الخليج

اقتصاد, تقنية وسيارات

10 أغسطس 2021 17:27 مساء

ارتفاع متوسط تكلفة اختراق البيانات إلى 3.56 مليون دولار

- **رسائل التصيد الاحتيالية الإلكترونية تقفز 62٪ خلال 3 أشهر**
- **الشركات الصغيرة والمتوسطة في مرمى الهجمات الإلكترونية**
- **مخصص للتصيد الاحتيالي URL حظر 393000 عنوان**
- **ضحية لبرمجيات الفدية الضارة 1300**

العالمية في مجال الحماية الإلكترونية، تقرير التهديدات الإلكترونية لمنتصف عام Acronis «أصدرت شركة «أكرونيس عرضة لمخاطر محددة وذلك (SMBs) 2021، وأطلقت في التقرير تحذيراً بأن الشركات الصغيرة ومتوسطة الحجم بناءً على اتجاهات الهجمات التي تم رصدها في أثناء أول ستة أشهر من العام.

وقد كشف التقرير عن أنه في أثناء النصف الأول من عام 2021، تعرَّضت 4 من بين 5 مؤسسات إلى اختراق في آلية الأمان الإلكتروني ناشئ عن ثغرة أمنية في النظام البيئي لمُورّد الخدمات التابع لجهة خارجية الذي تتعامل معه. وهذا الأمر يحدث في الوقت الذي ارتفعت فيه تكلفة اختراق البيانات إلى ما يقارب 3.56 مليون دولار أمريكي، مع ازدياد

سريع لمتوسط المبالغ المدفوعة مقابل برمجيات الفدية الضارة بنسبة 33% إلى ما يزيد على 100000 دولار أمريكي. وبينما يمثل هذا الأمر ضربة مالية هائلة لأية مؤسسة، فإن هذه المبالغ المالية ستكون بمثابة إعلان الوفاة لمعظم الشركات الصغيرة ومتوسطة الحجم، والذي تظن Acronis أنه يمثل مصدر قلق هائل في النصف الثاني من عام 2021.

بينما تؤثر الزيادة في معدل» Acronis وأوضح كانديد ويست، نائب رئيس قسم أبحاث الحماية الإلكترونية في شركة الهجمات على المؤسسات بكافة أحجامها، هناك شيء ما لا يتم الإبلاغ عنه بشكل كافٍ في تغطية اتجاهات التهديدات الإلكترونية الحالية، وهو حجم التأثير الواقع على مجتمع الشركات الصغيرة». «فبخلاف الشركات الأكبر حجماً، لا تمتلك الشركات الصغيرة ومتوسطة الحجم الأموال أو الموارد أو الخبرات في أطقم العمل اللازمة لمواجهة التهديدات القائمة في الوقت الحالي. لهذا السبب، تلجأ هذه الشركات إلى موفري خدمات تكنولوجيا المعلومات – ولكن إذا كان موفرو خدمات تكنولوجيا المعلومات هؤلاء عرضة للخطر- فإن تلك الشركات الصغيرة ومتوسطة الحجم تقع تحت رحمة مرتكبي الهجمات».

ومن خلال استخدام تقنيات الهندسة الاجتماعية لخداع المستخدمين الغافلين بالضغط على المرفقات أو الروابط الضارة، ارتفع معدل رسائل البريد الإلكتروني بغرض التصيد الاحتيالي بنسبة 62% من الربع الأول إلى الربع الثاني. ويمثل هذا الارتفاع المفاجئ مصدر قلق محددًا بما أنه يتم نشر 94% من البرمجيات الضارة عبر البريد الإلكتروني. وفي أثناء الفترة الزمنية نفسها، قامت Acronis بحظر ما يزيد على 393000 عنوان URL الاحتيالي مخصص للتصيد وضار للعملاء، حيث أدى ذلك إلى منع مرتكبي الهجمات من الوصول إلى بيانات قيّمة وتثبيت البرمجيات الضارة في نظام العميل.

عمليات ترشيح البيانات متواصلة في الزيادة. في عام 2020، تعرَّض ما يزيد على 1300 ضحية لبرمجيات الفدية الضارة إلى تسريب بياناتهم بشكل علني بعد وقوع إحدى الهجمات، حيث يسعى مرتكبو الجرائم الإلكترونية إلى زيادة أرباحهم المالية إلى أقصى حد ممكن من الحوادث الناجحة. في أثناء النصف الأول من عام 2021، تم بالفعل نشر ما يزيد على 1100 حالة تسريب للبيانات – وهو ما يعكس حدوث زيادة لهذه العمليات بنسبة 70% للعام الحالي.

لا يزال العاملون عن بُعد، هم الهدف الرئيسي. يتواصل الاعتماد على العاملين عن بُعد في أعقاب وقوع جائحة كوفيد-19. ويستخدم ثلثا العاملين عن بُعد الآن أجهزة العمل لأداء المهام الشخصية ويستخدمون أجهزة المنزل الشخصية لتنفيذ أنشطة الشركة. ونتيجة لذلك، يعمل مرتكبو الهجمات بنشاط على استكشاف العاملين عن بُعد. وقد لاحظت شركة Acronis وقوع ما يزيد على ضعف رقم الهجمات الإلكترونية العالمية، مع زيادة بنسبة 300% في شن الهجمات بالقوة المفرطة ضد الأجهزة التي تعمل عن بُعد عبر بروتوكول سطح المكتب البعيد (RDP).