بيان صحفي

العلاقات الإعلامية
شارون ديفان
أوك كونسلتينغ للعلاقات العامة
+971 50 8444 823
sharon@oakconsulting.biz

تقرير سيسكو السنوي للأمن الإلكتروني 2017: عودة أساليب الهجوم الكلاسيكية، وسيسكو تخفّض الوقت اللازم للكشف عن التهديدات إلى ست ساعات

مدراء الأمن يكشفون عن التكلفة الفعلية للخرق الأمني والإجراءات التي تتخذها المؤسسات في النسخة العاشرة من التقرير

دبي، الإمارات العربية المتحدة، 8 فبراير 2017: أظهر تقرير سيسكو السنوي للأمن الإلكتروني 2017 أن أكثر من ثلث المؤسسات التي واجهت خرقاً أمنياً في العام 2016 تعرضت لخسائر ملموسة تمثلت في فقدان العملاء أو الفرص أو الإيرادات بنسب تفوق 20 بالمائة. وتعمل تسعون بالمائة من تلك المؤسسات على تعزيز تقنيات وإجراءات الدفاع ضد التهديدات بعد التعرض للهجوم، وذلك من خلال الفصل بين وظيفتي تقنية المعلومات والأمن (38 بالمائة) وزيادة تدريب الموظفين للتوعية الأمنية (38 بالمائة) وتطبيق أساليب تخفيف المخاطر (37 بالمائة). استطلع التقرير آراء حوالي 3000 مدير أمني وقائد للعمليات الأمنية في 13 دولة ضمن دراسة قياس الاداء للقدرات الأمنية، وهي جزء من تقرير سيسكو السنوي للأمن الإلكتروني.

وفي عامه العاشر، سلّط التقرير العالمي الضوء على التحديات والفرص التي تواجهها فرق الأمن في دفاعها ضد التطور المستمر للجريمة الإلكترونية والتغير الدائم في أنماط الهجوم. وتحدث مدراء الأمن عن قيود تتعلق بالميزانية، بالإضافة إلى ضعف التوافق بين الأنظمة ونقص الكفاءات المدرّبة كأكبر المعيقات التي تقف في وجه تطوير موقفهم الأمني. كما كشف القادة عن كون أقسامهم الأمنية بيئات متزايدة التعقيد، إذ تستخدم 65 بالمائة من المؤسسات منتجات أمنية يتراوح عددها من ستة إلى أكثر من 50 منتجاً، الأمر الذي يزيد إحتمال اتساع الثغرات في الكفاءة الأمنية.

في تعليقه على هذا الجانب قال **شكري عيد، المدير التنفيذي لدول المنطقة الشرقية لدى سيسكو الشرق الأوسط**: "في العام 2017 يصبح الفضاء الإلكتروني رديفاً للأعمال، وهذا يتطلب تغير الأساليب واختلاف النتائج. لا بد من التحسين المتواصل بلا كلل، وينبغي قياس ذلك من خلال الفاعلية والتكلفة والمخاطر المدارة بحكمة. يقدم تقرير العام 2017 السنوي للأمن الإلكتروني -وآمل أنه يبرر- عدداً من الإجابات التي تساعدنا في مواجهة المصاعب المتعلقة بالميزانية والموظفين والابتكار والبنية."

ولاستغلال تلك الثغرات، تظهر بيانات تقرير سيسكو السنوي للأمن الإلكتروني أن المجرمين الإلكترونيين يقودون عودة لأساليب الهجوم "الكلاسيكية"، كالإعلانات الضارة والبريد الإلكتروني التطفلي – حيث بلغ الأخير مستويات لم نشهدها منذ عام 2010. يعتبر البريد الإلكتروني التطفلي مسؤولاً عن حوالي ثلثي (65 بالمائة) من مجموع رسائل البريد الإلكتروني، بحيث تتسم نسبة 8 إلى 10 بالمائة منها بأنها ضارة. يرتفع حجم البريد الإلكتروني التطفلي عالمياً وغالباً ما تساهم في نشره شبكات كبيرة ومزدهرة من الأجهزة (البوت نت أو الروبوتات الإلكترونية الخبيثة).

