آراء ورؤى عالمية

الأمن السيبراني

الجزء الأول: التوظيف والتطوير للجيل القادم

الجزء الثاني: الذكاء الاصطناعي - صديق الأمن السيبراني وعدوه

الجزء الثالث: إدارة مخاطر الطرف الثالث للأمن السيبراني

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام ناجي فياض وعضوية السيد محمد شهاب والسيدة داليا ابو كروم

The Institute of Internal Auditors

المحتويات

الجزء 1: التوظيف والتطوير للجيل القادم

نبذة عن الخبراء

أنيتا وابيرسكا ، CISA

أنيتا هي مديرة أمن المعلومات ومنتجات الامتثال في AuditBoard. لديها أكثر من 15 عاما من الخبرة في مجالات تدقيق تكنولوجيا المعلومات والامتثال وانضمت إلى AuditBoard للتركيز على جهود تطوير المنتجات التي تخدم مستخدمي مخاطر تكنولوجيا المعلومات والامتثال ، والاستفادة من خبرتها في الصناعة. بدأت أنيتا حياتها المهنية في KPMG و PwC ، حيث ساعدت العملاء على تنفيذ وتقييم أطر عمل مثل SOC 1 و SOC 2. عملت مع شركات من مختلف الأحجام لتنفيذ وإدارة برامج الامتثال ذات التعقيد المتفاوت، بما في ذلك إدارة السياسات على مستوى الشركة، وبرامج إدارة مخاطر الطرف الثالث، وعملت عن كثب مع الإدارة لتنفيذ الضوابط لتلبية متطلبات إطار الأمان، والعمل مع الإدارة التنفيذية لضمان الامتثال يدعم الأهداف الاستراتيجية للشركة.

عدي جولفادي ، CISA ، CAMS ، CPA ، CIA

عدي هو العضو المنتدب في مجموعة النزاعات والامتثال والتحقيقات في ستاوت ، ويشارك في قيادة ممارسات الامتثال التنظيمي والجرائم المالية على المستوى الوطني. عدي هو قائد في مجال الجرائم المالية والتدقيق الداخلي وتدقيق نظم المعلومات والممارسات الاستشارية للمخاطر ولديه أكثر من 20 عاما من الخبرة. وهو متخصص في تقديم المشورة لمجالس الإدارة ولجان التدقيق والإدارة العليا بشأن الامتثال للجرائم المالية الأكثر تحديا ، وتكنولوجيا المعلومات ، والمخاطر السيبرانية ، والحوكمة ومسائل المخاطر والامتثال بما في ذلك إدارة مخاطر المؤسسة ، وحوكمة برنامج مكافحة غسل الأموال والعقوبات ، والتحقق من صحة النماذج ، والتدقيق الداخلي القائم على المخاطر ، وتكنولوجيا المعلومات ، وتدقيق وضوابط الأمن السيبراني. يتراوح عملاء عدي من بعض أكبر البنوك والمؤسسات المالية في العالم إلى شركات الخدمات المالية الأصغر.

مقدمة

يشكل الأمن السيبراني تهديدا كبيرا للمؤسسات بغض النظر عن حجمها. *تعكس الأمثلة الحديثة مدى السرعة التي يمكن أن تسوء بها الأمور. أدى هجوم إلكتروني إلى تعطيل الشحنات من شركة Ace Hardware Corporation إلى تجارها وأجبرها على وقف خدمة طلبات العملاء عبر الإنترنت مؤقتا. وأدى هجوم آخر طالب بفدية على شركة اتصالات تشيلية كبرى إلى تعطيل الخدمات بما في ذلك مراكز البيانات والوصول إلى الإنترنت والصوت عبر بروتوكول الإنترنت. ومما يدل على أن الكيانات الأصغر يمكن أن تتأثر أيضا ، توقف الوصول العام عبر الإنترنت إلى سجلات الأراضي وفهارس المواليد والوفيات والزواج بسبب هجوم إلكتروني في مقاطعة كاباروس ، نورث كارولاينا.*

يعد التدقيق الداخلي مناسبا تماما للعب دور رئيسي في المساعدة على إدارة المخاطر السيبرانية، ولكن يجب أن يكون لديه الموارد التي يحتاجها لأداء هذا الدور. يجب أن يكون لديه المعرفة والمهارات اللازمة لتحديد وتقديم المشورة بشأن التهديدات السيبرانية التي تواجه المؤسسة. عند إجراء تقييم للأمن السيبراني ، "من الأهمية بمكان إشراك متخصصي التدقيق الذين يتمتعون بالعمق المناسب للمهارات الفنية والمعرفة ببيئة المخاطر الحالية" ، وفقا لشركة Deloitte.[1]

هذا الموجز هو الأول في سلسلة من ثلاثة أجزاء حول الأمن السيبراني. نظرا لأن قادة التدقيق الداخلي يجب أن يفهموا التهديدات قبل أن يتمكنوا من توظيفها لمواجهتها، فإنها تبدأ بدراسة تحديات الأمن السيبراني للمدققين الداخليين ومؤسساتهم. كما يغطي الخيارات والاستراتيجيات التي يمكن لقادة التدقيق الداخلي اتباعها لضمان حصولهم على المواهب التي يحتاجونها لمعالجة المخاطر السيبرانية المستمرة.

[1] "الأمن السيبراني ودور التدقيق الداخلي - دعوة عاجلة للعمل" ، شركة Deloitte Development LLC ، 2017.

تهديد واضح

لا يزال الأمن السيبراني يمثل أكبر المخاطر

جهود الأمن السيبراني للتدقيق الداخلي تتزايد

*"**يجب على المدققين الداخليين النظر إلى المؤسسة بأكملها** واتخاذ نهج قائم على المخاطر" ، قالت أنيتا وابيرسكا ، CISA ، مديرة أمن المعلومات ومنتجات الامتثال في AuditBoard. "المخاطر السيبرانية على رأس القائمة بالنسبة لمعظم المؤسسات."*

يبدو أن المدققين الداخليين يدركون جيدا التهديد الذي تشكله المخاطر السيبرانية. تم تحديد الأمن السيبراني باعتباره الخطر الأكبر في عام 2024 ، وفقا لمسح عالمي لقادة التدقيق الداخلي أجرته مؤسسة التدقيق الداخلي. تم إدراج الأمن السيبراني ، إلى جانب رأس المال البشري واستمرارية الأعمال ، كأهم ثلاثة مخاطر في استطلاع المخاطر تحت المجهر 2024[2] لأكثر من 4,200 رئيس تنفيذي للتدقيق (CAEs) ، حيث أدرج 73٪ من المشاركين الأمن السيبراني كأكبر خمسة مخاطر.

في أمريكا الشمالية، وصف 78٪ من قادة التدقيق الداخلي الأمن السيبراني بأنه خطر مرتفع أو مرتفع جدا في مؤسساتهم، وفقا لمعهد المدققين الداخليين لعام 2023 نبض أمريكا الشمالية للتدقيق الداخلي.[3] كان المدققون الذين شملهم الاستطلاع يكرسون 10٪ من خطط التدقيق الخاصة بهم للأمن السيبراني ، بينما تشكل مخاوف تكنولوجيا المعلومات 9٪ أخرى. بالإضافة إلى ذلك ، قام ما يقرب من 70٪ من الوظائف بمراجعة المجالات عالية المخاطر التي تشمل الأمن السيبراني وتكنولوجيا المعلومات سنويا أو بشكل مستمر ، وفقا لنتائج استطلاع Pulse.

تتضمن بعض مخاطر الأمن السيبراني التي يجب وضعها في الاعتبار ما يلي:

- *الانتهاكات التي تمكن المجرمين من سرقة المعلومات الهامة أو التي تعرض بيانات العملاء أو شركاء الأعمال.*
- *هجمات برامج الفدية التي تجعل من المستحيل على المؤسسات أداء الوظائف الرئيسية أو الوصول إلى المعلومات الضرورية دون دفع فدية لمجرمي الإنترنت أولا.*
- *البرامج الضارة التي يمكن أن تعيث فسادا في النظام.*

للهجمات الإلكترونية عواقب تتجاوز ما هو واضح ، مثل الخسائر المالية عند تعطل وظائف العمل أو إذا فقد العملاء أو شركاء الأعمال الثقة في المؤسسة وتوقفوا عن التعامل معها. والأكثر من ذلك، بمجرد اكتشاف حادث إلكتروني، يجب على المؤسسات استثمار الوقت والمال في تحقيقات الطب الشرعي لفهم ما حدث ومتى، وإجراء العلاج لإصلاح أي ضرر، وتحديد ما إذا كانت تداعيات مثل هذه الهجمات جوهرية من المنظورين المالي والتشغيلي من أجل تلبية متطلبات إعداد التقارير التنظيمية.

ليس من المستغرب إذن أن يتوسع الإنفاق على الأمن السيبراني بسرعة. في بداية عام 2023 ، توقعت Canalys أن يقفز الإنفاق العالمي على الأمن السيبراني بنسبة 13.2٪ خلال العام ، مع احتمال أن يصل إلى 224 مليار دولار.[4]

و قال عدي جولفادي ، CISA ، CAMS ، CPA ، CIA ، العضو المنتدب في مجموعة النزاعات والامتثال والتحقيقات في Stout "لقد أدركت الشركات أن هذه التهديدات تحمل عواقب تجارية ومالية حقيقية للغاية"، و" إن التهديدات كلها بالتأكيد على رأس اهتمامات لجان التدقيق ، و "يطلب من التدقيق الداخلي تكثيف وتوفير الضمانات في هذه المجالات".

