دليل يستهدف مستوى مجلس الإدارة: قيادة الأمن السيبراني

أساسيات إدارة المخاطر السيبرانية

أكد قدرتك على الإجابة عن الأسئلة التالية بشكل إيجابي:

1. هل تلبي مؤسستك **المتطلبات القانونية والتنظيمية ذات الصلة؟**
2. هل حددت مؤسستك **عدد الهجمات السيبرانية التي تعرضت لها واختبرت مرونتها المالية؟**
3. هل تمتلك مؤسستك **خطة تحسين** لضمان أن الهجمات تقع ضمن معدل المخاطر المتفق عليه؟
4. هل يُناقش مجلس الإدارة **بانتظام معلومات دقيقة وواضحة وقابلة للتنفيذ متعلقة بالمرونة السيبرانية للمؤسسة المدعومة من الإدارة؟**
5. هل لدى مؤسستك **خطط استجابة للحوادث خضعت مؤخرًا لاختبار تجريبي**، بما في ذلك على مستوى مجلس الإدارة؟
6. هل **أدوار الأشخاص الرئيسيين المسؤولين عن إدارة المخاطر السيبرانية** واضحة ومتماشية مع خطوط الدفاع الثلاثة؟
7. هل أجريت **تصديقًا وتأكيدًا مستقلين** لوضع المخاطر السيبرانية لمؤسستك؟

الإشراف

باعتباره أعلى مستوى قيادي في مؤسستك، يتحمل المجلس المسؤولية الكاملة عن التحكم في المخاطر السيبرانية وبالتالي يجب أن يشرف على إستراتيجية المؤسسة وسياساتها والأنشطة في هذا المجال. تحديدًا، يجب على مجلس الإدارة:

⇒ تحمل المسؤولية المطلقة عن الإشراف على المخاطر السيبرانية والمرونة، سواء كمجلس إدارة كامل أو من خلال تفويض لجنة مجلس إدارة معينة بالإشراف.
⇒ تعيين مسؤول شركة واحد، عادةً مدير أمن المعلومات، ليكون مسؤولاً عن الإبلاغ عن قدرة مؤسستك على إدارة المرونة السيبرانية والتقدم في تنفيذ أهداف المرونة السيبرانية. التأكد من أن هذا المسؤول يتمتع بتواصل منتظم مع المجلس، وسلطة كافية، وإتقان للموضوع المعني، والخبرة والموارد اللازمة لتنفيذ هذه المهام.
⇒ تحديد مدى تحمل مؤسستك للمخاطر سنويًا؛ ضمان الاتساق مع إستراتيجية شركتك ومعدل المخاطر.
⇒ الحرص على إجراء مراجعة مستقلة للمرونة السيبرانية لمؤسستك سنويًا.
⇒ الإشراف على ابتكار خطط المرونة السيبرانية وتنفيذها واختبارها وتحسينها بصورة مستمرة، لضمان التوافق في جميع أنحاء مؤسستك وأن مدير أمن المعلومات (CISO) أو الموظف الآخر المسؤول يقدم تقارير عنها بصفة منتظمة إلى مجلس الإدارة.
⇒ دمج المرونة السيبرانية وتقييم المخاطر في إستراتيجية الأعمال الشاملة لمؤسستك، وإدارة المخاطر، ووضع الميزانية، وتخصيص الموارد، بهدف دمج المخاطر السيبرانية بشكل كامل في المخاطر التشغيلية الشاملة.
⇒ راجع دائمًا أداءك لما ورد أعلاه وفكر في الحصول على مشورة مستقلة لضمان التحسين المستمر.

البقاء على اطلاع

يعتمد الإشراف الفعال لمجلس الإدارة على المخاطر السيبرانية على مدى دراية الأعضاء بالموضوع والمعلومات الحديثة.

⇒ تأكد من أن جميع الأفراد الذين ينضمون إلى مجلس الإدارة يتمتعون بمهارات ومعرفة مناسبة ومحدثة لفهم وإدارة المخاطر التي تمثلها التهديدات السيبرانية.
⇒ اطلب المشورة المنتظمة من الإدارة فيما يتعلق بتعرض مؤسستك للمخاطر الحالية والمستقبلية، والمتطلبات التنظيمية ذات الصلة، والمعايير الصناعية والاجتماعية لمعدل المخاطر الذي تتبناه. علاوة على ذلك، شارك في جلسات إحاطة منتظمة بشأن أحدث التطورات فيما يتعلق ببيئة التهديدات والبيئة التنظيمية، والتخطيط المشترك والزيارات إلى الأقران والقادة الذين يطبقون أفضل الممارسات في مجال الأمن السيبراني، وتبادل الحوكمة والإبلاغ على مستوى مجلس الإدارة.
⇒ حمل الإدارة مسؤولية تقديم تقييم كمّي ومفهوم للمخاطر والتهديدات والأحداث السيبرانية كعنصر دائم في جدول أعمال اجتماعات مجلس الإدارة.
⇒ كن على وعي دائم بالتحديات التنظيمية المستمرة مثل نقاط الضعف في سلسلة التوريد، والتبعيات المشتركة، والفجوة في تبادل المعلومات بين مجالس الإدارة بشأن إدارة المخاطر السيبرانية.

تمهيد السبيل

بالتعاون مع الإدارة العليا، يجب أن يضع مجلس الإدارة القيم الأساسية لمؤسستك ويمثلها، ويحدد ثقافة المخاطر والتوقعات فيما يتعلق بالمرونة السيبرانية.

⇒ تعزيز ثقافة يتعرف فيها الموظفون على جميع المستويات على مسؤولياتهم المهمة في ضمان المرونة السيبرانية لمؤسستك. القيادة بالقدوة.
⇒ قم بالإشراف على دور الإدارة في تعزيز ثقافة المخاطر لمؤسستك والحفاظ عليها. عزز ثقافة المخاطر وقم بمراقبتها وتقييمها، مع مراعاة تأثير الثقافة على السلامة والصحة، وإجراء تغييرات عند الضرورة.
⇒ وضح أنك تتوقع من جميع الموظفين التصرف بنزاهة والإبلاغ الفوري عن أية عملية عدم امتثال ملحوظة داخل مؤسستك أو خارجها.

