

الفدية» و«التزييف» و«الابتزاز» تتصدر الهجمات المعلوماتية 2023»



أجمع خبراء ومتخصصون في حماية البيانات والأمن السيبراني على أن دولة الإمارات تعمل عن كثب على حماية تحولها الرقمي العمود الفقري للاقتصاد المعرفي عبر التكامل والتعاون بين جميع إدارات المعلومات في الجهات الحكومية الاتحادية والمحلية والشركات العالمية الخاصة العاملة في هذا القطاع الحيوي.

وأشاروا إلى أن تحول الإمارات الرقمي وارتباطها المعلوماتي الوثيق عبر شبكات الانترنت العالمية بالإضافة إلى نموها الاقتصادي اللافت يجعلها هدفاً مستمراً لمجموعات وأفراد قرصنة المعلومات التي تستهدف البيانات للحصول على الأموال أو حتى التخريب.

الصورة



حذر الخبراء من تواصل وشدة الهجمات الإلكترونية والسيبرانية على الدولة والمنطقة في عام 2023 عبر ما يسمى

بهجمات «طلب الفدية» أو «التزييف العميق» أو الهجمات البرمجية الخبيثة وغيرها ما يستدعي ضرورة اليقظة التامة عبر تأهيل الكوادر البشرية وتحديث أنظمة وبرمجيات الحماية بصورة مستمرة، بالإضافة إلى الاستعانة بتقنيات الذكاء الاصطناعي التي بدأت تدخل قطاع حماية المعلومات وشبكات الانترنت مؤخراً بقوة

• قيمة البيانات

يؤكد جوني كرم، مدير عام ونائب الرئيس الإقليمي للأسواق الناشئة الدولية في «فيريتاس تكنولوجيز» استمرار الهجمات الإلكترونية في الزيادة والتطور، ما يجعل مواكبة الأمن السيبراني تحدياً مستمراً، لذا أصبح من الأولويات الضرورية اتخاذ التدابير المناسبة لحماية بياناتهم

ليكون بمثابة تأكيد (PDP) وقال: أطلقت دولة الإمارات بداية 2022 أول قانون اتحادي لحماية البيانات الشخصية مهم على القيمة الكبيرة للبيانات في الاقتصاد الرقمي وأهمية حمايته وفي 2023، ستشرع الشركات في التعامل مع مسألة الامتثال بجدية أكبر، حيث سيكون قد مر عام منذ دخول القانون حيز التنفيذ

وأضاف، سيشمل ذلك الحصول على رؤية أكبر لبيانات الشركة والعملاء، وضمان شرعية معالجة البيانات، ودعم حقوق الخصوصية الفردية، وضمان شغل مناصب معالج البيانات ومراقب البيانات للاستجابة لمتطلبات مسألة الامتثال لدولة الإمارات



وأوضح كرم، عندما تتولى إدارة البيانات الذاتية مسؤولية مساعدة فرق تكنولوجيا المعلومات، فسوف تتمكن من اتخاذ القرارات الاستباقية وتطبيق السياسات بكفاءة أكبر ويمكنها التعرف على خصائص البيانات المختلفة وتطبيق أي سياسات تخزين، حماية أو حذف منطقية. لذلك، عند إنشاء بيانات جديدة، ستتم حمايتها تلقائياً، وتخزينها بشكل آمن، والوصول إليها بشكل محدود وحذفها في الوقت المناسب

• تزايد قراصنة الإنترنت

قال أشرف كحيل، مدير تطوير الأعمال في الشرق الأوسط وإفريقيا وتركيا لدى «غروب-آي بي»: تهيمن برامج الفدية على مشهد التهديدات الإلكترونية والسيبرانية في المنطقة خلال 2023 في حين أن مجرمي الإنترنت يزدادون باستمرار ما يؤدي إلى زيادة التكاليف على الشركات المتضررة

وأوضح كحيل أن قيمة سوق الأمن السيبراني في الإمارات تبلغ حالياً نحو 1.8 مليار درهم «490 مليون دولار» ومن المتوقع أن ينمو 14.5% سنوياً على مدى السنوات ال 5 المقبلة

