ترنيمة الإدارة العليا
TONE at TOP®

تزود الإدارة العليا ومجالس الإدارة ولجان التدقيق بمعلومات موجزة عن مواضيع الحوكمة.

العدد ١٢٥ | أكتوبر ٢٠٢٤

دور المجلس في الصمود السيبراني

هل شركتك على استعداد للتصدي للهجمات السيبرانية القادمة؟ تتوقع معظم المؤسسات أن تواجه هجومًا سيبرانيًا في المستقبل، ويتوقع قادة الأعمال والأمن السيبراني بأن أعمالهم ستتعرقل نتيجة حدث سيبراني في الاثني إلى أربعة عشر شهرًا المقبلة، وذلك وفقًا لمؤشر سيسكو لجاهزية الأمن السيبراني لعام ٢٠٢٤.

يترتب على الهجمات السيبرانية العديد من العواقب، مثل اختراق البيانات ذات الطبيعة الحساسة، وشلّ العمليات، والإضرار بالعلاقات مع الأطراف الثالثة، والإضرار بسمعة الشركة. وفي تقرير "المخاطر تحت المجهر لعام ٢٠٢٥" الصادر عن معهد المدققين الداخليين، صنف قادة التدقيق الداخلي الأمن السيبراني كأكبر خطر بهامش كبير عن الفئات الأخرى من المخاطر. وأفادوا بأن الأمن السيبراني هو المجال الذي يقضي عليه التدقيق الداخلي معظم وقته وجهده.

ووفقًا لنفس التقرير، يتربع الأمن السيبراني على قمة المخاطر التي يتوقع القادة أن توجهه مؤسساتهم في غضون ثلاث سنوات من الآن، وذلك مع الصعود السريع للثورة الرقمية (بما في ذلك الذكاء الاصطناعي) مقارنة بالمسوح السابقة ليحوز على المرتبة الثانية. وذكر التقرير أن: "الذكاء الاصطناعي يزيد من مخاطر الأمن السيبراني ومخاطر الاحتيال حول العالم"، ويأتي الأمن السيبراني على رأس المجالات التي يؤثر عليها الذكاء الاصطناعي تأثيرًا سلبيًا.

وفي بيئة لا يرد فيها السؤال عما إذا كان الهجوم سيحدث، بل متى سيحدث، يكون الصمود السيبراني حاسمًا في مساعدة الشركات لمواجهة هذا الهجوم. ويمكن للشركات بذل جهود حثيثة لحماية نفسها من الهجمات السيبرانية، ويجب عليها لزامًا أن تكون مستعدة لمواجهة هذه الهجمات والتعافي منها.

الصمود السيبراني هو "القدرة على توقع الظروف السلبية والضغوط والهجمات والاختراقات للأنظمة التي تستخدم أو تعتمد على الموارد السيبرانية ومواجهتها والتعافي منها والتكيف معها. ويهدف الصمود السيبراني إلى تمكين تحقيق أهداف المهام أو الأعمال التي تعتمد على الموارد السيبرانية في البيئات السيبرانية المحفوفة بالنزاعات" — المعهد الوطني للمعايير والتكنولوجيا

التوقعات الجديدة للمجالس

تعكف الجهات التنظيمية والمساهمون على دراسة مسؤوليات المجلس في مجال الأمن السيبراني ويضعون توقعات جديدة ليتمكن المديرون من مراقبة مواطن الضعف في مؤسساتهم. وبموجب قاعدة نهائية بعنوان: "إدارة مخاطر الأمن السيبراني، والاستراتيجية، والحوكمة، والافصاح عن الحوادث"، تحدد هيئة الأوراق المالية والبورصات الأمريكية الإفصاحات المطلوبة من الشركات العامة، وعلى الأخص التي تتناول الإفصاح عن حوادث الأمن السيبراني الجسيمة، والإفصاحات الدورية حول كيفية قيام الشركة المسجلة بتقييم المخاطر وتحديدها وإدارتها، وكذلك عن دور الإدارة في تقييم هذه المخاطر وإدارتها. كما تنص القواعد النهائية على الإفصاح عن رقابة المجلس على مخاطر الأمن السيبراني.