دليل المستوى التنفيذي: قيادة الأمن السيبراني

- تحديد حالة النضج المنشودة لمؤسستك،
- فهم مكان تهديدات الأمن السيبراني في قائمة أولويات المخاطر الخاصة بمؤسستك،
- تحديد الفجوات بين الحالة الحالية للأمن السيبراني والحالة المستهدفة المنشودة،
- تنفيذ الخطط لتحقيق النضج والحفاظ عليه،
- إعادة تقييم نضج الأمن السيبراني والمخاطر والأهداف المتعلقة به في مؤسستك باستمرار، و
- التفكير في استخدام اختبار اختراق من جهة خارجية أو اختبارات اختراق الفريق الأحمر،
- التفكير في الاستعانة بتدابير وقائية مثل شراء تأمين سيبراني.

⇒ قيادة جهود الموظفين خلال عملية تقييم المخاطر لتسهيل الاستجابة في الوقت المناسب من جميع أنحاء المؤسسة.

⇒ تحليل نتائج تقييم المخاطر وتقديمها للإشراف التنفيذي، بما في ذلك أصحاب المصلحة الرئيسيين ومجلس الإدارة.

⇒ الإشراف على أي تغييرات في الحفاظ على أو زيادة الاستعداد للأمن السيبراني المنشود في مؤسستك، مع ضمان أن أي خطوات يتم اتخاذها لتحسين الأمن السيبراني تتناسب مع المخاطر وميسورة التكلفة لمؤسستك.

⇒ الإشراف على أداء المراقبة المستمرة بحيث تظل بارعة وسريعة في معالجة المخاطر السيبرانية الناشئة.

الثقافة المؤسسية

الأمن السيبراني لمؤسستك ليس عملية تُجرى لمرة واحدة أو مهمة يقوم بها عدد قليل من الموظفين؛ إنه عامل يجب مراعاته في جميع القرارات والعمليات التجارية وممارسة يجب على جميع الموظفين الحفاظ عليها. لتشجيع الأمن السيبراني الشامل المستمر داخل مؤسستك، عليك:

⇒ بدء مناقشات حول الأمن السيبراني مع فريق القيادة والتواصل بانتظام مع الموظفين المسؤولين عن إدارة المخاطر السيبرانية.

⇒ جعل التدريب على الأمن السيبراني جزءًا من تدريب جميع الموظفين الجدد، لضمان أن جميع الموظفين على اطلاع دائم بالوثائق التي تُقر بالالتزام بسياسات الأمن السيبراني الخاصة بمؤسستك ووقعوا عليها وأن قسم تكنولوجيا المعلومات أو الموظفين الفنيين الآخرين قاموا بإطلاعهم على أفضل الممارسات.

⇒ تنظيم تدريب متكرر على الأمن السيبراني لجميع الموظفين فيما يتعلق بمسؤولياتهم الأمنية القصيرة والطويلة الأجل.

⇒ ضمان مراعاة الأمن السيبراني دائمًا عندما تقوم مؤسستك بتقييم البائعين المحتملين وتبادل البيانات مع الجهات الخارجية.

⇒ مراجعة سياسات الأمن السيبراني لمؤسستك سنويًا.

⇒ تشجيع مشاركة المعلومات التطوعية حول تهديدات وحوادث الأمن السيبراني داخل مؤسستك ومع النظراء الموثوقين.

الإدارة

يبدأ الأمن السيبراني لمؤسستك وينتهي عند أعلى مستوى إداري. ينبغي أن يكون الرئيس التنفيذي وأعضاء مجلس الإدارة على دراية دائمة بالمخاطر ويتحملوا المسؤولية والمساءلة الكاملة عن أنشطة الأمن السيبراني وموظفيه. يجب عليك:

⇒ تعيين مدير أمن المعلومات (CISO) في حالة عدم وجوده، أو إذا كانت الموارد محدودة للغاية، تعيين شخص من داخل مؤسستك للقيام بمهام مدير أمن المعلومات.

⇒ التعاون مع مدير أمن المعلومات أو الموظفين الفنيين الآخرين لوضع إستراتيجية وإطار عمل الأمن السيبراني المُخصّصين للمخاطر السيبرانية الخاصة بالمؤسسة، وذلك باستخدام المعايير والإرشادات الدولية والمحلية والخاصة بالمجال.

⇒ توضيح الأدوار والمسؤوليات الواضحة للموظفين الذين يقومون بتنفيذ الأمن السيبراني للمؤسسة وإدارته.

- العمل مع مدير أمن المعلومات لتحديد أدوار الأمن السيبراني المناسبة وحقوق الوصول لجميع مستويات الموظفين.
- الإشراف على التواصل والتعاون لضمان أن إدارة الأمن السيبراني شمولية، وبالأخص إذا تمت مشاركة مسؤوليات الأمن السيبراني بين عدة موظفين أو أقسام متعددة داخل المؤسسة (مثل وجود أقسام منفصلة لأمن المعلومات والمخاطر والتكنولوجيا).

⇒ التأكد من أن مدير أمن المعلومات لديه خط اتصال واضح ومباشر لإطلاعك ومجلس الإدارة على التهديدات في الوقت المناسب.

⇒ دعوة المدير التنفيذي لأمن المعلومات أو الموظفين الفنيين الآخرين إلى اجتماع موجز للإدارة العليا بشكل روتيني.

⇒ ضمان أن سياسات الأمان في المؤسسة ومعاييرها وآليات إنفاذها وإجراءاتها موحدة على مستوى جميع الفرق وخطوط العمل.