وتشير بيانات «آي بي إم» إلى أن تكلفة حوادث الأمن السيبراني في المنطقة وصلت إلى مستوى مرتفع جديد قدره 6.93 مليون دولار لكل خرق للبيانات، وهو أعلى بكثير من المتوسط العالمي البالغ 4.24 مليون دولار لكل حادثة



• نقاط الضعف

وأضاف كحيل، في عام 2022، شهدنا أن هجمات برامج الفدية أصبحت مكوناً حيوياً في ترسانة الحرب الجيوسياسية. علاوةً على ذلك، ابتكرت الجهات الخبيثة تقنيات معقدة بشكل متزايد لبرامج الفدية، مثل الابتزاز المزدوج، لتعظيم أرباحها من خلال مهاجمة نقاط الضعف في البنى التحتية الحيوية والشركات الكبيرة بشكل متكرر.

أضف إلى ذلك، سمحت التطورات التكنولوجية الأخيرة بأن تصبح برامج الفدية طريقة غير مكلفة نسبياً لاستهداف الشركات. في الواقع، تتوفر عروض جديدة مثل برامج الفدية كخدمة بسهولة على الويب المظلم، وقد لعبت دوراً رئيسياً في الارتفاع الأخير في هجمات برامج الفدية التي شوهدت في المنطقة والعالم.

ونعتقد أن برامج الفدية ستستمر في الازدهار في عام 2023 وستظل أكبر تهديد إلكتروني للأعمال والمؤسسات. سيواصل مجرمو الإنترنت التكيف المستمر وتطوير تقنيات جديدة لتعزيز فعالية هجماتهم، فقد أصبحت أكبر مجموعات برامج الفدية أكثر تنظيماً، نظراً لاستمرار عدم الاستقرار الاقتصادي، فمن المرجح أن يؤدي ذلك إلى مزيد من إغراء المجرمين الإلكترونيين لزيادة وتيرة هجماتهم.

• جهود متضافرة

وشدد كحيل على أن دولة الإمارات بذلت جهوداً متضافرة لتعزيز وترسيخ استراتيجيتها للأمن السيبراني في كل من القطاعين العام والخاص، وأعلنت الدولة مؤخراً عن تبني معايير الأمن السيبراني للجهات الحكومية، ومع استمرار المنطقة في دفع أجندتها للتحويل الرقمي وزيادة عدد الأجهزة المتصلة بالإنترنت، تزداد فرص مجرمي الإنترنت، لذا ستحتاج المؤسسات العامة والخاصة إلى إعطاء الأولوية للاستثمارات في الأمن السيبراني.

• الوعي بالمخاطر

يشير عماد فهمي، مدير هندسة النظم الإقليمي بشركة «نتسكاوت» إلى أنه ونظراً لأن العالم أصبح متنقلاً ومتصلاً بالإنترنت بشكل متزايد، فإن الفرص الجديدة لإحداث الضرر والدمار متاحة باستمرار لجهات التهديد الفاعلة.

ويعد الوعي بالأوضاع العالمية والتقييم المستمر للمخاطر أمراً بالغ الأهمية للبقاء في هذا العصر من الاضطراب المتعمد عبر الإنترنت الناجم عن الأحداث الاجتماعية والسياسية. نظراً لأننا نواجه المزيد من عدم اليقين في المستقبل، يجب على المنظمات الإقليمية ضمان الحماية المناسبة للخواص والخدمات والتطبيقات والمحتوى والبنية التحتية الداعمة التي تواجه الجمهور بشكل مناسب.

• عواقب وخيمة

من جانبه قال رواد درويش، مدير المبيعات الإقليمي لحلول الشبكات في دول «الخليج» بشركة «كيسايت تكنولوجيز»: تعرضت المنظمات في المنطقة لعدد متزايد من الهجمات الإلكترونية، والتي كان للعديد منها عواقب وخيمة على سمعتها ونموها ولا تزال التهديدات المتمثلة في البرامج الضارة وهجمات حجب الخدمة الموزعة و برامج الفدية والتصيد الاحتيالي والخداع تستهدف المؤسسات والمستهلكين الإقليميين المعرضين للخطر وبطبيعة الحال، أدى ذلك إلى زيادة الاهتمام بتحسين أدوات وموارد الأمن السيبراني.

