NEWS RELEASE

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

تقرير سيسكو السنوي للأمن يكشف عن تدني الثقة بالدفاع وارتفاع تأثير الهجمات الإلكترونية

المؤسسات تخطو خطوات واسعة لتحسين موقفها الأمني في وجه الهجمات التي تستغل ضعف البنية التحتية وتسرب البيانات عبر امتدادات المتصفح

دبي، الإمارات العربية المتحدة، 20 يناير 2016: أظهر تقرير سيسكو السنوي للأمن 2016، والذي صدر اليوم ليبرز أهم التوجهات في استقصاء التهديدات والأمن الإلكتروني، أن 45 بالمائة فقط من المؤسسات حول العالم تشعر بالثقة حيال موقفها الأمني، في الوقت الذي يشنّ فيه المهاجمون مزيداً من الحملات المتطورة والجريئة.

وفيما تراود الشكوك المسؤولين حول متانة الأمن في مؤسساتهم، يوافق 92 بالمائة منهم على أن المشرّعين والمستثمرين سيتوقعون أن تتمكن الشركات من إدارة مستوى تعرضها لمخاطر الأمن الإلكتروني. ويعمل أولئك القادة على تعزيز الإجراءات التي من شأنها تأمين مستقبل المؤسسة، وبخاصة في ظل التحول الرقمي في عملياتها.

يسلّط التقرير الضوء على التحديات التي تواجهها الشركات نظراً لتطور الهجمات بوتيرة سريعة، فهم يتعاملون باستمرار مع موارد قانونية لإطلاق حملات تمكنهم من تحقيق مزيد من المكاسب. كما أن الهجمات المباشرة من قبل المجرمين الإلكترونيين، والتي تعتمد على ادوات طلب الفدية وحسب، تحقق لهم مكاسب بواقع 34 مليون دولار سنوياً في الحملة الواحدة. ولا تزال تلك الأنشطة الإجرامية جارية دون أن توقفها الجهود التشريعية.

تواجه المؤسسات التحديات الأمنية التي تعيق قدرتها على كشف وتقليل الهجمات الإلكترونية العادية والاحترافية والتعافي منها، فيما تزيد المخاطرة في حال الشبكات القديمة والبنية التنظيمية والممارسات التي لم تعد تصلح لمواجهة التهديدات.

وبهذا فإن الدراسة تدق ناقوس الخطر لتدعو المؤسسات حول العالم لمزيد من التعاون والاستثمار في تعزيز الإجراءات والتقنيات والأفراد بهدف حماية أصولها من أولئك الخصوم.

أبرز نتائج البحث:

- **انخفاض مستوى الثقة وازدياد الشفافية:** فقد قالت أقل من نصف المؤسسات التي شملتها الدراسة بأنها تشعر بالثقة حول قدرتها على تحديد نطاق المخاطر في الشبكة ومعالجة الأضرار. ولكن الأغلبية العظمى من موظفي التمويل والمسؤولين عن الأعمال اليومية للمؤسسات يتفقون بأن المشرعين والمستثمرين يتوقعون من المؤسسات توفير مستوى أعلى من الشفافية حول مخاطر الأمن الإلكتروني المستقبلية. يشير ذلك إلى أن الأمن أصبح مشكلة ذات أهمية على مستوى مجالس الإدارة.
- **البنية التحتية القديمة:** انخفض عدد المؤسسات التي قالت بأن بنيتها التحتية حديثة تماماً بواقع 10 بالمائة بين عامي 2014 و2015 ووجدت الدراسة بأن 92 بالمائة من الأجهزة المتصلة بالإنترنت تعاني من نقاط ضعف معرفة، بينما لم تعد 31 بالمائة من الأجهزة التي شملتها الدراسة خاضعة لدعم البائع أو صيانته.
- **اعتبار المنشآت الصغيرة والمتوسطة الحلقة الأضعف:** فيما تدرس المزيد من المؤسسات سلسلة التوريد وشراكاتها مع الشركات الصغيرة، تجد بأن تلك المنشآت تستخدم أدوات وإجراءات أقل للدفاع ضد التهديدات. وعلى سبيل المثال، انخفض عدد المنشآت الصغيرة والمتوسطة التي تستخدم الأمن الشبكي بين عامي 2014 و2015 بواقع 1 بالمائة، مما يشير إلى وجود خطر محتمل يهدد المؤسسات التي تعمل معها بسبب ضعف في بنية الشراكة.
- **ازدياد تعهيد الأعمال:** ضمن توجهاتها الرامية لمواجهة نقص أعداد الأفراد الموهوبين، تدرك المؤسسات من مختلف الأحجام قيمة تعهد الخدمات لموازنة الجانب الأمن لديها. ويتضمن ذلك كلاً من الاستشارات والتدقيق الأمني والاستجابة للحوادث. وتقوم المنشآت الصغيرة والمتوسطة، والتي غالباً ما تفتقر إلى الموارد الكافية لتعزيز موقفها الأمني بشكل فعال، بتحسين منهجيتها الأمنية من خلال بعض الجهود التي تتضمن التعهيد – والذي ارتفعت نسبته إلى 23 بالمائة في العام 2015 مقارنة مع 14 بالمائة في العام السابق.
- **تغيير أنشطة الخوادم:** نقل المجرمون الإلكترونيون أهدافهم إلى الخوادم غير الآمنة، كتلك التي تستضيف WordPress مثلاً، ليستفيدوا من منصات التواصل الاجتماعي كسبيل لأغراضهم الخبيثة. ويذكر أن عدد نطاقات WordPress التي تعرضت للاستغلال من قبل المجرمين الإلكترونيين ارتفع بنسبة 221 بالمائة بين شهري فبراير وأكتوبر 2015.
- **تسرب البيانات عبر المتصفح:** على الرغم من أن فرق الأمن ترى في المتصفح مصدر التهديدات الأدنى، فإن الامتدادات الضارة للمتصفح كانت من أبرز مصادر تسرب البيانات بشكل كبير، حيث أثرت على أكثر من 85 مؤسسة. يشمل ذلك برمجيات الإعلان والإعلانات الضارة وحتى المواقع الإلكترونية العادية وإعلانات الوفيات، والتي أدت إلى اختراق المواقع التي لا تحدّث برمجياتها باستمرار.

