إسرائيل ملجأ السعودية في الحرب الافتراضية

بيّن تقير "سيسكو" السنوي للأمن الإلكتروني لعام 2017 الأثر المالي المحتمل للهجمات على المؤسسات باختلافها من الشركات الكبرى إلى المشاريع الصغيرة والمتوسطة. فقد واجهت أكثر من 50 في المئة من المؤسسات، انتقاداً جماهيرياً بعد التعرض لخرق أمني، بينما كانت الأنظمة المالية والعمليات هي الأكثر تأثراً.

كشف تقرير "سيسكو" السنوي للأمن الإلكتروني لعام 2017 أن أكثر من ثلث المؤسسات التي واجهت خرقاً أمنياً في عام 2016 تعرضت لخسائر ملموسة تمثلت في فقدان العملاء أو الإيرادات بنسب تفوق 20 في المئة.

وتعمل 90 في المائة من تلك المؤسسات على تعزيز تقنيات ضد التهديدات بعد التعرض للهجوم، وذلك من خلال الفصل بين وظيفتي تقنية المعلومات والأمن. وأكد قادة العمليات الأمنية أن 65 في المئة من المؤسسات تستخدم منتجات أمنية يراوح عددها بين ستة وأكثر من 50 منتجاً، ما يزيد احتمال اتساع الثغرات في الكفاءة الأمنية.

وفي عامه العاشر، سلّط التقرير العالمي الضوء على الفرص التي تواجهها فرق الأمن في دفاعها ضد التطور المستمر للجريمة الإلكترونية والتغير الدائم في أنماط الهجوم. ولاستغلال تلك الثغرات، تظهر بيانات تقرير "سيسكو" أن المجرمين الالكترونيين يقودون عودة لأساليب الهجوم الكلاسيكية، كالإعلانات الضارة والبريد الإلكتروني التطفلي.

ويعتبر البريد الإلكتروني التطفلي مسؤولاً عن حوالي ثلثي 65 في المائة من مجموع رسائل البريد الإلكتروني. وفي ظل تزايد القرصنة الالكترونية والتي تعد من أكثر مهددات تدمير الأمن المعلوماتي انتشاراً، اعتمد برنامج "التحول الوطني" ضمن "رؤية 2030" في السعودية مبادرات لتعزيز التحول الرقمي المشترك تماشياً مع التزام الرؤية بتنمية البنية التحتية الرقمية.

وسمح الاحتلال الإسرائيلي مؤخراً لشركات إسرائيلية مختصة بمكافحة القرصنة الإلكترونية "السايبر" ببيع منتجاتها التكنولوجية للسعودية. ويأتي ذلك بهدف شراء خدمات استخبارية متعلقة بـ"السايبر" لمصلحة العائلة المالكة، حيث جرى تزويد السعوديين ببرمجيات ساعدتهم على متابعة الرأي العام السعودي على

الشبكة العنكبوتية.