ومن المتوقع أن تصل قيمة سوق الأمن السيبراني في المنطقة وإفريقيا إلى نحو 2.893 مليار دولار 2026 وفي 2023، نتوقع أن تصبح الهجمات الخبيثة أكثر تعقيداً، كما ستنتشر تقنية التزييف العميق التي تستخدم الذكاء الاصطناعي لإنشاء صور لأحداث مزيفة.

• التزييف العميق

وأضاف درويش، يحذر خبراء الأمن المعلوماتي والسيبراني منذ سنوات من احتمال وقوع هجمات الهندسة الاجتماعية باستخدام التزييف العميق، ستنتزع التكنولوجيا بدرجة كبيرة خلال 2023 لرؤية المتسللين يستفيدون منها بنجاح لاستهداف المستهلكين والشركات.

ونتوقع زيادة في إنشاء الصور والصوت الذي تم إنشاؤه والمحادثات التي تبدو واقعية، مصممةً لخداع المستلمين لمشاركة البيانات الشخصية أو غيرها من المعلومات الحساسة.

وسيشن المتسللون هجمات ببرمجيات خبيثة لا هواة فيها، كما سيقومون بتحديث وتطوير هجماتهم بشكل دائم وعبر إنشاء برامج ضارة تستهدف أي مجال أو نظام أساسي أو قطاع أعمال معين.

وسيحتاج الدفاع الأمني للمؤسسات إلى مواكبة ذلك وإذا لم تقم الشركات بتضمين أحدث موجات التهديدات المصممة خصيصاً لقطاع أعمالها عند اختبار الأمن السيبراني، فإنها معرضة لخطر ترك باب مفتوح للبرامج الضارة الجديدة أو المتحولة.

وفي عام 2023، ستعيد المنظمات الإقليمية فحص حلول الأمن السيبراني واعتبارات الإنفاق، ولطالما كانت المنظمات مترددة تاريخياً في اعتماد برامج وخدمات قائمة على الشبكة والسحابة بسبب مخاوف أمنية.

وتوقع درويش أن تتم معالجة هذه المشكلات خلال 2023 باستخدام إمكانيات التشفير القوية والتحكم الأكبر في الوصول إلى معلومات القياس والبيانات، ما يوفر للمستخدمين ضماناً لا مثيل له لسلامة البيانات من الفحص إلى السحابة والعكس. نتيجةً لذلك، نتوقع المزيد من الاستثمارات في أمان السحابة والشبكات.

• هجمات أكثر تدميراً

وأشار جوناثان مبيستيد، نائب الرئيس للمبيعات في المنطقة وبريطانيا وإفريقيا بشركة «نتسكوب» إلى أن عام 2022 أعطى دروساً قوية حول أهمية أمان البيانات وتعقيدات بناء وضع أمني قوي وسط النماذج التنظيمية المتغيرة، فتم ترسيخ العمل عن بُعد والعمل الهجين على مدار الـ 12 شهراً الماضية.

وأظهر تقرير السحابة والتهديدات 2022 أن حوالي نصف الأدوار المكتبية في المنطقة لا تزال تعمل عن بُعد، وأن التطبيقات السحابية التي يستخدمها هؤلاء العمال هي الآن مصدر أكثر من 40% من تنزيلات البرامج الضارة في المنطقة.

وسيستمر عام 2023 في تحدي المنظمات على مستوى العالم وداخل المنطقة ومن المحتمل أن يزداد اعتماد السحابة محلياً بشكل أكبر بعد الإعلانات المهمة بين موردي السحابة الرئيسيين لخطط إنشاء بنية تحتية داخل المنطقة – لدعم متطلبات اختصاص البيانات المحلية.