تقييم المخاطر وإدارتها

يعتمد ضمان الوعي الجيد بالأمن السيبراني والتأهب له على تحليل مستمر قائم على المخاطر. لتحسين الأمن السيبراني لمؤسستك، عليك:

⇒ وضع تقييم لمخاطر الأمن السيبراني وإدارتها كأولوية ضمن عمليات إدارة المخاطر والحوكمة الأوسع نطاقًا لمؤسستك. العمل مع مدير أمن المعلومات أو الموظفين الفنيين الآخرين على وضع خطة لإجراء تقييم للمخاطر يتضمن:

- وصفًا لأصول مؤسستك ومختلف مستويات الاعتماد على التكنولوجيا،
- تقييمًا لنضج مؤسستك والمخاطر الكامنة المرتبطة بالتبعيات التكنولوجية لأصولها،

دليل على مستوى مدير أمن المعلومات: حماية مؤسستك

وضع برنامج لأمن المعلومات قائم على المخاطر

1. حدد أنواع المعلومات التي تُخزنها شركتك وتستخدمها

⇒ اذكر جميع أنواع المعلومات التي تُخزنها شركتك أو تستخدمها (مثل، أسماء العملاء وعناوين البريد الإلكتروني).

2. حدد قيمة معلوماتك

⇒ اطرح أسئلة رئيسية لكل نوع من أنواع المعلومات:

- ماذا سيحدث إذا تم الإعلان عن هذه المعلومات؟
- ماذا سيحدث لعملي إذا كانت هذه المعلومات غير صحيحة، في حالة تم التلاعب بسلامة البيانات، مثلاً؟
- ما الذي سيحدث لشركتي إذا لم أتمكن أنا أو عملائي من الوصول إلى هذه المعلومات؟

3. ضع قائمة جرد

⇒ حدد التكنولوجيا التي ترتبط بالمعلومات التي حددتها. يمكن أن يشمل ذلك الأجهزة (مثل، أجهزة الكمبيوتر) وتطبيقات البرامج (مثل، البريد الإلكتروني للمستعرض). ضمّن الصنع والطراز والأرقام التسلسلية ومعرفات أخرى. تتبع موقع كل منتج. بالنسبة للبرنامج، حدد الجهاز (الأجهزة) الذي تم تحميل البرنامج عليه.

⇒ عند الاقتضاء، قم بتضمين تكنولوجيات من خارج عملك (مثل "السحابة") وأي تقنيات حماية موجودة لديك مثل جدران الحماية.

4. حاول فهم التهديدات ونقاط الضعف لديك

⇒ راجع بانتظام التهديدات ونقاط الضعف التي قد يواجهها القطاع المالي وقدر احتمالية تأثرك. (يمكن العثور على المعلومات من خلال شهادة CERT الوطنية، ومؤسسة FS-ISAC، وفصل مؤسسة InfraGard المحلي، وغير ذلك.)

⇒ قم بإجراء فحص أو تحليل لنقاط الضعف مرة واحدة في السنة على الأقل.

5. قم بإنشاء سياسة للأمن السيبراني

⇒ تعاون مع الإدارة العليا في مؤسستك لوضع إستراتيجية أمن سيبراني والحفاظ عليها، والتي يتم تصميمها وفقًا للمخاطر المذكورة أعلاه وتستمد معلوماتها من المعايير والإرشادات الدولية والمحلية والخاصة بالمجال. تقدم المبادئ التوجيهية مثل إطار عمل NIST، وأداة تقييم الأمن السيبراني الخاصة بـ FFIEC، ومعيار الأيزو 27001 نماذج لبناء هذه السياسات وتحسينها.

⇒ قُم بتدريب جميع الموظفين على تفاصيل السياسة واطلب منهم التوقيع على الوثائق التي تؤكد على دورهم في مواصلة تعزيز الأمن السيبراني لمؤسستك من خلال الالتزام بالسياسة.

حاول تجنب التلف الناجم عن البرمجيات الخبيثة

⇒ قم بتنشيط جدار الحماية وحدد قوائم التحكم في الوصول (**ACLs**) لإنشاء منطقة عازلة بين الشبكة والإنترنت. قيد الوصول باستخدام إعداد القائمة البيضاء، وليس بإدراج عناوين أو خدمات **IP** معينة في القائمة السوداء.

⇒ استخدم برامج مكافحة الفيروسات والحماية من برامج التجسس على جميع أجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة.

⇒ صحح جميع البرامج والبرامج الثابتة من خلال تطبيق أحدث تحديثات البرامج المقدمة من الشركات المصنعة والبائعين. "التحديث تلقائيًا" حيثما كان ذلك متاحًا.

⇒ اجعل خطوة تثبيت البرامج الجديدة مُقتصرة على موظفي تكنولوجيا المعلومات الذين يتمتعون بحقوق إدارية.

⇒ احتفظ بسجلات الأنشطة التي تم إنشاؤها بواسطة أجهزة أو برامج الحماية/الكشف وراقبها. اعمل على حماية السجلات باستخدام كلمة المرور والتشفير.

⇒ حافظ على مزامنة جميع ساعات المضيف. إذا كانت أجهزة المؤسسة لديك تحتوي على إعدادات ساعة غير متسقة، فسيكون ترابط الحدث أكثر صعوبة عند وقوع الحوادث.

⇒ تحكم في الوصول إلى الوسائط القابلة للإزالة مثل بطاقات **SD** ووحدات الذاكرة الفلاشية (**USB**). شجع الموظفين على نقل الملفات عبر البريد الإلكتروني أو التخزين السحابي بدلاً من ذلك. اعمل على توعية الموظفين بمخاطر استخدام وحدات **USB** من مصادر خارجية أو إعطاء وحدات **USB** الخاص بهم للآخرين.

