الخليج

اقتصاد, تقنية وسيارات

18 مايو 2021  17:15 مساء

# ثلاثة أرباع مسؤولي أمن المعلومات غير مستعدين للتعامل مع هجوم إلكتروني

دبي: «الخليج»

أصدرت «بروف بوينت»، الشركة المتخصصة في مجال الأمن السيبراني والامتثال، الثلاثاء تقريرها الافتتاحي لعام الذي يبرز «Voice of the CISO Report- 2021 بعنوان: «رؤى كبار المسؤولين التنفيذين في أمن المعلومات التحديات الرئيسية التي تواجههم بعد عام شهد فيه تغيرات وتحديات غير مسبوقة؛ إذ قال 72% من كبار المسؤولين التنفيذين في أمن المعلومات إن مؤسستهم غير مستعدة للتعامل مع هجوم إلكتروني؛ بينما أفاد 70٪ أن الخطأ البشري هو أكبر نقاط ضعفهم الإلكترونية، ما يثبت أن نموذج العمل من المنزل الذي فرضته جائحة «كوفيد-19» التي وضعت كبار المسؤولين التنفيذين في أمن المعلومات تحت اختبار كبير بشكل لم يسبق له مثيل.

ويقيّم تقرير هذا العام ردود استطلاعات الرأي العالمية من طرف ثالث من أكثر من 1400 من كبار المسؤولين التنفيذين في أمن المعلومات في الشركات المتوسطة والكبيرة عبر مختلف القطاعات، وعلى مدار الربع الأول من العام 2021 تم إجراء مقابلات مع 100 من كبار رؤساء أمن المعلومات في كل سوق في 14 دولة من بينها: الإمارات

والمملكة العربية السعودية و الولايات المتحدة الأمريكية وكندا والمملكة المتحدة وفرنسا وألمانيا وإيطاليا وإسبانيا والسويد وهولندا وأستراليا واليابان وسنغافورة.

ويستكشف التقرير ثلاثة مجالات رئيسية: مخاطر التهديد وأنواع الهجمات الإلكترونية التي يواجهها كبار المسؤولين التنفيذين في أمن المعلومات يوميًا؛ ومستويات استعداد الموظفين والشركات لمواجهتها وتأثير دعم القوى العاملة المختلطة، حيث تستعد الشركات لإعادة فتح مكاتبها، كما يغطي التقرير التحديات التي يواجهها كبار المسؤولين التنفيذين في أمن المعلومات في أدوارهم، وموقعهم بين C-suite وتوقعات الأعمال لفرقهم.

وقالت لوسيا ميليكا مسؤولة أمن المعلومات العالمية لدى«بروف بوينت»: «في العام الماضي، واجهت فرق الأمن في هذا المشهد الجديد والمتغير جراء جائحة «كوفيد-19» وهذاالسيبراني حول العالم تحدياً لتعزيز وضعها الأمني يتطلب تحقيق التوازن بين دعم العمل عن بعد وتجنب انقطاع الأعمال مع تأمين تلك البيئات و تزايد مرونة مستقبل العمل، ويمتد هذا التحدي الآن إلى العام المقبل وما بعده، وإضافة إلى تأمين العديد من نقاط الهجوم وتثقيف المستخدمين حول العمل البعيد المدى والهجين، يجب على كبار المسؤولين التنفيذين في أمن المعلومات غرس الثقة بين العملاء وأصحاب المصلحة الداخليين والسوق بأن مثل هذه الإعدادات قابلة للتطبيق إلى أجل غير مسمى».

ومن بين النتائج الرئيسية التي توصل إليها التقرير في دولة الإمارات العربية المتحدة أن كبار المسؤولين التنفيذين في أمن المعلومات في حالة تأهب قصوى عبر مجموعة من التهديدات في مواجهة مشهد لا هوادة فيه من الهجمات، إذ يشعر 68٪ من كبار المسؤولين في أمن المعلومات الذين شملهم الاستطلاع في دولة الإمارات بأنهم معرضون لخطر التعرض لهجوم إلكتروني مادي في الأشهر الـ 12 المقبلة، وعندما سئلوا عن أنواع الهجمات التي يتوقعون مواجهتها تصدرت القائمة التهديدات الداخلية (29٪) والتصيد (28٪) وتسوية البريد الإلكتروني للأعمال (25٪).

وعلى الرغم من هيمنتها على العناوين الرئيسية الأخيرة، كانت هجمات سلسلة التوريد وبرامج الفدية تشكل مصدر قلق في أسفل القائمة بنسبة (G Suite أو O365 مماثل بنسبة 22٪. كان اختراق الحساب السحابي (تم اختراق حسابات 15٪ – وهي أدنى نسبة في جميع المناطق.