بيان صحفي

للاتصالات الإعلامية
شارون ديفان
أوك كونسلتينغ للعلاقات العامة ش.م.ح
هاتف:823 8444 50 971+
بريد إلكتروني: sharon@oakconsulting.biz

تقرير سيسكو الأمني نصف السنوي يكشف عن تعقيد متزايد للتهديدات الإلكترونية واستمرار الابتكار لتجنب الكشف واختراق الإجراءات الأمنية

التقرير يؤكد حاجة المؤسسات في الإمارات إلى الاستثمار في التقنيات المتكاملة لتقليل الزمن اللازم للكشف عن التهديدات ومعالجتها في غضون ساعات

دبي، الإمارات العربية المتحدة، 10 أغسطس 2015: كشف تقرير سيسكو الأمني نصف السنوي لعام 2015، والذي نشر اليوم ويهتم بتحليل توجهات استقصاء التهديدات والأمن الإلكتروني، عن حاجة المؤسسات الملحّة إلى تقليل وقت الكشف عن التهديدات لتتمكن من مواجهة الهجمات المعقدة والتهديدات الخطرة.

يغطي التقرير جانبين أساسيين:

i. **استقصاء التهديدات**

يقدم القسم لمحة عامة عن آخر الأبحاث التي أجرتها سيسكو عن التهديدات، ويناقش الجوانب التالية:

- استخدام المجرمين بشكل متزايد للنماذج التي تتضمن برمجيات "مايكروسوفت أوفيس"
- الأساليب الجديدة من مبتكري البرمجيات الضارة لتجنب الكشف
- خطر مواجهة البرمجيات الضارة في مجموعة محددة من القطاعات
- الوقت المستغرق للكشف عن التهديدات
- آخر الأخبار حول البريد الإغراقي وتنبيهات التهديد واستغلال ثغرات "جافا" والإعلانات الخبيثة.

ii. **التحليل والمشاهدات**

يركّز هذا القسم على اندماج القطاع الأمني والمفاهيم الناشئة للدفاع المتكامل ضد التهديدات. ومن المواضيع الأخرى التي يركز عليها، أهمية تعزيز الثقة والأمن في المنتجات، وقيمة دمج مؤسسات الخدمات الأمنية

بيان صحفي

للمجتمع في قطاع يندر فيه الأشخاص المؤهلون في المجال الأمني. يناقش التقرير دور الإطار الشامل للحوكمة الإلكترونية في استدامة الابتكار في الأعمال والنمو الاقتصادي على المستوى العالمي.

أبرز ملامح التقرير نصف السنوي للعام 2015:

لا زال الخصوم يعملون على تطوير ابتكارات جديدة تمكنهم من اختراق الشبكات دون اكتشافهم، وتجنب كافة الإجراءات الأمنية. ومن النتائج البارزة الأخرى التي خرجت بها الدراسة:

- ازدياد استغلال الثغرات ونقاط الضعف في برنامج Adobe Flash، فهي تظهر بشكل دوري في برمجيات الاختراق الشائعة مثل Angler و Nuclear، إذ لا زال الأول يتصدر حالات الاختراق ي القطاع من حيث المستوى الإجمالي لرضا المستخدمين والفعالية. تمثل برمجيات Angler أنواع التهديدات الشائعة التي تتحدى المؤسسات في الوقت الذي يخلق فيه الاقتصاد الرقمي وإنترنت الأشياء أهدافا جديدة للهجمات وفرصاً متعددة للمهاجمين لتحقيق المكاسب.
- يوظف مفكرو الجرائم، ومنهم مستخدمو برامج الفدية، فرقاً من محترفي التطوير الخبراء لمساعدتهم في زيادة أرباحهم.
- ينتقل المجرمون إلى الشبكات غير المعرفة من أمثال Tor و Invisible Internet Project ليتمكنوا من نقل اتصالات التحكم والقيادة إلى مكان لا يسمح بالكشف عنهم.
- عاد المهاجمون من جديد لاستخدام برمجيات مايكروسوفت أوفيس لنشر البرمجيات الخبيثة، وهو أسلوب قديم تخلى عنه الكثيرون قبل العودة إليه من جديد فيما يبحث الخصوم عن طرق جديدة للتفوق على أساليب الحماية الأمنية.
- يقوم بعض مبتكري برمجيات الاختراق بدمج نصوص من رواية جين أوستن *Sense and Sensibility* في صفحات الإنترنت التي تستضيف تلك البرمجيات، وفي تلك الحالة فإن برامج مكافحة الفيروسات والحلول الأمنية ستقوم على الأرجح بفهرسة تلك الصفحات على أنها مخصصة للقراءة ولا ضرر منها.
- يزيد مبتكرو البرمجيات الخبيثة من استعمالها لأساليب متنوعة، كأسلوب صندوق الرمل sandbox لإخفاء وجودهم على الشبكات.
- يزداد حجم البريد التطفلي في الولايات المتحدة الأمريكية والصين واتحاد دول روسيا ولكنه لا يزال مستقراً نسبياً في المناطق الأخرى خلال الأشهر الخمسة الأولى من العام 2015.
- يولي قطاع الأمن اهتماماً أكبر بالتقليل من الثغرات ونقاط الضعف في الحلول ذات المصدر المفتوح
- استمراراً لأحد التوجهات التي غطاها تقرير سيسكو السنوي الأمني للعام 2015، فإن استغلال ثغرات "جافا"

بيان صحفي

سجل انخفاضاً في النصف الأول من العام 2015.

