تقرير الأمن السيبراني السنوي لعام 2017: "سيسكو" تنجح في تقليص وقت إكتشاف التهديدات من 14 ساعة الى 6 ساعات

20% خسارة في عدد العملاء والإيرادات لأكثر من ثلث المنظمات التي شهدت إنتهاكًا في عام 2016

القاهرة- مارس 2017 :
أكدت شركة Cisco العالمية أن أكثر من ثلث المنظمات التي شهدت انتهاكًا في عام 2016 تعرضت لخسارة كبيرة في عدد العملاء والفرص والإيرادات بنسبة أكثر من 20 % نقلاً عن تقرير الأمن السيبراني السنوي لعام 2017 والصادر عن شركة سيسكو والذي تم على عينة من 3000 من كبار المسئولين عن امن المعلومات في مؤسسات 13 دولة.

وإستنادا إلى مؤشر قدرات الأمن، رصد التقرير نتائج تفيد بأن 90% من هذه المنظمات قاموا بتحسين التكنولوجيات وأدوات مكافحة التهديدات بعد الهجمات التى تعرضوا لها عن طريق فصل المهام الأمنية وتكنولوجيا المعلومات وبلغت نسبتهم (38 %)، وزيادة التدريب على الوعي الأمني للموظفين (38 %)، وتنفيذ تقنيات تخفيف المخاطر (37 %).

واليوم في العام العاشر للتقرير العالمي يبرز التحديات والفرص للفرق الأمنية للدفاع ضد التطور المستمر للجرائم السيبرانية وتغيير أشكال الهجوم، حيث يؤكد كبار المسئولين عن وحدات الأمن بوجود قيود الميزانية، وسوء التوافق بين الأنظمة بعضها البعض، وعدم توافر المواهب المُدربة كأكبر العوائق التي تحول دون النهوض بأوضاع الأمان الخاصة بهم، كما أيضاً يكشف أن أقسام القادة الأمنية عبارة عن بيئات معقدة مما يزيد من إحتمال وجود فجوات في سد الثغرات الأمنية.

وأظهر تقرير الأمن السيبراني أن المجرمين يعاودون الظهور بطرق تقليدية كلاسيكية مثل الإعلانات المضللة والبريد الإلكتروني غير المرغوب SPAM، خاصة من خلال البريد الإلكتروني غير المرغوب بطريقة لم نشهدها منذ عام 2010. وبلغت نسبته ما يقترب من ثلثي (65٪) البريد الإلكتروني وتراوحت نسبة الضرر فيه مابين 8-10%، ورصد التقرير أيضاً زيادة حجم البريد المزعج العالمي والذي ينتشر بسرعة عن طريق الشبكات الكبيرة والمزدهرة.

وتعليقا على هذا التقرير، أكد المهندس ياسر موسى الرئيس التنفيذي للتكنولوجيا بشركة سيسكو العالمية لمنطقة أفريقيا: "أن حجم المخاطر التى تتعرض لها المؤسسات والهيئات سواء الحكومية أو الخاصة تدفع الجميع إلى التفكير في حجم هذه التهديدات والتسلح بأدوات تقنية وأمنية تحاول صد أي هجوم لأنه قد يكون باباً خلفيا لتهديدات كبيرة مما يكبد الشركات والمؤسسات خسائر فادحة، مشيراً إلى أن شركة Cisco تتابع التقدم في تقليل "وقت الإكتشاف"، من خلال تقليل الوقت بين وقت الإختراق ووقت إكتشاف التهديد ".

وأضاف: "أن تسريع وقت الإكتشاف بات أمراً بالغ الأهمية، حيث قامت شركة Cisco بخفض وقت الإكتشاف من متوسط 14 ساعة في أوائل 2016 إلى ما يصل الى ست ساعات في النصف الأخيرمن عام 2016، ويعتمد هذا الرقم على إشتراك بيانات تتبع المستخدم التي تم تجميعها من المنتجات الأمنية لشركة Cisco المنتشرة في جميع أنحاء العالم "

كما أن زيادة المرور الرقمي يخلق مساحة أكبر للهجوم في ظل المؤشرات التى تؤكد على زيادة معدل نقل البيانات العالمي إلى ثلاثة أضعاف بحلول عام 2020، وأن66% من معدل نقل البيانات سيكون عبر الشبكات اللاسلكية "واي فاي" والأجهزة المحمولة.

التكلفة التجارية للتهديدات السيبرانية، خسارة العملاء والعائد

كشف تقرير الأمن السيبراني لعام 2017 عن الأثر المالي المحتمل من الهجمات على الشركات مع اختلاف أحجامها سواء كانت الكبيرة وصولاً إلى الشركات الصغيرة والمتوسطة، فإن أكثر من 50 % من المنظمات واجهت المراقبة العامة بعد الإنتهاك الأمني، لقد كانت العمليات والنظم المالية هي الأكثر تأثرًا، وتليها سمعة العلامة التجارية والمحافظة على العملاء، وبالنسبة للمنظمات التي شهدت الهجوم، كان التأثير الكبير.

تأمين الأعمال، والحفاظ على اليقظة

ذكر تقرير الأمن السيبراني لعام 2017 أن 56 % من تنبيهات الأمان يتم التحقيق فيها وأقل من نصف التنبيهات الشرعية يتم علاجها، في حين أن المدافعين يثقون في أدواتهم التى يعتمدون عليها، وتنصح شركة Cisco بإجراءات إحترازية لمنع وكشف والتخفيف من التهديدات وتقليل المخاطر.

- في عام 2007، ذكر تقرير الأمن السنوي أن تطبيقات الويب والأعمال كانت الأهداف، في كثير من الأحيان عن طريق الهندسة الإجتماعية، أو المخالفات التي تُفرض على المستخدم في عام 2017، أصبح القراصنة يهاجمون التطبيقات القائمة على السحابة، وتصاعد البريد المزعج.
- قبل عشر سنوات، كانت هجمات البرمجيات الضارة ترتفع، مع استفادة الجريمة المنظمة منها. وفي ظل إقتصاد اليوم، يقوم اللصوص الآن بتشغيل الجرائم الإلكترونية كأعمال تجارية، وتقديم حاجز منخفض لخيارات الدخول إلى العملاء المحتملين. كما يمكن أن يكون مرتكبي اليوم أي شخص، في أي مكان. حيث أنه لا يتطلب خلفية أمنية ويمكن بسهولة شراء مجموعات الفيروسات المعطلة للأمان الجاهزة.