كجزء من دورها الرقابي، يجب على المجالس ضمان وضع المديرين التنفيذيين والفرق التابعة لهم معايير عالية للأمن السيبراني، وفقًا لمقالة صادرة عن ماكنزي تحت عنوان: "مجالس الإدارة: الدفاع النهائي للأمن السيبراني في الشركات الصناعية". ويجب عليهم بعد ذلك الرقابة على جهود الأمن السيبراني، وتحديد مستوى تحقيق الأهداف، وما إذا كانت الفرق تتحمل مسؤولية الأمن السيبراني. وتذكر المقالة أن: "المجلس هو خط الدفاع الأخير في ضمان التخطيط لهذه المبادرات وتوفير التمويل اللازم لها".

الأمن السيبراني مُصمم لجعل من الصعب على المؤسسات الاستمرار في تسيير أعمالها كالمعتاد. ويتمحور الصمود السيبراني حول البقاء على اطلاع وعلى استعداد بحيث تكون الخيارات والأولويات واضحة عند حدوث أزمة. ولضمان بقاء المؤسسة على أهبة الاستعداد، يجب على المجالس تحديد ما إذا كانت هناك خطط موثقة لإدارة الأزمات، والاستجابة للحوادث، والتعافي من الكوارث، وأن هذه الخطط تخضع للاختبار بصورة دورية من قبل الإدارة باستخدام تدريبات المحاكاة النظرية، وذلك وفقًا لكتاب بعنوان: "الإشراف على المخاطر السيبرانية: دور مجلس الإدارة" الصادر عن شركة برايس ووتر هاوس كوبرز. ويجب أن تركز التمارين على تحديد أدوار ومسؤوليات واضحة لتوضيح عملية اتخاذ القرارات الإدارية أثناء الأزمات.

تتلقى العديد من المجالس بطاقة أداء أو لوحة تحكم سيبرانية من الإدارة تسلط الضوء على المخاطر الحالية والتقدم المحرز في تحقيق أهداف الأمن السيبراني. وتشير شركة برايس ووترهاوس كوبرز "PwC" في هذا السياق إلى عدة مجالات يمكن أن تكون جزءاً من تقرير مرفوع للمجلس:

- خطة استراتيجية متعددة السنوات وخطة عمل للسنة الحالية.
- تفاصيل حول تخصيص موارد الأمن السيبراني موزعة حسب التمويل والموظفين.
- تقييم النضج باستخدام إطار عمل معترف به، مثل إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا والابتكار.
- عملية جرد للأنظمة ذات المهام الحرجة يتم تحديثها بانتظام.
- ملخص للمخاطر السيبرانية الرئيسية للمؤسسة.
- مراجعة للحوادث الأمنية الهامة التي تعرضت لها المؤسسة.
- معلومات عن جهود تدريب الموظفين وتوعيتهم.
- تفاصيل عن إطار عمل جاهزية المؤسسة للحوادث، بما في ذلك معلومات عن بوليصة التأمين السيبراني.
- تفاصيل حول استراتيجية الطرف الثالث لمواجهة المخاطر السيبرانية.
- المعلومات التي تقيس جهود المؤسسة مقارنةً بنظيراتها.
- تفاصيل حول التطورات القانونية والتنظيمية الرئيسية ذات الصلة.
- الدروس المستفادة من الهجمات السيبرانية الأخيرة.

في حين أن حماية المؤسسة من الهجمات أمرٌ بالغ الأهمية، إلا أنه يجب على المجالس التذكر بأن الحماية لوحدها تقتصر على معالجة القضايا التي تعلم المؤسسة مسبقًا بوجودها. وللأسف وبفضل تسلحهم بالأدوات التكنولوجية الجديدة التي تستخدم الذكاء الاصطناعي، فإن المجرمين السيبرانيين المبتكرين يطورون باستمرار طرق جديدة لإحداث الضرر. ولذلك، "لتخفيف المخاطر السيبرانية بشكل سليم، يجب على قيادة الشركات وضع خطط قوية وصلبة للاستجابة والتعافي السريعين لتتمكن الشركات من الأستمرار في أعمالها"، نقلًا عن مقال معهد ماساتشوستس للتكنولوجيا بعنوان: "الآن تتحمل مجالس إدارة الشركات مسؤولية الأمن السيبراني أيضًا".

نبذة عن معهد المدققين الداخليين

معهد المدققين الداخليين (IIA) جمعية مهنية عالمية غير ربحية يضم أكثر من ٢٤٥,٠٠٠ عضوًا عالميًا، وقد منح أكثر من ٢٠٠,٠٠٠ شهادة مدقق داخلي معتمد (CIA) في جميع أنحاء العالم. وتأسس المعهد في عام ١٩٤١م، ويُعرف عالميًا بأنه الجهة الرائدة في مهنة التدقيق الداخلي التي تقدم المعايير والشهادات والتعليم والبحوث والإرشادات الفنية. لمزيد من المعلومات، تفضلوا بزيارة الموقع: theiia.org.

