لماذا تهدف شركات العالم إلى توظيف قراصنة الإنترنت؟

سجل عام 2017 ارتفاعًا كبيرًا في عدد الهجمات الإلكترونية على مستوى العالم مقارنة مع السنوات السابقة، ورغم أن العام الماضي حدث عدد كبير من الاختراقات الإلكترونية والتي كانت على مستوى عالٍ من التطور، فإن عمليات الاختراق الحالية أكثر دقة ودمارًا وخطورة من السابق.

كما تمكن القراصنة من شن حملات هجومية متطورة للغاية وعلى نطاق واسع، حتى وصل عدد هذه الاختراقات إلى أكثر من 45 ألف اختراق في أكثر من 100 دولة حول العالم، ومن ضحاياها مواقع شركات النفط والطاقة والاتصالات والمصارف والمستشفيات، وغيرها من الحسابات الشخصية والأجهزة الحكومية.

وبناء على هذا التهديد الأمني، حاولت عدة دول إنشاء نظام متين يتصدى لهذه الضربات ويمنعها من استغلال بياناتها أو تسريبها وتعطيلها، ومن هذه الدول الولايات المتحدة الأمريكية والتي طالب فيها نائب وزير العدل رود روزنشتاين، بتوظيف قراصنة الإنترنت أصحاب القبعات البيضاء الأخلاقيين، والذين يعملون على مواجهة ومعالجة الأخطاء الأمنية في الحواسيب وحماية أنظمتها من قراصنة القبعات السوداء.

وأوضح وزير العدل روزنشتاين، أن "إيجاد نقاط الضعف في الأجهزة والبرامج سيساعدنا في القضاء على الثغرات الأمنية في أنظمتنا"، وأضاف "يجب على جميع الشركات أن تعيد النظر في سياسات الأمن الخاص بمعلوماتها وذلك من خلال دعوة القراصنة الأخلاقيين للعمل معنا".

كما أشار أن وزارة العدل أعدت بالفعل برنامجًا خاصًا بها لتجنب الانتهاكات الإلكترونية التي قد تهاجم أجهزتها، وهذا الأمر الذي تقوم به وزارة الدفاع والتي تخطت العديد من الأزمات من خلال هذه الإدارة الناجحة التي أدارها أصحاب القبعات البيضاء قبل أن يقوم الهاكرز بالتسلل إلى شبكتها.

ما المقلق من تعيين الهاكرز في الشركات؟

تزايدت القدرات الأمنية الإلكترونية في العالم، ومع ذلك نمت التهديدات الهجومية بشكل واضح، ولهذا قررت عدة شركات استغلال مهارات وخبرات الهاكرز الأخلاقيين في حماية ومعالجة أنظمتها.

وتنصح الشركات بالابتعاد عن قراصنة القبعات السوداء تمامًا وتحذر من توظيفهم أو التعامل معها، لأن أهدافهم الشخصية تطغي على مهمتهم في حماية نظام أو جهاز معين.

ولكن بنفس الوقت، تتخوف هذه الشركات من هكر القبعات الأولى وذلك لأن لديهم نفس قدرات فكر القبعات السوداء بما يتعلق بالاختراقات الأمنية والتي قد توصلهم إلى المعلومات التي يحتاجونها لأغراض أو مكاسب شخصية، خاصة أنهم من صمموا النظام أو البرنامج المعالج للثغرات والهجمات الإلكترونية.

مسألة الثقة في هذا المجال تكاد أن تكون معدومة، وخاصة أن هؤلاء الأشخاص يمكنهم الوصول إلى أكثر المعلومات سرية وحساسية مثل الاتفاقيات السرية والبيانات التفصيلية للدول والأشخاص، إضافة إلى قدرتهم على الوصول إلى الحسابات المصرفية والشخصية

كما يقول بعض الخبراء إنه من الأفضل الاستفادة من معرفة هؤلاء القراصنة دون توظيفهم في مناصب تمكنهم من التلاعب بأمن معلومات الشركة، وبهذا تكون الشركات تعلمت كيف يعمل "الأشرار" دون أن تعمل معهم بشكل مباشر، ودون أن يعملوا ضدهم وضد أمنها.

ومن الواضح أن مسألة الثقة في هذا المجال تكاد أن تكون معدومة، وخاصة أن هؤلاء الأشخاص يمكنهم الوصول إلى أكثر المعلومات سرية وحساسية مثل الاتفاقيات السرية والبيانات التفصيلية للدول والأشخاص، إضافة إلى قدرتهم على الوصول إلى الحسابات المصرفية والشخصية.

