

"فورس بوينت" تكشف عن التهديدات الأمنية المتوقعة خلال 2018



الثلاثاء 21 نوفمبر 2017 07:11 م

نشرت شركة "فورس بوينت" ForcePoint المتخصصة في مجال الحلول الأمنية الاللكترونية، اليوم تقريرها السنوي الخاص بالتوقعات الأمنية لعام 2018، الذي تطرق من خلاله خبراء الشركة إلى التهديدات التي سوف تواجه المؤسسات خلال الأشهر القادمة

بالإضافة إلى البيئات المتغيرة باستمرار التي تواجه خبراء الأمن السيبراني، قالت الشركة إن هناك موجة هائلة من الدوافع التي ستثير المزيد من النقاشات والحوارات حول مواضيع الخصوصية وسيؤدي هذا التوجه العام والضخم إلى تحولات بنوية وهيكلية على صعيد الخصوصية، كما أنه سينعكس بقوة على الطرق والسبل التي تتبعها المؤسسات في جمع إدارة البيانات

وترى شركة فورس بوينت أن صناعة الحلول الأمنية كانت تركز على جملة من الأمور الخاطئة، فالمناطق الأمنية التقليدية بدأت بالتآكل أو بالانهيار، وبالتالي ينبغي اتباع رؤى واستراتيجيات أمنية أفضل عوضاً عن التركيز على بناء جدران حماية أكبر "فقد باتت مسألة فهم كيفية وسبب تفاعل الناس مع البيانات الهامة، بغض النظر عن مكان حفظها، أمرًا بالغ الأهمية ولا تزال البيانات الهامة والحيوية تواصل هجرتها إلى السحابة، ومع استمرار تطور البرمجيات الخبيثة، وعلى الرغم من تنامي معدلات الاستثمار في التقنيات الدفاعية، إلا أن الضوابط الأمنية التقليدية برهنت على ضعفها وعدم فعاليتها".

وفي هذا السياق قال الدكتور ريتشارد فورد، كبير العلماء لدى شركة فورس بوينت: "إن فهم ومعرفة نقاط التقاء الأشخاص مع البيانات الهامة والملكيات الفكرية يقع في قلب سياسة التوقعات التي نتبعها وبوضع السلوك والممارسات والأهداف الاللكترونية في قلب عملية تصميم الحلول الأمنية، فإن هذه الصناعة ستحظى بفرصة التصدي للتحديات المفروضة، ومواكبة موجة التغيرات الهائلة التي تشهدها بيئة التهديدات".

وتابع فورد حديثه قائلاً: "نعلم أن الحلول المصممة ضد تسريب البيانات وبرمجيات الفدية الخبيثة ستستمر في التركيز على مفهوم العلاج والوقاية، لكن المخاطر التي تركز على السلوك تقف حاليًا وراء العديد من الحوادث الأمنية لذا، ينبغي ألا يقف سلوك الأشخاص بموقف معارض للممارسات الآمنة، فالمساران متوازيان ولا يستبعد أحدهما الآخر كما أن المستخدمين لديهم القدرة على تعريض أنظمتهم الخاصة للخطر، عن غير قصد، في دقيقة واحدة، وأن يشكلوا مصدرًا للابتكار في الدقيقة التي تليها، لكننا لا نستطيع تمكين المستخدمين إلا إذا ألعنا بشكل كامل بالطرق والسبل التي يتفاعلون بها مع بيانات الشركات الهامة".

