مركز سمت للدراسات
SMT Studies Center

بعد الاختراق الروسي..
حلول لمواجهة الاختراق الإلكتروني

الأحد, 18 نوفمبر 2018

قراءة خاصة 154

مع التقدم التكنولوجي وسيطرة الآلة على معطيات القرن الـ٢١، ظهر مصطلح "الاختراق الإلكتروني". ويُعرف الاختراق في العالم التقني بأنه "قدرة الوصول إلى هدف تكنولوجي بطريقة غير مشروعة، عن طريق ثغرات في نظام الحماية الخاص بالهدف"؛ إذ يعمل من خلالها المخترق على التجسس، ومن ثَمَّ سرقة المعلومات ونشرها للعامة، ومن الممكن أن يعمد المخترِق إلى تعطيل النظام.

ولعل اللافت في الأمر، هو ازدياد تلك الهجمات الإلكترونية في الفترة الأخيرة، وهو ما نستدل عليه مما أكدته شركة (كاسبرسكي لاب) الروسية في تقريرها، إذ أكدت أنها استطاعت خلال الربع الثالث من عام ٢٠١٦، صدَّ أكثر من مليون هجمة مالية خبيثة على المستخدمين، مشيرة إلى أن نسبة الهجمات ازدادت في الربع الأخير من عام ٢٠١٦ بنسبة ١٥.٦ ٪؛ إذا ما تمت مقارنتها بالربع الثالث من العام ذاته، وما كشفته شركة " آي بي إم" أن متوسط الخسائر التي تتكبدها الشركة جراء عملية الاختراق الحالية ارتفع بنسبة ٦.٩ ٪ (١).

> الاختراقات الإلكترونية ليست وليدة اللحظة.. فكثير من الوقائع التاريخية شاهدة على تطبيق البعض لذلك المصطلح.

حوادث تاريخية

الاختراقات الإلكترونية ليست وليدة اللحظة.. فكثير من الوقائع التاريخية شاهدة على تطبيق البعض لذلك المصطلح. ومع كثرة المستخدمين لشبكة الإنترنت، صارت مسألة الحصول على بيانات هؤلاء المستخدمين تمثل فرصةً كبيرةً للمخترقين .

- في عام ٢٠١٠ تمَّ إطلاق "فيروس ستكسنت" داخل محطات الطاقة النووية في إيران, وفي لحظات أصبح من الصعب التحكم في أنظمة التحكم داخل المفاعل. إذ قام هذا البرنامج بالسيطرة على أكثر من ٥٠٠٠ جهاز طرد مركزي, من أصل ٨٨٠٠ جهاز داخل المفاعل، وهو ما أدى إلى تدمير الآلاف من عينات اليورانيوم سرًا.(٢)
- في عام ٢٠١٢ تعرضت الشبكة الاجتماعية المهنية الأكبر على شبكة الإنترنت "لينكد إن" لاختراق كبير، وتمَّ الكشف عن ٦.٥ مليون حساب بشكل مؤكد بناءً على إشعارات تعيين كلمات المرور من جديد.

• في عام ٢٠١٣ تمَّ الكشف عن اختراق ٥٠٠ مليون حساب في شبكة "ياهو" ليزيد الوضع سوءًا، ويدق المسمار الأخير في جدرانها التي بدأت بالتهاوي، إلا أنه في أكتوبر ٢٠١٧ كانت المفاجأة بتعرض ثلاثة مليارات حساب للاختراق وليس ٥٠٠ مليون فقط.(٣)

• في ٢٠١٦ نشر أحد القراصنة الأميركيين أرقام هواتف وعناوين البريد الإلكتروني لـ٢٠٠ عضو ديمقراطي سابقين وحاليين في الكونغرس .(٤)

اختراقات روسية

يبدو أنه وسط الحرب التكنولوجية الدائرة بين دول العالم الكبرى والمتعلقة بتوسيع النفوذ في العالم، وتصارع الولايات المتحدة الأميركية وروسيا على تصدر الهيمنة والظهور بمظهر القائد الأول لدول العالم، انتهجت الاستخبارات الروسية طرقًا إلكترونية عدة لمراقبة ما يحدث في دول أوروبا والولايات المتحدة الأميركية، ما جعلها تدخل قفص الاتهام في عدة دول غربية بشن عمليات قرصنة إلكترونية، ووصل الأمر لذروته عندما أعلنت وزارة العدل الأميركية عن توجيه اتهامات لـ٧ أشخاص قالت إنهم أفراد من الاستخبارات العسكرية الروسية بالتورط في شن عمليات اختراق إلكتروني في إطار مؤامرة تخريبية شملت مختلف أنحاء العالم(٥).

الاختراقات الروسية، فتحت النار عليها وأعادت للأذهان ملفات هامة رُجح أن موسكو كان لها يد بها، ومن أهم تلك الملفات: ما يتعلق بالاختراق الإلكتروني المنسوب لروسيا في عام ٢٠١٦ بتهمة التدخل لدعم التصويت لخروج بريطانيا من الاتحاد الأوروبي. ويتمثل الآخر في الاتهامات بالتلاعب بنتائج الانتخابات الرئاسية الأميركية في ٢٠١٦ عن طريق الاختراق الإلكتروني للعملية الانتخابية.

