بيان صحفي

تقرير سيسكو نصف السنوي للأمن الإلكتروني 2017 يتوقع هجمات جديدة "لتدمير الخدمة" بالتزامن مع نمو حجم وأثر التهديدات

حاجة القطاعات الرئيسية إلى تحسين الوضع الأمني في ظل التقارب بين تقنية المعلومات وتقنية العمليات

دبي، الإمارات العربية المتحدة، 24 يوليو 2017 - يكشف تقرير سيسكو® نصف السنوي للأمن الإلكتروني 2017 (MCR) عن التطور السريع للتهديدات والتزايد الملموس في نطاق الهجمات وأثرها، حيث يتوقع هجمات محتملة لتدمير الخدمة DeOS. يمكن لتلك الهجمات تقويض النسخ الاحتياطية وشبكات الأمان لدى المؤسسات، وهي العناصر اللازمة لاسترجاع النظم والبيانات في أعقاب التعرض للهجمات. كما أن انتشار إستخدام إنترنت الأشياء دفع العديد من القطاعات الرئيسية إلى جلب مزيد من عملياتها إلى شبكة الإنترنت، مما زاد من المساحات المتاحة للهجوم وعزّز قدرة المهاجمين على زيادة حجم وأثر تلك التهديدات.

فقد أظهرت الهجمات الأمنية الأخيرة مثل WannaCry و Nyetya مدى سرعة انتشار الهجمات وفداحة آثارها رغم أنها تبدو كهجمات الفدية التقليديه، إلا أنها أكثر تدميراً بكثير. وتمثل تلك الحوادث إنذاراً بما تسميه سيسكو بهجمات تدمير الخدمة، والتي بوسعها التسبب بأضرار أوسع نطاقاً لتترك الشركات عاجزة تماماً عن التعافي.

تواصل تقنيات إنترنت الأشياء توفير مزيد من الفرص الجديدة للمجرمين الإلكترونيين، وستلعب نقاط الضعف الأمني المتاحة للاستغلال من جانب المهاجمين دوراً محورياً في تمكين تلك الحملات وتصعيد أثرها. كما تشير الأنشطة الأخيرة التي قامت بها أنظمة الروبوتات عبر إنترنت الأشياء إلى أن بعض المهاجمين قد يكونون بصدد إرساء الأسس لإطلاق تهديدات إلكترونية بعيدة المدى والتأثيرات، قد تسبب تعطيلاً في شبكة الإنترنت ذاتها.

في تعليقه على هذا الجانب **قال ستيف مارتينو، نائب الرئيس والمدير الأول لأمن المعلومات لدى سيسكو:** كما تبين الهجمات الأخيرة مثل WannaCry و Netya، فإن خصومنا يصبحون أكثر إبداعاً وابتكاراً في كيفية تصميم هجماتهم مع مرور الوقت. وفيما تتخذ معظم المؤسسات خطوات لتحسين الأمن بعد التعرض لخرق أمني، فإن الشركات من مختلف القطاعات تعيش سباقاً مستمراً ضد المهاجمين، حيث يصبح الأمن فعالاً فقط بعد سد كافة الثغرات الواضحة وجعله أولوية للشركة."

يشار إلى أن قياس فعالية الممارسات الأمنية في وجه تلك الهجمات أمر بالغ الأهمية، وفي هذا الصدد، تعمل سيسكو على متابعة التقدم المحرز في تخفيض الوقت اللازم للكشف TTD – أي الفترة الزمنية بين التعرض للهجمة والكشف عن التهديد المترتب عليها. وتعدّ سرعة الكشف عن التهديدات عنصراً حيوياً في احتواء مساحة نشاط المهاجمين وتقليل الأضرار المترتبة على الاختراقات. تمكنت سيسكو منذ نوفمبر 2015 من تقليل متوسط الزمن اللازم للكشف عن الهجمات من 39 ساعة إلى حوالي 3 ساعات ونصف في الفترة بين نوفمبر 2016 و مايو 2017. ويرتكز هذا الرقم على بيانات القياس عن بعد، والتي تم الحصول عليها بطريقة إختيارية من مختلف منتجات سيسكو الأمنية المستخدمة حول العالم.

من جانبه قال **سكوت مانسون، مدير الأمن الإلكتروني لدى سيسكو في الشرق الأوسط وتركيا:** لا يزال التعقيد من العوامل التي تعيق الجهود الأمنية للعديد من المؤسسات. فمن الجليّ أن سنوات من الاستثمار في المنتجات المتخصصة التي لا يمكنها التكامل معاً يتيح فرصاً هائلة للمهاجمين الذين يستطيعون بسهولة التعرّف إلى نقاط الضعف والثغرات في الجهود الأمنية. ولتقليل الوقت اللازم للكشف عن التهديدات والحدّ من الآثار المترتبة عليها، ينبغي على القطاع الانتقال إلى مقاربة أكثر تكاملاً وهيكلية لتعزيز إمكانات الرؤية والإدارة وتمكين فرق الأمن من سدّ الثغرات."

