قرصنة المواقع السعودية تكشف عيوب الأمن السيبراني في الشرق الأوسط

بلومبرج - التقرير

بعد أكثر من عام من غرق الطفل السوري الذي جرفت الأمواج جثته إلى الشاطئ في تركيا، والذي تسببت صورته بصدمة للعالم، ظهرت صورته مرة أخرى على شاشات الكمبيوتر في جميع أنحاء السعودية، هذه المرة كمقدمة لهجمة إلكترونية.

وأدت الهجمة التي نفذت الشهر الماضي إلى تعطيل الآلاف من أجهزة الكمبيوتر في عدة وزارات سعودية، في استخدام نادر للأسلحة السيبرانية، التي تهدف لتدمير أجهزة الكمبيوتر وحذف البيانات. واستخدم المهاجمون، الذين لم يعلنوا مسؤوليتهم حتى الآن، نفس البرمجيات الضارة التي استخدمت في هجوم العام 2012 ضد شركة أرامكو السعودية للنفط، والمعروفة بأرامكو السعودية، والتي أدت إلى تدمير 35 ألف جهاز كمبيوتر خلال ساعات.

ويعتبر الشرق الأوسط، وهو موطن لما يقرب من نصف احتياطيات العالم من النفط والكثير من غازه الطبيعي، عامل جذب لبعض أعلى الهجمات الإلكترونية في العالم، كما يقول تقرير برايس ووتر هاوس كوبرز في مارس 2016، ومن المتوقع أن يزداد التهديد في ظل زيادة النشاط الإلكتروني في خصم الصراعات والتوترات الجيوسياسية في المنطقة.

ويقول جيمس لويس، نائب رئيس مركز الدراسات الاستراتيجية والعالمية في واشنطن: "خلال العامين الماضيين، كانت وزارة الدفاع الأمريكية تحاول جعل دول الخليج تزيد من تشديد دفاعاتها، وافق بعضهم، لكن السعودية لم تفعل".

الضرر غير واضح

حجم الضرر ليس واضحاً، على الرغم من أن شخصين قد تحدثا عن خرق للأمن قالوا إنه استهدف البنك المركزي السعودي ووزارة النقل، والوكالة التي تدير مطارات البلاد، النقطة المضيئة هي أن السعوديين كانوا قادرين على استعادة بعض البيانات المفقودة من خلال أنظمة الدعم، واستعادوها بشكل أسرع من هجمة عام 2012، على حد قول أحد الأشخاص القريبين.

قد أنكر البنك المركزي، المعروف باسم مؤسسة النقد العربي السعودي، تعرض أنظمتها للاختراق، وقالت الهيئة العامة للطيران المدني، إن الضرر الذي لحق بشبكاتها كان محدودًا فقط في بعض أنظمة المكاتب ورسائل البريد الإلكتروني الخاصة بالموظفين.

وفي حين كان الهجوم مشابهًا للهجوم الذي استهدف "أرامكو" قبل 4 سنوات، إلا أن أثره كان "أقل كثيرًا" ولم يتسبب في تعطيل النقل أو خدمات الطيران، كما يقول عباد العباد، المدير التنفيذي للتنمية الاستراتيجية والتواصل بالمركز القومي للأمن السيبراني.

السوق الإلكتروني

وقال وائل فتوح، المتخصص في ضمان مخاطر التكنولوجيا "سيكون لدينا دائما سباق بين أولئك الذين يستغلون نقاط ضعف الأمن ومن يتصدون لهم".

وتهدد الهجمات الإلكترونية في الشرق الأوسط ما هو أكثر من الحكومات والمنشآت العامة، فهي تعرض التنمية الاقتصادية للخطر.. فالسوق الإلكتروني الإقليمي الموحد قد يتسع ليشمل 160 مليون مستخدم بحلول عام 2025، ويضيف 95 مليار دولار لإجمالي الناتج المحلي، وفقا لشركة ماكينزي للاستشارات، والسعودية والإمارات العربية المتحدة وبعض الدول العربية الأخرى في مقدمة هذا النمو.

وقال موهيت شريفاستافا، المحلل المتخصص في الأمن: "إن التبني السريع للتحويل الرقمي في الإمارات العربية المتحدة ودول مجلس التعاون الخليجي جعل من المنطقة هدفا جذابا لمجموعة واسعة من الاختراقات الأمنية".

وقبل 6 سنوات، كشفت شركة "فاير آي" هجمات إلكترونية إجرامية على بنوك الشرق الأوسط شنت من خلال مرفقات رسائل البريد الإلكتروني.

ستوكسنت.. وفليم

وقال مسؤولون أمريكيون، إن إيران كانت وراء هجمة 2012 ضد أرامكو السعودية، كما اشتبه المحققون أيضا في اشتراك قرavanaugh إيرانيين في هجمة نوفمبر على الهيئات الحكومية السعودية، ولم يكن المسؤولون الإعلاميون الإيرانيون متاحين للرد.

كما كانت إيران أيضا ضحية للتخريب السيبراني، فقد تسبب فيروس يسمى "ستوكسنت" في خروج منشآت تخصيب اليورانيوم الرئيسية في البلاد عن العمل في العام 2012، كما تسبب فيروس "فليم" في شل صناعة الطاقة الإيرانية بعد عامين، مشيرة إلى أن إسرائيل متورطة في كلا الحادئين.

ويشير هجوم الشهر الماضي على السعودية إلى أن الاستثمار وحده لا يضمن الحماية، فشركات الشرق الأوسط من بين أعلى 10 شركات في العالم من حيث شراء تقنيات الأمن السيبراني ولكنها في آخر 50 شركة في التعليم والتدريب، وفقا لتقرير "بي دابليو سي"، والذي أجرى استقصاء لـ 10 آلاف شركة، 300 منهم في

الشرق الأوسط.

وأكد محمد الزعروني، القائم بأعمال المدير العام للمعلومات والحكومية الإلكترونية بهيئة تنظيم الاتصالات، في مؤتمر عقد في أبوظبي الشهر الماضي، أن الأمر يحتاج أكثر من مجرد تخصيص موارد مالية لحماية أنفسنا من التهديدات السيبرانية الحالية، وأن بناء القدرات البشرية بنفس القدر من الأهمية. وقال جينس مونراد، المحلل الاستخباراتي الكبير بشركة "فاير آي"، إنه يرى مؤشرات إيجابية بخصوص الأمن السيبراني في الشرق الأوسط، بما في ذلك الوعي بالأمر والدعم الحكومي الأقوى. وقال: "لكن هذا تحديا معقدا.. من المهم للمؤسسات إدراك أن تحدياتهم المتعلقة بالأمن السيبراني لا يمكن حلها بالتكنولوجيا وحدها".