⇒ قم بإعداد عوامل تصفية البريد العشوائي وأمان البريد الإلكتروني في خدمات البريد الإلكتروني.

⇒ اعمل على حماية جميع الصفحات المتاحة على مواقع الويب التي تواجه الجمهور باستخدام التشفير والأدوات الأخرى المتاحة.

⇒ فكر في توظيف خدمة اختبار الاختراق لتقييم أمن أصول مؤسستك وأنظمتها.

تدريب الموظفين

⇒ قدم دورات تدريبية إلزامية للأمن السيبراني أثناء إلحاق الموظفين الجدد وعلى فترات منتظمة لجميع الموظفين الحاليين، مرة واحدة سنويًا على الأقل. طالب الموظفين بما يلي:

- استخدام كلمات مرور قوية على جميع الأجهزة والحسابات المهنية وشجعهم على القيام بالشيء نفسه للأجهزة الشخصية واستخدام مدير كلمات المرور،
- اجعل جميع أنظمة التشغيل، والبرنامج والتطبيقات مُحدثة عبر جميع الأجهزة،
- استخدام المصادقة الثنائية على جميع الحسابات،
- الحفاظ على أمان تفاصيل الحساب وبطاقات الوصول وإغلاق الأجهزة عند عدم استخدامها،
- الامتناع عن مشاركة تفاصيل الحساب أو البيانات الحساسة الأخرى عبر البريد الإلكتروني غير المشفر أو الاتصالات المفتوحة الأخرى،
- تجنب فتح المرفقات على الفور أو النقر فوق الروابط في رسائل البريد الإلكتروني غير المرغوب فيها أو المشبوهة،
- التحقق من صحة رسالة بريد إلكتروني مشبوهة أو مربع منبثق قبل تقديم المعلومات الشخصية، والانتباه التام لعنوان البريد الإلكتروني،
- والإبلاغ عن أي حوادث أو تهديدات أمنية داخلية أو خارجية محتملة، أو سوء تعامل مع البيانات أو الأجهزة إلى الموظفين الفنيين و/أو الإدارة العليا في مؤسستك.

⇒ اختبر بانتظام وعي الموظف من خلال مشكلات تتم محاكاتها مثل إرسال رسائل بريد إلكتروني على غرار التصيد الاحتيالي من حسابات وهمية. استخدم أي إخفاقات لتكون فرصًا للتعلم بدلاً من العقاب.

حماية بياناتك

⇒ قم بإنشاء نُسخًا احتياطية منتظمة من بياناتك المهمة (مثل المستندات، رسائل البريد الإلكتروني، التقويمات) وتحقق من إمكانية استعادتها. فكر في حفظ نسخ احتياطية على السحابة.
⇒ تأكد من أن الجهاز الذي يحتوي على النسخة الاحتياطية غير متصل بشكل دائم بالجهاز الذي يحتفظ بالنسخة الأصلية، لا ماديًا ولا عبر شبكة محلية.
⇒ قم بتثبيت واقيات أجهزة الحماية من التغير المفاجيء في شدة الكهرباء، واستخدم المولدات، وتأكد من توصيل جميع أجهزة الكمبيوتر وأجهزة الشبكة المهمة بمصادر طاقة غير متقطعة.
⇒ استخدم حل إدارة الأجهزة المحمولة (MDM).

الحفاظ على سلامة أجهزتك

⇒ قم بتشغيل حماية رقم التعريف الشخصي وحماية كلمة المرور للأجهزة المحمولة. قم بتكوين الأجهزة بحيث يمكن تتبعها أو إزالتها عن بُعد أو إغلاقها عن بُعد عند فقدها أو سرقتها.
⇒ اعمل على إبقاء أجهزتك (وجميع التطبيقات المثبتة) مُحدثة، باستخدام خيار "التحديث التلقائي" إذا كان متاحًا.
⇒ عند إرسال بيانات حساسة، لا تتصل بنقاط اتصال Wi-Fi العامة - استخدم الاتصالات الخلوية (بما في ذلك الربط والمحولات الملحقة) أو استخدم شبكات خاصة افتراضية.
⇒ استبدل الأجهزة التي لم تعد جهات التصنيع تدعمها بأجهزة حديثة.
⇒ حدد إجراءات الإبلاغ عن المعدات المفقودة أو المسروقة.

استخدام كلمات المرور

⇒ تأكد من أن جميع أجهزة الكمبيوتر تستخدم منتجات التشفير التي تتطلب كلمة مرور لبدء التشغيل. قم بتشغيل حماية كلمة المرور أو حماية رقم التعريف الشخصي للأجهزة المحمولة.
⇒ استخدام كلمات مرور قوية، وتجنب كلمات المرور المتوقعة (مثل، passw0rd) والمعرفات الشخصية (مثل، أسماء الأسرة والحيوانات الأليفة). اطلب من جميع الموظفين القيام بالشيء نفسه.
⇒ استخدم مصادقة ثنائية (2FA) حيثما أمكن.
⇒ غيّر كلمات المرور الافتراضية الصادرة من الشركة المصنعة على جميع الأجهزة، بما في ذلك الشبكات وأجهزة إنترنت الأشياء، قبل توزيعها على الموظفين.
⇒ تأكد من أن الموظفين يمكنهم إعادة تعيين كلمات المرور الخاصة بهم بسهولة. قد ترغب أيضًا في مطالبة الموظفين بتغيير كلمة المرور الخاصة بهم على فترات منتظمة (على سبيل المثال بشكل ربع سنوي أو نصف سنوي أو سنوي).
⇒ فكر في استخدام برامج إدارة كلمات المرور. إذا كنت تستخدم واحدًا، فتأكد من أن كلمة المرور "الرئيسية" (التي توفر الوصول إلى جميع كلمات المرور الأخرى) قوية.