The IIA

1035 Greenwood Blvd.
Suite 401
Lake Mary, FL 32746 USA

الاشتراك المجاني

تفضلوا بزيارة theiia.org/Tone للتسجيل والاشتراك المجاني.

آراء القرّاء

أرسلوا اسئلتكم وتعليقاتكم إلى البريد الالكتروني:
Tone@theiia.org

التدقيق الداخلي: شريك موثوق في مجال الأمن السيبراني

يجب على المجلس أن تكون واعية بالقيمة التي يمكن أن تضيفها وظائف التدقيق الداخلي إلى جهود الأمن السيبراني، حيث يقدم التدقيق الداخلي خدمات تأكيد ومشورة فريدة وموضوعية ومستقلة في مجال استراتيجية الأمن السيبراني والحوكمة والضوابط. ويشير مقال برايس ووترهاوس كوبرز إلى أن: "العديد من الشركات تستفيد من المدققين الداخليين لمراجعة العمليات والضوابط السيبرانية، بما فيها القدرة على الصمود والاستجابة"

يمكن لوظائف التدقيق الداخلي المساهمة في الصمود السيبراني من خلال عدة طرق، مثل تدقيق عمليات التعافي من الحوادث السيبرانية والاستجابة لها. ويطرح تقرير المخاطر تحت المجهر للسنة الماضية بعض أوجه القيمة التي يمكن أن يضيفها المدققون الداخليون، وتشمل القائمة التي ما زالت سارية حتى اليوم:

- تقييم مستوى الوعي والمعارف والمهارات في الأجزاء الرئيسية للشركة - مثل المجلس — لضمان أن تكون استجابات الأمن السيبراني فعّالة وتواكب العصر.
- تقييم التسلسل الإداري بين رئيس أمن المعلومات، ورئيس المعلومات، والمجلس لضمان التواصل الواضح بخصوص المخاطر وتعميم التوصيات، مع إمكانية تصعيدها إلى أعلى مستوى عند الضرورة.
- تقييم مدى تواتر وتوقيت وفعّالية حملات محاكاة اختبار التصيد الاحتيالي وغيرها من أنشطة التوعية ومستويات مشاركة الموظفين، وكذا مدى تكامل الموظفين مع عمليات التدريب والمتابعة.
- تنفيذ سيناريوهات لتثقيف المجلس بشأن مسؤولياتهم في مجال الحوكمة واختبار مدى فعالية واكتمال عمليات التخفيف من المخاطر.
- تقييم مدى فعّالية بيئة الرقابة الداخلية ومدى تضمين الضوابط في الخطين الأول والثاني وفقًا لنموذج الخطوط الثلاثة لمعهد المدققين الداخليين الداخليين، مع إيلاء اهتمام خاص للممارسات التي يجدها الموظفون معرقلة أو تطفلية ومن المحتمل أن يتجاهلها الموظفون أو ينسوها أو يتحايلوا عليها.
- تقييم مدى نجاح هيكل الحوكمة في المؤسسة في تمكين التعاون خلال الخطوط الثلاثة.
- تحديد مدى مراقبة المؤسسة للمستجدات العالمية في لوائح الأمن السيبراني والتكنولوجيا، ومدى سهولة تغيير الضوابط الداخلية لتلبية المتطلبات المستقبلية.