دعوة للتصرف:

تتسارع وتيرة سباق الابتكار بين شركات الأمن والخصوم، مما يضع المستخدمين والمؤسسات في ظل مخاطر متزايدة. على الشركات أن تكون متيقظة عند تطوير الحلول الأمنية المتكاملة لمساعدة المؤسسات لتعمل بشكل استباقي ينسجم مع الأشخاص والإجراءات والتقنيات المناسبة.

- **الدفاع المتكامل ضد التهديدات** – تواجه المؤسسات تحديات بالغة لتطوير الحلول والمنتجات، فيما تحتاج إلى دراسة بنية متكاملة للدفاع ضد التهديدات لتكون أساس الأم في كل مكان ويمكن تطبيقها في أي نقطة من نقاط التحكم.
- خدمات لسد الثغرات – فيما يشهد قطاع الأمن مزيداً من التشتت والثغرات، في الوقت الذي تسود فيه التهديدات الديناميكية ومعضلة التكيف مع النقص المستمر في أصحاب الخبرة المؤهلين، فإن على الشركات الاستثمار في الحلول الأمنية المستدامة، والخدمات المهنية الفعالة والموثوقة.
- إطار شامل للحوكمة الإلكترونية – الحوكمة الإلكترونية الشاملة غير مهيأة للتعامل مع مشهد التهديدات الناشئة أو التحديات الجغرافية السياسية. فموضوع الحدود، وكيف يمكن للحكومات جمع البيانات عن المواطنين والمؤسسات ومشاركتها عبر مناطق الاختصاص القضائي، عقبة كبيرة تواجه تحقيق الحوكمة الإلكترونية الشاملة فيما يعتبر التعاون الدولي في المجال محدوداً. لا بد من وجود إطار حوكمة إلكترونية تعاوني متعدد الأطراف لتحقيق استدامة الابتكار في الأعمال والنمو الاقتصادي على المستوى العالمي.
- الشركات الموثوقة – على المؤسسات التعامل في تلبية متطلباتها مع شركات تقنية تتسم بالشفافية ويمكنها توفير الحلول التقنية الملائمة لمنتجاتها لتعتبر جديرة بالثقة. على تلك المؤسسات تطبيق المفهوم في جميع جوانب تطوير المنتجات بدءاً من سلسلة التوريد وطوال فترة حياة منتجاتها، وعليها أن تطلب من الشركات توفير الدعم وتعزيز الأمن بموجب عقود فيما بينها.

في تعقيبه على الأمر قال السيد ربيع دبوسي، مدير عام سيسكو الإمارات: "لا يمكن للمؤسسات في الإمارات الرضوخ للتسوية حتى وإن كانت تميل إلى التنازل اليوم. فعلى القطاع التقني تعزيز أدائه وتوفير منتجات وخدمات تتميز بالمرونة والاعتمادية، فيما يتعين على قطاع الأمن توفير إمكانات معززة ومبسطة في الوقت ذاته للكشف والوقاية والتعافي من الهجمات. هنا تتجلى ريادة سيسكو ودورها المتميز، فكثيراً ما نسمع أن استراتيجية الأعمال واستراتيجية الأمن تمثل اثنتين من أهم القضايا التي تهم عملاءنا، لأنهم يبحثون عن شراكات موثوقة معنا. فالثقة ترتب ارتباطاً وثيقاً بالأمن، والشفافية هي الأساس في تقديم التقنيات الرائدة في القطاع، إلا أنها تمثل نصف المعركة وحسب. أما نحن فملتزمون

بيان صحفي

تجاه الجانبين: الإمكانات الأمنية الرائدة في القطاع والحلول الموثوقة في كافة فئات المنتجات. كما تؤكد نتائج التقرير الحاجة إلى تطبيق الحلول المتكاملة في الشركات والعمل مع المزودين الجديرين بالثقة، والشراكة مع مزودي الخدمات الأمنية للتوجيه والتقييم. "

مصادر الدعم:

MSR Infographic

Cisco Security Blog

Cisco Security products and solutions

تويتر: @CiscoSecurity فيسبوك: http://facebook.com/ciscosecurity

نبذة عن شركة سيسكو:

تعمل شركة "سيسكو"، الرائدة عالمياً في مجال تقنية المعلومات والمدرجة في بورصة الأوراق المالية "ناسداك" تحت الرمز (NASDAQ: CSCO) ، على مساعدة الشركات في استغلال الفرص المستقبلية من خلال إثبات أن تحقيق الإنجازات المذهلة يكون عبر تمكين الاتصال الشبكي لما هو غير متصل. لمتابعة أخبار سيسكو، الرجاء زيارة. http://thenetwork.cisco.com

###