---

[2] "المخاطر تحت المجهر 2024" ، مؤسسة التدقيق الداخلي ، 2023

[3] "نبض التدقيق الداخلي في أمريكا الشمالية 2023," معهد المدققين الداخليين ، 2023

[4] "الاستثمار في الأمن السيبراني ينمو بنسبة 13٪ في عام 2023" ، 18 ، Canalys يناير 2023 ، https://www.canalys.com/newsroom/cybersecurity-forecast-2023

التحديات

نهج الأمن السيبراني ، التوظيف المناسب لنضج المؤسسة

الفهم الواضح للبيئة السيبرانية أمر أساسي

لتوظيف الأشخاص المناسبين لمساعدة التدقيق الداخلي في دعم إدارة المخاطر السيبرانية *وتزويدهم بفرص التطوير المناسبة ، من المهم أن نفهم تماما ظروف ومخاطر الأمن السيبراني الفريدة للمؤسسة. وينبغي النظر في عدة عوامل وتحديات.*

عقلية يدوية

اعتاد العديد من فرق التدقيق الداخلي تقليديا على التفكير في الضوابط الداخلية والعمليات المختلفة من منظور يدوي. ومع ذلك ، فإن التحول الرقمي المستمر للأعمال يتطلب أن تكون الفرق على دراية بكيفية قيام الحلول الرقمية بتعزيز وتحسين عمليات التدقيق الداخلي والعمليات الأخرى في جميع أنحاء المؤسسة ، بما في ذلك الأمن السيبراني. وفي الوقت نفسه، يجب على المدققين الداخليين أيضا فهم المخاطر التي يشكلها التحول الرقمي نفسه على المؤسسات، حيث يستغل مجرمو الإنترنت المتطورون بشكل متزايد نقاط الضعف التي يمكن أن تخلقها البيئات الرقمية.

على سبيل المثال ، إذا كانت المؤسسة تعمل في السحابة أو تستخدم أو تخطط لاستخدام أي تقنية متقدمة أو ناشئة ، فستحتاج إلى أشخاص عملوا مع هذه الأدوات. ليس من الضروري أن يكون أعضاء الفريق خبراء في التكنولوجيا ، كما قال Waberska ، ولكن التعرض للبيئة السحابية أو الحلول الأخرى سيوفر معرفة أكبر بالمخاطر ذات الصلة. بالإضافة إلى التوظيف لهذه المهارات ، يجب أن تتأكد فرق التدقيق أيضا من تضمين التقنيات الجديدة في تدريبها وتطوير الموظفين الحاليين.

الضوابط الداخلية

يتم تدريب المدققين الداخليين للتأكد من أن المؤسسة لديها الضوابط المناسبة للحماية من المخاطر التي تواجهها. فيما يتعلق بالمخاطر السيبرانية ، يجب أن تعمل الضوابط الداخلية على ضمان عدم تعرض تكنولوجيا المعلومات الخاصة بالمؤسسة للخطر وأن وظائف العمل يمكن أن تظل قيد التشغيل.

لتحديد مخاطر الأمن السيبراني وتقديم المشورة بشأنها ، ستحتاج فرق التدقيق الداخلي إلى أن تكون على دراية بضوابط أمن تكنولوجيا المعلومات للتقنيات التي تستخدمها مؤسستهم. في العمل مع السحابة ، على سبيل المثال ، ستختلف عناصر التحكم عن تلك المستخدمة مع مراكز البيانات الداخلية ، كما قال Waberska. سيحتاجون أيضا إلى فهم الضوابط المناسبة بالنظر إلى التهديد الذي يمكن أن تشكله الجريمة الإلكترونية على الخصوصية والآثار المترتبة على خطط التدقيق لبرنامج الخصوصية في مؤسستهم.

لوائح الإفصاح وحماية البيانات

تتم دعوة المؤسسات الآن إلى أن تكون أكثر انفتاحا بشأن الإبلاغ عن جهود الأمن السيبراني الخاصة بها. سيتعين على المدققين الداخليين فهم القواعد التي تؤثر على شركاتهم وأن يكونوا قادرين على تقييم احتياجات الامتثال. في أحد الأمثلة المهمة ، في أغسطس 2023 ، أصدرت لجنة الأوراق المالية والبورصات الأمريكية قرار نهائي بشأن إدارة مخاطر الأمن السيبراني والاستراتيجية والحوكمة والإفصاح عن الحوادث ، والذي يتطلب من الشركات المدرجة توفير قدر أكبر من الشفافية عندما تتعرض لهجوم إلكتروني والكشف عن معلومات محددة حول جهودها للتخفيف من المخاطر السيبرانية. وقدم معهد المراجعين الداخليين تعليقات على القرار عندما كان في مرحلة الاقتراح. وهي تخطط

لمواصلة العمل مع هيئة الأوراق المالية والبورصات لتطوير إرشادات التنفيذ ، خاصة فيما يتعلق بتحديد أهمية الحادث السيبراني وتحديد مصطلح "الأمن السيبراني" بشكل أفضل.

نظرا لطبيعة الأعمال التجارية المتعددة الجنسيات بشكل متزايد والعدد المتزايد من لوائح الأمن السيبراني في جميع أنحاء العالم ، يجب أن يصبح المدققون الداخليون على دراية بجميع قوانين أمن البيانات والخصوصية التي قد تؤثر على مؤسساتهم ، مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي. والواقع أنه وفقا لمؤتمر الأمم المتحدة للتجارة والتنمية، وضع 137 بلدا من أصل 194 بلدا تشريعات لضمان حماية البيانات والخصوصية.

أنظمة تكنولوجيا المعلومات

إن أي مؤسسة لديها حتى التكنولوجيا الأساسية هي في الواقع تتعامل مع نوع من أنظمة تكنولوجيا المعلومات ، وكلها عرضة للمخاطر السيبرانية. نظرا لحجم الأنظمة ونقاط الضعف والتهديدات المحتملة التي تنطوي عليها ، من المهم للشركات والتدقيق الداخلي فهم الأنظمة الأكثر أهمية. "لن نتمكن أبدا من وضع نفس المستوى من الضوابط حول جميع الأنظمة" ، أشار Waberska. سيتضمن تحديد الأولويات طرح أسئلة مثل:

- ما هي الأنظمة الاساسية والحاسمة لعمل المؤسسة؟ من الممكن الإجابة على هذا السؤال من خلال النظر فيما إذا كانت المؤسسة ستتمكن من الاستمرار في إدارة الأعمال أو تحقيق الأهداف الرئيسية بدونها وإلى متى.
- أي من هذه الأنظمة يعالج البيانات الأكثر حساسية؟ قد يشمل ذلك معلومات الشركة السرية أو معلومات التعريف الشخصية (PII).
- أي منها يحتوي على بيانات فريدة أو يصعب استبدالها؟[5]

الأطراف الثالثة

عادة ما تلجأ المؤسسات الصغيرة والمتوسطة الحجم الى أطراف ثالثة للتعامل مع بياناتها. يمكن أن يحدث ذلك من خلال تطبيق سحابي أو ، بالنسبة للمؤسسات الكبيرة ، من خلال مركز معالجة في الخارج. وأشار جولفادي إلى أن هؤلاء الأطراف قد يتعاملون مع البيانات التنظيمية المهمة ومعلومات تحديد الهوية الشخصية للعملاء ، وقد يتم وضع البيانات في أي مكان في العالم. لهذا السبب ، "من المهم للغاية فهم المشهد الكامل لأصول تكنولوجيا المعلومات" ، بما في ذلك مكان وجودها وما إذا كانت الضوابط المناسبة موجودة حول تلك الأصول ، كما قال.

يجب على المؤسسات تقييم عمليات الأمن السيبراني للأطراف الثالثة قبل مشاركة البيانات معها ومراقبة تلك العمليات بمجرد أن تبدأ الأطراف الثالثة في استخدام البيانات ، وفي بعض الحالات تحتفظ بالحق في تدقيق الأطراف الثالثة. قال Waberska: "إذا كنت تشارك بيانات العملاء مع طرف آخر ، فأنت بحاجة إلى التأكد من أنهم سيحمونهم بنفس الطريقة التي ستحميها شركتك". يجب على الشركات مراجعة تقارير التصديق الخاصة بطرف ثالث مثل SOC 2 ، والتي تقيم ضوابطها الداخلية لمعرفة مدى معالجتها للمخاطر ، أو أنواع أخرى من الضمانات أو الشهادات المتعلقة بحماية فئات البيانات ذات الصلة.

ضمان الوصول الآمن والتوافر

وأشار غولفادي إلى أن هناك مفاضلة بين التأكد من قدرة المؤسسة على حماية البيانات والأنظمة وفي الوقت نفسه ضمان توفر المعلومات والأنظمة للاستخدام حسب الحاجة لتحقيق أهداف العمل. للحفاظ على التوازن ، سيتعين على المؤسسات اختيار عناصر التحكم التي تحمي البيانات دون جعل الوصول إلى المعلومات الضرورية لخدمة العملاء أو وظائف العمل المهمة الأخرى مرهقا. يجب أن يكون هذا التحديد أسهل بمجرد أن تنظر المؤسسة في الأنظمة التي تتطلب أعلى مستوى من الأمان. قد يحتاج البعض إلى الحماية باستخدام المصادقة متعددة العوامل وبروتوكولات التشفير وبرامج منع فقدان البيانات ، بينما لن يتطلب البعض الآخر هذا المستوى من الدقة.

---

[5] "رؤى CISA - الأصول السيبرانية الآمنة عالية القيمة (HVAs)" ، وزارة الأمن الداخلي الأمريكية ، https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-SecureHighValueAssets_S508C.pdf

تعزيز موارد التدقيق الداخلي

لا يزال التوظيف في مجال الأمن السيبراني يمثل أولوية قصوى

توظيف وتطوير المواهب السيبرانية للتدقيق الداخلي

في خضم كل هذه المخاطر، كيف يمكن للتدقيق الداخلي بناء *فريق يمكنه معالجتها* ***والحفاظ عليه*** *؟ ستختلف تفاصيل الإجابة حسب المؤسسة ، ولكن هناك بعض التوصيات التي تنطبق على الجميع.*

ابحث عن مزيج من المهارات

لمعالجة المخاطر السيبرانية، تحتاج فرق التدقيق الداخلي إلى فهم عميق للجانب التقني للأمن السيبراني بالإضافة إلى القدرة على فهم العواقب التي قد تترتب على القضايا الأمنية على الأعمال. في الماضي ، كان مدققو تكنولوجيا المعلومات يميلون إلى أن يكونوا أقوياء في الجوانب التقنية لأمن المعلومات ، لكنهم في كثير من الأحيان لم يركزوا على كيفية تأثير المخاطر ذات الصلة على قدرة المؤسسة على تحقيق أهداف أعمالها. يمكن أن تكون القدرة على توضيح تأثير الأعمال ذات قيمة خاصة إذا احتاج التدقيق الداخلي إلى الحصول على موافقة الإدارة للاستثمارات اللازمة في التكنولوجيا أو الضوابط المحسنة أو التوظيف الإضافي.

