الخليج

اقتصاد, آراء وتحليلات, مقالات

21 أغسطس 2023 14:22 مساء

كيف يمكن للمؤسسات التعامل مع الهويات المخترقة؟

الكاتب

إميل أبو صالح

إن سرقة هوية الموظفين، تمثل تهديداً متزايداً في المشهد الرقمي حالياً، حيث تدرك الشركات الخطر الذي يواجهها، والمتمثل في أن الأفراد يستطيعون الوصول إلى أكثر البيانات حيوية للمؤسسات، وأن العديد منهم يمكن أن يتعرضوا للخداع دون علمهم، ما يعرض أمان مؤسساتهم للخطر.

ويعتمد الكثير من الهجمات السيبرانية الحالية على الهويات المخترقة، بما في ذلك برامج الفدية، بدلاً من اختراق الأنظمة من خلال الضوابط التقنية، فإدراك العملاء للخطر، يعد أكثر فعالية من سرقة بيانات الاعتماد وتسجيل الدخول، ونظراً لصعوبة الكشف عن هذه الهجمات، فإن معظم المؤسسات غير مدركة لهذا الخطر.

غالباً، ما يبدأ الهجوم بسرقة تفاصيل الوصول من موظف واحد، ثم ينتقل إلى التسبب في الاختراق للخوادم والأجهزة النهائية وتنزيل البيانات الحساسة للمؤسسة، عندما يهاجم قراصنة الإنترنت أحد المضيفين، فإنه نادراً ما يكون هدفه النهائي، لذلك يجب أن يرتقي بصلاحية الوصول، وينتقل جانبياً لتحقيق أهدافه.

الإمارات تتفوق على 14 دولة في التدريب على الأمن السيبراني

جدير بالذكر أن المؤسسات في دولة الإمارات العربية المتحدة، تولي أهمية قصوى لمسألة التدريب على الأمن السيبراني، ووفقاً لتقرير «ستيت أوف ذا فيش»، للعام 2023، يتلقى 74% من المؤسسات في الإمارات التدريب على مواضيع الأمان، التي تستهدف مؤسساتهم، وبذلك تتفوق على 14 دولة أخرى في الدراسة، علاوة على ذلك، يتلقى 64% من المؤسسات في الإمارات تدريباً لجميع موظفيها، وهو أمر مشجع، لكن يجب على المؤسسات أن تتذكر أن الوعي

.السيبراني والتدريب، هما برنامج مستمر بدلاً من ممارسة مرة واحدة، للتأكد من الوقاية من الهجمات المستقبلية

وفي ظل التهديد المتزايد للأنظمة الأمنية، فمن المهم أن تتذكر المؤسسات أن البريد الإلكتروني لا يزال النقطة الأكثر شيوعاً لدى القراصنة الإلكترونيين، بغض النظر عن هدفهم النهائي. وقد تعرضت بعض المؤسسات والشركات العاملة في دولة الإمارات لهجمات سيبرانية متنوعة، حيث كشف تقرير حديث صادر عن «بروف بوينت» بعنوان «ستيت أوف ذا فيش»، للعام 2023؛ بأن 86% من هذه الهجمات كانت ناجحة، وأدت 26% منها إلى سرقة بيانات الاعتماد و/أو اختراق الحساب، حيث عرض الموظفون بيانات الاعتماد الخاصة بهم عن غير قصد، ما يمنح العملاء الخطر وصولًا إلى البيانات الحساسة وحسابات العمل. بالإضافة إلى ذلك، عانت 64% من المؤسسات في الإمارات محاولة هجوم .استنزاف، عن طريق البريد الإلكتروني خلال العام الفائت، وتعرض 70% منها للإصابة الناجحة