ولن تختفي برامج الفدية قريباً وإن النموذج آخذ في النضج، مع انتشار الابتزاز المزدوج، ولا يظهر المهاجمون رحمة تجاه أهداف مساعيهم الخبيثة ولا يبدو أن أحداً آمناً

وعلى شبكة الانترنت المظلمة، نرى التوافر المتزايد لبرامج الفدية كخدمة، ما يعني أنه حتى المهارات الإلكترونية لا تشكل عقبة أمام أصحاب النوايا السيئة

ومن المحتمل أن نرى المزيد من المجموعات تنفذ هجمات أكثر تدميراً، والمزيد من الشركات التابعة تشارك في هذه الهجمات، وحمولات وأدوات أحدث تُستخدم جنباً إلى جنب مع تقنيات أحدث مثل التعاون مباشرة مع المطلعين الضارين

وبالإضافة إلى برامج الفدية الضارة، نشهد أيضاً زيادة كبيرة في هجمات سلسلة توريد البرامج في السنوات الأخيرة

ونظراً لاكتشاف المزيد من الثغرات الأمنية في التعليمات البرمجية المصدر للتطبيق، خاصة بين البرامج مفتوحة المصدر، نتوقع أن يستمر هذا النوع من الهجوم في النمو. وهذا يستدعي الانتباه إلى حاجة المنظمات إلى تعزيز تدابيرها واستراتيجياتها لأمن سلسلة توريد البرمجيات

ودعا مبستيد إلى ضرورة استعداد الشركات لحماية نفسها من بيئة التهديدات المتطورة. من المقبول أن الأمن السيبراني ليس حلاً لمرة واحدة، ولكنه حل متطور باستمرار. نظراً إلى كون الشركات تفر بهذا الإدراك وتتصرف بناءً عليه، يمكنها الدفاع عن نفسها وبياناتها ومستخدميها بشكل أفضل

• التحليل السلوكي

ويقول طلال شيخ، مدير الدراسات بكلية الرياضيات وعلوم الحاسوب، بجامعة «هيريوت وات دبي»: يمكن أن يساعد الذكاء الاصطناعي والتعلم الآلي المؤسسات على تحسين دفاعها الأمني والاستجابة لها من خلال أساليب متطورة ليس فقط من خلال السرعة والدقة، ولكن أيضاً من خلال بناء نماذج سلوكية تسمح بالكشف عن التهديدات الأمنية والمخاطر المحتملة وتحليلها في الوقت الفعلي

وأضاف، يمكن للذكاء الاصطناعي تحديد الحالات الشاذة التي قد تشير إلى التهديدات السيبرانية من خلال منهجيات التحليل السلوكي، ويمكنه تحليل السلوك الأساسي لحسابات المستخدمين ونقطة النهاية والخوادم وتحديد الأنماط غير العادية ويساعد ذلك في حماية المؤسسات حتى قبل الإبلاغ عن الثغرات الأمنية بمجرد اكتشاف التهديدات السيبرانية المحتملة، كما يمكن للذكاء الاصطناعي الاستجابة بشكل مستقل لانتهاكات البيانات في الوقت الفعلي دون تدخل بشري إذا لزم الأمر

وأشار إلى أن الذكاء الاصطناعي والتعلم الآلي يعدان عاملين أساسيين في أتمتة الأمن السيبراني، فحلول مكافحة البرامج الضارة هي شكل رئيسي من أشكال الدفاع عن الأمن السيبراني، مدفوعة جزئياً بالتعلم الآلي، فيمكن أن يساعد الاكتشاف والاستجابة المدار آلياً وذكياً، جنباً إلى جنب مع تنسيق الأمان والأتمتة والاستجابة في اكتشاف التهديدات السيبرانية مثل برامج الفدية في الوقت الفعلي والاستجابة لها، كما تساعد أساليب المصادقة المستندة إلى السياق والمخاطر على تقليل احتمالية الاختراق إلى الأنظمة

وقال شيخ: لا يمكن استبدال محلي الأمن بالكامل بالذكاء الاصطناعي في هذه المرحلة، على الرغم من قدرة الذكاء الاصطناعي على اكتشاف التهديدات والاستجابة لها لا تزال المنظمات بحاجة إلى مهيئين مهرة وبشريين في مجال الأمن السيبراني.

