الخليج

اقتصاد, آراء وتحليلات, مقالات

26 يناير 2023 21:36 مساء

الميزانية الكبيرة لا تكفي.. على التنفيذيين قيادة الأمن السيبراني

الكاتب

عمر كشتعاري

يتغير العالم باستمرار، ويتغير معه مشهد التهديد السيبراني؛ حيث أدى نقل الشركات لأنظمتها وعمليّاتها وشبكاتها وبياناتها إلى شركات سحابية إلى ظهور تهديدات سيبرانية بشكل مستمر، والتي تشكّل خطراً على وجود الشركات واستقرارها.

أصبح الأمن السيبراني من أبرز المخاوف للمديرين التنفيذيين وقادة الأعمال على حد سواء؛ حيث إن هذه الهجمات تشكّل خطراً كبيراً على أمن مؤسساتهم ونموّها. زاد هذا الخطر خلال الجائحة، عندما بدأ الناس يعملون عن بُعد، ممّا خلق نقاط ضعف جديدة ضمن نظام الشركات. وبما أن هذا التغيير يحمل في طياته الكثير من المخاطر فإنه بنفس الوقت يوفر فرصاً جديدة للشركات التي تقوم بإدارة عمليات الأمن السيبراني الخاصة بها بشكل صحيح.

وهذا ما أدى إلى زيادة أهمية التخطيط الاستراتيجي لعمليات الأمن السيبراني من قِبل المناصب القيادية واعتباره أولوية قصوى لاستراتيجية الشركة.

وعلى الرغم من زيادة الاستثمار في الأمن السيبراني، فإن الحوادث والآثار والتكاليف المرتبطة به آخذة في الارتفاع. فقد أنه في عام 2021 واجهت الشركات ما معدله 270 هجوماً إلكترونياً بزيادة (Accenture) وجدت الأبحاث من شركة قدرها 31% على العام السابق. ونتيجة لذلك، ارتفعت التكاليف المتعلقة بأمن الشركات؛ حيث من المتوقع أن تدفع الأعمال حول العالم ما يصل إلى 10.5 تريليون دولار سنوياً نتيجة للحوادث السيبرانية.

هناك تحوّل ملحوظ في طريقة تخطيط الأمن السيبراني وتنفيذه؛ حيث شغل في السنتين الأخيرتين قائمة أولويات المديرين التنفيذيين. وأصبحت مسؤولية وضع استراتيجية الأمن السيبراني الصائبة وإطلاقها وتنفيذها لا تقع على عاتق الرئيس التنفيذي لأمن المعلومات فقط؛ بل يشاركه بها جميع المسؤولين على مستوى الإدارة العليا مباشرةً، لا سيّما من

.قبل الرؤساء التنفيذيين والرؤساء الماليين؛ إذ لا يريد أحد المخاطرة بأمن الشركة

لتحقيق النجاح في هذا النموذج الجديد، يجب على الرؤساء التنفيذيين مواءمة فرقهم التشغيلية والأمنية ضمن استراتيجية واحدة موحّدة لخلق بيئة آمنة وموثوقة لعملائهم وموظفيهم ومورّديهم؛ حيث أظهرت أحدث الدراسات من (Accenture) المتعلقة بمرونة الأمن السيبراني، أن 5% فقط من الشركات تنجح في هذه المواءمة بشكل صحيح، مما يخلق فرصاً وميزة تنافسية غير مسبوقة للشركات التي تأخذ أمن المعلومات على محمل الجد.

مسؤولية أمن الشركة ليست مختصة بموظفي تكنولوجيا المعلومات وحدهم؛ فهي مسؤولية جماعية لكل من يعمل داخل المنظمة؛ حيث إن المخاطر الأمنية للشركة، يمكن أن تتأثر بسوء سلوك أو إهمال من قِبل أي موظف لديها. وقد تنجم تهديدات داخلية عن موظّفين غير مبالين أو غير مطّلعين، سواء كانت هذه التهديدات من موظفين حاليين أو سابقين. وكلما امتلك الموظف امتيازات خاصة تمكنه من الوصول إلى موارد أكثر حساسية للشركة، ازدادت خطورة التهديدات الداخلية للأمن السيبراني؛ لذا فمن المهمّ التعاون على الصعيد الداخلي مع الموارد البشرية للحرص على إطلاع جميع الموظّفين وتوعيتهم حول تهديدات الأمن السيبراني، والتأكد من منح الموظّفين الامتيازات أو حقوق الوصول الضرورية لعملهم فقط، ومنع حقوق الوصول إلى المعلومات عن الموظفين السابقين.