- **البقعة العمياء في نظام اسماء النطاقات DNS:** وجد التقرير بأن حوالي 92 بالمائة من البرمجيات الضارة المعروفة استخدمت في نظام أسماء النطاقات في الأساس. فهو يعتبر بمثابة البقعة العمياء في المنظومة الأمنية، لأن فرق الأمن وخبراء النطاق عادة يعملون في مجموعات مختلفة في المؤسسات ولا يتفاعلون فيما بينهم بالقدر الكافي.
- **زمن الكشف أصبح أسرع:** يبلغ الزمن التقديري للكشف عن جريمة إلكترونية في القطاع حدوداً غير مقبولة تتراوح بين 100 إلى 200 يوم. عملت سيسكو على تقليل هذا الرقم من 46 إلى 17.5 ساعة منذ نشر تقرير سيسكو الأمني نصف السنوي عام 2015. واتضح أن تقليل فترة الكشف عن التهديدات ساهم في تقليل الأضرار الناجمة عن الهجمات الأمنية وتخفيض المخاطر والأثر المترتب على العملاء والبنية التحتية حول العالم.
- **أهمية الثقة:** فيما تعمل المؤسسات على تبني المزيد من استراتيجيات التحول الرقمي لعملياتها، فإن الحجم الإجمالي للبيانات والأجهزة والخدمات يساهم في إبراز الحاجة إلى الشفافية والثقة والمسؤولية تجاه العملاء.

للاطلاع على تقرير سيسكو السنوي للأمن 2016 بالكامل، وقراءة المزيد عن توصيات سيسكو حول ما يمكن للمؤسسات القيام به لتخفيض المخاطر، يمكنكم النقر هنا.

عن التقرير

يعمل تقرير سيسكو السنوي للأمن 2016 على تحليل أبرز التوجهات والمشاكل في الأمن الإلكتروني على أيدي خبراء الأمن لدى "سيسكو" في ما يتعلق بالتطورات التي يشهدها كل من قطاع الأمن والمجرمون الإلكترونيون آملين باختراق الدفاعات الأمنية. كما يسلّط التقرير الضوء على أهم النتائج التي توصلت إليها دراسة سيسكو السنوية الثانية للإمكانات الأمنية، والتي تركز على إدراك العاملين في مجال الأمن للوضع الأمني في مؤسساتهم. ويختتم التقرير بتحليل التوجهات الجغرافية السياسية وآراء حول مستوى فهم مخاطر الأمن الإلكتروني والثقة، ومبادئ الدفاع المتكامل ضد التهديدات.

في تعليقه على التقرير قال جون ن. ستيوارت، النائب الأول للرئيس ومدير الأمن والثقة لدى سيسكو: "يكمن الأمن في مرونة التصميم وتحقيق الخصوصية وشفافية الثقة. وفيما يتجلى إنترنت الأشياء والتحول الرقمي في كل مؤسسة، فلا بد من تعزيز القدرات التقنية وبنائها وتطبيقها في كل تلك العناصر، لنتجنب خلق مزيد من الديون التقنية. فعلينا بدلاً من ذلك مواجهة التحديات بحزم اليوم."

من جانبه قال رابح دبوسي، مدير عام سيسكو – الإمارات العربية المتحدة: "أصبحت الحاجة ملحة الآن أكثر من أي وقت مضى لتعزيز التعاون والتواصل والتنسيق – داخل المؤسسات وبينها على مستوى قطاع الأمن الإلكتروني – بحيث تتمكن المؤسسات من التصدي التهديدات الأمنية بكفاءة وفعالية. وعلى المؤسسات المختلفة في دولة الإمارات العربية المتحدة

الاستثمار في الكفاءات والإجراءات والتقنيات التي تساهم في تعزيز مرونتها وقدرتها على مواجهة الهجمات الجديدة وتدعم قدرتها التنافسية في العصر الرقمي الجديد".

الموارد الإضافية

Cisco Video with Chuck Robbins, John N. Stewart: 2016 Cisco Annual Security Report: Executive Perspectives
Cisco Annual Security Report
Cisco Blog: Forewarned is Forearmed: Announcing the 2016 Cisco Annual Security Report
تابعوا "سيسكو" عبر موقع تويتر على @CiscoSecurity
تابعوا صفحة سيسكو على فيسبوك

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

###