اقتصاد, أسواق الإمارات

19 مارس 2024 17:34 مساء

من الشركات في الإمارات فقدت بيانات خلال 2023 % 94

دبي: «الخليج»

أصدرت شركة «بروف بوينت»، المتخصصة في مجال أمن المعلومات والامتثال، الثلاثاء، تقريرها الأول من نوعه بعنوان «مشهد فقدان البيانات»، الذي يسلط الضوء على كيفية معالجة مسألة فقدان البيانات وحمايتها. ويتطرق إلى التهديدات الداخلية، مثل تحديات البيانات الكبرى الحالية، مثل انتشار البيانات وقراصنة الإنترنت المتطورين، والذكاء الاصطناعي الناشئ (GenAI). وتشير الدراسة إلى أن فقدان البيانات يعد من المشاكل الناجمة عن تفاعل بين الأفراد والآلات. جدير بالذكر أن «المستخدمين المهملين»، يعدّون المسبب الأول في مثل هذه الحوادث أكثر من الأنظمة المخترقة، أو غير المكونة بشكل صحيح.

وبينما تكثف الشركات استثماراتها في تقنيات وحلول حماية البيانات ومنعها من الفقدان، يؤكد التقرير أن هذه الاستثمارات غالباً ما تكون غير كافية. ووفقاً للتقرير؛ 94% من المؤسسات المستطلعة في دولة الإمارات، تعرضت لفقدان البيانات في العام الماضي. وقد واجه ما يقرب من (94%) من المتأثرين نتائج سلبية، مثل اضطراب الأعمال، وخسارة الإيرادات (أبلغت عنها 55% من المؤسسات المتضررة في الدولة) أو الانتهاك/ الغرامة التنظيمية47%.

وصرح إميل أبو صالح، المدير الإقليمي لدى «بروف بوينت» في الشرق الأوسط وإفريقيا وتركيا: «تمثل مسألة فقدان

البيانات تهديداً خطيراً، حيث يمكن أن يؤدي الإهمال البسيط إلى فقدان البيانات الحرجة. لذا فمن الضروري بالنسبة إلى الموظفين فهم الدور الذي يلعبونه في حماية البيانات، وأنه ليس مجرد مشكلة تقنية».

وقال ريان كاليمبر، مدير الاستراتيجية الرئيسي لدى «بروف بوينت»: «يسلط التقرير الضوء على الجوانب الأساسية المتسببة بفقدان البيانات لا سيما الحرجة منها؛ ومن بين الأسباب الرئيسية هي التفاعل البشري. وفي هذا الإطار، فإن المستخدمين المهملين وقراصنة الإنترنت من بين الأسباب الرئيسية في مثل تلك الحوادث. في حين أن أدوات الذكاء الاصطناعي تتولى المهام الشائعة وتصل إلى البيانات السرية؛ ولذلك، فإن الشركات تحتاج إلى إعادة التفكير في استراتيجيات الوقاية من فقدان البيانات لمعالجة السبب الجذري لفقدانها ـ المسبب الأول هو الفرد».

يستعرض تقرير مشهد فقدان البيانات لعام 2024 آراء ووجهات نظر المستطلعين البالغ عددهم 600 محترف أمني، في منظمات تضم 1000 موظف، أو أكثر، عبر 17 صناعة، من 12 دولة؛ مدعومة ببيانات من منصة حماية المعلومات التي اشترتها «بروف بوينت» مؤخراً. (Tessian) وشركة

أبرز النتائج

1- فقدان البيانات يُعد مشكلة واسعة الانتشار ومن الممكن التصدي لها: تعرضت المؤسسات إلى ما يعادل أكثر من 24 حادث فقدان بيانات لكل مؤسسة في دولة الإمارات خلال العام الماضي)، وقال 75%حادث واحد شهرياً (متوسط من المستجيبين، إن السبب الرئيسي يكمن في الأفراد المهملين؛ من خلال تحويل الرسائل البريدية بشكل غير صحيح، وزيارة مواقع الصيد الاحتيالي، وتثبيت البرامج غير المصرح بها، وإرسال البيانات الحساسة عبر البريد الإلكتروني إلى حساب شخصي.