تشهد جولفادي المزيد من الجهود لبناء فرق تمزج المعرفة التقنية مع فهم أهداف العمل والعمليات وسلاسل القيمة. في بعض الحالات، تجد فرق التدقيق الداخلي مهنيين يتمتعون بكلتا المهارتين، ولكن في حالات أخرى، تضم الفرق مهنيين تكمل مهاراتهم بعضها البعض. يمكن للمؤسسة النظر في تقديم التدريب لإعطاء كل نوع من المهنيين معرفة عملية أساسية بالانضباط الآخر.

دمج المهارات في التقنيات الناشئة

تضيف العديد من فرق التدقيق الداخلي محترفين ذوي خبرة في تحليلات البيانات والذكاء الاصطناعي والتعلم الآلي بينما يبتعدون عن طريقة الاختبار القائم على العينات. "يمكنك استخدام الذكاء الاصطناعي لاختبار مجموعة البيانات كاملة وتحسين الكشف عن الحالات الشاذة" ، قال جولفادي. وهذا لا يعزز الكفاءة والموثوقية فحسب، بل يساعد أيضا المدققين الداخليين على مواكبة مجرمي الإنترنت، الذين أصبحوا أكثر تطورا في استخدامهم للتقنيات الجديدة.

النظر في الاستعانة بمصادر خارجية

تجلب بعض فرق التدقيق الداخلي فريقا خارجيا لتعزيز المهارات الفنية أو الخاصة بعمل المؤسسة. يمكن دمج المهنيين ذوي الخبرة المتخصصة في الأمن السيبراني أو أمن تكنولوجيا المعلومات في فريق التدقيق الداخلي على أساس مشروع مؤقت أو على المدى الطويل حسب الحاجة. عندما يعمل أعضاء فريق التدقيق الداخلي جنبا إلى جنب مع هؤلاء الخبراء ، يمكنهم مساعدة الخبراء على تعزيز معرفتهم والخوض بشكل أفضل في عمليات الشركة وإجراءاتها. في الوقت نفسه ، يمكن أن يساعد العمل مع الخبراء الخارجيين في توسيع قاعدة معارف أعضاء الفريق. عند تقييم خيار الاستعانة بمصادر خارجية ، توصي جولفادي بفحص شهادات أعضاء الفريق وخبراتهم السابقة للتأكد من أنها تتطابق مع مهارات الفريق الحالية أو تعززها.

ضع في اعتبارك التعاون

في بعض الأحيان قد تكون الخبرة التي يحتاجها فريق التدقيق الداخلي متاحة داخليا في مجالات مثل تكنولوجيا المعلومات أو الأمن أو الامتثال. تقدم الشراكة الجيدة ، مع الحفاظ على استقلالية المدقق ، أعضاء فريق التدقيق الداخلي إلى مجموعة من الأفكار والمعرفة الجديدة حول النظام البيئي التكنولوجي للمؤسسة ومخاطرها. كما أنه يمهد الطريق لعمليات تدقيق مثمرة في المستقبل لأن الفرق الأخرى ستعرف أن التدقيق

الداخلي يشاركهم هدفهم المتمثل في حماية المؤسسة من المخاطر غير الضرورية وضمان قدرتها على تحقيق أهدافها. يمكن أن يساعد التواصل المفتوح الفرق الأخرى في التغلب على أي قلق بشأن أهداف التدقيق الداخلي أيضا. "تركز فرق تكنولوجيا المعلومات والأمن على إصلاح المشكلات المهمة وإيجاد الحلول" ، قال Waberska. "إنهم يفهمون المخاطر والحاجة إلى تخفيفها. إن قدرة التدقيق الداخلي على إجراء محادثة تركز على المخاطر تفسر سبب ضرورة وجود ضوابط معينة لجعل التدقيق الداخلي أكثر فعالية".

بناء العلاقات الداخلية

يمكن لجميع أعضاء فريق التدقيق الداخلي الاستفادة من بناء والحفاظ على العلاقات مع المهنيين الآخرين في فرق الأمن والامتثال وتكنولوجيا المعلومات في مؤسستهم للتعرف على عملهم الحالي، حتى لو لم يتعاونوا في مشروع معين. قال وابرسكا: "إن فهم ما يحدث في بيئة الشركة أمر مهم للغاية" ، ويمكن لهذه العلاقات أن تضمن حصول الفريق على تحديثات في الوقت المناسب. وقالت إن عمليات التدقيق المحددة ستكشف عن الاتجاهات والتهديدات ، "لكن من الأفضل معرفة ما الذي يتغير في أقرب وقت ممكن".

الاستفادة من الموارد المتاحة

وقال وابرسكا: "إذا خصصت فرق التدقيق الداخلي وقتا لتعلم التقنيات الحديثة على الأقل على مستوى عال والمخاطر التي تأتي معها ، فإنها ستبقى على اطلاع دائم بالمخاطر الحالية والناشئة". وتشمل الخيارات مركز موارد الأمن السيبراني التابع لمعهد المدققين الداخليين، والذي يتضمن مجموعة متنوعة من إرشادات الأمن السيبراني والأبحاث وبرامج الشهادات والمعلومات حول المؤتمرات ذات الصلة، مثل المؤتمر الافتراضي السنوي للأمن السيبراني الذي ينظمه معهد المدققين الداخليين. يوفر AuditBoard مجموعة متنوعة من موارد الأمن السيبراني ، والتي يمكن الوصول إليها من خلال صفحة الموارد الخاصة به .

يستكشف برنامج Risk in Focus 2024 ، من مؤسسة الدراسات التابعة للمعهد الدولي للمدققين الداخليين، مخاطر الأمن السيبراني على مستوى العالم ويقدم وجهات نظر إقليمية فريدة حول كيفية النظر إلى الأمن السيبراني والمخاطر الرئيسية الأخرى وإدارتها في جميع أنحاء العالم.

استنتاج

وجد استطلاع نبض معهد المدققين الداخليين لعام 2023 أن نمو موظفي التدقيق الداخلي *آخذ في الازدياد ولكنه لم يعد بعد إلى مستويات ما قبل جائحة كورونا. يجب أن يتذكر قادة التدقيق الداخلي أن الأجيال القادمة إلى القوى العاملة تتمتع بالذكاء الرقمي. وأشار غولفادي إلى أنه من الذكاء التفكير في أفضل الطرق لاستخدام المعرفة التي يجلبونها. كما ستميز متاجر التدقيق الداخلي نفسها في بيئة توظيف تنافسية من خلال توفير الفرصة لجيل جديد لاستخدام التقنيات الناشئة مثل الذكاء الاصطناعي والتعلم الالي لتقديم رؤى من شأنها أن تساعد في حل مشاكل العمل الحرجة. مع استمرار التدقيق الداخلي في إعادة بناء الفرق أو توسيع خبراتهم لمواجهة تحديات جديدة، يجب عليهم استخدام النصائح والرؤى الواردة في هذا الموجز في تخطيطهم.*

الجزء 2: الذكاء الاصطناعي - صديق الأمن السيبراني وعدوه

نبذة عن الخبراء

أنيتا وابيرسكا ، CISA

أنيتا هي مديرة أمن المعلومات ومنتجات الامتثال في AuditBoard. لديها أكثر من 15 عاما من الخبرة في مجالات تدقيق تكنولوجيا المعلومات والامتثال وانضمت إلى AuditBoard للتركيز على جهود تطوير المنتجات التي تخدم مستخدمي مخاطر تكنولوجيا المعلومات والامتثال ، والاستفادة من خبرتها في الصناعة. بدأت أنيتا حياتها المهنية في KPMG و PwC ، حيث ساعدت العملاء على تنفيذ وتقييم أطر عمل مثل SOC 1 و SOC 2. عملت مع شركات من مختلف الأحجام لتنفيذ وإدارة برامج الامتثال ذات التعقيد المتفاوت، بما في ذلك إدارة السياسات على مستوى الشركة، وبرامج إدارة مخاطر الطرف الثالث، وعملت عن كثب مع الإدارة لتنفيذ الضوابط لتلبية متطلبات إطار الأمان، والعمل مع الإدارة التنفيذية لضمان الامتثال يدعم الأهداف الاستراتيجية للشركة.

تيري جرافنشتاين ، CGAP ، CRISC ، CISA ، CISSP ، CPA ، CIA ، CGEIT

تيري هو نائب الرئيس الأول لمجلس الإدارة العالمي لمعهد المدققين الداخليين (IIA) لعام 2023-24 والرئيس التنفيذي للتدقيق في الاتحاد الائتماني الفيدرالي للبنتاغون (PenFed). وقد تم تكريمها من قبل معهد المدققين الداخليين كواحدة من "أفضل عشرة قادة لفكر التدقيق في العقد" لمساهماتها في المهنة المتعلقة بالسايبر والتكنولوجيا، كما تم إدخالها في قاعة ممارسي التدقيق المتميزين في معهد المدققين الداخليين. وقد شغلت مناصب قيادية في سيتي بنك وديلويت وشغلت منصب المفتش العام المعين لمجلس النواب الأمريكي.

مقدمة

يعتبر الأمن السيبراني كأهم المخاطر للمدققين الداخليين *، وسيظل هذا هو الحال في المستقبل المنظور. في الواقع ، إنه الخطر الفردي الذي يستهلك الحيز الأكبر من وقتهم وجهدهم ، وفقا ل Risk In Focus 2024. وسألت سلسلة التقارير، التي أعدتها مؤسسة التدقيق الداخلي التابعة لمعهد المدققين الداخليين، الرؤساء التنفيذيين والمديرين التنفيذيين للتدقيق من جميع أنحاء العالم عن أهم المخاطر التي تواجهها مؤسساتهم، وكيف يتوقعون أن تتغير صورة التهديد في السنوات الثلاث المقبلة.*

تظهر نتائج المخاطر تحت المجهر لعام 2024 مدى تعقيد الأمن السيبراني كخطر والتحديات الإضافية الناجمة عن التغيرات شبه المستمرة في التكنولوجيا وكيف يمكن استخدامها. وقد انعكس هذا أيضا في نتائج التقرير. ومن المتوقع أن يرتفع خطر الاضطراب الرقمي من المركز الخامس الى المركز الثاني على قائمة التهديدات في غضون ثلاث سنوات.