البريد الإلكتروني لا يزال النقطة الأكثر شيوعاً لدى القراصنة الإلكترونيين

كما أكد التقرير أن 28% من الموظفين في الإمارات يُعيدون استخدام كلمات المرور لعدة حسابات ذات صلة بالعمل، ما يمكن أن يعرض جميع الحسابات المرتبطة للخطر، إذا أُخترق واحد فقط منها. يمكن أن تسبب الإجراءات الخاطئة من قبل الموظفين في خلق مشكلات للمؤسسات. في الواقع، أفادت 72% من هذه المؤسسات بتعرضها لفقدان البيانات، بسبب إجراءات داخلية من قبل موظفين في عام 2022.
ولمكافحة التحدي المتزايد لهويات الموظفين المخترقة، يجب على المؤسسات أن تنظر إلى سلسلة الهجوم بأكملها، .كجزء من استراتيجية فعالة لحماية التهديدات

فلنبدأ بالخطوة الأولى، والتي تتمثل في وقف الاختراق الأولي في الأساس، وهذا هو المكان الذي تصبح فيه استراتيجية أمان البريد الإلكتروني القوية ضرورية، من هجمات الاحتيال عبر البريد الإلكتروني للشركات «بي إي سي»، والاستيلاء على حسابات السحابة، أو استخدام قراصنة الإنترنت لطرف ثالث موثوق به، لاختراق المؤسسة من خلال مورد لديها، .حيث يمكن أن يؤدي البريد الإلكتروني الأولي إلى الاختراق

وغالباً ما يتنكر قراصنة الإنترنت بأشخاص يثق بهم ضحاياهم، ويخدعونهم لإجراء مدفوعات مالية مزيفة. يمكن أن تشمل هذه الاحتيالات الهدايا وبطاقات الهدايا، إعادة توجيه الدفع واحتيال فواتير الموردين. بعد الاختراق الأولي، يكون .لديهم وصول إلى النطاق، ما يمنحهم الوصول إلى حسابات البريد الإلكتروني والقدرة على ارتكاب الاحتيال

من خلال مجموعة تقنية من قواعد بوابة البريد الإلكتروني، وتحليل التهديدات المتقدم، والمصادقة على البريد الإلكتروني، والرؤية في تطبيقات السحابة، يمكن للمؤسسات منع غالبية الهجمات المستهدفة قبل وصولها إلى .الموظفين

أكثر من 99% من التهديدات السيبرانية يتطلب تفاعلًا بشرياً لتحقيق النجاح

يجب على المؤسسات أيضاً تطبيق أرقى الوسائل التكنولوجيا، للتحديد والاستجابة للمستخدمين المخترقين، وإزالة ما يحتاج إليه قراصنة الإنترنت لإتمام جريمتهم: وصول الحسابات المميزة. ستساعد النهج الفريد للاكتشاف والاستجابة

لتهديدات الهوية «آي تي دي آر»، المؤسسات على معالجة مخاطر الهوية المميزة، وفهم الآثار المحتملة للاختراق، مثل الوصول إلى البيانات الحساسة والملكية الفكرية.

فإن الجمع بين الأفراد والعمليات والتكنولوجيا أمر حاسم، وإن عنصر الأمان هو مسؤولية مشتركة، ويجب تمكين الأفراد على جميع المستويات داخل المؤسسات، بما يكفي لفهم الأمان والسلوكيات الخطيرة، التي يمكن أن تؤدي إلى الانتهاكات.

ووفقاً للتقرير، فإن أكثر من 99% من التهديدات السيبرانية، يتطلب تفاعلًا بشرياً لتحقيق النجاح، ويجب تدريب كبار الموظفين بشكل متكرر على الهجوم، ليكونوا جزءاً حيوياً من دفاع المؤسسة والتصدي لأية هجمات، وإن برامج التدريب والتوعية ضرورية، ويجب أن تناسب كل فئة وظيفية، كما يجب على المؤسسات التأكد من أن البرامج مصممة خصيصاً للمستخدم ـ حتى يكون لها صلة بعملهم وحياتهم الشخصية.