حماية شركتك من الاختراق

2019-01-26انسياد

ميكو نيميلا

غالباً ما نعتقد أن القراصنة أشخاص منعزلون اجتماعياً "نفترض أن العباقرة يجلسون في السرير ومعهم جهاز الكمبيوتر"، مثل نظرية دونالد ترامب خلف سرقة رسائل البريد الالكتروني للحزب الديمقراطي في 2016. يعلم خبراء الأمن السيبرالي مثلي شخصياً أنه في حين قد يتعذر على القراصنة الاندماج في الشركات (على الأقل ليس ظاهرياً)، إلا أنهم متعاونون لحد كبير. فمن دون القدرة على التفاعل مع بعض عبر الانترنت، ستقل الجرائم الالكترونية للقراصنة لحد كبير.

يتطلب تخطيط وتنفيذ عمليات الاختراق لعدة أشخاص، ويميل الجيل الجديد من المخترقين إلى عدم هدر الوقت. فعوضاً عن البدء من نقطة الصفر، يفضلون عملية تشبه إلى حد كبير التعهيد الجماعي. على سبيل المثال يخطف أحد القراصنة ذاكرة تخزين مؤقتة لكلمات المرور المشفرة من مخدم الشركة ويقوم بتحميلها إلى الشبكة المظلمة (web Dark)، ليتلقاها مخترق آخر يقوم بفك الشيفرات. يمكن بعد ذلك بيع كلمات المرور أو استخدامها لأغراض سيئة من أحد الطرفين أو كلاهما، او مخترق آخر تعرض لها.

من واقع خبرتي، فإن معدل اختراق الشركة الحالي- أي البيانات التي تم الكشف عنها من خلال المخترقين- يعتبر أفضل مؤشر على مدى وشدة احتمالية تعرض الشركة لنشاطات اجرامية سيبرالية على المدى القريب والمتوسط. لذا من الضروري أن تعلم الشركات إلى مدى مكشوفة. لكن ذلك ليس بالأمر السهل، فقد تظهر المواد على الشبكة المظلمة لعدة دقائق – وهي فترة كافية لزرع بذور التخريب التي قد تنبت في أي لحظة لاحقاً.

مؤشر الاختراق السيبرالي

أعمل منذ 2016 مع فريق من الباحثين لتطوير معيار عالمي للاختراق السيبرالي ينطبق على جميع المؤسسات. وقد أسفرت جهودنا حتى الآن على مؤشر CEI (مؤشر الاختراق السيبرالي)، والذي تم تحديثه في 2018. بناءً على نشاطات الشبكة المظلمة (web Dark) والشبكة العميقة (web Deep) وخروقات البيانات خلال الاثني عشرة شهراً الأخيرة، صنف مؤشر CEI اختراقات المؤسسات عبر مؤشرات أسواق الأسهم في 11 دولة: أستراليا وفنلندا وألمانيا وهونغ كونغ وإندونيسيا وإيطاليا وماليزيا وسنغافورة وجنوب إفريقيا والمملكة المتحدة والولايات المتحدة.

بحسب مؤشر CEI يشمل الاختراق الكشف عن معلومات هامة (على سبيل المثال الاتصالات الداخلية ومذكرات على مستوى عالي)، وبيانات اعتماد (مثل أسماء المستخدمين وكلمات المرور أو معلومات أخرى تخول الأشخاص غير المصرح لهم الوصول إلى أنظمة محظورة) واستهداف مجموعة القراصنة (بما في ذلك هجمات ايديولوجية منسقة معروفة بالمقاومة الالكترونية "hacktivists").

الشركات الصغيرة والمتوسطة يجب أن تبقى على حذر

قمنا خلال النسخة الأخيرة لمؤشر CEI، بتحسين المنهجية لتتناسب وحجم الشركة بالاستناد لعدد الموظفين. بما ينسجم مع حقيقة أن الشركات الأكبر حجماً تخترق بشكل أكبر حتماً وبالتالي تقييمها للمخاطر يكون أكثر دقة.