أذونات التحكم

⇒ تأكد من أن جميع الموظفين لديهم حسابات قابلة للتحديد بشكل فريد تتم المصادقة عليها في كل مرة يمكنهم فيها الوصول إلى الأنظمة الخاصة بالمؤسسة.
⇒ امنح امتيازات إدارية فقط لموظفي تكنولوجيا المعلومات الموثوق بهم والموظفين الرئيسيين واسحب امتيازات المسؤول في محطات العمل للمستخدمين القياسيين.
⇒ لا تمنح الموظفين إمكانية وصول إلا إلى أنظمة البيانات المحددة التي يحتاجون إليها لوظائفهم وتأكد من عدم امتلاكهم إمكانية تثبيت أي برنامج دون إذن.
⇒ تحكم في الوصول المادي إلى أجهزة الكمبيوتر الخاصة بالمؤسسة وقم بإنشاء حسابات مستخدمين لكل موظف.

تأمين شبكات Wi-Fi وأجهزتك

⇒ تأكد من أن شبكة Wi-Fi في مكان العمل آمنة ومشفرة باستخدام WPA2. غالبًا ما تأتي أجهزة التوجيه بخاصية تشفير مغلقة، لذا تأكد من تشغيلها. تحمي كلمة المرور الوصول إلى جهاز التوجيه، لذا احرص على تحديث كلمة المرور من الإعداد الافتراضي المحدد مسبقًا. أوقف تشغيل أي خصائص "إدارة عن بُعد".
⇒ قم بإعداد نقطة الوصول اللاسلكية أو جهاز التوجيه بحيث لا يبث اسم الشبكة، والمعروف باسم معرف مجموعة الخدمات (SSID).
⇒ حدد الوصول إلى شبكة Wi-Fi فقط عن طريق السماح للأجهزة التي بها عناوين معينة بالتحكم في الوصول إلى الوسائط. إذا احتاج العملاء إلى Wi-Fi، فقم بإنشاء شبكة عامة منفصلة.
⇒ قم بتمكين تسجيل بروتوكول التكوين الديناميكي للمضيف (DHCP) على أجهزة شبكتك للسماح بسهولة تتبع جميع الأجهزة التي كانت على شبكتك.
⇒ قم بتسجيل الخروج بصفتك مسؤولاً بعد إعداد جهاز التوجيه.
⇒ حافظ على تحديث برنامج جهاز التوجيه. تعرف على التحديثات عن طريق تسجيل جهاز التوجيه لدى الشركة المُصنعة والاشتراك للحصول على التحديثات.

تجنُب هجمات التصيد الاحتيالي

⇒ تأكد من عدم قيام الموظفين بتصفح الويب أو التحقق من رسائل البريد الإلكتروني على الخوادم أو من حساب له امتيازات المسؤول.
⇒ قم بإعداد عوامل تصفية الويب والبريد الإلكتروني. فكر في حظر الموظفين عن زيارة المواقع الإلكترونية المرتبطة عادةً بتهديدات الأمن السيبراني.
⇒ علِّم الموظفين البحث عن علامات التصيد الاحتيالي الواضحة، مثل سوء الهجاء والأخطاء في القواعد النحوية، أو الإصدارات ذات الجودة المنخفضة من الشعارات القابلة للتعريف. هل يبدو عنوان البريد الإلكتروني للمرسل شرعيًا؟
⇒ تفحص الجهاز بحثًا عن البرامج الضارة وغيّر كلمات المرور في أقرب وقت ممكن إذا كنت تشك في حدوث هجوم. لا تعاقب الموظفين إذا أصبحوا ضحية لهجوم تصيد احتيالي (فهذا لا يشجع الأشخاص على الإبلاغ في المستقبل).

دليل على مستوى مدير أمن المعلومات: حماية عملائك

نصيحة فردية للعملاء والموظفين لحماية البيانات المالية

انصح موظفيك وعملاءك باتباع إرشادات الأمن السيبراني الواردة أدناه في سلوكهم الشخصي لزيادة استعدادهم وحماية بياناتهم المالية من التهديدات الإلكترونية.

1. نفذ ممارسات الصحة العامة الأساسية عبر أجهزتك.

⇒ استخدام كلمات مرور قوية على جميع الأجهزة الشخصية والمهنية، والنظر في استخدام مدير كلمات المرور.
⇒ حافظ على تحديث أنظمة التشغيل والبرامج والتطبيقات الأخرى على أجهزة الكمبيوتر والأجهزة المحمولة.
⇒ قم بتثبيت برامج مكافحة الفيروسات ومكافحة البرامج الضارة ومكافحة برامج الفدية التي تمنع البرامج الضارة وتكتشفها وتزيلها.
⇒ استخدم برنامج جدار حماية لمنع الوصول غير المصرح به إلى جهاز الكمبيوتر.
⇒ استخدم منتجات الأمان فقط من الشركات ذات السمعة الطيبة. اقرأ المراجعات من الكمبيوتر ومنشورات المستهلكين وانظر في استشارة الشركة المصنعة لجهاز الكمبيوتر أو نظام التشغيل.

2. كن حذرًا عند التعامل مع المعلومات الحساسة.

⇒ لا ترسل كلمات مرور الحساب المصرفي أو بيانات الحساب المالي الحساسة الأخرى عبر البريد الإلكتروني غير المشفر.
⇒ تعامل بذكاء عندما يتعلق الأمر بمكان اتصالك بالإنترنت وكيفية قيامك بذلك لأغراض الخدمات المصرفية أو الاتصالات الأخرى التي تتضمن معلومات شخصية حساسة. يمكن أن تكون شبكات Wi-Fi العامة وأجهزة الكمبيوتر في أماكن مثل المكتبات أو مراكز أعمال الفنادق محفوفة بالمخاطر.

3. قاوم التصيد الاحتيالي.