يتناول هذا الموجز، وهو الثاني في سلسلة من ثلاثة أجزاء حول الأمن السيبراني، كيفية مساهمة الذكاء الاصطناعي في تحديات وفرص الأمن السيبراني، وما يحتاج المدققون الداخليون إلى معرفته حول مجال المخاطر الناشئ والمتطور لأخذه بالاعتبار حول الأمن السيبراني. يحمل الذكاء الاصطناعي وعدا كبيرا كأداة متطورة لتحسين الكفاءة والإنتاجية وإدارة المخاطر في أي مؤسسة تقريبا. ومع ذلك ، فإنه يطرح أيضا تحديات جديدة لإدارة المخاطر ، بما في ذلك الاعتبارات الأخلاقية ، ومخاطر التحيز الرقمي ، والاعتماد المفرط أو الأعمى على استخدام الذكاء الاصطناعي. في حين أنه يمكن أن يكون أداة قيمة في المعركة ضد الهجمات الإلكترونية ، إلا أن الجهات الفاعلة السيئة تستخدمها أيضا لارتكاب جرائمها.

الذكاء الاصطناعي في العمل

سيف إلكتروني ذو حدين

يجب أن يستكشف التدقيق الداخلي استخدامات وتهديدات الذكاء الاصطناعي

يشير مصطلح الذكاء الاصطناعي إلى التكنولوجيا التي يمكن أن تحاكي الذكاء البشري *، مثل التعلم والتفكير والعمل على حل مشكلة صعبة. وهو يشمل عدة أنواع من التقنيات ، بما في ذلك التعلم الآلي* (Machine learning) *، أو قدرة النظام على التعلم من البيانات وتطبيق هذا التعلم.*

إحدى الطرق التي يمكن أن يعزز بها الذكاء الاصطناعي والتعلم الآلي بشكل كبير جهود الأمن السيبراني هي اكتشاف التهديدات وتحليل البيانات ، كما قالت أنيتا وابيرسكا ، مديرة أمن المعلومات ومنتجات الامتثال في AuditBoard. يحاول مجرمو الإنترنت التسلل إلى شبكة المؤسسة من خلال البحث عن نقاط الضعف وتحطيم دفاعات الشبكة. في الماضي ، اعتمدت المؤسسات على مسؤولي النظام لمنع هذه التهديدات الخارجية. ومع ذلك ، بسبب تقدم الأتمتة والتقنيات الأخرى ، فإن الحجم المتزايد من المحاولا من الجهات الفاعلة السيئة قد طغى على القدرة على المراجعة البشرية الفعالة ، على حد قولها. الذكاء الاصطناعي معالجة هذه المشكلة. يمكنه مراجعة كميات كبيرة من إدخالات الشبكة والتعرف على الأنماط والتعلم منها بمرور الوقت ، وفهم ما إذا كان حدث معين أو مجموعة من الأحداث يمكن أن تشكل تهديدا للمؤسسة. وقالت: "هذا هو أحد أكثر استخدامات الذكاء الاصطناعي تأثيرا في هذه البيئة".

بالإضافة إلى ذلك، تتمتع أدوات الكشف عن البرامج الضارة الأكثر تطورا بقدرات أفضل، بما في ذلك القدرة على حظر أحد أهم أسباب الخروقات الأمنية والحوادث - التصيد الاحتيالي. يمكن أن يقلل ذلك أو يزيل احتمالية حدوث أخطاء بشرية - مثل فتح رابط على بريد إلكتروني للتصيد الاحتيالي وتعريض شبكات الشركة للبرامج الضارة - لأن الأدوات تقوم بتصفيتها قبل وصولها إلى البريد الوارد لشخص ما ، كما قال Waberska. (راجع الشريط الجانبي لمزيد من المعلومات حول بعض الطرق التي يمكن الذكاء الاصطناعي من خلالها تحسين دفاعات الأمن السيبراني.)

يمكن الذكاء الاصطناعي أيضا البحث بسرعة عن الحالات الشاذة وتحديد المشكلات التي تحدث بالفعل داخل شبكة المؤسسة ، وهو أمر لا يستطيع البشر القيام به على مثل هذه البيانات واسعة النطاق. ومن الأمثلة على ذلك الوصول غير المصرح به إلى أنظمة الشركة. يمكن للموظف السابق إتاحة الوصول عن غير قصد لمجرم الإنترنت من خلال مشاركة كلمة مرور أو كتابتها أو قد يعيد الدخول إلى النظام بقصد ضار بنفسه. في الماضي ، كان على المدقق الداخلي الذي يتحقق من

- *تعزيز المكافحة الذكية للتهديدات من خلال جمع المعلومات الأمنية من مجموعة من المصادر، والبحث بشكل استباقي عن التهديدات، والمساعدة في إدارة التهديدات من خلال تخفيف عبء العمل على محللي أمن الشركة.*[6]

استخدام الذكاء الاصطناعي كأداة للأمن السيبراني

وفقا لجمعية IEEE Computer Society ، تتضمن بعض الطرق التي يمكن الذكاء الاصطناعي من خلالها تعزيز دفاعات الأمن السيبراني للمؤسسة ما يلي:

- *الكشف عن الأنشطة الخبيثة ، من خلال قياس الأنشطة المقبولة وتحديد الحالات الشاذة والتهديدات بشكل مستمر وفي الوقت الفعلي.*
- *دعم تحديد تهديدات البرامج الضارة من خلال فحص خصائص الملفات أو أنماط التعليمات البرمجية لاكتشاف تلك غير الآمنة.*
- *تحسين قدرة الشركة على التعامل مع هجمات يوم الصفر أو التهديدات الأخرى غير المعروفة.*

[6] "الذكاء الاصطناعي للأمن السيبراني والجريمة السيبرانية: كيف يحارب الذكاء الاصطناعي نفسه" ، غوراف بيلاني ، جمعية IEEE للكمبيوتر ، 6 سبتمبر 2023.

الوصول غير المصرح به بين العمال السابقين إجراء مقارنة يدوية للأشخاص الذين لديهم إمكانية الوصول وأولئك الذين لم يعد ينبغي أن يكون لديهم ، ثم كتابة بريد إلكتروني إلى فريق تكنولوجيا المعلومات يوضح بالتفصيل أي مشكلات ، كما أشار تيري جرافنشتاين ، كبير مسؤولي التدقيق في الاتحاد الائتماني الفيدرالي في البنتاغون. يمكن للذكاء الاصطناعي ، من ناحية أخرى ، البحث عبر منصات متعددة ، ومقارنة البيانات في نظام كشوف المرتبات ونظام الوصول ، وإنشاء بريد إلكتروني إلى الفرق المناسبة حول أي حالات شاذة.

يجب أن يدرك المدققون الداخليون أن أهداف مجرمي الإنترنت ليست في كثير من الأحيان مجرد سرقة البيانات ، ولكن التسلل إلى الأنظمة وتعطيلها عن طريق تغيير البيانات ، كما قال جرافنشتاين. على المستوى الدولي، يمكن للجهات الفاعلة السيئة التلاعب بالبنية التحتية الحيوية للدولة، مثل النقل والطاقة النووية والخدمات المصرفية وغيرها الكثير، ولكن العواقب يمكن أن تكون كبيرة أيضا بالنسبة للمؤسسات من أي حجم كانت.

اعتبارات إدارة المخاطر

القيم الأخلاقية والتحيز والاعتماد المفرط

يمكن أن يساعد التدقيق الداخلي المؤسسات على تجنب مشاكل الذكاء الاصطناعي

إلى جانب فوائدها العديدة *، يأتي الذكاء الاصطناعي مع قائمة اعتبارات المخاطر الخاصة بها. بعض التهديدات هي داخلية ولكنها يمكن أن تكون ضارة مثل الهجمات الإلكترونية.*

القيم الأخلاقية

تتعلق العديد من المخاوف في هذا المجال بنماذج الذكاء الاصطناعي التوليدية (Generative AI) *واللغات الكبيرة*(Large Language) *التي يمكن استخدامها من قبل المدققين الداخليين لإنشاء التقارير وكتابة التعليمات البرمجية ورسم التوصيات والتحليلات، من بين احتمالات أخرى. ومع ذلك ، فإن هذه الأدوات تثير أيضا أسئلة أمنية وأخلاقية للمؤسسات. "هناك خطر من أن ينظر الموظفون إلى هذه الأدوات على أنها لعبة" ، قال جرافنشتاين.*

وقالت إن الضوابط السيبرانية التقليدية المستخدمة في التقنيات السابقة تنطبق أيضا على هذه الأنظمة ، لكن "تداعيات عدم القيام بذلك بشكل جيد تتضخم". من بين أمور أخرى ، كما سيتم مناقشته بمزيد من التفصيل ، يمكن للأنظمة توفير معلومات متحيزة أو غير دقيقة أو ملفقة تماما ، اعتمادا على كيفية تدريبهم. يشير Grafenstine أيضا إلى العواقب المكلفة والمحرجة المحتملة على أعمال الشركة وسمعتها إذا كانت تستخدم روبوت محادثة يواجه العملاء تم تدريبه على بيانات الإنترنت ذات المصادر السيئة والإجابات غير الصحيحة، خاصة عندما يكون لروبوت الدردشة تأثير سلبي كبير على العملاء. لهذه الأسباب ، يجب أن تكون هناك مراجعة بشرية لأي شيء ينتجه نظام الذكاء الاصطناعي التوليدي عندما لا تكون المؤسسة على دراية كاملة بالبيانات التي تم تدريبها عليها. "يجب على الشركة أن تمتلك الإجابات" ، قال جرافنشتاين.

في حين أن استخدام برامج الذكاء الاصطناعي التوليدية مثل ChatGPT قد انفجر منذ ظهورها لأول مرة في أواخر عام 2022 ، فإن نشر المعلومات على الذكاء الاصطناعي التوليدية المتاحة للجمهور يمكن أن يعرض بيانات الشركة أو العميل ومعلومات التعريف الشخصية ، تماما كما قد تفعل حادثة قرصنة ، وهي اعتبار كبير للمخاطر. عندما ينشر الموظفون استعلامات تتضمن معلومات الشركة في برامج الذكاء الاصطناعي التوليدية العامة ، سيحتفظ البرنامج بهذه المعلومات وربما يستخدمها للرد على استفسارات أخرى خارج المؤسسة ، مما يعرضها للعرض العام. وحذر جرافنشتاين من أن هذا لا يمكن أن ينشر المعلومات السرية فحسب ، بل يمكن للجهات الفاعلة السيئة أيضا استخدام التفاصيل التي يكتشفونها في الذكاء الاصطناعي التوليدية المتاحة للجمهور لهندسة طريقهم إلى أنظمة الشركة ، باستخدام التصيد الاحتيالي أو أدوات أخرى.