• الأهداف الأكثر شيوعاً

وقال جميل أبو عقل، المدير الإقليمي لهندسة المبيعات بشركة «مانديانت»: إن الجهات الحكومية والقطاعات المالية والرعاية الصحية والتجزئة تظل الأهداف الأكثر شيوعاً للمهاجمين السيبرانيين وبغض النظر عن القطاع أو حجمه، ينبغي تعزيز دفاعاتها واختبارها بصورة منتظمة. وأضاف، يحرص المهاجمون على تغيير أسلوبهم بانتظام لتجنب الاكتشاف، ما يجعل المدافعين يكافحون لمواكبة ذلك والتصدي لهم عبر تعزيز الدفاعات الإلكترونية والتحقق منها باستمرار.

وأوضح أن دولة الإمارات تعد هدفاً بارزاً يستقطب المهاجمين والتهديدات السيبرانية، نظراً لاقتصادها المتقدم ودورها المحوري في المنطقة.

وعلى مدار العشر سنوات الماضية، نمت تهديدات قراصنة برمجيات الفدية وعمليات الابتزاز المعقدة بشكل كبير وأصبحت تشكّل تهديداً كبيراً للأمن السيبراني للمؤسسات من جميع الأشكال والأحجام ويواصل قراصنة برمجيات الفدية الابتكار واستخدام تكتيكات جديدة لنشر برمجياتهم وتكثيف حملات الهجوم من خلال التهديد بإغلاق البنية التحتية الحيوية، وتعريض الصحة العامة والسلامة للمخاطر، وتحويل الموارد العامة الحيوية، وتعطيل المؤسسات التعليمية، والتأثير في خصوصية البيانات.

وذكر أبو عقل أنه من الضروري جداً تفعيل آلية مكافحة هجمات برمجيات الفدية عبر تقسيم الشبكة للتحكم بشكل أفضل في تدفق حركة المرور عبرها، ووضع ضوابط وصول أكثر إحكاماً تستخدم أقل الامتيازات وأفضل الممارسات التي تحتاج إلى المعارف المتعمقة للحد من التحكم في الأجزاء الحيوية داخل الشبكة.

• عناوين الإنترنت

يُعد نظام أسماء النطاقات أحد الأسس التي يقوم Edgio «قال ريتشارد يو - مدير إدارة المنتجات في شركة «إيدجيو» عليها الإنترنت، حيث يعمل على مطابقة النطاقات (من متصفح الويب أو طلبات التطبيقات) مع عناوين بروتوكول الإنترنت ذات الصلة.

ولا يمكن لمستخدمي الإنترنت، عند تعطل هذا النظام، إيجاد المخدّم الذي يستضيف الموقع الإلكتروني، ما يجعله غير متاح تماماً وبالتالي، لا بدّ من حماية خدمات النظام لضمان استمرارية توافر المواقع الإلكترونية ومنصات التجارة الإلكترونية ووظائف الإنترنت الأخرى للمستخدمين والعملاء.

ولاحظنا ارتفاعاً في معدلات حالات حجب الخدمة واستغلال التطبيقات وبرمجيات الفدية وهجمات حشو الاعتمادات، إضافةً إلى زيادة نقاط الضعف المشتركة في التطبيقات وعمليات الاستغلال ذات الصلة بنسبة 25% على أساس سنوي.

وأكد يو أن اعتماد حل أمني شامل يسهم في منح قادة الشركات أفضل فرصة لإحباط محاولات المجرمين السيبرانيين وضمان المحافظة على سرية وسلامة وتوافر بياناتهم وتطبيقاتهم وبنيتهم التحتية، ويجب أن يشتمل هذا الحل على (الحماية من هجمات حجب الخدمة وخدمات البنية التحتية الحيوية (مثل نظام أسماء النطاقات

"حقوق النشر محفوظة" لصحيفة الخليج. © 2024