الخليج

اقتصاد, تقنية وسيارات

9 مايو 2023 18:05 مساء

من رؤساء أمن المعلومات في الإمارات لديهم ضوابط كافية لحماية 61% بياناتهم

أصدرت شركة «بروف بوينت»، للأمن السيبراني والامتثال، الثلاثاء، تقريرها السنوي بعنوان «وجهات نظر رؤساء أمن المعلومات للعام 2023»، والذي يسلط الضوء على التحديات والتوقعات والأولويات الرئيسية لدى كبار مسؤولي أمن المعلومات.

وفي هذا السياق، أشار التقرير إلى أن «معظم رؤساء أمن المعلومات في الإمارات، بدؤوا يشعرون بالمخاوف الذين كانوا يعانوا منها في وقت مبكر من جائحة كوفيد-19، حيث يشعر 75% ممن شملهم الاستطلاع بأنهم معرضون لخطر هجوم إلكتروني مادي، مقارنة بـ 44% في العام السابق».

وأشارت الشركة إلى أن «النتائج التي استخلصها التقرير في نسخة هذا العام تعيد الأذهان إلى العام 2021، حيث اعتقد 68% من رؤساء أمن المعلومات في الدولة أن وقوع هجوم مادي كان وشيكاً جداً في أي وقت».

وبالمثل، انعكست المشاعر حول مستويات التأهب، حيث يشعر 57% ممن شملهم الاستطلاع بأنهم غير مستعدين للتعامل مع هجوم إلكتروني مستهدف، مما يدل على زيادة معتدلة عن العام الماضي بنسبة 47% وانخفاضاً من 72%

في عام 2021. كما أشار التقرير إلى أن 61% من رؤساء أمن المعلومات في الإمارات يعتقدون أن لديهم ضوابط كافية لحماية بياناتهم.

• آثار عمليات التسريح

ورغم أن المؤسسات والشركات قد تغلبت إلى حد كبير على الاضطرابات التي حدثت خلال العامين الماضيين، بحسب التقرير، إلا أن آثار الاستقالة العديدة وعملية دوارن الموظفين زادت من حدة المخاطر، والتي تفاقمت بسبب الموجة الأخيرة من عمليات التسريح الجماعي للموظفين، حيث يقول 75% من رؤساء أمن المعلومات في الدولة أن الموظفين الذين تركوا الشركة أثروا تأثيراً سلباً فيما يخص فقدان البيانات. ورغم أن 47% من رؤساء الأمن اضطروا إلى تعامل مع فقدان المعلومات الحساسة خلال الـ 12 شهراً الماضية، إلا أن 61% فقط أن قالوا أنهم يمتلكون أنظمة حماية كافية للحفاظ على البيانات.

هذا ويحلل التقرير ردود الأفعال ووجهات نظر الأطراف الثالثة العالمية من أكثر من 1600 من رؤساء أمن المعلومات في المؤسسات والشركات ذات الأحجام الكبيرة والصغيرة عبر مختلف الصناعات. وعلى مدار الربع الأول من العام 2023، تم إجراء مقابلات مع 100 مدير أمن المعلومات في كل سوق في 16 دولة: الإمارات العربية المتحدة والمملكة العربية السعودية والولايات المتحدة وكندا والمملكة المتحدة وفرنسا وألمانيا وإيطاليا وإسبانيا والسويد وهولندا وأستراليا واليابان وسنغافورة وكوريا الجنوبية والبرازيل.

ويناقش التقرير الاتجاهات العالمية والاختلافات الإقليمية حول ثلاثة مواضيع مركزية: التهديدات والمخاطر التي يواجهها رؤساء أمن المعلومات بشكل يومي، وتأثير الموظفين على الاستعداد الإلكتروني للمؤسسات وأنظمة الدفاعات التي يبنيها مسؤولو أمن المعلومات، خاصة وأن الانكماش الاقتصادي يضغط على ميزانيات الأمن. ويقيس الاستطلاع أيضاً التغييرات في التوافق بين قادة الأمن ومجالس إدارتهم، فضلاً عن استكشاف كيفية تأثير علاقتهم على الأولويات الأمنية.

