الخليج

اقتصاد, تقنية وسيارات

17 مايو 2022 16:47 مساء

من رؤساء أمن المعلومات في الإمارات غير مستعدين لهجوم إلكتروني 47%

يتوقعون هجمات إلكترونية مادية خلال الـ 12 شهراً المقبلة 44%

دبي: «الخليج»

أصدرت شركة بروف بوينت، تقريرها السنوي «وجهات نظر رؤساء أمن المعلومات لعام 2022»، والذي يسلط الضوء على التحديات الرئيسية التي تواجه كبار مسؤولي أمن المعلومات لصد الهجمات الإلكترونية.

وأشار التقرير إلى أنه على الرغم من أن رؤساء أمن المعلومات حول العالم تبنوا طرقاً جديدة في العمل بسبب مستجدات جائحة كوفيد خلال عام 2021؛ فإن الكثيرين يشعرون بالسيطرة أكثر ضمن بيئتهم الأمنية.

وأكد التقرير أن 44% من رؤساء أمن المعلومات في دولة الإمارات على احتمالية تعرض مؤسساتهم لخطر هجوم إلكتروني مادي خلال الـ 12 شهراً المقبلة؛ مقارنة بنسبة 68% بحسب تقرير العام الماضي.

وهناك فرق شاسع بين الشعور بأن الشركة مستعدة لصد الهجمات الإلكترونية وبين الاستعداد الفعلي للتصدي لها.

وترجع هذه الثقة المتزايدة لدى رؤساء أمن المعلومات إلى قدراتهم على التعامل مع التحديات والتغيرات خلال جائحة كوفيد-19 ولا تستند إلى حقائق ملموسة في مستويات الاستعداد لمواجهة هذه المخاطر؛ إذ يكشف التقرير عن أن

47% من رؤساء أمن المعلومات في دولة الإمارات لا يزالون يشعرون بأن مؤسستهم غير مستعدة للتصدي لأي هجمات إلكترونية، بينما يعتبر 50% منهم أن الخطأ البشري هو من أكبر الثغرات الإلكترونية، لاسيما في ظل تبني أنظمة العمل عن بعد من أي مكان؛ وموجة الاستقالة الكبرى التي فرضت تحديات جديدة أمام حماية البيانات.

وقد قيم تقرير هذا العام طرفاً ثالثاً عالمياً، من خلال استطلاع أكثر من 1400 من رؤساء أمن المعلومات من مختلف المؤسسات المتوسطة والكبيرة ومن عدة قطاعات. وخلال الربع الأول من عام 2022، تم إجراء مقابلات مع 100 مدير تنفيذي في كل سوق عبر 14 دولة شملت: الولايات المتحدة وكندا والمملكة المتحدة وفرنسا وألمانيا وإيطاليا وإسبانيا والسويد وهولندا والإمارات العربية المتحدة والمملكة العربية السعودية وأستراليا واليابان وسنغافورة.

وقال أندرو روز، رئيس أمن المعلومات في الشرق الأوسط وإفريقيا لدى بروف بوينت: «مما لا شك فيه أن الهجمات السيبرانية البارزة أدت إلى تعطيل سلاسل التوريد. ودائماً ما تحظى هذه المواضيع باهتمام بالغ من مختلف القطاعات وتحتل جدول أعمال مجالس الإدارة؛ مما دفع الجهات المنظمة إلى إصدار تشريعات جديدة لتعزيز الأمن السيبراني. وقد شكل عام 2021 تحدياً آخر أمام رؤساء أمن المعلومات حول العالم. وفي ظل حرصهم على التكيف مع طرق العمل الجديدة، تزداد مستويات الثقة بشأن وضعهم الأمني السيبراني. ومع تلاشي تأثير الوباء بشكل تدريجي على فرق الأمن؛ يكشف تقرير Voice of the CISO 2022 عن قضية 2022 ملحة، فمع ترك القوى العاملة وظائفها أو عدم الانضمام إلى القوى العاملة مرة أخرى، باتت فرق الأمن الآن تتعامل مع مجموعة من الثغرات الأمنية لحماية المعلومات والتهديدات الداخلية».

من جانبه قال إميل أبو صالح المدير الإقليمي لدى شركة بروف بوينت في الشرق الأوسط وإفريقيا: «بعد عامين من الاضطراب والتغيرات غير المسبوقة وطرق العمل الجديدة بسبب جائحة كوفيد- 19، كان لابد لرؤساء أمن المعلومات من تركيز جهودهم لصد الهجمات الإلكترونية التي تستهدف الموظفين خلال نظام العمل الهجين. وقد انصب تركيزهم نحو منع الهجمات المحتملة مثل اختراق البريد الإلكتروني للأعمال واختراق الحسابات السحابية والتهديدات الداخلية. ويشعر رؤساء أمن المعلومات، بشكل عام، الآن بمزيد من التحكم في بيئة العمل وقد يكون شعوراً زائفاً بالأمان. ويكشف تقريرنا عن الخطأ البشري باعتباره أكبر نقاط الضعف السيبرانية للمؤسسة، ويجب أن تكون زيادة الوعي بالأمن السيبراني في المؤسسة ضمن أولوية رؤساء أمن المعلومات للحد من المخاطر التي تحيط بالأمن السيبراني».