الاعتماد المفرط الأعمى على مخرجات الذكاء الاصطناعي

أي محترف هو المسؤول في النهاية عن الأدوات التي يستخدمونها والمعلومات التي يولدونها. وينطبق هذا بشكل خاص على المدققين الداخليين، الذين يمكن أن ينتهكوا معاييرهم الخاصة إذا اعتمدوا كثيرا على البيانات أو المحتوى الذي لم يتم التحقق من صحته. "أن تكون موثوقا به هو اختصاصنا " ، قال جرافنشتاين.

التحيز الخوارزمي ***Algorithmic Bias***

يتم تدريب الآلات على التعلم بناء على خوارزميات محددة ويمكن أن تتأثر المعلومات التي تنتجها ، عن قصد أم لا ، بناء على تلك الخوارزميات. على سبيل المثال ، قد تقوم الخوارزميات بتصفية السير الذاتية للنساء المستخدمة في قرار التوظيف إذا كان الموظفون الحاليون في دور معين هم في الغالب من الذكور أو قد يفضلون طلبات الرهن العقاري من المشترين البيض إذا كان معظم حاملي الرهن العقاري الحاليين من البيض.[7] "إنهم لا يحاولون عمدا أن يكونوا خبيثين ، لكن التحيزات موجودة من الاساس" ، قال جرافنشتاين.

[7] "بالنسبة للأقليات ، يمكن لخوارزميات الذكاء الاصطناعي المتحيزة أن تلحق الضرر بكل جزء من الحياة تقريبا" ، المحادثة ، 24 ، www.theconversation.com أغسطس 2023.

حماية الذكاء الاصطناعي والحماية منها

الضوابط الداخلية ضرورية

حماية سلامة والوصول الى أنظمة الذكاء الاصطناعي

يعد الأمان على الذكاء الاصطناعي نفسه والقدرة على استخدامه من الاعتبارات الخطيرة الأخرى *للمؤسسات والمدققين الداخليين. يجب أن تكون هناك ضوابط على من يمكنه الوصول إلى موارد الذكاء الاصطناعي ، وكيفية حماية القدرة على تغيير التعليمات البرمجية ، ومن يسمح له بنقل المعلومات من منطقة الاختبار إلى الإنتاج. بصفتي مدققا داخليا ، "أريد التأكد من أنه يمكنني معرفة ما إذا كانت خوارزمية الذكاء الاصطناعي قد تم تغييرها أو إذا كان بإمكان شخص ما تعطيلها في منتصف العملية وتغييرها" ، قال جرافنشتاين. كما يجب أن يكون المدققون الداخليون على دراية بالنطاق المحتمل للتداخل. قالت: "إذا كان بإمكاني الوصول إلى الذكاء الاصطناعي لشركتك ، يمكنني تغييراكثر من مجرد معاملة ". بدلا من ذلك ، يمكن للمرتكب الوصول إلى مجموعة البيانات أو مستودع البيانات بالكامل للمؤسسة ، أو أي شيء آخر يمكن الذكاء الاصطناعي الوصول إليه.*

"فقط لأنك نفذت حلا يستفيد من الذكاء الاصطناعي لا يعني أنك الآن مضاد للرصاص ،"

أنيتا وابرسكا
AuditBoard

في الوقت نفسه ، من المهم أن تدرك أن الذكاء الاصطناعي تسهل على مجرمي الإنترنت إنشاء برامج ضارة بسرعة ، وأتمتة الهجمات ، وتحسين فعالية عمليات الاحتيال أو هجمات الهندسة الاجتماعية باستخدام أدوات مثل التزييف العميق ، والتي تغير مقاطع الفيديو أو الصور رقميا ، ومولدات الصوت لإنشاء صور أو رسائل خاطئة. "أصبح مشهد التهديد السيبراني أكثر خطورة ، ويلعب الذكاء الاصطناعي دورا كبيرا فيه" ، وفقا لمقال IEEE Computer Society.[8]

وقال وابيرسكا إن المدققين الداخليين يجب أن ينظروا إلى الذكاء الاصطناعي كأداة هجومية ودفاعية. وقالت: "لمجرد أنك نفذت حلا يستفيد من الذكاء الاصطناعي لا يعني أنك الآن مضاد للرصاص". في حين أن الهجمات السابقة غالبا ما شنها قراصنة واحد على مؤسسة واحدة ، يمكن الذكاء الاصطناعي تنفيذ هجمات على نطاق أوسع بكثير ، وضرب مؤسسات متعددة. يمكن الذكاء الاصطناعي تحسين البرامج الضارة من خلال التعلم من البرامج السابقة واستخدام هذه المعرفة لإنشاء برامج ضارة أقوى وأفضل ، والقيام بذلك بمفرده دون الحاجة إلى مطور. قال وابرسكا: "إذا كان الذكاء الاصطناعي يحاول اقتحام مؤسستك ، فقد يكون أقوى بكثير من الحل الحالي الخاص بك". يمكن للمدققين الداخليين التأكد من أن مؤسساتهم تفهم ومستعدة لمعالجة هذه المخاطر. لا يمكن لفريق التدقيق الداخلي تنفيذ الحلول ، ولكن يمكنهم إجراء محادثة مستنيرة مع فريق الأمن لمعرفة ما إذا كانوا يفكرون في هذه التهديدات وينفذون الحلول. وقال وابرسكا: "سيستغرق الأمر وقتا حتى تتبنى المؤسسات حلولا جديدة ، ولكن من المهم أن تكون على دراية بالتهديدات وأن يكون لديك خطة للدفاع عن نفسك".

لا تنس العنصر البشري

بينما تستعد المؤسسات لدرء التهديدات السيبرانية الخارجية، يجب على المدققين الداخليين أن يضعوا في اعتبارهم الخطر الذي تشكله التهديدات غير المقصودة التي يشكلها موظفوهم. تنجح محاولات التصيد الاحتيالي ، على سبيل المثال ، بسبب خطأ بشري في الفشل في إدراك أن مجرم الإنترنت يحاول الدخول إلى النظام أو إلى كلمة مرور مهمة أو بيانات سرية أخرى. قال وابرسكا: "يجب على المدققين الداخليين النظر في كيفية قيام المؤسسة بتثقيف المستخدمين حول هذه التهديدات". على وجه الخصوص ، قد لا يفهم الموظفون أن رسائل البريد الإلكتروني

[8] "الذكاء الاصطناعي للأمن السيبراني والجريمة السيبرانية: كيف يقاتل الذكاء الاصطناعي نفسه" ، غوراف بيلاني ، الاتجاهات التقنية لجمعية الكمبيوتر IEEE 6 ، سبتمبر 2023.

للتصيد الاحتيالي قد تطورت. في حين أنه كان من السهل في السابق اكتشاف العلامات الحمراء مثل الأخطاء الإملائية أو الخطوط الغريبة ، يتم استخدام الذكاء الاصطناعي لكتابة رسائل البريد الإلكتروني للتصيد الاحتيالي الأكثر تعقيدا وواقعية. وقالت: "إنها تبدو حقيقية للغاية ، ومن الأسهل بكثير على الجهات الفاعلة السيئة توليدها".

استنتاج

يعد تهديد الهجمات الإلكترونية سمة دائمة لممارسة الأعمال التجارية *في العالم الرقمي ، ويمثل الذكاء الاصطناعي واستخدامه المتطور تطورا جديدا واستفزازيا في معركة إدارة المخاطر ضد هذا التهديد. يلعب المدققون الداخليون دورا مهما في:*

- *التأكد من أن القيادة والفرق الرئيسية على دراية بالفوائد والمخاطر المتعلقة الذكاء الاصطناعي.*
- *تحديد وتقديم توصيات حول كيفية تعزيز الذكاء الاصطناعي جهود الأمن السيبراني المختلفة داخل المؤسسة.*
- *تعزيز الوعي بالحاجة إلى النظر في الدفاعات المحدثة ضد أدوات الهجوم السيبراني التي تعمل بالطاقة الذكاء الاصطناعي.*
- *توفير ضمان بشأن فهم الشركة واستخدامها لتقنيات الذكاء الاصطناعي.*

يمكن أن يكون الذكاء الاصطناعي والتقنيات ذات الصلة بمثابة موارد قيمة ، لكنها ليست حل نهائي. "يمكن أن تكون التطورات التكنولوجية رائعة طالما أنك تعرف كيفية استخدامها بطريقة ذكية وآمنة" ، قال Waberska. "يجب عليك دائما استخدام الحكم المهني في التفكير في ما تحصل عليه."

تذكر أيضا أنه في حين أن كونك متحفظا هو أحد مزايا المدققين الداخليين ، إلا أنه لا ينبغي أن يرفضوا التعاون ، كما قال جرافنشتاين. يجب على المدققين الداخليين تقديم مشورة جيدة بشأن الرقابة والمخاطر، بما في ذلك رؤى حول مخاطر الفشل في مواكبة التكنولوجيا. وقالت: "إنه خطر كبير عدم تبني التكنولوجيا ، لكننا بحاجة إلى القيام بذلك بطريقة مدروسة".

الجزء 3: إدارة مخاطر الأمن السيبراني للطرف الثالث

نبذة عن الخبراء

ريتشارد ماركوس ، TPECS ، CISM ، CRISC ، CISA

ريتشارد ماركوس هو نائب الرئيس لأمن المعلومات في AuditBoard ، حيث يركز على المنتجات والبنية التحتية وأمن تكنولوجيا المعلومات للشركات ، بالإضافة إلى قيادة المسؤولية عن مبادرات الامتثال الداخلي الخاصة ب AuditBoard. وبهذه الصفة ، أصبح مستخدما قويا لمنتج AuditBoard ، مستفيدا من مجموعة الميزات القوية للمنصة لتلبية حالات استخدام الامتثال وتقييم المخاطر والتدقيق.