من خلال دراسة النتيجة من منظور حجم الشركة، وجدنا فجوة كبيرة يجب أن يتنبه لها كبار المسؤولين في الشركات الصغيرة والمتوسطة. ففي مختلف البلدان والقطاعات، تكون الشركات الأكبر أقل تعرضاً للاختراقات السيبرالية بالعموم، بالرغم من أن حجمها قد يجعلها هدفاً أكثر إغراءً للقراصنة.

في الواقع كان حجم الشركة هو نقطة الارتكاز هذا العام لمقياس CEI أكثر من القطاع للتنبؤ لاختراق الشركة نسبياً. ومن المفاجئ أن الاختلافات بين القطاعات تكاد لا تذكر، بالرغم من كونه سائداً أن قطاعات بعينها معرضة للاختراق أكثر من غيرها (الطاقة، والقطاع المصرفي على سبيل المثال).

تساعد طبيعة الهجمات السيبرالية كونها جماعية في تفسير هذه الظاهرة. فكون معظم القراصنة يلجأون إلى الشبكة المظلمة للحصول على المعلومات عوضاً عن الذهاب إلى المصدر، فإن الشركات الأصغر وغير المحصنة تستهدف بشكر متكرر لسبب بسيط، كون أنظمة الأمن السيبالي في الشركة أقل إحكاماً.

لكن يوجد أنباء جيدة للشركات الصغيرة والمتوسطة. نظراً لكون المجرمين السيبراليين يسعون خلف الربح السريع، فمجرد وضع قواعد أساسية وحماية قد يستثني الشركة من القائمة المستهدفة. على سبيل المثال، قد يكون من الوارد تفادي العديد من الهجمات الالكترونية المكلفة في حال تم حظر الموظفين عن استخدام البريد الالكتروني للشركة لإنشاء حسابات شخصية على الانترنت، ووسائل التواصل الاجتماعي وغيرها. فبالنسبة للمخترق فإن البريد الالكتروني للموظف قد يكون بمثابة بوابة للولوج إلى بيانات الشركة.

أصبحت حلول الأمن السيبراني الجاهزة أفضل من السابق. ووجود نظام حماية عادي قد يكون كفيلاً بردع القراصنة اللاهثين خلف صيد سهل.

اعلم لأي مدى انت مخترق

كيف يجب على القياديين النظر إلى مؤشر CEI؟ من جانبي، أرى من الأفضل التركيز على مدى تعرض شركتك للاختراق أكثر من التركيز على المنافسين. فأي شكل من أشكال الاختراق -حتى ولم يتسبب بضرر فوري- قد يسبب الضرر للشركة، كونه سيجذب قراصنة آخرين. فهو أشبه بوجود دم في الماء، وهو أمر كفيل بجذب أسماك القرش إليها.

رسالتنا إلى الشركات، والشركات الصغيرة والمتوسطة بشكل خاص، البدء بتطبيق إجراءات الأمن السيبراني وبرامج التوعية في أقرب وقت ممكن (في حال لم تبدأ بذلك). ولا تخشى ذلك فقد يكون ذل أقل تكلفة واستهلاكًا للوقت مما تعتقد.

وأبدأ بمراقبة وتتبع مدى تعرضك للاختراق. فهو الطريقة الوحيدة لرؤية شركتك من خلال عيون

القراصنة، وبالتالي الطريقة الأكثر دقة لقياس المخاطر والضعف.

* ميكو نيميلا، مدير والرئيس التنفيذي في "سايبر إنتليجنس هاوس" وكالة استخبارات إلكترونية مقرها سنغافورة. ومؤسس Silverskin ومؤلف كتاب a of Anatomy Cyberattack.

https://knowledge-arabia.insead.edu

.....

* الآراء الواردة لا تعبر بالضرورة عن رأي شبكة النبأ المعلوماتية