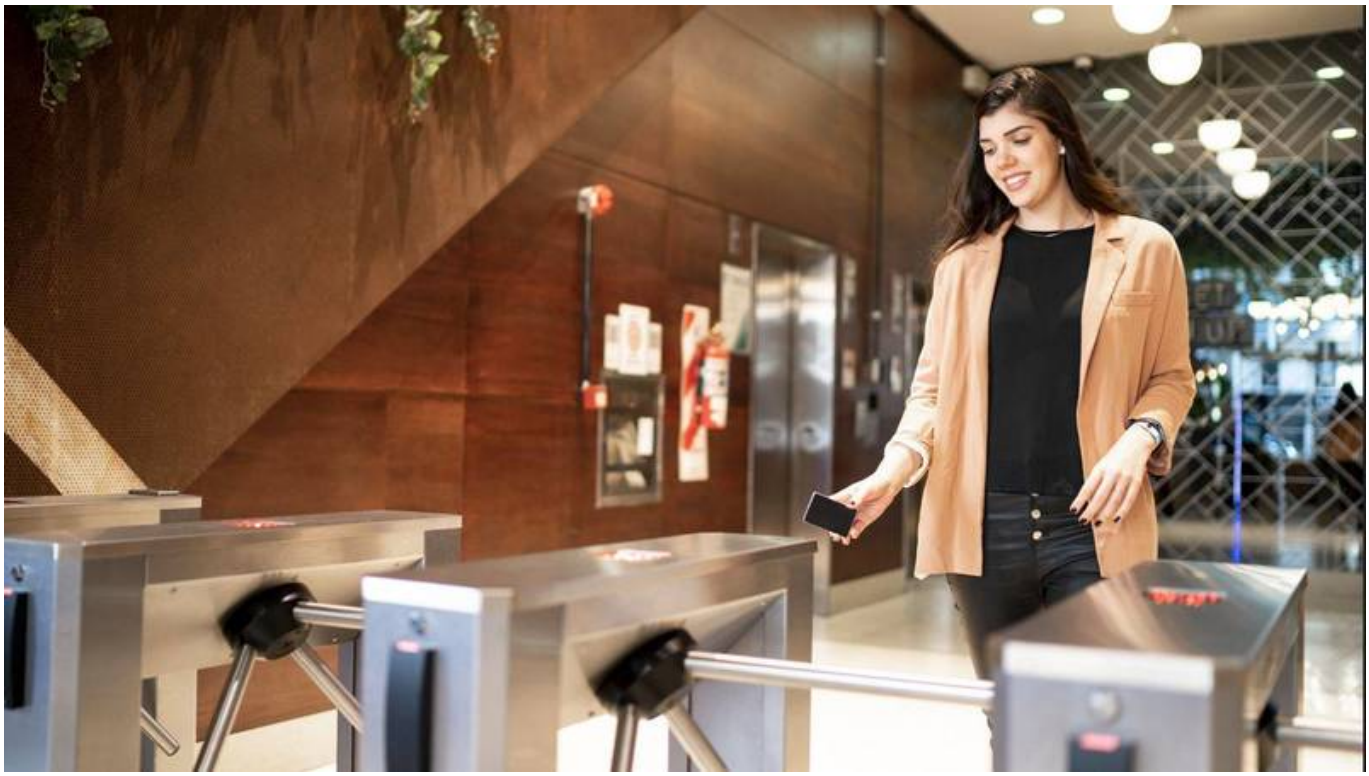
اقتصاد, تقنية وسيارات

24 نوفمبر 2022 11:52 صباحا

مليون دولار متوسط تكلفة اختراق البيانات مع ارتفاع الهجمات 4.35 الإلكترونية



دعت شركة «جينيتك» المتخصصة في مجال الأمن والسلامة العامة واستقصاء بيانات الأعمال، الشركات من مختلف الأحجام، إلى توخي الحذر حول مخاطر الأمن الإلكتروني التي تمثلها الأنظمة القديمة للتحكم في الوصول إلى البيانات.