جون أ. ويلر

جون أ. ويلر هو المؤسس والرئيس التنفيذي لشركة Wheelhouse Advisors ، وهي شركة استشارية تنفيذية عليا تساعد الشركات العالمية على تحقيق رؤية أكبر للمخاطر وفهمها. يستفيد من خبرته في إدارة المخاطر والأمن السيبراني والأعمال الرقمية والمخاطر التشغيلية وإدارة المخاطر المتكاملة لتوفير التوجيه الاستراتيجي والحلول التكنولوجية لعملائه.

مقدمة

أصبح العالم مترابطا بشكل متزايد ، والقطاعات الاقتصادية ليست استثناء. *اليوم ، يعتمد كل قطاع أعمال رئيسي تقريبا في بعض القدرات على أطراف ثالثة. في الأجيال السابقة ، ربما كان هذا في المقام الأول من منظور مادي ، حيث يعتمد طرف على آخر للحصول على السلع أو الخدمات. في حين أن هذا لا يزال صحيحا ، فقد أصبح الاتصال بين الأطراف الآن متشابكا مع العالم الرقمي.*

بطبيعة الحال ، في حين أن هناك العديد من الفوائد التي يمكن الحصول عليها من هذا الاتجاه - خاصة فيما يتعلق بالكفاءة والإنتاجية والوفاء بشكل أفضل بالتزامات الاستدامة - هناك أيضا مخاطر يجب أخذها في الاعتبار. وفقا لاستطلاع ديلويت العالمي لإدارة مخاطر الطرف الثالث لعام 2022 ، فإن 73٪ من المستجيبين لديهم الآن اعتماد متوسط إلى عالي المستوى على مزودي الخدمات السحابية من الأطراف الثالثة ، ومن المتوقع أن يرتفع هذا الرقم إلى 88٪ في السنوات القادمة.[9] ومع ذلك ، لكي تنجح هذه العلاقات ، يجب أن تكون هناك ثقة ضمنية بين المؤسسات بأن البيانات المنقولة ستكون آمنة قدر الإمكان ضد الهجمات الإلكترونية أو خروقات البيانات أو الحوادث السيبرانية الأخرى ذات الصلة. ولكسب هذه الثقة، يجب أن يكون لدى المؤسسات برنامج مخصص وشامل لإدارة مخاطر الطرف الثالث (TPRM) يمارس العناية الواجبة عند إعداد موردي الطرف الثالث ومراقبتهم باستمرار خلال دورة حياة العلاقة.

ومع ذلك ، فإن الحقيقة هي أنه في كثير من الأحيان تفترض الشركات الثقة دون بذل العناية الواجبة الكافية أولا . "يمكن لأي طرف ثالث - بائع أو مزود لمكونات المنتج أو شريك أو عميل - أن يمثل مخاطر إلكترونية جديدة لمؤسستك" ، قال ريتشارد ماركوس ، نائب الرئيس لأمن المعلومات في AuditBoard. "لقد تزايدت الحاجة إلى إدارة قوية للمخاطر من طرف ثالث بمرور الوقت ، والعديد من المؤسسات لا تواكب ذلك."

وباعتباره الجزء الأخير من هذه السلسلة المكونة من ثلاثة أجزاء حول الأمن السيبراني، سيسلط موجز المعرفة العالمي هذا الضوء على مدى أهمية المخاطر السيبرانية المرتبطة بالأطراف الثالثة ويتناول أين يمكن للمدققين الداخليين أن يتعاملوا مع إدارة المخاطر السيبرانية من طرف ثالث.

---

9 2022 المسح العالمي لإدارة مخاطر الطرف الثالث ، ديلويت ، 2022 ، https://
www.deloitte.com/content/dam/Deloitte/us/Documents/TPRM_Survey_Report_Interactive.pdf.

تحد كبير

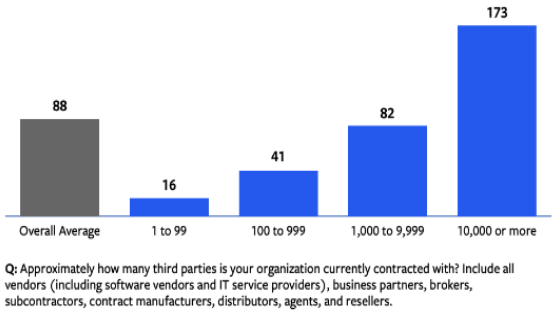
المخاطر السيبرانية تهيمن على مناقشة إدارة مخاطر الطرف الثالث

خطر في ازدياد

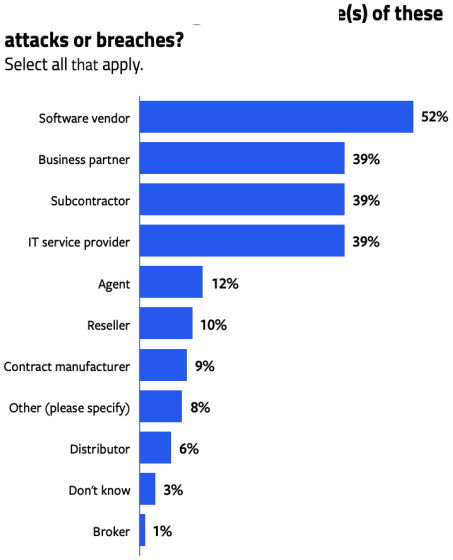
قام تقرير حديث صادر عن CyberRisk Alliance *، برعاية AuditBoard ، باستطلاع آراء 209 من قادة الأمن وتكنولوجيا المعلومات والمديرين التنفيذيين ومديري الأمن والمتخصصين في الامتثال في الولايات المتحدة. لقد كشفت عن مدى اتساع المخاطر السيبرانية للطرف الثالث. تشمل رؤى الاستطلاع ما يلي:*

- *في المتوسط ، تستخدم الشركات 88 شريكا خارجيا (بما في ذلك بائعي البرامج وبائعي خدمات تكنولوجيا المعلومات وشركاء خدمات تكنولوجيا المعلومات وشركاء الأعمال والوسطاء والمقاولين من الباطن والمصنعين المتعاقدين والموزعين والوكلاء والبائعين). تختلف الأرقام بشكل كبير بناء على حجم المؤسسة ، حيث تستخدم الشركات التي تضم 1-99 موظفا 16 شريكا في المتوسط ، بينما تستخدم الشركات التي تضم 10000 موظف أو أكثر 173 في المتوسط (انظر الشكل 1).*
- *أفاد 57٪ من المشاركين أنهم كانوا ضحايا لحادث أمن تكنولوجيا المعلومات (إما هجوم أو خرق) في الأشهر ال 24 الماضية. بالإضافة إلى ذلك ، شهدت المؤسسات في المتوسط حادثين أمنيين مرتبطين بطرف ثالث في العامين الماضيين.*
- *ومن بين الضحايا، قال 52٪ إن مصدر الهجوم كان بائع برامج، بينما قال 39٪ إن شريكا تجاريا أو مقاولا من الباطن أو مزود خدمات تكنولوجيا المعلومات كان مسؤولا عن الحادث (انظر الشكل 2).[10]*

الشكل 1



الشكل 2



ملاحظة: الرسوم البيانية والبيانات الواردة في الشكل 1 والشكل 2 مأخوذة من "مخاطر الطرف الثالث: المزيد من الأطراف الثالثة + رؤية محدودة لسلسلة التوريد = مخاطر كبيرة للمؤسسات" ، بواسطة CyberRisk Alliance و Auditboard. ص. 9 و ص. 18 ، يناير 2023.

10. "مخاطر الطرف الثالث: المزيد من الأطراف الثالثة + رؤية محدودة لسلسلة التوريد = مخاطر كبيرة للمؤسسات" ، تحالف CyberRisk ومجلس التدقيق ، يناير 2023 ، https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

مواكبة التغيير

النسبة المئوية للمؤسسات التي تعتمد على التقنيات اليدوية لإدارة المخاطر السيبرانية من طرف ثالث

تقرير المخاطر الرقمية لمجلس التدقيق لعام 2023 المخاطر المتفشية، والتجزئة المستمرة، وتسريع الاستثمار التكنولوجي

تتنوع الأسباب الرئيسية لهذه المشكلات ، لكنها تنشأ من مزيج من نماذج الأعمال المتغيرة بسرعة وعدم القدرة على تحديث عمليات إدارة مخاطر الطرف الثالث لتتناسب مع التغيير ، وفقا لجون ويلر ، المؤسس والرئيس التنفيذي لشركة Wheelhouse Advisors. قال ويلر: "من واقع خبرتي ، فإن أكبر المخاطر وأكثرها صلة تنشأ عن تغيير كبير. ويقود تحدي النمو تغييرا كبيرا من خلال تحفيز الشركات على إنشاء منتجات وخدمات رقمية جديدة".

حول هذه النقطة ، قام ويلر بتأليف "تقرير المخاطر الرقمية لعام 2023: المخاطر المنتشرة ، والتجزئة المستمرة ، وتسريع الاستثمار التكنولوجي" في استطلاع شمل أكثر من 130 من قادة ادارة المخاطر في الولايات المتحدة ، أفاد 21٪ أنهم لا يجرون تقييما نوعيا أو كميا للمخاطر عند إدارة ومراقبة المخاطر الرقمية للطرف الثالث ، ويعتمد 56٪ فقط على مناهج التقييم النوعي ، وهي محدودة مقارنة بالتقييمات الكمية.[11]

وقال ويلر إن ما يثير القلق بنفس القدر هو أنه من بين الشركات التي تدير المخاطر الرقمية مثل المخاطر السيبرانية للجهات الخارجية ، لا تزال نسبة مذهلة تبلغ 44٪ تعتمد على التقنيات اليدوية (جداول البيانات والبريد الإلكتروني ومحركات الأقراص المشتركة و Sharepoint) للقيام بذلك. وقال: "إنه نهج يستغرق وقتا طويلا للغاية". "الحقيقة هي أن الحوكمة القديمة المجزأة وغير المرنة والمدفوعة بالامتثال ، لا يمكن لبرامج GRC [الحوكمة والمخاطر والامتثال] ببساطة توفير قدرات المخاطر المتصلة اللازمة لمواكبة المخاطر الرقمية - ونتيجة لذلك ، لا تزال معظم المؤسسات تعتمد على العمليات اليدوية المجزأة."

