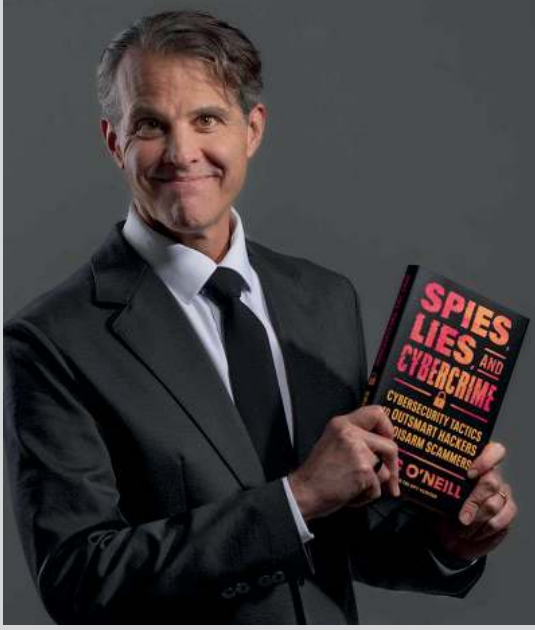
فقد يكون اقتصاد الجرائم الإلكترونية واسعاً، وقد يكون المهاجمون متطورين، وقد تجعل التقنيات الحديثة بعض أشكال الخداع أكثر إقناعاً. لكن معظم الأفراد والمؤسسات يستطيعون رفع مستوى أمنهم بدرجة كبيرة من خلال اتباع ممارسات منضبطة.

فالأمن لا يتحقق بمنتج واحد، ولا بمجرد افتراض أن جهات إنفاذ القانون ستتولى المشكلة بعد وقوعها. بل يُبنى خطوة خطوة: بيانات تُحمى، وطلب يُتحقق منه، ونظام يُحدث، وصلاحيات تُقيد، ونسخة احتياطية تُختبر، وقرار صحيح يُتخذ في الوقت المناسب.

والمبدأ الأساسي بسيط: أفهم طريقة تفكير المهاجم، وأزل الفرص السهلة أمامه، وتحقق قبل أن تثق، واستعد للتحرك.

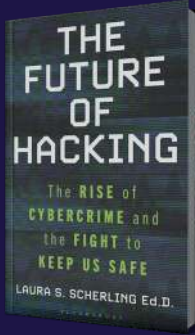
ففي عالم رقمي يمكن فيه تزييف المظاهر، والتلاعب بالهويات، وتسريب البيانات خلال ثواني، لا يكمن أقوى دفاع في الخوف، بل في الاستعداد، وفهم السياق، وطرح الأسئلة الصحيحة، والتحقق المستقل، والتصرف الحاسم عند الحاجة.

نبذة عن المؤلف:



إريك أونيل عميل سري سابق في مكتب التحقيقات الفيدرالي الأمريكي، وهو متحدث عام وخبير أمني يلقي محاضرات دولية حول التجسس والأمن القومي والأمن السيبراني والاحتيايل والاجتهاد المؤسسي والدفاع والاختراق وموضوعات أخرى.

كتب أخرى مقترحة:



The Future of Hacking

Laura S. Scherling

2025



Ransom War

Max Smeets

2025



We Know You Can
Pay a Million

Anja Shortland

2026

تواصلوا
معنا على
MBRF News
mbrae
www.mbrae

مؤسسة محمد بن راشد آل مكتوم للمعرفة
MOHAMMED BIN RASHID AL MAKTOUM
KNOWLEDGE FOUNDATION

للاطلاع على المزيد من إصدارات
«كتاب في دقائق»، امسح رمز
الاستجابة السريعة.



إنجازات معرفية ترسم أثراً عالمياً

400+

مليون وصول ومشاهدات
قمة المعرفة

300

كتاب برنامج دبي
الدولي للكتابة

1,715+

جلسة
استراحة معرفة

195

دولة امتداد
معرفي عالمي

2

مليون كتاب ضمن
مبادرة «عائليتي تقرأ»

4.9

مليون مستخدم لمركز
المعرفة الرقمي



MBRF_Knowledge



mbrf_news



mbrf.ae