⇒ لا تفتح مرفقات البريد الإلكتروني على الفور أو تنقر على روابط في رسائل بريد إلكتروني غير مرغوب فيها أو مشبوهة. توقف. فكر. انقر.
⇒ كن حذرًا إذا اتصل بك شخص ما على نحو غير متوقع عبر الإنترنت أو عبر الهاتف وطلب معلوماتك الشخصية. حتى عند الاتصال بالعناوين المعروفة، قلل مشاركة المعلومات الشخصية عبر البريد الإلكتروني.
⇒ تذكر أنه لن تقوم أي مؤسسة مالية بإرسال بريد إلكتروني لك أو الاتصال بك وطلب معلومات سرية لديها بالفعل.
⇒ افترض أن طلب الحصول على معلومات من بنك لم تقم مطلقًا بفتح حساب فيه هو عملية احتيال.
⇒ تحقق من صحة رسالة بريد إلكتروني مشبوهة أو مربع منبثق قبل تقديم المعلومات الشخصية. انتبه جيدًا إلى عنوان البريد الإلكتروني.

إدارة الحسابات

⇒ اطلب من العملاء استخدام معرفات مستخدمين وكلمات مرور قوية لتسجيل الدخول إلى خدماتك. أبلغهم بعدم استخدام كلمة المرور نفسها التي يستخدمونها للحسابات الأخرى.
⇒ استخدم التحقق الفوري والتحقق في الوقت الفعلي والتحقق من الإيداع التجريبي والتحقق من الهوية و/أو الأسئلة خارج المحفظة للتحقق من صحة العملاء الحقيقيين وتقليل فرصة الاحتيال.
⇒ العرض، يتطلب بشكل مثالي، مصادقة ثنائية للعملاء لاستخدامها عند تسجيل الدخول إلى خدماتك.
⇒ تحقق بانتظام من حسابات المستخدم لاكتشاف علامات الاحتيال.

حماية البيانات

⇒ فكّر في بيانات العملاء التي يجب على مؤسستك جمعها لتقديم خدماتها، وكن حذرًا من جمع أي بيانات خاصة بالعملاء تتجاوز ذلك.
⇒ ضع سياسات الاحتفاظ بالبيانات ووزعها. تخلص من بيانات العملاء عندما لم تعود هناك حاجة إليها.
⇒ قم بتشفير بيانات العملاء عند نقلها وعندما تكون غير نشطة.
⇒ ضع سياسات أمان البيانات لتوضيح طرق نقل البيانات المعتمدة مقابل المقيدة وتحديد ما هو مقبول لجميع الموظفين عند التعامل مع بيانات العميل. تأكد من توثيق هذه السياسات وإبلاغها وفرضها على جميع الموظفين ومراجعتها وتحديثها بشكل دوري.

تأمين تطبيقات الويب العامة

⇒ قم بتنفيذ HTTPS على تطبيق (تطبيقات) الويب العام الخاص بمؤسستك وقم بإعادة توجيه جميع حركات مرور HTTP إلى HTTPS.
⇒ استخدم سياسة أمن المحتوى على موقع (مواقع) الويب لمنع هجمات البرامج النصية عبر الموقع واصطياد النقرات وحقن الرموز الأخرى.
⇒ قم بتمكين تثبيت المفتاح العام على موقع (مواقع) الويب لمنع الهجوم الوسيط.
⇒ تأكد من عدم استخدام تطبيق (تطبيقات) الويب العام أبدًا لملفات تعريف الارتباط بهدف تخزين معلومات العميل الحساسة أو البالغة الأهمية (مثل، كلمات المرور) وأن لديها تواريخ انتهاء صلاحية تحفظية لملفات تعريف الارتباط (عاجلاً وليس آجلاً). فكر في تشفير المعلومات المخزنة في ملفات تعريف الارتباط التي تستخدمها.
⇒ فكر في تعيين خدمة اختبار الاختراق لتقييم أمن تطبيق (تطبيقات) الويب العام مرة واحدة على الأقل في العام.

تدريب الموظفين

⇒ علّم موظفيك المساءلة والإستراتيجيات للحد من الخطأ البشري الذي قد يكشف بيانات العملاء. وهذا يعني تقديم المشورة للقيام بما يلي:

- اقتصار وصولهم إلى بيانات العملاء ونقلها على ما هو ضروري فقط لأداء وظائفهم،
- الحفاظ على ممارسات أمنية قوية على جميع الأجهزة والحسابات التي تتعامل مع بيانات العملاء باستخدام كلمات مرور قوية، وتمكين المصادقة الثنائية، وتحديث البرنامج، وعدم النقر فوق الروابط المشبوهة، و
- الإبلاغ عن أي حوادث أو تهديدات أمنية داخلية أو خارجية محتملة، أو سوء إدارة للبيانات إلى موظفي المؤسسة الفنيين و/أو إدارتها العليا.

⇒ تأكد من فهم موظفيك للوثائق وتوقيعها للالتزام بسياسات حماية بيانات مؤسستك وأمانها حتى لا ينتهكونها، بحيث يتقنون التعامل مع العملاء، وبالتالي لا يتواصلون مع العملاء بطريقة غير محمية.

إخطار العملاء

⇒ فهم البيئة التنظيمية لمؤسستك عندما يتعلق الأمر بمعالجة انتهاكات بيانات العملاء لضمان استعدادك للامتثال عند وقوع الحوادث.

⇒ عندما تصبح مؤسستك على علم بحادث الوصول غير المصرح به إلى معلومات العملاء الحساسة، قم بإجراء تحقيق لتُحدد على الفور احتمالية إساءة استخدام المعلومات أو حدوث ذلك بالفعل. اتبع أفضل ممارسات الإخطار وأخطر العميل (العملاء) المعني وفقًا لذلك في أقرب وقت ممكن، وذلك عن طريق تقديم:

- وصف عام للحادث والمعلومات التي تم اختراقها،
- رقم هاتف لمزيد من المعلومات والمساعدة،
- تذكير "بالبقاء يقظًا" على مدار الـ 12 إلى 24 شهرًا القادمة،
- توصية بالإبلاغ عن حالات سرقة الهوية المشتبه بها فورًا،
- وصف عام للخطوات التي تتخذها المؤسسة المالية لحماية تعرض المعلومات لمزيد من الوصول أو الاستخدام غير المصرح به،
- معلومات الاتصال الخاصة بوكالات الإبلاغ عن الائتمانات، و
- وأي معلومات أخرى مطلوبة بموجب اللوائح التي يجب على مؤسستك الامتثال لها.