يعتبر قياس فعالية الممارسات الأمنية في وجه تلك الهجمات أمراً بالغ الأهمية، وفي هذا الصدد تقوم سيسكو بتتبع التقدم المحرز في تقليل الوقت اللازم للكشف عن التهديدات – وهو الفترة الزمنية بين التعرض للتهديد وبين الكشف عنه. ولا شك في أن زيادة سرعة الوقت اللازم للكشف عن التهديدات أمر في غاية الأهمية لتقييد حركة المهاجمين والضرر الذي تسببه هجماتهم. وقد نجحت سيسكو في تخفيض الوقت اللازم للكشف عن التهديدات من زمن وسيط قدره 14 ساعة أوائل العام 2016 إلى ست ساعات فقط في النصف الثاني من العام. ويقوم الرقم على تقنية اختيارية للقياس عن بعد يتم جمعها من منتجات سيسكو الأمنية المستخدمة حول العالم.

من جانبه قال **سكوت مانسون، مدير الأمن الإلكتروني لدى سيسكو في الشرق الأوسط وتركيا**: " من أبرز قياساتنا التي أبرزها تقرير سيسكو السنوي للأمن الإلكتروني 2017 مقياس "الوقت اللازم للكشف عن التهديدات" وهو الوقت المستغرق للعثور على الأنشطة الضارة وتخفيف آثارها. عملنا على تخفيض ذلك الوقت إلى رقم متدن قدره 6 ساعات فقط، بينما طورنا مقياساً آخر هو "الوقت اللازم للتطور"، والذي يدرس مدى سرعة المهاجمين في تغيير هجماتهم بشكل يخفي هويتهم. وبفضل تلك المقاييس وغيرها، والتي تم استنباطها من نتائج التقرير، وبفضل التعاون مع المؤسسات لأتمتة وتكامل دفاعاتها ضد التهديدات، أصبح بإمكاننا تقديم مساعدة أفضل في تقليل المخاطر المالية والتشغيلية التي تواجهها فيما تتمكن من تنمية أعمالها."

تكلفة الهجمات الإلكترونية على الأعمال: خسارة العملاء والإيرادات

بيّن تقرير سيسكو السنوي للأمن الإلكتروني 2017 الأثر المالي المحتمل للهجمات على المؤسسات باختلافها – من الشركات الكبرى إلى المشاريع الصغيرة والمتوسطة. فقد واجهت أكثر من 50 بالمائة من المؤسسات انتقاداً جماهيرياً بعد التعرض لخرق أمني، بينما كانت الأنظمة المالية والعمليات هي الأكثر تأثراً، تتلوها سمعة العلامة التجارية والقدرة على الاحتفاظ بالعملاء. وكان الأثر بالغاً على المؤسسات التي تعرّضت للهجمات:

- فقدت اثنان وعشرون بالمائة من المؤسسات المعرّضة للخرق الأمني عملاء لها – حيث بلغت النسبة أكثر من 20 بالمائة من قاعدة العملاء لدى 40 بالمائة من تلك المؤسسات.
- خسرت تسعة وعشرون بالمائة من المؤسسات نسبة من إيراداتها، فاقت 20 بالمائة من الإيرادات لدى 38 بالمائة من المؤسسات المعنية.
- واجهت ثلاثة وعشرون بالمائة من المؤسسات المعرّضة للخرق الأمني خسارة فرص الأعمال، وبنسبة تفوق 20 بالمائة لدى 42 بالمائة من تلك المؤسسات.

عمليات القرصنة ونماذج "الأعمال" الجديدة

شهد العام 2016 تحوّل القرصنة إلى عمل مؤسسي، من خلال التغيرات الديناميكية في المشهد التقني بقيادة التحول الرقمي، مما يعني إتاحة مزيد من الفرص للمجرمين الإلكترونيين. وفيما يستمر المهاجمون بالاستفادة من الأساليب التي أثبتت نجاحها، فإنهم في الوقت ذاته يوظفون مقاربات جديدة تعكس هيكلية "القيادة المتوسطة" لدى المؤسسات التي يستهدفونها.