• ضغوط متزايدة

وقال إميل أبو صالح، المدير الإقليمي لدى شركة «بروف بوينت» في الشرق الأوسط وأفريقيا: «أدت سنوات من العمل المستمر عن بُعد والهجين إلى زيادة المخاطر حول حوادث التهديد الداخلي حيث كشف التقرير عن أن 43 رؤساء أمن المعلومات في دولة الإمارات يوافقون على أن الموظفين الذين يتركون المؤسسة يتسببون في فقدان البيانات»، مشيراً الى أن «التحديات المتزايدة لحماية الأفراد والبيانات والتوقعات الكبيرة والإرهاق وعدم اليقين بشأن المسؤولية الشخصية، تضع رؤساء أمن المعلومات في دولة الإمارات تحت ضغوط متزايدة وتحد كبير».

وأضاف: «لمعالجة هذا الخطر المحتمل، يجب بناء أنظمة دفاعية متعددة الطبقات، بما في ذلك حل مخصص لإدارة ، بحيث تتمتع المؤسسات بحماية جيدة من التهديدات التي تركزالتهديدات الداخلية وتدريب قوي على الوعي الأمني على الأفراد الذين هم الهدف الأساسي لقراصنة الإنترنت».

• تزايد المخاوف

ومن بين النتائج الأساسية التي استخلصها التقرير عن دولة الإمارات، تزايد المخاوف عند رؤساء أمن المعلومات في الدولة، حيث شعروا أيضاً بأنهم غير مستعدين أكثر من العام الماضي. وأفاد 75% من رؤساء أمن المعلومات في الدولة بأنهم يشعرون بخطر التعرض لهجوم إلكتروني مادي خلال الأشهر الـ 12 المقبلة، مقارنة بـ 44% في العام

الماضي و 68% في عام 2021. وعلاوة على ذلك، يعتقد 57% أن مؤسستهم غير مستعدة للتعامل مع هجوم إلكتروني مستهدف، مقارنة بـ 47% في العام الماضي و 72% في العام 2021».
وتفاقم فقدان البيانات الحساسة بسبب معدل دوران الموظفين، حيث أفاد 47% من رؤساء أمن المعلومات في الدولة بأنهم اضطروا إلى تعامل مع خسارة مادية لبيانات حساسة خلال الـ 12 شهراً الماضية، واتفق 75% منهم على أن الموظفين الذين تركوا المؤسسة قد ساهموا في ذلك. على الرغم من هذه الخسائر، إلا أن 61% من رؤساء أمن المعلومات في الإمارات يعتقدون أن لديهم ضوابط كافية لحماية بياناتهم.

• الاحتيال عبر البريد الإلكتروني

ويتصدر الاحتيال عبر البريد الإلكتروني قائمة التهديدات الأكثر أهمية، حيث يشير التقرير إلى أن «أهم التهديدات التي يتصورها مسؤولو أمن المعلومات في الدولة هي نفسها تقريباً تلك التي كانت في العام الماضي، وذلك بسبب الاحتيال عبر البريد الإلكتروني (اختراق البريد الإلكتروني للنشاط التجاري) واختراق الحسابات السحابية الطريق، ولكن هذا العام تبعتهما البرامج الضارة والتصيد الاحتيالي، بينما انضمت البرامج الضارة في العام الماضي إلى التهديدات الداخلية باعتبارها من أبرز الاهتمامات الأخرى».
وأضاف التقرير: «من المرجح أن تدفع معظم المؤسسات فدية إذا تأثرت ببرامج الفدية، حيث يعتقد 59% من رؤساء أمن المعلومات في الدولة أن مؤسساتهم ستدفع مقابل استعادة الأنظمة ومنع إصدار البيانات إذا تعرضت لهجوم من برامج الفدية خلال الأشهر الـ 12 المقبلة، بينما يعتمدون على التأمين لتحويل المخاطر؛ حيث قال 56% إنهم سيقدمون مطالبة بالتأمين الإلكتروني لاسترداد الخسائر المتكبدة في أنواع مختلفة من الهجمات».