وقال كريستيان مورين، نائب رئيس هندسة المنتجات وكبير مسؤولي الأمن لدى الشركة: «تستخدم العديد من الشركات أنظمة قديمة للتحكم في الوصول يرجع عمرها إلى 10 سنوات أو أكثر. وعلى الرغم من أن هذه الأنظمة القديمة لا تزال تسمح للموظفين بالدخول والخروج، فإن هناك احتمالًا كبيراً أن تستخدم هذه الأنظمة تقنيات معرضة بشدة للتهديدات الإلكترونية الحديثة».

ويمكن لمكامن الضعف في الأنظمة القديمة للتحكم في الوصول أن تضعف من مشهد الأمن الإلكتروني لدى المؤسسات بشكل يعرضها لمخاطر كبيرة، حيث يمكن لمجرمي الإنترنت استغلال نقاط الضعف في بيانات اعتماد

.لأنظمة التحكم في الوصول أو وحدات التحكم، أو الخوادم أو القراء أو محطات العمل المتصلة بالشبكة

وسيتمكن مجرمو الإنترنت، بمجرد نجاحهم في اختراق بيانات اعتماد نظام التحكم في الوصول، من الانتقال إلى شبكة المؤسسة والتحكّم في الأنظمة الأخرى الموجودة لدى الشركة، أو استعراض المعلومات السرية أو سرقتها من .السجلات الداخلية، أو شن هجمات تستهدف تعطيل الأنظمة الرئيسية

• تكلفة مرتفعة

وعادة ما تدفع الشركات المتضررة ثمناً باهظاً لهذه الخروق، فقد ارتفع متوسط تكلفة خرق البيانات من 4.24 مليون دولار أمريكي في عام 2021 إلى 4.35 مليون دولار أمريكي في عام 2022؛ لذا فقد بات من المهم جداً توعية المؤسسات بالمخاطر التي ترتبط بمواصلة استخدام الأنظمة القديمة، والمزايا التي يمكن أن توفّرها الحلول الإلكترونية .الجديدة للوصول إلى البيانات

• توصيات

ترقية النظام: لم يتم تصميم الأنظمة القديمة لتكون قادرة على مواجهة التهديدات الجديدة التي نشهدها في يومنا هذا. وعند تقييم نظام جديد للتحكم في الوصول أو ترقية نظام حالي، يجب التأكد من أن الأمن الإلكتروني هو مكوّن رئيسي ضمن آلية اختيار المزوّدين، واستخدم بيانات اعتماد آمنة متقدمة وأحدث بروتوكولات الاتصالات، لتأمين نقل البيانات، نظراً لسهولة استنساخ بيانات الاعتماد القديمة باستخدام الأدوات المتاحة، وتثقيف الموظفين والشركاء بأفضل ممارسات الأمن الإلكتروني، والتأكد من تغيير كلمات المرور بشكل منتظم، والتحقق بشكل منتظم من تحديثات .البرامج الحاسوبية، والبرامج الثابتة والقيام بتثبيتها بمجرد توفرها

واستخدام نظام مركزي لإدارة الوصول إلى الهوية لضمان المصادقة الافتراضية والمادية، وتفويض الموظفين من أجل تحكم أفضل، وصيانة أكثر فاعلية للأنظمة التقنية، وإنشاء شبكة مخصصة لأنظمة التحكّم في الوصول، بحيث يكون هناك فصل واضح للشبكات على أساس الهدف منها، واختيار مزود خدمات أمنية قادر على ضمان الامتثال لشهادات الأمان المعمول بها، والتأكد من استخدام نظام التحكم في الوصول إلى معايير مثبتة لتشفير البيانات، ومصادقة متعددة العوامل، والعمل مع الشركاء الذين يتمتعون بإدارة قوية لمخاطر سلسلة التوريد، وفرق متخصصة .في مراقبة التهديدات الإلكترونية، والتأكد من تحديث البرامج بشكل منتظم وتصحيحها حسب الحاجة

وقد شهدت تقنيات التحكم في الوصول تطورات كبيرة خلال السنوات الأخيرة. وبات العملاء يتمتعون بقدرة على تحرير أنفسهم تدريجياً من حلول الملكية، ويطالبون بحلول أكثر مرونة وانفتاحاً. لقد أدخلت الشركات المطورة .للخدمات التقنية جيلًا جديداً من الحلول الأكثر أماناً عبر الإنترنت التي تقدم مزايا تتجاوز مجرد قفل الأبواب وفتحها