- أساليب هجوم الجديدة تماثل الهرمية المؤسسية للشركات: استخدمت مجموعة من حملات الإعلانات الضارة وسطاء (أو بوابات) تقوم بدور المدير المتوسط وتخفي هوية النشاط الضار. وبهذا يمكن للمهاجمين التحرك بسرعة أكبر والحفاظ على اتساع مجال العمل وتجنّب اكتشافهم.
- الفرص والمخاطر المرتبطة بالبنية السحابية: تم تصنيف سبعة وعشرين بالمائة من التطبيقات السحابية من طرف ثالث، والتي يقدمها الموظفون بهدف إيجاد فرص جديدة للأعمال وتعزيز الكفاءة، على أنها ذات مستوى مرتفع من المخاطرة وتسبب مخاوف أمنية جمّة.
- البرمجيات الإعلانية بالنمط القديم، وهي البرمجيات التي تقوم بتنزيل الإعلانات دون تصريح من المستخدم، لا تزال تواصل نجاحها بعد أن أصابت 75 بالمائة من المؤسسات التي جرى استطلاعها.
- ظهر الجانب المضيء من خلال انخفاض استخدام أدوات الهجوم الكبرى، ومنها أنغلر ونيوكلير ونيوترينو، بعد أن تمت الإطاحة بمالكيها عام 2016، لكن أسماء أصغر سارعت لملء الثغرة الناشئة.

تأمين الأعمال و إستمرار اليقظة

يبين تقرير سيسكو السنوي للأمن الإلكتروني 2017 أن 56 بالمائة من التنبيهات الأمنية فقط يتم التحقق منها، مع معالجة أقل من نصف التنبيهات الصحيحة. وعلى الرغم من ثقة المدافعين بأدواتهم، إلا أنهم يواجهون تحديات التعقيد وطواقم العمل بشكل يسبب ثغرات في

بيان صحفي

الوقت والمجال المتاح للمهاجمين للاستفادة منها. وتنصح سيسكو بالخطوات التالية لتجنب التهديدات والكشف عنها والتخفيف من المخاطر والآثار:

- جعل الأمن من أولويات الأعمال: لا بد للقيادة التنفيذية تولي مسؤولية الأمن وتمويله ودعمه كأحد أولويات الأعمال.
- قياس الانضباط التشغيلي: من خلال مراجعة الممارسات الأمنية وترقيع أو إدارة الدخول إلى النقاط المؤدية لأنظمة الشبكات والتطبيقات والوظائف والبيانات.
- اختبار فعالية الأمن: وذلك بوضع مقاييس واضحة واستخدامها للتحقق من متانة الممارسات الأمنية والعمل على تحسينها.
- تبني مقاربة دفاعية متكاملة: اجعل التكامل والأتمتة من أهم معايير التقييم اللازمة لتحسين إمكانات الكشف وتسهيل تعدد الأنظمة وتوافقيتها وتقليل الوقت اللازم للكشف عن التهديدات وإيقافها. وبعد ذلك يصبح بإمكان الفرق الأمنية التركيز على التحقيق في التهديدات الفعلية وحلها.

تقرير سيسكو السنوي للأمن الإلكتروني - 10 سنوات من البيانات والبصائر

شهد الأمن الإلكتروني تغييرات جمة منذ انطلاق تقرير سيسكو السنوي الأول للأمن الإلكتروني عام 2007. وفيما استمر المهاجمون بالاستعانة بالتقنيات ليصبحوا أكثر تدميراً بينما ساهمت التقنية في دعم المدافعين وتطوير إمكاناتهم، فلا يزال إرساء الأسس الأمنية يتمتع بالأهمية ذاتها.