• مخاطر سلسلة التوريد

وأظهر التقرير أن «مخاطر سلسلة التوريد تأتي من بين الأولويات الرئيسية، حيث يقول 56% من رؤساء أمن المعلومات في الدولة أن لديهم ضوابط كافية للتخفيف من مخاطر سلسلة التوريد، وهي زيادة متواضعة عن نسبة 49% في العام الماضي. في حين أن هذه الحماية قد تبدو مناسبة في الوقت الحالي. ومن الآن فصاعدًا، ربما يشعر رؤساء أمن المعلومات بضيق أكبر للموارد، حيث يقول 65% أن ميزانياتهم قد تأثرت بالفعل».
ويلفت التقرير إلى أن «تنامي مخاطر الأفراد يعد من مصادر القلق المتزايد، حيث اتفق 59% من رؤساء أمن المعلومات في الدولة على أن الخطأ البشري يعد أكبر نقطة ضعف إلكترونية تهدد أمن شركاتهم، مقابل 50% في العام 2022 و70% في عام 2021»، مشيراً الى أن «في الوقت نفسه، يعتقد 56% من رؤساء أمن المعلومات أن الموظفين يفهمون دورهم في حماية المؤسسة، مقارنة بـ 51% في عام 2022 و69% في عام 2021، كل ذلك يؤكد المجهودات المصنية لبناء ثقافة أمنية قوية».

• تناغم أكثر

وبحسب التقرير، يعد رؤساء أمن المعلومات والمجالس أكثر تناغمًا، حيث يوافق 63% من رؤساء أمن المعلومات في الدولة على أن أعضاء مجلس إدارتهم يتعاملون معهم في قضايا الأمن السيبراني. وهذه زيادة كبيرة عن 47% من رؤساء أمن المعلومات الذين شاركوا هذا الرأي العام الماضي وهي نفس النسبة في العام 2021.
واعتبر التقرير أن «زيادة الضغوط على رؤساء أمن المعلومات من شأنها أن تجعل العمل غير مستدام بشكل متزايد، حيث يشعر 59% من رؤساء أمن المعلومات في الدولة أنهم يواجهون توقعات وظيفية غير معقولة، وهي زيادة كبيرة

عن العام الماضي الذي سجل 38%».
وأضاف:«في حين أن العودة إلى واقعهم الجديد قد تكون أحد الأسباب وراء هذا الرأي، فإن القلق المرتبط بالوظيفة لدى رؤساء أمن المعلومات يعد من أحد الأسباب التي ساهمت في هذه النسبة المتزايدة؛ حيث أعرب 60% عن قلقهم بشأن المسؤولية الشخصية، بينما قال 59% أنهم قد عانوا من الإرهاق خلال الأشهر الـ 12 الماضية».

• الصمود في حماية البيانات

من جانبه، قال ريان كالمبر، نائب الرئيس التنفيذي لاستراتيجية الأمن السيبراني لدى بروف بوينت: «يجب أن يظل قادة الأمن صامدين في حماية أفرادهم وبياناتهم، وهي مهمة تزداد صعوبة لا سيما أن المخاطر تأتي من موظفي الشركة وقد يتسببون في فقدان البيانات الحساسة بشكل كبير. وتدل الهجمات المدمرة الأخيرة إلى أن أمام رؤساء أمن المعلومات طريق أكثر صعوبة، لا سيما بالنظر إلى الميزانيات الأمنية غير المستقرة وضغوط العمل الجديدة. والآن وفي ظل زياد الشعور بالقلق، يجب على رؤساء أمن المعلومات التأكد من أنهم يركزون على الأولويات الصحيحة لتحريك مؤسساتهم نحو المرونة الإلكترونية».