من جهة أخرى، يقول نائب رئيس المجلس الإداري للتجارة الإلكترونية سين ليم: "القرصنة الأخلاقية واحدة من أسرع المجالات نموًا في العالم، ويرجع ذلك إلى أن الدول ومؤسساتها أدركت حاجاتها لهؤلاء الأشخاص.

كما يشير ليم أن هناك العديد من الأفكار القبيحة التي تلاحق القراصنة ولا يمكن إنكار تخوف الكثيرين عند توظيفهم داخل شركاتهم، ولكن في نفس الوقت، لا يمكن التخلي عن مهاراتهم وخاصة عندما

نفكر أن للقراصنة دوافع وأهداف مختلفة، ويوضح أن الدافع الأول والعام هو "الحاجة إلى المال" وهذا ما تستطيع الشركات توفيره لهم قدر المستطاع.

من أشهر الشركات التي عينت قراصنة أخلاقيين هي جوجل، والتي وظفتهم للكشف عن المشاكل الأمنية في شبكة الإنترنت، وغيرها مثل آبل ومايكروسوفت

ومن جانب آخر، يتابع ليم قائلا: "لا تتلخص جميع الشركات من مخاوفها من القراصنة، وفي بعض الأحوال تحصر مهامهم على تقديم المشورة والنصيحة وتحديد الثغرات والمشاكل الأمنية وعيوبها"، وهذا دون أن يستطيعوا الوصول إلى المعلومات والبيانات الحساسة أو الشخصية.

وفي نفس السياق، قال مسؤولون إن البرامج التدريبية أو التجريبية يمكن أن تكشف الكثير عن أهداف القراصنة ومهاراتهم في نفس الوقت، إذ تكون هذه الفترة لامتحان دوافعهم وقدراتهم دون أن يكونوا على علم بالمعلومات التي لا قد تهدد أمن الشركة ومستقبلها، كما اقترح هذا الفريق تأسيس برنامج مكافأة إضافة إلى الراتب الثابت لتقديم الدعم المادي الكامل وكسب انتمائهم للشركة التي يعملوا بها.

ومن أشهر الشركات التي عينت قراصنة أخلاقيين هي جوجل، والتي وظفتهم للكشف عن المشاكل الأمنية في شبكة الإنترنت، وغيرها مثل آبل ومايكروسوفت.

أجور عالية لقراصنة القبعات البيضاء

يقول نائب الرئيس وكبير الموظفين الفنيين لعمليات الأمن في أوروبا والشرق الأوسط راج ساماني: "عادة ما يكون الدافع الأساسي وراء الجرائم الإلكترونية هو المال"، واعتمادًا على هذه الحقيقة والسمعة الشائعة عنهم فإن الشركات تقدم أجور عالية لهم لضمانهم في صفها.

تدفع بعض الشركات رواتب عالية أو مكافآت كبيرة إلى حد ما لهؤلاء الهكر، على سبيل المثال، تدفع شركة مايكروسوفت نحو 15 ألف دولار لمن يكتشف أي خلل إلكتروني في أنظمتها، و100 ألف دولار عند العثور على تقنيات أو وسائل غير معروفة، والتي تتطلب أحيانًا من المطورين والمبرمجين إعادة النظر في بنية النظام نفسه، كما ظهرت شركات متخصصة في تقديم خدمات القراصنة الأخلاقيين لحل

مشاكلهم الأمنية.

هناك نوعان من الشركات، النوع الأول مخترق، والثاني مخترق ولا يدري

ومع ارتفاع عمليات الجرائم الإلكترونية في السنوات الأخيرة، انتشرت مقولة تفيد بأن "هناك نوعان من الشركات، النوع الأول مخترق، والثاني مخترق ولا يدري"، وهذه إشارة إلى قوة الهجمات الإلكترونية التي تقوم باصطياد البيانات المهمة لدوافع ابتزازية.

وتبعًا لمصادر معهد بونيمون، فإن متوسط الخسائر السنوية للشركات من الهجمات الإلكترونية في العالم تجاوز 7.7 مليون دولار لكل مؤسسة، إذ أنفقت المؤسسات في جميع أنحاء العالم 73.7 مليار دولار في العام الماضي على الأمن المعلوماتي الإلكتروني وذلك وفقًا لما صرحته منظمة البيانات العالمية.