دليل على مستوى مدير أمن المعلومات: حماية الاتصالات للجهات الخارجية

كيفية اختيار البائعين مع وضع الأمن السيبراني في الاعتبار

اطرح الأسئلة التالية على البائعين المحتملين لقياس استعدادهم للأمن السيبراني والوعي به وبالتالي التأثير الذي سيحدثونه على ملف المخاطر بمؤسستك:

1. **ما الخبرة التي يمتلكونها؟** تعرف على تاريخ البائع في خدمة العملاء. هل قاموا بخدمة عملاء مشابهين لمؤسستك من قبل؟
2. **هل وثقوا امتثالهم لمعايير الأمن السيبراني المعروفة** مثل إطار عمل NIST أو معيار الأيزو 27001، أو هل يمكنهم تقديم تقرير SOC2؟
3. **أي من بياناتك و/أو أصولك سيحتاجون إلى الوصول إليها لأداء خدماتهم؟** هل يطلبون أي وصول غير ضروري على ما يبدو؟
4. **كيف يخططون لحماية أصول مؤسستك وبياناتها الموجودة في حوزتهم؟**
5. **كيف يديرون المخاطر السيبرانية الخاصة بالجهة الخارجية؟** هل يمكنهم تقديم معلومات عن سلسلة التوريد الخاصة بهم؟
6. **ما خطتهم للتعافي من الكوارث واستمرارية الأعمال** في حالة وقوع حادث يؤثر في أصول المؤسسة و/أو بياناتها؟
7. **كيف سيحافظون على بقاء مؤسستك على اطلاع بأحدث التطورات؟** ما خطتهم للتعريف بالاتجاهات والتهديدات والتغييرات داخل مؤسستهم؟

تحديد المخاطر من خلال الجهات الخارجية

⇒ قم بإنشاء قائمة محدثة بالعلاقات مع جميع البائعين، والأصول والبيانات المعروضة في كل منها، واحتفظ بها.
⇒ راجع البيانات التي يستطيع كل بائع أو جهة خارجية الوصول إليها. تأكد من أن هذا المستوى من الوصول يلتزم بمبدأ "أقل الامتيازات".
⇒ رتب علاقاتك مع البائع والجهات الخارجية (منخفضة، متوسطة، عالية) استنادًا إلى التأثير الذي قد يحدثه خرق أنظمتهم على مؤسستك.
⇒ بدءًا من أكبر البائعين المعرضين للمخاطر، قم بتقييم إمكانات الأمن السيبراني لكل مزود. يُعد الالتزام بالمعايير ذات الصلة نقطة بداية جيدة. ضع خطة للتقييم الأمني المنتظم. قد تحتاج أحيانًا إلى إجراء تقييمات في الموقع للبائعين ذوي أعلى المخاطر و/أو الوصول الأكبر لبيانات العملاء.

إدارة أمن الجهة الخارجية

⇒ قم بإجراء العناية الواجبة الشاملة. حدد توقعات الأمن السيبراني في طلبات مؤسستك للمقترحات والعقود واستمرارية العمل والاستجابة للحوادث واتفاقات مستوى الخدمة مع البائعين. اتفق على المسؤوليات والالتزامات في حالة وقوع حادث سيبراني.
- استفسر عن ممارسات الأمن السيبراني الخاصة بجهات خارجية أخرى مثل، المؤسسات المالية التي تتعامل معها أو تشارك البيانات معها. يجب أيضًا على البائعين وأي منظمات أخرى، تشارك البيانات بها أو تعرض الأصول إليها، اتباع أي متطلبات أمن سيبراني على مؤسستك الالتزام بها.

⇒ استخدم التدابير المحددة والمتفق عليها لمراقبة امتثال البائعين لمعايير الأمن السيبراني.
⇒ تحقق مع البائعين الذين يتعاملون مع البيانات الحساسة لمعرفة ما إذا كانوا يقدمون المصادقة الثنائية العوامل أو التشفير أو إجراءات أمنية أخرى لأي حسابات لديك.
⇒ تأكد من أن جميع برامج الجهة الخارجية والأجهزة التي تقوم بتثبيتها تحتوي على مصافحة أمان بحيث يتم تأمين عمليات التشغيل من خلال رموز المصادقة ولن يتم تنفيذها إذا لم يتم التعرف على الرموز.
⇒ إذا صادفت منتجات بائع مزيفة أو غير مطابقة للمواصفات، فاعمل على التفاوض بشأن قرار أو أي استراتيجية للخروج من التعامل معه.
⇒ قم سنويًا بتقييم عقود البائعين والتأكد من استمرارها في تلبية متطلباتك المتعلقة بالتوجيه الإستراتيجي وأمان البيانات التنظيمية. عند إنهاء العقد، قم بتضمين شروط حول استعادة الأصول أو البيانات الخاصة بالمؤسسة والتحقق من أن البائع يحذف الأصول أو البيانات بالكامل، وقم بمنع أي وصول إلى الأنظمة أو الخوادم الخاصة بالمؤسسة.