جهات دولية أخرى عانت – أيضًا - من الاختراقات الروسية، إذ قالت وكالة المخابرات السويسرية إن أنشطة التجسس الروسي تتزايد في البلاد، وذلك بعد ضبط عملاء روس يشتبه بأنهم حاولوا اختراق مواقع في سويسرا. وكذلك قالت وزيرة الدفاع الفرنسية "فلورنس بارلي" في ٧ سبتمبر الماضي إن روسيا حاولت اعتراض الاتصالات التي يبثها قمر فرنسي إيطالي مشترك يستخدمه جيشا البلدين لتأمين الاتصالات(٦).

> مع كثرة المستخدمين لشبكة الإنترنت، صارت مسألة الحصول على بيانات هؤلاء المستخدمين تمثل فرصةً كبيرةً للمخترقين

حلول لمواجهة الاختراق الإلكتروني

من المؤشرات السابقة يبدو أن الاختراق الإلكتروني قد أصبح آفة العصر وأداة طيعة في يد جهات عدة للوقوف في وجه منافسيه وهو ما فعلته روسيا أخيرًا. لذا، فإنه يجب البحث عن حلول عدة لمواجهته أو محاولة تقليل أخطاره المحتملة في الفترة القادمة .

- يجب على المؤسسات الكبرى العمل على اعتماد شبكة داخلية، وربط أجهزة محددة منها بالشبكة، شريطة ألا تحتوي على أي معلومات هامة "كأرقام سرية لحسابات ونحو ذلك".
- أمن تكنولوجيا المعلومات لا يتركز فقط في مدى فاعلية الحل الأمني بحد ذاته، بل يتعلق - أيضًا - بمستوى وعي وذكاء المستخدم في مجال التعامل مع الفضاء الإلكتروني. لذا، فإن الحلول الأمنية وحدها تكون غير مجدية في هذا الصدد ويجب تطوير الحلول التكنولوجية.
- العمل على تطوير قطاعات التكنولوجيا داخل أجهزة المخابرات لجميع الدول لرفع درجات الحساسية تجاه الاختراقات .
- من المهم – أيضًا - عدم وضع أي معلومات هامة في ذاكرة الجهاز، والاتجاه إلى تخزين المعلومات المهمة في ذاكرة خارجية.
- عدم نشر المعلومات الخاصة للجميع، فقد تستخدم هذه المعلومات لانتحال الشخصية.
- تغيير كلمة السر بصورة مستمرة، مع أهمية عدم اعتماد كلمات السر المشهورة، كتاريخ الميلاد لتسلسل في الأرقام، أو الأحرف.

• عدم الدخول إلى المواقع غير المعروفة التي يتم استخدام عبارات جاذبة لدخولها، مع أهمية عدم تحميل أي برامج أو مواد منها.

• عدم إرسال الهوية الخاصة، أو جواز السفر، أو أي معلومات خاصة إلى المواقع، إلا ذات الاعتماد الرسمي منها .(٧)

• استخدام أحدث النسخ من برامج الحماية من الفيروسات, واستعمالها بشكل دوري.

• استخدام كلمات سر قوية, مكونة من حروف, وأرقام, ولا تحتوي اسمك, أو تاريخ ميلادك، بالإضافة إلى استخدام كلمة سر مختلفة لكل حساب من حساباتك على شبكة الإنترنت.

إضافة إلى فكرة هامة تعتمد على ما يسمى بـ"جغرافيا الأرض" أثارها الباحث السعودي، الدكتور زياد السلوم، وهي تتعامل مع منتج يتيح للمستخدم الحصول على كلمة مرور، تعتمد على جغرافيا الأرض، ضاربًا في ذلك مثلاً بأن يكون منزلك أو موقع عملك أو أي مكان آخر، حتى لو كان معلمًا سياحيًا، كلمتك الخاصة للوصول لحساباتك، مبينًا أن لكل مكان رمزًا خاصًا به يحصل عليه الشخص عند التسجيل بالخدمة .(٨)

بعد الحديث السابق، نتوقع أن تحتل التكنولوجيا جانبًا هامًا من صراعات الأيام القادمة بين دول العالم، وخاصة بعد الاختراقات الروسية للعديد من الدول، واستخدام روسيا للأداة التكنولوجية لإكسابها ميزة تنافسية .

> الاختراق الإلكتروني أصبح آفة العصر وأداة طيعة في يد جهات عدة للوقوف في وجه منافسيه وهو ما فعلته روسيا أخيرًا

المراجع

١ - اي بي إم: متوسط خسائر الشركة من حوادث الاختراق في المنطقة يبلغ ٤.٩٤ مليون دولار،البوابة العربية للأخبار التقنية
https://bit.ly/2RPh4rY

٢ - أعظم عمليات الاختراق والقرصنة الإلكترونية حتى الآن، عرب فيد.
https://bit.ly/2z0mklE

٣ - أكبر حوادث الاختراق حجمًا وتأثيرًا في الألفية الجديدة على الإطلاق، أراجيك.
https://bit.ly/2RI4Dhm

٤ - أشهر ١٠ عمليات قرصنة حول العالم في السنوات الأخيرة، رصيف ٢٢.
https://bit.ly/2KdoVuY

٥-موسكو في قفص الاتهام.. هل تقف روسيا وراء الهجمات الإلكترونية على الغرب؟ صوت الأمة. https://bit.ly/2y3SXOu

٦ - التجسس.. أداة روسية لاختراق الدول الأوروبية، الحرة .
https://arbne.ws/2RJP3BZ

٧- المرجع السابق.

٨ - وداعًا للهكر.. تقنية جديدة تمنع الاختراقات الإلكترونية، الأسواق العربية.
https://bit.ly/2T78whA

خدمات مركز سمت