مخاطر متزايدة ومتطورة

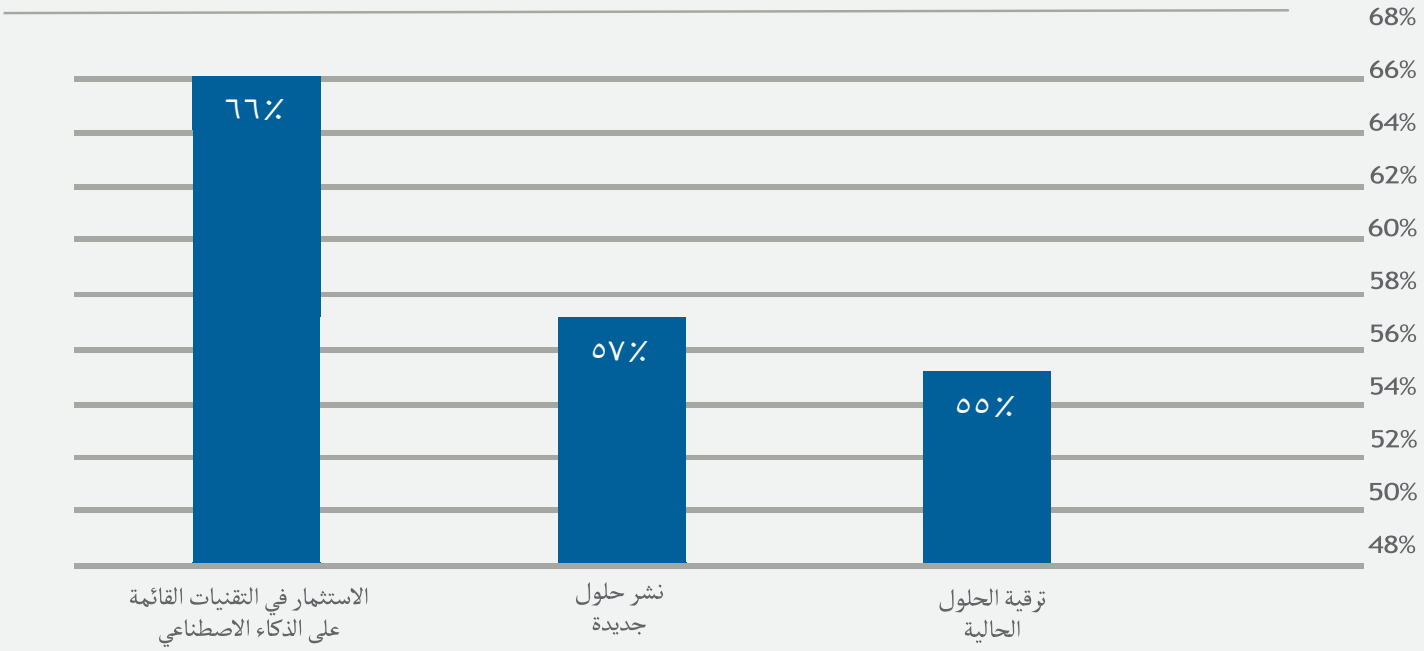
مع التطور السريع الذي تشهده التكنولوجيات الجديدة، فإن العديد من الأدوات الجديدة تجعل تنفيذ الهجمات السيبرانية أكثر سهولة. وعلى الرغم من أن الذكاء الاصطناعي ونحوه من الأدوات يُمكن أن تعزز جهود الأمن السيبراني، إلا أنها يمكن أن تُسهل أيضًا التصيد الاحتيالي والرسائل غير المرغوب فيها، والابتزاز والإرهاب، والتضليل والتدخل في الانتخابات، وفقًا لجين إيسترلي، رئيسة وكالة الأمن السيبراني وأمن البنية التحتية التابعة للحكومة الفيدرالية. وتشير أيضًا إلى أن الذكاء الاصطناعي التوليدي يُتيح للمهاجمين السيبرانيين فرصًا جديدة ويسمح للمجرمين السيبرانيين الأقل تطورًا بإحداث الفوضى.

يجب أن يلجأ أعضاء المجلس إلى فرق التدقيق الداخلي لديهم للحصول على معلومات ونصائح مهمة حول أفضل طريقة لمنع الهجمات السيبرانية وتقييم سرعة الاستجابة للهجمات بمجرد حدوثها. ويمكن للمدققين الداخليين تقديم تقييمات مستقلة لبيئة الرقابة وأي مخاطر محددة يمكن أن تساعد في تمكين المؤسسة من التعافي على أكمل وجه من أي هجوم.

أسئلة لأعضاء المجالس:

- كيف نرصد التهديدات السيبرانية الجديدة، بما فيها كيفية استجابة المؤسسات الأخرى لها؟
- كيف تقيس المؤسسة قدرتها على الصمود السيبراني وتقيّمها؟
- كيف نستخدم هذه المعلومات لتكييف استعدادنا للهجوم واستجاباتنا المحتملة؟
- ما هي خططنا للتعافي من الكوارث؟ ما مدى نجاحها في الماضي؟ ماذا تعلمنا من تلك التجارب؟
- ما هي الوظائف المسؤولة مسؤولية مباشرة عن استراتيجيات الصمود السيبراني؟
- هل يدرك كافة الموظفون الحاجة للصمود السيبراني والدور الذي يمكن أن يؤديه في هذا المجال؟

كيف تُعزز الشركات من أمنها السيبراني؟



المصدر: مؤشر سيسكو لجاهزية الأمن السيبراني لعام ٢٠٢٤.