وطرحت شركة فورس بوينت ثمانية توقعات لهذا العام، وفيما يلي لمحة عن هذه التوقعات:

عودة معارك الخصوصية مرة أخرى

تعتقد الشركة أن وجهة نظر المستخدمين للخصوصية تغيرت خلال السنوات الأخيرة، مع التلاشي المستمر للخط الفاصل بين البيانات "الشخصية" و"العامية". فهناك توتر وقلق بين الحقوق الفردية والحدود الأمنية من حيث الدوافع القانونية، والتقنية، والاجتماعية، والسياسية، التي تجتمع معًا لتشكل ما تطلق عليه شركة فورس بوينت مصطلح "حروب الخصوصية"، التي يقف بها خبراء التكنولوجيا ضد حرية الشخص العادي الذي يسير في الشارع، وتنقسم الآراء حول هذا الأمر ما بين الهيئات الحكومية، وبيئة العمل، والمنزل

وتتوقع الشركة أن يشهد عام 2018 احتدام النقاش بشأن المواضيع المرتبطة بالخصوصية، ولن ينحسر هذا الأمر ضمن الدوائر الحكومية فحسب، بل سيتخطاه لينتشر بين الأشخاص العاديين

تجميع البيانات: منجم من الذهب ينتظر من يستثمره

ذكرت فورس بوينت أنه على الرغم من أن عملية اختراق Equifax الشهيرة هزت قطاع الطول الأمنية، فالأثر الكامل لهذا الاختراق الكبير لم تظهر انعكاساته بعد، إذ ترى الشركة أن هذه العملية هي بداية موجة عاتية من الاختراقات التي تستهدف تطبيقات الشركات المستضافة التي تحتوي على معلومات حول معدلات المبيعات، والتوجهات المستقبلية، والعملاء، أو على تلك التي تدير حملات التسويق العالمية. هذا، وتسعى الجهات المهاجمة إلى اتباع الطرق الأقل مقاومة وحماية، فإذا ما تمكنوا من العثور على رابط نقطة ضعف أو ثغرة أمنية في النظام يحتوي ما يسعون وراءه من البيانات الشخصية، فسوف يستغلونها مباشرة. وتتوقع الشركة أن تُخترق مجموعات البيانات خلال عام 2018 باستخدام طرق هجومية معروفة.

صعود موجة عمليات قرصنة العملات الرقمية

بالتزامن مع تنامي أهمية العملات الرقمية، بما فيها استثمارها كوسيلة لتوليد الإيرادات من الجريمة الإلكترونية، تتوقع شركة فورس بوينت أن تتعرض الأنظمة المحيطة بهذه العملات للعديد من الهجمات بوتيرة متصاعدة. كما تتوقع رصد أعداد متزايدة من البرمجيات الخبيثة التي تستهدف بيانات وحسابات اعتماد المستخدم الخاصة بعمليات تبادل العملات الرقمية، حيث سيوجه مجرمو الإنترنت اهتمامهم نحو نقاط الضعف (الثغرات الأمنية) في الأنظمة التي تعتمد على التقنيات القائمة على تقنية البلوك تشين.

تطور وانتشار تقنيات الأشياء: الحدث الذي لا مفر منه

تعتقد فورس بوينت أن الاعتماد واسع النطاق على أجهزة إنترنت الأشياء ضمن بيئات المستهلكين والشركات على حد سواء، إلى جانب إمكانية الوصول إليها بكل سهولة وعدم خضوعها للرقابة في معظم الأحيان، لقد أدى إلى جعلها هدفًا سائغًا بالنسبة لمجرمي الإنترنت، الذين يسعون إلى أسرها للتفاوض عليها كفدية، أو لاستثمارها لصالحهم بشكل مستمر على المدى الطويل ضمن الشبكة.

ورغم إمكانية المساومة على احتجاز مثل هذه الأشياء المتصلة بالشبكة، إلا أنه من المستبعد، وفقًا للشركة، أن يحدث هذا الأمر خلال عام 2018. ومع ذلك، فإن التهديد الجديد الذي سيظهر خلال عام 2018 سيتمثل في صعود وانتشار هذه الأشياء. وبما أن تقنيات إنترنت الأشياء ستتيح إمكانية الوصول إلى كل من القدرات المتطورة والكميات الهائلة من البيانات الهامة، فإننا سنشهد العديد من الهجمات في هذا السياق، وقد نشهد أيضًا دمج هجمات الوسيط (MITM) مع ما سبق. وقد لا تخضع تقنيات إنترنت الأشياء للمساومة، إلا أنها ستصبح هدفًا للهجمات الكبيرة.