مشهد التهديدات: أساليب رائجة وأخرى تراجعت

راقب الباحثون الأمنيون لدى سيسكو تطوّر البرمجيات الضارة خلال النصف الأول من العام 2017 وتعرّفوا إلى التغيرات الحاصلة في أسلوب المهاجمين في تنفيذ الهجمات والتشويش والمراوغة وتجنّب الكشف. كما لاحظت سيسكو بشكل خاص أن المهاجمين يطلبون من الضحايا بشكل متزايد تفعيل التهديدات عبر النقر على الروابط أو فتح الملفات، حيث أنهم يطورون برمجيات ضارة خالية من الملفات، تبقى في ذاكرة الجهاز ويكون من الأصعب الكشف عنها أو التحقق منها نظراً لأنها تُمسح عند إعادة تشغيل الجهاز. وأخيراً، يعتمد المهاجمون على بنية تحتية لا مركزية بلا هوية معروفة، ومنها خدمات Tor الوسيطة التي تمكنهم من السيطرة بشكل مخفي على الأوامر والأنشطة دون التعرف إلى هويتهم.

وفيما لاحظت سيسكو انخفاضاً حاداً في برمجيات استغلال الثغرات، تعود الهجمات التقليدية إلى الواجهة بشكل واضح:

- فقد ارتفع حجم البريد الإغراقي ارتفاعاً كبيراً فيما يتجه المهاجمون إلى الأساليب المجرّبة التي أثبتت نجاحها - كالبريد الإلكتروني – لنشر البرمجيات الضارة وتحقيق الإيرادات. ويتوقع باحثو التهديدات لدى سيسكو أن حجم رسائل البريد الإغراقي مع المرفقات الضارة سيواصل الارتفاع بينما تستمر أحوال برمجيات استغلال الثغرات في التغيير.
- تعتبر برمجيات التجسس وبرمجيات الإعلانات، والتي غالباً ما يتجاهلها العاملون في مجال الأمن على اعتبارها مصدر إزعاج أكثر منها مصدر تهديد، أشكالاً من البرمجيات الضارة التي تبقى لفترات طويلة وتسبب مخاطر للمؤسسات. وقد أجرت سيسكو أبحاثها على عينة من 300 شركة على مدى أربعة أشهر، لتجد أن ثلاث عائلات من برامج التجسس السائدة أصابت 20 بالمائة من العيّنة. أما في البيئة المؤسسية فيمكن لبرمجيات التجسس سرقة معلومات المستخدم والشركة وإضعاف الموقف الأمني للأجهزة بالإضافة إلى زيادة احتمالات التعرض للبرمجيات الضارة.
- كما أن التطورات التي تشهدها برمجيات طلب الفدية، ومنها نمو برمجيات الفدية كخدمة، تسهّل على المجرمين تنفيذ تلك الهجمات مهما كان مستوى مهاراتهم. ومن الجدير بالذكر أن برمجيات طلب الفدية تصدرت عناوين الأخبار وأدت إلى خسائر تفوق مليار دولار أمريكي عام 2016، إلا أن هذا الرقم قد يكون مضللاً لبعض المؤسسات التي ربما تواجه مخاطر أكبر لم يتم الإبلاغ عنها بعد. وفي الوقت ذاته تزدهر هجمة سرقة بريد الأعمال BEC، وهي هجمة تعتمد على الهندسة الاجتماعية تصمم فيها رسائل البريد الإلكتروني بشكل يغري المؤسسات لتحويل الأموال إلى المهاجمين، إذ أثمرت تلك الهجمات المربحة عن سرقة 5.3 مليار دولار في الفترة ما بين أكتوبر 2013 وديسمبر 2016، بحسب مركز شكاوى الجرائم الإلكترونية.

القطاعات المختلفة تواجه تحديات مشتركة

فيما يواصل المجرمون تعزيز مستويات تعقيد وتكثيف هجماتهم، تواجه الشركات في جميع القطاعات تحديات لمواكبة حتى المتطلبات الأساسية للأمن الإلكتروني. ففي الوقت الذي تتقارب فيه تقنية المعلومات وتقنية العمليات من خلال إنترنت الأشياء، تجد المؤسسات صعوبة جمة في إمكانات الرؤية وتقليل التعقيد. استطلعت سيسكو آراء ما يقارب 3000 خبير أمني في 13 دولة ضمن دراستها التي تحمل عنوان "دراسة قياس الاداء للقدرات الأمنية" لتجد أن فرق الأمن تجد صعوبة بالغة في مواجهة الحجم الهائل من الهجمات في مختلف القطاعات، مما أدى إلى أن تقتصر جهود الحماية لدى الكثير منها على رد الفعل وحسب.

- لا تحقق أكثر من ثُلثي المؤسسات في التنبيهات الأمنية، وفي بعض القطاعات، كالرعاية الصحية والنقل، يقترب الرقم إلى 50 بالمائة.
- وحتى في أكثر القطاعات استجابة (كالقطاع المالي والرعاية الصحية)، تعمل الشركات على تخفيف أثر أقل من 50 بالمائة من الهجمات التي يعرفون أنها صحيحة.
- تشكل إنتهاكات الأمن تنبيهاً حقيقياً ودعوة للاستيقاظ. ففي معظم القطاعات، يؤدي الخرق الأمني إلى تحسين طفيف على الأقل في 90 بالمائة من المؤسسات، بينما تشهد بعض القطاعات (كالنقل) مستوى أقل من الاستجابة يتجاوز 80 بالمائة بقليل.