- ذكر تقرير سيسكو السنوي للأمن الإلكتروني عام 2007 بأن تطبيقات الويب والأعمال كانت من ضمن أهداف الهجمات، وغالبا ما يكون ذلك عبر الهندسة الاجتماعية أو خروقات تتم من خلال المستخدمين. وفي عام 2017 أصبح القراصنة يهاجمون التطبيقات السحابية وتصاعد حجم البريد الإلكتروني التطفلي.
- كانت هجمات البرمجيات الضارة في ارتفاع مستمر قبل عشر سنوات، لتستفيد منها أنشطة الجريمة المنظمة. أما في اقتصاد الظل المعاصر، فقد أصبح بإمكان اللصوص إدارة الجريمة الإلكترونية كعمل يوفر لهم خيارات الدخول إلى الشبكات دون معيقات صعبة لدى العملاء المحتملين. يمكن أن يكون المهاجمون اليوم أي شخص في أي مكان، فهم لا يحتاجون للخبرة الأمنية ويمكنهم بسهولة شراء أدوات جاهزة للهجوم.
- تتبع تقرير العام 2007 ما مجموعه 4773 تنبيه أمني من حلول Cisco IntelliShield، ليصل إلى مستوى مقارب للمشاهدات في قاعدة البيانات الوطنية لنقاط الضعف. أما في تقرير العام 2017 فقد ارتفع حجم تنبيهات نقاط الضعف خلال الفترة الزمنية ذاتها بواقع 33 بالمائة إلى 6380. ونعتقد بأن الزيادة ناجمة عن ارتفاع الوعي الأمني وازدياد المساحات المعرّضة للهجمات ونشاط المهاجمين.
- في عام 2007 نصحت سيسكو المدافعين بأن تكون لديهم مقاربة شمولية للأمن ودمج الأدوات والإجراءات والسياسات معاً وتثقيف الأطراف المعنية ليتمكنوا من حماية بيئاتهم. وكانت المؤسسات تتطلع إلى المزودين للحصول على الإجابات الشاملة، والتي غالباً ما كانت تضيع سدى بسبب تقديم الحلول الجزئية التي تفيد في نقاط محددة وحسب. أما في عام 2017 يواجه مدراء الأمن صعوبات بسبب تعقيد بيئاتهم، إلا أن سيسكو تواجه تلك المشكلة من خلال مقاربة هيكلية نحو الأمن، تساعد العملاء في جني المزيد عبر استثماراتها الأمنية القائمة وتعزز قدراتها، فيما تقلل مستوى التعقيد.

عن التقرير

يعمل تقرير سيسكو السنوي للأمن الإلكتروني، وهو الآن في عامه العاشر، على دراسة أحدث المعلومات الاستقصائية المتعلقة بالتهديدات، والتي قام بجمعها خبراء الأمن لدى سيسكو لتزويد القطاع بمعلومات وبصائر توضّح التوجهات الأمنية للعملاء. كما يسلّط تقرير العام 2017 الضوء على أبرز نتائج دراسة سيسكو السنوية الثالثة لقياس الاداء للقدرات الأمنية، والتي تدرس بدورها رؤية مسؤولي الأمن للوضع الأمني في مؤسساتهم. يستعرض التقرير التوجهات الجيوسياسية، والتطورات العالمية المتعلقة بمركزية وتوطن البيانات، وأهمية الأمن الإلكتروني كشأن يخصّ مجالس الإدارة.

بيان صحفي

للاطلاع على تقرير سيسكو السنوي للأمن الإلكتروني 2017 بالكامل، وقراءة المزيد عن توصيات سيسكو حول ما يمكن للمؤسسات القيام به لتخفيض المخاطر، يمكنكم النقر هنا.

مصادر إضافية:

فيديو سيسكو مع ديفيد أولفيتش، جون ن. ستيوارت: تقرير سيسكو السنوي للأمن الإلكتروني
تقرير سيسكو السنوي للأمن الإلكتروني
مدونة سيسكو: التفوق المستمر على التهديدات المتطورة – الإعلان عن تقرير سيسكو السنوي للأمن الإلكتروني 2017
إنفوغرافيك تقرير سيسكو السنوي للأمن الإلكتروني 2017
الرسوم البيانية لتقرير سيسكو السنوي للأمن الإلكتروني

حول سيسكو

سيسكو هي الرائد العالمي في مجال التكنولوجيا والتي تمكّن الإنترنت من العمل منذ عام 1984. الشركة مدرجة في بورصة الأوراق المالية "ناسداك" تحت الرمز (CSCO). يساعد موظفونا ومنتجاتنا وشركاؤنا المجتمع في التواصل الآمن واغتنام الفرص الرقمية المستقبلية اليوم. اكتشف المزيد عبر الرابط newsroom.cisco.com وتابعنا على تويتر @Cisco

سيسكو وشعار سيسكو هي علامات تجارية أو علامات تجارية مسجلة لمؤسسة سيسكو و/أو الشركات التابعة لها في الولايات المتحدة وبلاد أخرى. ويمكن الاطلاع على قائمة علامات سيسكو التجارية عبر الموقع www.cisco.com/go/trademarks. إن كافة العلامات التجارية الأخرى المذكورة في هذه الوثيقة هي ملك لأصحابها. إن استخدام كلمة الشريك لا يتضمن علاقة شراكة بين سيسكو وأي شركة أخرى.