وهذا أمر مثير للقلق بشكل خاص فيما يتعلق بأنماط الهجوم المتغيرة للجهات الفاعلة السيئة، والتي تزداد تعقيدا يوما بعد يوم. "إذا نظرت إلى الأسباب الجذرية لكيفية حدوث الخروقات في العقود القليلة الماضية ، فقد حدث معظمها على الباب الأمامي ، في طبقات التطبيق أو البنية التحتية. هذا هو المكان الذي استثمرت فيه فرق الأمن وقتها ومواردها. لكن المهاجمين أذكياء. سيبحثون عن المسار الأقل مقاومة ، وفي كثير من الأحيان سيكون ذلك من خلال الأبواب الخلفية الناجمة عن الثغرات في تدابير الأمن السيبراني التابعة لجهات خارجية ، "قال ماركوس.

الضغوط التنظيمية

يساهم المشهد التنظيمي المتغير باستمرار في الضغط الذي تشعر به المؤسسات حول المخاطر السيبرانية للأطراف الثالثة ، والذي تسارع مؤخرا ليتناسب مع سرعة المخاطر. وتشمل هذه التغييرات التعليمات الجديدة التي تضعها الحكومة الفيدرالية الأمريكية على شركائها في سلسلة التوريد ، والتي كان لها آثار تدريجية عبر العديد من الصناعات. قال ماركوس: "قد تعتقد أن الاجراءات الفيدرالية لمزيد من الشفافية فيما يتعلق بأمن البيانات ستؤثر فقط على الشركات التي تتعامل مع الحكومة الفيدرالية ، ولكن هناك متطلبات الطرف الثالث والرابع التي تتدفق عبر سلسلة التوريد وتتسلسل عبر التسلسل الهرمي أو مقدمي الخدمات". وهذا يخلق ثقافة المساءلة التي تتخلل الكثير من الصناعات".

كما بدأت الهيئات التنظيمية في اتخاذ المزيد من الخطوات الرسمية لمعالجة مخاطر الأمن السيبراني من طرف ثالث. وسيشمل ذلك القواعد الجديدة التي سنتها مؤخرا لجنة الأوراق المالية والبورصات الأمريكية (SEC) مثل القواعد الجديدة التي تتطلب من المسجلين الكشف عن

11. "تقرير المخاطر الرقمية 2023: المخاطر المنتشرة ، والتجزئة المستمرة ، وتسريع الاستثمار التكنولوجي" ، جون أ. ويلر ، مجلس التدقيق ، يوليو 2023 ، https://www.auditboard.com/resources/ebook/digital-risk-report-2023/.

حوادث الأمن السيبراني المادية. قال ماركوس: "حتى لو لم تكن القواعد أو اللوائح الجديدة قابلة للتطبيق في شركتك بشكل مباشر، فإن هذه القواعد تتغلغل في ثقافة الأمن السيبراني". "إنه تغيير ثقافي يخلق توقعا للشفافية والمساءلة."

مقاربة التدقيق الداخلي

نصائح واستراتيجيات ومجالات جديرة بالاهتمام

ترسيخ ثقافة العمل السيبراني

المؤسسات ليست جاهلة بهذه العيوب. *والواقع أن معظمهم يدركون هذه المشاكل إلى حد ما، حتى وإن كان هذا الوعي لا يترجم دائما إلى فهم وعمل على نطاق المؤسسة. على الرغم من أن عددا قليلا من وظائف التدقيق الداخلي يمكن أن تدعي أن لديها معرفة كافية بالأمن السيبراني لمعالجة الجوانب الفنية للأمن السيبراني لطرف ثالث بشكل مباشر ، إلا أن ما يمكنهم فعله هو الاستفادة من مواقفهم الفريدة لتوحيد وجهات نظر مختلف أصحاب المصلحة المشاركين في إدارة هذه المخاطر (على سبيل المثال ، القانونية والمشتريات وتكنولوجيا المعلومات والأطراف الثالثة نفسها). بالإضافة إلى ذلك، يمكن للمدققين الداخليين استخدام تفاعلهم المباشر مع لجنة التدقيق ومجلس الإدارة للتأكد من توصيل وجهة النظر هذه بانتظام وبدقة.*

وقال ويلر إن وجهة النظر هذه مهمة للغاية للرؤساء التنفيذيين والقادة التنظيميين لتحفيز الإجراءات المناسبة ، وهو شيء يجب أن تبذل وظائف إدارة المخاطر جهدا لفهمه بما يكفي للتعبير عنه. وقال: "يحتاج الرؤساء التنفيذيون إلى رؤى في الوقت الفعلي من داخل المؤسسة وخارجها ، عبر البيئة الكاملة للأصول التكنولوجية التي تتغير ديناميكيا". "من خلال هذه العملية ، سيكون لديهم فهم أفضل لمنتجاتهم وخدماتهم الرقمية."

ومع ذلك، فإن الوحدة داخل المؤسسة ليست كافية. يجب أن تشمل أصحاب المصلحة من خارج المؤسسة. قال ماركوس: "يجب أن يكون هناك شخص معين مسؤول عن كل علاقة مع طرف ثالث للحفاظ على العلاقة بالبائع ، والاحتفاظ بمعلومات الاتصال بالبائع ، وإدارة شروط العقد". "تختلف علاقات الجهات الخارجية من بائع إلى آخر - قد يزود البعض مؤسستك بدعم العملاء المعين أو فريق النجاح الذي يقدم خدمات تكميلية ، بينما يتخذ البعض الآخر نهج "جاهز غب الطلب". إن الحفاظ على خطوط اتصال مفتوحة وواضحة بين مؤسستك وأطرافها الثالثة هو عنصر رئيسي ولكن غالبا ما يتم تجاهله في إدارة مخاطر الطرف الثالث الفعالة.

إن خلق مثل هذه الثقافة لا يمكن أن يحفز العمل الوقائي فحسب؛ بل يمكنه أيضا زيادة سرعة ردود الفعل عند حدوث هجوم إلكتروني أو اختراق. في تقرير CyberRrisk Alliance ، قال 20٪ من المستجيبين إن الأمر قد يستغرق أسبوعا أو أكثر لتقييم هجوم أو خرق ، وعزوا التأخير إلى الصعوبات في الحصول على البائعين أو الشركاء للإبلاغ عن الهجوم أو تحمل المسؤولية عنه.[12] يمكن أن يؤدي إنشاء ثقافة إلكترونية إيجابية وشفافة داخل المؤسسة وعبر سلسلة التوريد الخاصة بها إلى تقليل هذه الأوقات من أسبوع إلى ساعات ، مما يقلل بشكل كبير من الخسائر في هذه العملية.

قال ماركوس: "يجب أن تبنى عملية إدارة مخاطر الطرف الثالث بأكملها حول ثقافة المساءلة التي يكون فيها الجميع على دراية بمخاطر الطرف الثالث".

نهج المراقبة المستمرة على أساس مستوى المخاطر

12. "مخاطر الطرف الثالث: المزيد من الأطراف الثالثة + رؤية محدودة لسلسلة التوريد = مخاطر كبيرة للمؤسسات" ، تحالف CyberRisk ومجلس التدقيق ، فبراير 2023 ، https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

بالإضافة إلى دوره في تحديد طريقة التعامل ، يمكن للتدقيق الداخلي ويجب أن يكون عاملا ذو قيمة في صياغة برنامج إدارة مخاطر الطرف الثالث من حيث صلته بالمخاطر السيبرانية - وتقييمه باستمرار.

قال ماركوس: "أود أن أقول إن المسؤولية الأساسية عن التدقيق الداخلي ، تماما كما هو الحال في معظم الحالات ، هي تقييم فعالية برنامج TPRM". "يمكن أن يشمل ذلك جردا كاملا أو تصورا لجميع الأطراف الثالثة المستخدمة في المؤسسة ، وفهم المخاطر التي يمكن أن تتعرض لها هذه الأطراف الثالثة للمؤسسة ، وفهم كيفية تقييم المؤسسة لقوة الضوابط في تلك المؤسسات التابعة لجهات خارجية."

مرة أخرى، في حين ينبغي استخدام خبراء في هذا المجال للتحليل الفني، فإن العديد من مبادئ إدارة المخاطر التي يستخدمها التدقيق الداخلي تنطبق على هذا الموضوع.

على سبيل المثال، يجب أن يكون لدى التدقيق الداخلي فهم راسخ لتحليل المخاطر، وغالبا ما يتم تصوره باستخدام الخرائط الحرارية أو غيرها من الأدوات. يمكن استخدام هذه التكتيكات كدليل لأصحاب المصلحة المسؤولين عن تأهيل ومراقبة الطرف الثالث لفهم فهم أفضل لمن وماذا يجب تحديد أولوياته.

وقال ماركوس: "إن أهم عامل نجاح لبرنامج إدارة استعراض السياسات هو هيكلة أنشطة المراقبة المستمرة وإضفاء الطابع الرسمي عليها على أساس مستوى المخاطر". "يجب أن تحظى الأطراف الثالثة ذات المخاطر العالية بمزيد من الاهتمام بشكل متكرر ، ويجب أن تحظى الأطراف الثالثة الأقل خطورة باهتمام أقل تواترا." ويتابع أنه في حين أن الطرف الثالث المعني قد لا يمثل خطرا كبيرا في حد ذاته ، فإن طبيعة العلاقة - مثل نوع البيانات التي يتم نقلها (على سبيل المثال ، البيانات السرية ، وبيانات العملاء ، وبيانات الملكية) - يمكن أن ترفع أو تقلل من تصنيف المخاطر.

للمساعدة في هذه المهمة، يستخدم AuditBoard المثال التالي (الشكل 3) كنقطة انطلاق لكيفية هيكلة المراجعات المتعلقة بفئات المخاطر الثلاث التالية:[13]

الشكل 3

Risk Tier Characteristic	Tier 1 – High Risk	Tier 2 – Medium Risk	Tier 3 – Low Risk
Data Access	Confidential	Proprietary	Public or None
Review Frequency	1 Year	2 Years	3 Years
Review Requirements	Onsite Audit Controls Questionnaire Certification Review	Certification Review	None

ملاحظة: الرسوم البيانية والبيانات الواردة في الشكل 1 والشكل 2 مأخوذة من "الإدارة الفعالة للمخاطر الثالثة: التكتيكات الرئيسية وعوامل النجاح" من قبل مجلس التدقيق. ص. 8 ، 2022.

