

سوء التفاهم يتسبب في 67% من الحوادث الأمنية التقنية



أقر 67% من كبار المديرين في الإمارات والسعودية، بأن سوء التفاهم مع أقسام تقنية المعلومات أو فرق الأمن التقني في مؤسساتهم، أدى إلى وقوع حادث أمن رقمي واحد على الأقل فيها. وفي المقابل أشار 37% من المديرين التنفيذيين من غير المختصين في مجال تقنية المعلومات، إلى تراجع التعاون بين مختلف فرق العمل. وقال 42% منهم إن الموقف يجعلهم يشككون في مهارات زملائهم وقدراتهم عندما يصبح التواصل مع موظفيهم العاملين في مجال أمن تقنية المعلومات غير واضح.

وأجرت «كاسبرسكي» دراسة استطلاعية عالمية شملت أكثر من 1,300 من قادة الأعمال، لتحديد مدى تأثير التفاهم بين المديرين التنفيذيين من جهة، و فرق أمن المعلومات من جهة أخرى، في القدرة المؤسسية على الصمود. ومن ناحية أخرى، كانت دراسة تحليلية أجرتها شركة «فورستر» حديثاً أظهرت أن الشركات تقضي في المتوسط 37 يوماً، وتنفق 2.4 مليون دولار للكشف عن خرق أمني رقمي والتعافي منه.

ووفقاً لنتائج الدراسة، فإن جميع الموظفين تقريباً من غير العاملين في مجال تقنية المعلومات (97%) قد تعرّضوا لموقف يتعلق بأمن تقنية المعلومات انطوى على سوء تفاهم. أما بشأن العواقب، فغالباً ما تؤدي إشكاليات التواصل إلى

تأخّر كبير في المشاريع (63%)، ووقوع حوادث في الأمن الرقمي (62%). وقال نحو ثلث المستطلعة آراؤهم (24% و29%) على التوالي، إنهم واجهوا هذه المشكلات أكثر من مرة. وتشتمل الآثار السلبية الأخرى على الخسائر المالية، وفقدان موظفين مهمين، وتدهور العلاقات بين فرق العمل، وهي مواقف حدثت لـ60% من المشاركين في الدراسة. وإضافة إلى التأثير السلبي في مؤشرات الأعمال، فإن من شأن التواصل المبهم مع موظفي أمن تقنية المعلومات، أن يؤثر أيضاً في الحالة العاطفية للفريق ويثير تساؤلات المديرين التنفيذيين حول مهارات موظفي أمن تقنية المعلومات وقدراتهم. من ناحية أخرى، أقر 30% من المديرين التنفيذيين بأن سوء التفاهم يُفقد الثقة في سلامة سير العمل، بينما قال 32% منهم، إن هذا الوضع يجعلهم متوترين، ما يؤثر في أداء عملهم.

وبهذه المناسبة، أكد أليكسي فوفك، رئيس أمن المعلومات لدى كاسبرسكي، أن وضوح التواصل بين المديرين التنفيذيين للشركة وإدارة أمن تقنية المعلومات شرط أساسي لنجاح منظومة الأمن المؤسسي. وقال: «يُكمن التحدي هنا في أن نضع أنفسنا في محلّ الآخرين، حتى نستطيع أن نتوقع ونمنع حدوث سوء التفاهم. وهذا يعني من ناحية، وجوب أن يعرف كبار مسؤولي أمن المعلومات لغة الأعمال الأساسية، لكي يتمكنوا من شرح الأخطار بشكل أفضل، وتوضيح الحاجة إلى تدابير السلامة. كما ينبغي لكبار مسؤولي الأعمال في المقابل، أن يعرفوا أن أمن المعلومات في القرن الحادي والعشرين جزء أساسي من الأعمال التجارية، وأن تخصيص جزء من الموازنات له يعد استثماراً في حماية أصول الشركة».