على إدارة تقنية المعلومات أن تتضمن كفاءات ومتخصصين في مجال الأمن السيبراني، لتكون قادرة على مواجهة أيّ هجمات سيبرانية مستهدفة. وهنا يكمُن الفرق بين أمن المعلومات والأمن السيبراني؛ حيث يعنى فريق تكنولوجيا المعلومات بالإصلاح والدعم، بينما يختص فريق الأمن السيبراني في التأمين والحماية وإيجاد الثغرات الأمنية للمؤسسة.

ومع ذلك، لا تزال هناك فجوة في المواءمة بين الرؤساء التنفيذيين لأمن المعلومات وكبار القادة الآخرين في الشركة. ويأتي سوء الفهم هذا من الاعتقاد القديم بأن الأمن السيبراني هو مسؤولية تقنية المعلومات فقط، وليست تحدياً تجارياً فريداً يتطلب مجموعة مختلفة من المهارات ومنهجية تفكير مختلفة كلياً. إضافة إلى أن فرق تكنولوجيا المعلومات التقليدية غير مجهزة للتعامل مع وابل من الهجمات التي تواجهها المنظمات بشكل يومي.

في الأغلب تؤدي هذه المعتقدات الخطأ إلى عزل فرق أمن المعلومات، بدلاً من وصفها بعامل تمكين استراتيجي مضمّن في نسيج المنظمة. مع زيادة اعتماد الحوسبة السحابية، فإن تقنيات اتصال إنترنت الأشياء والجيل الخامس، تجعل عالمنا أكثر اتصالاً من أي وقت مضى. على نحو متزايد، يتم اتخاذ قرارات شراء تقنيات جديدة بواسطة تطبيقات خارجية بدلاً من التعديل على البنية التحتية لتكنولوجيا معلومات الشركة. على الرغم من أن هذا المنهج قد يوفر المال والوقت، فإنه يعرض الشركة إلى مخاطر مستقبلية باهظة التكاليف. على النقيض، إذا ما تمت إدارة عمليات الأمن السيبراني بشكل صحيح عبر تقييم المخاطر وإدارتها مقدماً، فلن يؤدي هذا النهج إلى توفير الوقت والمال على المدى الطويل فحسب؛ بل سيؤدي أيضاً إلى زيادة الثقة والمرونة الإلكترونية في هذا العصر الرقمي الجديد.

يعد الأمن السيبراني تحدياً جديداً نسبياً، وسيتطلب فهمه تعاوناً أكبر بين الرؤساء التنفيذيين للشركة والرؤساء التنفيذيين لأمن المعلومات وقادة الأعمال الرئيسيين الآخرين في الشركة. سيتطلب ذلك من الرؤساء التنفيذيين طرح الأسئلة الصعبة، ودراسة مؤسساتهم بشكل معمّق لتحديد وتقييم المخاطر الإلكترونية على نحو فعّال، وأن يكونوا على دراية أكبر بأحدث طرق تقديم المبادرات الأمنية. مما سيؤدي إلى المزيد من الازدهار والتناغم بين فريق أمن المعلومات وكافة فرق المؤسسة الداخلية.

لقد تبنّت مجموعة اكويتي نهجاً شاملاً للدفاع الإلكتروني يعمل على مواءمة الأشخاص والعمليات والتكنولوجيا معاً في انسجام تام لبناء استراتيجية موحّدة متماسكة فيما يتعلق بالأمن السيبراني. تتضمن هذه الاستراتيجية أفضل الممارسات والمبادئ المتعلقة بأمن المعلومات على جميع مستويات العمل، بدءاً من مجلس الإدارة ووصولاً إلى الفرق التشغيلية وغيرها من الفرق. ونقوم في إكويتي بتعزيز مكانتنا كواحد من أكثر وسطاء الخدمات المالية الموثوق بهم عبر وضع الأمن السيبراني على قائمة أولوياتنا ومواكبة التحديات التي تنشأ عن تطوّر مشهد التهديد السيبراني بشكل مستمر.

«الرئيس التنفيذي لأمن المعلومات، مجموعة «إكويتي *