2-البريد الإلكتروني المحول بشكل غير صحيح، يعد أحد أبسط وأهم الأسباب المؤدية إلى فقدان البيانات: وفقاً للبيانات لعام 2023؛ فإن نحو ثلث الموظفين قاموا بإرسال رسالة بريد إلكتروني (Tessian) والإحصاءات الصادرة عن واحدة، أو اثنتين، إلى المستقبِل الخطأ. وهذا يعني أن الشركة التي تضم 5000 موظف يمكن أن تتوقع التعامل مع نحو 3400 رسالة بريد إلكتروني محولة بشكل غير صحيح في السنة.

3-يمثل الذكاء الاصطناعي الناشئ أحد أبرز المجالات، التي تثير المخاوف والقلق في هذا المجال؛ وذلك في ظل تزايد حيث (Google Bardو Bing Chat Grammarly ChatGPT) حجم استخدام الأدوات الرقمية المتطورة مثل يزيد أعداد المستخدمين الذين يدخلون البيانات الحساسة في هذه التطبيقات.

4- يمكن أن تكون عواقب الأفعال الضارة مكلفة: قال 19% من المستجيبين إن المستخدم الخبيث مثل الموظفين، أو المتعاقدين، كانوا وراء حوادث فقدان البيانات.

5-الموظفون الذين يغادرون العمل من بين العوامل الخطرة المسببة في فقدان البيانات (22%): لا يعتقد الموظفون الذين يغادرون دائماً أنهم يتصرفون بشكل خبيث ـ بعضهم يشعرون ببساطة بالحق في المغادرة بالمعلومات التي أنتجوها. ويشير التقرير إلى أن 87% من تسرب الملفات غير الطبيعي بين المستأجرين في السحابة على مدار تسعة أشهر تسبب بها الموظفون الذين يغادرون العمل، ما يؤكد على الحاجة إلى استراتيجيات وقائية، مثل تنفيذ عملية استعراض أمنية لهذه الفئة من المستخدمين ذوي الامتيازات هم الأكثر خطورة: نحو ثلثي المستجيبين في دولة الإمارات (72%) الموظفين الذين لديهم وصول إلى البيانات الحساسة، مثل متخصصي الموارد البشرية والمالية، يمثلون أكبر مصدر لخطر فقدان البيانات. إضافة إلى ذلك، تظهر بيانات «بروف بوينت» أن 1% من المستخدمين مسؤولون عن 88% من حالات فقدان البيانات.

6- زيادة تبنّي وتحديث برامج الوقاية لحماية فقدان البيانات: تحرص العديد من الشركات على تطبيق برامج الوقاية من فقدان البيانات في الدولة؛ استجابة للتشريعات القانونية، حيث ذكر أكثر من ثلث (36%) من مشاركي الاستطلاع أن تحقيق معايير الامتثال التنظيمي هو السائق الرئيسي. وحماية خصوصية الموظفين والعملاء وتقليل التكاليف المرتبطة

بفقدان البيانات جاءا كأهم الدوافع للمؤسسات في الدولة (كلاهما بنسبة 50%).
وعلق كاليمبر: «تؤكد القنوات الناشئة على أهمية تطبيق برامج الوقاية لحماية فقدان البيانات بشكل منتظم، حيث تغيّر حيث DLP هذه الأنواع من التطورات السريعة سلوك المستخدمين. وهنا تأتي أهمية استراتيجيات مثل تنفيذ منصات تعمل على المساعدة في تقدم برامج الأمان عن طريق تمكين فرق الأمان من الحصول على رؤية كاملة للمستخدم والبيانات في جميع الحوادث ومعالجة النطاق الكامل لسيناريوهات فقدان البيانات المركزة حول الفرد».