الخليج

اقتصاد, أسواق عالمية

30 مايو 2023  17:30 مساء

# بالو ألتو نتوركس»: الرؤساء التنفيذيون يقدمون الأمن الإلكتروني على أداء» الاقتصاد

إعداد: خنساء الزبير

أظهرت المتابعات والإحصاءات مؤخراً تعرض الكثير من المواقع المهمة على مستوى العالم لهجمات إلكترونية، .وكانت العملات المشفرة أحد القطاعات المتضررة من هذه الهجمات

---

- **من الرؤساء التنفيذيين يشعرون بالمسؤولية بشكل كبير 51 %**
- **يفهمون تماماً المخاطر التي تواجهها مؤسساتهم 16 %**
- **يعتبرون أنفسهم مسؤولين بالكامل عن الأمن الإلكتروني لمؤسستهم 21 %**
- **واثقون بخططهم الكاملة والمجربة للحماية من التهديدات 78 %**
- **منهم سيعملون مع فريق الاستجابة في حالة وقوع هجوم 36 %**

وبدأ عدد متزايد من الأشخاص الذين هم في مواقع المسؤولية، وخاصة الرؤساء التنفيذيين، يدركون مدى خطر هذه الهجمات؛ فبحسب تقرير جديد صادر بعد دراسة من قبل شركة «بالو ألتو نتوركس» فإنهم يرونها مهدداً يفوق مشكلة عدم اليقين الاقتصادي.

وشملت هذه الدراسة الاستقصائية 2500 من الرؤساء التنفيذيين من الإمارات والمملكة المتحدة وألمانيا وفرنسا والبرازيل، وكشفت النتائج عن أن «الرؤساء التنفيذيين يخشون ما لا يعرفونه، بينما الكثير منهم لا يعتقدون أنهم مسؤولون عن حالة الأمن الإلكتروني لمؤسساتهم».

ورغم ذلك أظهرت الدراسة أن «هذا لم يؤد إلى مخاوف حيث يعتقد الأغلبية أنهم مستعدون بشكل جيد لسيناريو هجوم إلكتروني».

استشعار المسؤولية

وكشف التقرير عن أن 51% من الرؤساء التنفيذيين يشعرون بالمسؤولية بشكل كبير، حيث قالوا إنه «مع تزايد الهجمات الإلكترونية بسرعة فإن قدرتهم على الحفاظ على أمان أجهزة مؤسساتهم المتصلة بالإنترنت أمر يبقيهم مستيقظين أثناء الليل».

ولا تعرف الأغلبية حتى ما الذي يواجهونه حيث يشعر واحد فقط من كل ستة (16%) تقريباً، بأنهم يفهمون تماماً المخاطر التي تواجهها مؤسساتهم.

وحوالي خمسهم (21%) تقريباً يعتبرون أنفسهم مسؤولين بالكامل عن الأمن الالكتروني لمؤسستهم، في حين أن ربعهم (24%) يرون أنه دور الرئيس التنفيذي لتقنية المعلومات؛ لكنهم يعتبرون أنفسهم أيضاً مسؤولين إلى حدٍ ما.

ولكن الأغلبية العظمى تعتقد أنهم مستعدون بشكل جيد؛ فما يقرب من أربعة من كل خمسة (78%) واثقون بخططهم (الكاملة والمجربة) للحماية من التهديدات وإمكانية الاسترداد، حيث صرح 74% بأن مؤسساتهم يمكنها التكيف بسهولة مع التهديدات المتغيرة.

وفي الوقت ذاته سيعمل الثلث فقط (36%) مع فريق الاستجابة في حالة وقوع هجوم، وسيدفع 34% الفدية في حالة تعرضه لهجوم برمجيات الفدية.

الفدية ليست الحل

ويعارض كلٌ من خبراء الأمن الإلكتروني والقانونيين بشدة دفع الفدية، ويدعون إلى استخدام حلول النسخ الاحتياطية، لأن دفع الفدية المطلوبة ممن قام بالهجمة الإلكترونية لا يضمن استعادة النشاط التجاري لبياناته، ولا يضمن عدم تعرضه للهجوم مرة أخرى، فربما يتعرض له في اليوم التالي مباشرة من جهة أخرى أو من ذات الجهة. والمبلغ الذي يحصلون عليه من هذه الفدية، ربما يستخدمونه في تمويل هجمة جديدة ما يؤدي إلى تفاقم المشكلة. ورغم ذلك، فإن العديد من المؤسسات تفعل ذلك، لأنها ترى أنه أسرع طريقة لاستئناف عملها.