13. "الإدارة الفعالة لمخاطر الطرف الثالث: التكتيكات الرئيسية وعوامل النجاح" ، مجلس التدقيق ، يناير 2022 ، https://www.auditboard.com/resources/ebook/effective-third-party-risk-management-key-tactics-and-success-factors/?utm_campaign=effective-third-party-risk-management-key-tactics-and-success-factors-&0122022utm_medium=download-image&utm_source=blog.

لا ينتهي التدقيق بالطرف الثالث عند التعاقد معه بل يجب مراجعته باستمرار بناء على مستوى المخاطر المتصور. إن ضمان مواكبة أصحاب المصلحة لالتزاماتهم الخاصة بالمراجعات المنتظمة، فضلا عن العمليات التي يستخدمونها لإجراء مثل هذه المراجعات، يجب أن يقع بشكل مباشر ضمن عالم مخاطر التدقيق الداخلي. ويمكن أن تشمل الأفكار المتعلقة بهذه العمليات ما يلي:

- *التحقق من شهادات وتقارير الامتثال مثل SOC 2. تتضمن الأطر الشائعة للتحقق من شهادات الامتثال SOC 2 و ISO 27001 و NIST SP 800-161.*
- *استخدام الاستبيانات الموحدة. يمكن أن يشمل ذلك استبيان جمع المعلومات الموحد (SIG) أو CCM و CAIQ من تحالف أمان السحابة.*
- *استبيانات الضوابط الأمنية.*

احتضان الحلول البرمجية

للحفاظ على العديد من المتغيرات معا ، يجب أن يعطي التدقيق الداخلي بالإضافة إلى وظائف إدارة المخاطر الأخرى الأولوية للابتعاد عن العملية اليدوية لصالح حلول البرامج. وقال ماركوس: "يمكن أن يكون التدقيق الداخلي بطلا للاستثمار في التقنيات لجعل عمليات إدارة المخاطر من طرف ثالث أكثر كفاءة". "في كثير من الحالات ، فإن حجم المعلومات وحده يتطلب ذلك. أتذكر واحدة من أولى المؤسسات التي نفذت فيها ممارسات مخاطر الطرف الثالث - أجرينا تقييمات للمخاطر لخمسة أو ستة بائعين ثم فكرنا في توسيع هذه العملية لجميع البائعين. ومع ذلك ، فقد صدمنا عندما اكتشفنا أن هناك 17000 بائع في هذه الشركة. لا توجد طريقة للقيام بذلك بدون بعض المنصات التي تدعم التكنولوجيا لتسهيل التوسع إلى مئات أو آلاف أو عشرات الآلاف من البائعين ".

بالإضافة إلى ذلك، توفر هذه الحلول أيضا فرصة ممتازة للتدقيق الداخلي للتعاون بشكل أوثق مع وظائف المخاطر الأخرى التابعة لجهات خارجية. قال ماركوس: "تتضمن العديد من العوائق التي تحول دون التعاون مشاركة البيانات ومشكلات سير العمل". "إن وجود منصة تقنية حيث يمكن للفريقين تقييم البائعين معا - باستخدام نفس لوحة القيادة ، ونفس قاعدة بيانات البائعين ، وما إلى ذلك - يسمح لهم بالعمل معا بشكل أكثر كفاءة والدفع نحو نتائج مشتركة.

التركيز على مرحلة إنهاء التعاقد بالاضافة الى مرحلة البداية

نادرا ما تستمر علاقات الطرف الثالث إلى الأبد. ومع ذلك ، لمجرد انتهاء العلاقة رسميا لا يعني دائما إغلاق خطوط البيانات بين الأطراف. وبقدر ما قد يبدو ذلك واضحا، فإن هذه الخطوط المنسية مسؤولة عن بعض أكبر الثغرات الموجودة في أنظمة الأمن السيبراني التابعة لجهات خارجية في المؤسسات، مما يخلق "أبوابا خلفية رقمية" جاهزة للاستغلال عن قصد أو عن غير قصد. عند تقييم ممارسات المراجعة من طرف ثالث ، هذا شيء لا ينبغي أن يغفله التدقيق الداخلي.

قال ماركوس: "من الضروري أن تكون مهتما بالتفاصيل في مرحلة الإعداد". "في النظام البيئي الرقمي المتشابك اليوم ، من السهل تفويت حسابات أو خدمات أو مستخدمين تابعين لجهات خارجية يحتاجون إلى إزالتهم أو تعطيلهم. يجب إبطال امتيازات الوصول وتعطيل حسابات المستخدمين وإزالة أي برامج أو تطبيقات صادرة عن جهة خارجية. وهذا أمر يجب أن ينظر فيه التدقيق الداخلي بالتأكيد".

استنتاج

مستقبل المؤسسات هو سيبراني. *مع مرور كل عام ، من الواضح أن هذا الاتجاه موجود ليبقى - وفقط لأن الأمن السيبراني يتطلب مجموعات مهارات أكثر تخصصا لا يعني أن مشهد الأعمال سينتظر أصحاب المصلحة لتثقيف أنفسهم. الأمن السيبراني هو رحلة مستمرة للتعلم ، ويجب على جميع الأطراف المشاركة في علاقات الطرف الثالث النظر فيه على هذا النحو.*

لحسن الحظ ، هناك علامات إيجابية على أن المؤسسات تقبل هذا الواقع. في تقرير ذكاء الأعمال الصادر عن تحالف CyberRisk Alliance ، قال ما يقرب من اثنين من كل ثلاثة مشاركين إن الإجراء الأكثر شيوعا الذي استخدموه لمنع أو تخفيف مخاطر هجمات الطرف الثالث هو تدريب الموظفين.[14] في حين أن المخاطر المرتبطة بأطراف ثالثة لن تنتهي أبدا ، فإن السياسات والاستجابات ستنضج إلى النقطة التي يمكن فيها إدارتها بسهولة مثل أي مخاطر أخرى ثابتة. هذا الوقت ليس اليوم، لكننا في الطريق، وسيساعد ضمان إدارة مخاطر التدقيق الداخلي الفعال المؤسسات على الوصول بأمان.

14. "مخاطر الطرف الثالث: المزيد من الأطراف الثالثة + رؤية محدودة لسلسلة التوريد = مخاطر كبيرة للمؤسسات" ، تحالف CyberRisk ومجلس التدقيق ، فبراير 2023 ، https://www.auditboard.com/resources/ebook/third-party-risk-more-third-parties-limited-supply-chain-visibility-big-risks-for-organizations/.

عن المعهد الدولي للمدققين الداخليين IIA

المعهد الدولي للمدققين الداخليين *IIA* هو جمعية مهنية دولية غير لا تبغي الربح تخدم أكثر من 235 ألف عضو عالمي وقد منحت أكثر من 190,000 شهادة مدقق داخلي معتمد *CIA* في جميع أنحاء العالم. تأسس المعهد الدولي للمدققين الداخليين *IIA* في عام 1941 وهو معترف به في جميع أنحاء العالم باعتباره الرائد في مهنة التدقيق الداخلي في المعايير، الشهادات، التعليم، البحث، والارشاد التقني. لمزيد من المعلومات، قم بزيارة theiia.org

نبذة عن ديوان المحاسبة

AuditBoard هي المنصة الرائدة القائمة على السحابة التي تعمل على تحويل التدقيق والمخاطر والامتثال وإدارة ESG. يستفيد أكثر من 40٪ من Fortune 500 من AuditBoard لدفع أعمالهم إلى الأمام بمزيد من الوضوح وخفة الحركة. تم تصنيف AuditBoard من قبل العملاء على G2 و Capterra و Gartner Peer Insights ، وتم تصنيفها مؤخرا للسنة الخامسة على التوالي كواحدة من أسرع شركات التكنولوجيا نموا في أمريكا الشمالية من قبل Deloitte. لمعرفة المزيد، تفضل بزيارة: AuditBoard.com.

تنويه

في الجزء الثالث: دور التدقيق الداخلي في أخلاقيات الذكاء الاصطناعي، يتم تقديم وجهات النظر والآراء المعبر عنها من قبل الخبراء بصفتهم الشخصية ولا تعكس وجهات نظر وآراء شركة *Cboe Global Markets, Inc* والشركات التابعة لها.

ينشر المعهد الدولي للمدققين الداخليين *IIA* هذه الوثيقة لأغراض إعلامية وتعليمية. لا تهدف هذه المواد إلى تقديم إجابات نهائية لظروف فردية محددة وعلى هذا النحو يُقصد منها فقط استخدامها كقيادة فكرية مستنيرة من الأقران. إنها ليست توجيهات رسمية من المعهد الدولي للمدققين الداخليين (*IIA*).. يوصي المعهد الدولي للمدققين الداخليين بالتماس مشورة الخبراء المستقلين فيما يتعلق مباشرة بأي حالة محددة. لا يتحمل المعهد الدولي للمدققين الداخليين *IIA* أي مسؤولية عن أي شخص يعتمد فقط على هذه المواد.

تهدف ملخصات المعرفة العالمية إلى معالجة الموضوعات التي تكون في الوقت المناسب وذات صلة بجمهور التدقيق الداخلي العالمي، ويتم فحص كل موضوع يتم تناوله من قبل أعضاء اللجنة الاستشارية للمحتوى التطوعية في أمريكا الشمالية التابعة للمعهد الدولي للمدققين الداخليين (*IIA*). يتم تحديد الخبراء المتخصصين واختيارهم بشكل أساسي من قائمة المعهد الدولي للمدققين الداخليين (*IIA*) للمساهمين في التوجيه العالمي.

لتقديم طلب لإضافتك إلى قائمة المساهمين في الإرشاد العالمي، أرسل بريدًا إلكترونيًا إلى Standards@theiia.org. لاقتراح موضوعات لملخصات المعرفة العالمية المستقبلية، أرسل بريدًا إلكترونيًا إلى Content@theiia.org.

حقوق النشر

قام بترجمة هذه الوثيقة الى اللغة العربية فريق عمل من جمعية المدققين الداخليين في لبنان برئاسة عضو مجلس الحكام ناجي فياض وعضوية السيد محمد شهاب والسيدة داليا ابو كروم

يناير 2024

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101