ومن النتائج المهمة حسب القطاع:

- **القطاع العام** – من بين التهديدات التي خضعت للتحقيق، تم التعرف على 32 تهديداً فعلياً ولكن في النهاية تم تصويب 47 بالمائة فقط من تلك التهديدات الفعلية.
- **التجزئة** – قال اثنان وثلاثون بالمائة أنهم خسروا إيرادات بسبب الهجمات خلال العام الماضي، بينما خسر الرُبع عملاء او فرص أعمال.
- **التصنيع** – قال أربعون بالمائة من خبراء الأمن في قطاع التصنيع أنهم لا يمتلكون استراتيجية منهجية للأمن، ولا يتبعون ممارسات قياسية قائمة على سياسة لأمن المعلومات مثل ISO 27001 أو NIST 800-53 .

- **قطاع المرافق والخدمات** – قال خبراء الأمن أن الهجمات المركّزة (42 بالمائة) والتهديدات المتطورة المستمرة (40 بالمائة) كانت أكثر المخاطر الأمنية أثراً على مؤسساتهم.
- **الرعاية الصحية** – قالت سبعة وثلاثون بالمائة من مؤسسات الرعاية الصحية أن الهجمات المركزة شكلت خطراً أمنياً كبيراً على مؤسساتهم.

نصيحة سيسكو للمؤسسات

لمواجهة المهاجمين المعاصرين وإمكاناتهم المتطورة باستمرار، فإن على المؤسسات اتخاذ موقف استباقي في جهودها للحماية ضد التهديدات، وتقدم سيسكو للأمن النصائح التالية في هذا السياق:

- التحديث المستمر للبنية التحتية والتطبيقات بحيث لا يستطيع المهاجمون استغلال نقاط الضعف المعروفة للعموم.
- مواجهة التعقيد بالدفاعات المتكاملة، وتقليل الاستثمارات في النظم والأجهزة المنعزلة.
- إشراك القيادة التنفيذية في مرحلة مبكرة لضمان الفهم الكامل للمخاطر ومردود الحماية والقيود المرتبطة بالميزانية.
- وضع مقاييس واضحة واستخدامها للتحقق من جدوى الممارسات الأمنية وتحسينها.
- تعزيز فائدة التدريب الأمني للموظفين من خلال التدريبات المصممة وفقاً لدور كل منهم بدلاً من التدريب الموحد للجميع.
- موازنة الدفاع مع الاستجابة الفعالة، بحيث لا يتم إعداد الضوابط أو الإجراءات الأمنية دون استخدامها والرجوع إليها فعلياً.

من الجدير بالذكر أنه تمت دعوة مجموعة متنوعة من 10 شركاء لتقنيات الأمن من أجل تقرير سيسكو نصف السنوي للأمن الإلكتروني 2017، وذلك لمشاركة البيانات التي تستمد منها استنتاجات تتعلق بمشهد التهديدات. ومن بين الشركاء الذين ساهموا في التقرير أنومالي، فلاش بوينت، لوميتا، كواليز، رادوير، رابيد7، آر إس إيه، وساينت كوربوريشن، ثريت كونكت وتراب-اكس. وتعدّ منظومة سيسكو لشركاء تقنيات الأمن مكوّناً أساسياً لرؤية الشركة الرامية إلى توفير الأمن للعملاء بأسلوب يتسم بالبساطة والانفتاح والأتمتة.

عن التقرير

يدرس تقرير سيسكو نصف السنوي للأمن الإلكتروني 2017 أحدث البيانات الاستقصائية للتهديدات، والتي تم جمعها من خلال دراسة سيسكو لاستقصاء الأمن الجمعي. يوفر التقرير تصورات قائمة على البيانات ويستعرض توجهات الأمن الإلكتروني من النصف الأول من العام، إلى جانب التوصيات القابلة للتطبيق والرامية إلى تحسين الوضع الأمني. يقوم التقرير على بيانات تم الحصول عليها من نطاق ضخم، تصل إلى معدل يومي يفوق 40 مليار نقطة من القياسات عن بعد، حيث يقوم باحثو سيسكو بترجمة تلك البيانات الاستقصائية إلى جهود فعلية للحماية من خلال منتجاتنا وخدماتنا التي تتوفر على الفور لعملاء سيسكو حول العالم.

مصادر إضافية

مقطع فيديو عن الأمن من سيسكو مع ستيف مارتينو

تقرير سيسكو نصف السنوي للأمن الإلكتروني

مدونة سيسكو: تهديدات بأثر متصاعد: إعلان تقرير سيسكو نصف السنوي للأمن الإلكتروني 2017

رسومات تقرير سيسكو نصف السنوي للأمن الإلكتروني 2017

تابعو سيسكو على تويتر @CiscoSecurity

تابعوا سيسكو على فيسبوك

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

###