مشاركة المعلومات

⇒ تأكد من أن لديك قنوات اتصال ونقاط اتصال واضحة للتواصل بشأن المشكلات الأمنية مع بائعي مؤسستك ونظرائها.
⇒ شارك في مشاركة موثوقة في الوقت المناسب لمعلومات الأمن السيبراني القابلة للتنفيذ مع أصحاب المصلحة الداخليين والخارجيين (بما في ذلك الكيانات والسلطات العامة داخل القطاع المالي وخارجه).
⇒ تتبع التحديثات ذات الصلة حول ما تواجهه المنظمات الأخرى مع أطرافها الثالثة فيما يتعلق بالتهديدات ونقاط الضعف والحوادث والاستجابات لتعزيز دفاعات مؤسستك، وزيادة الوعي بالموقف، وتوسيع نطاق التعلم. كونك جزءًا من مؤسسات مشاركة المعلومات، على سبيل المثال، FS-ISAC، سوف يسهل التحديث.

دليل الاستجابة للحوادث

الاستجابة

⇒ نفذ إجراءات خطة الاستجابة للحوادث للحد من الأثر بما في ذلك ما يتعلق بإلحاق الضرر بالسمعة.
⇒ حدد الأنظمة المتأثرة/المتضررة وقيم الضرر.
⇒ حاول الحد من الضرر عن طريق إزالة (فصل) الأصول المتأثرة.
⇒ ابدأ بتسجيل جميع المعلومات بمجرد اشتباه الفريق في وقوع حادث. حاول الحفاظ على دليل على الحادث أثناء فصل/عزل الأصول المحددة المتأثرة على سبيل المثال، جمع سجلات تكوين النظام والشبكة وسجلات كشف التسلل من الأصول المتضررة.
⇒ قم بإخطار الأطراف الداخلية المناسبة والبائعين من جهات خارجية والسلطات، واطلب المساعدة إذا لزم الأمر.
⇒ ابدأ أنشطة الإخطار والمساعدة الخاصة بالعملاء بما يتفق مع القوانين واللوائح التنظيمية والتوجيهات بين الوكالات.
⇒ استخدم منصات مشاركة التهديدات مثل FS-ISAC أو MISP لإخطار المجال عن التهديد.
⇒ وثّق جميع الخطوات التي تم اتخاذها أثناء الحادث لمراجعتها لاحقًا.

الاستعادة

⇒ استعد الأصول المستردة إلى "نقاط الاسترداد" الدورية إذا كانت متاحة واستخدم بيانات النسخ الاحتياطي لاستعادة الأنظمة إلى حالة "جيدة" معروفة.
⇒ قم بإنشاء نسخ احتياطية "نظيفة" محدثة من الأصول التي تمت استعادتها واضمن تخزين جميع النسخ الاحتياطية للأصول الحيوية في موقع آمن ماديًا وبيئيًا.
⇒ تأكد من استعادة الأنظمة المصابة بالكامل واختبرها. تأكد من أن الأنظمة المتأثرة تعمل بشكل طبيعي.

المراجعة

⇒ قم بإجراء مناقشة حول "الدروس المستفادة" بعد وقوع الحادث - اعقد اجتماعات مع كبار الموظفين، والمستشارين المعتمدين وبائع (بائعي) دعم الكمبيوتر لمراجعة نقاط الضعف المحتملة أو التوصية بخطوات جديدة ليتم تنفيذها.
⇒ إذا أمكن، فحدد نقاط الضعف (سواء في البرامج أو الأجهزة أو العمليات التجارية أو سلوك الأفراد) التي أدت إلى الحادث وضع خطة للتخفيف منها.
⇒ ضع خطة للمراقبة للكشف عن أي حوادث مماثلة أو أحداث أخرى تتعلق بالقضايا المحددة.
⇒ شارك الدروس المستفادة والمعلومات حول الحادث في منصات مشاركة التهديدات مثل FS-ISAC.
⇒ ادمج الدروس المستفادة في بروتوكولات الاستجابة لحوادث المؤسسة.

الإعداد

⇒ تعاون مع القيادة العليا في مؤسستك والأفراد الآخرين ذوي الصلة لوضع خطة استجابة للحوادث واستمرارية الأعمال استنادًا إلى أكثر المخاطر إلحاحًا التي تم تحديدها في تقييم المخاطر السيبرانية لمؤسستك.

- ضع سيناريوهات للتهديدات لأنواع الحوادث المرتبطة بالمخاطر السيبرانية ذات الأولوية القصوى لمؤسستك. ركز على بناء القدرة على الاستجابة لتلك السيناريوهات.
- حدد داخل مؤسستك قائمة من نقاط الاتصال للاستجابة للحادث وسجلها واجعلها متاحة.
- حدد وسجل معلومات الاتصال لوكالات ومسؤولي إنفاذ القانون المحليين والاتحاديين.
- ضع أحكامًا تحدد أنواع الحوادث التي يجب الإبلاغ عنها، ومتى يجب الإبلاغ عنها، ولمن.
- ضع مبادئ توجيهية مكتوبة تحدد مدى سرعة استجابة الموظفين لحادث ما والإجراءات التي يجب تنفيذها، استنادًا إلى العوامل ذات الصلة مثل التأثير الوظيفي وآثار الحادث، وإمكانية الاسترداد المحتملة من الحادث.
- أبلغ جميع الموظفين بالاتصال بالفريق الفني - سيتمثل على الأرجح في موظفي تكنولوجيا المعلومات و/أو مدير أمن المعلومات/المدير التنفيذي/مدير آخر مماثل - عند وقوع حادث.
- انشر حلولاً لمراقبة إجراءات الموظفين ولتمكين تحديد التهديدات والحوادث الداخلية.
- قم بتضمين خطط استمرارية الأعمال لتنسيق الطريقة التي ستعمل بها مؤسستك مع الموردين والعملاء الأساسيين في حالة الطوارئ التجارية، بما في ذلك كيفية إجراء عمليات يدوية أو بديلة إذا لزم الأمر.
- قم بتضمين إجراءات مكتوبة لإيقاف تشغيل نظام الطوارئ وإعادة تشغيله.
- طور طرق استرجاع البيانات الاحتياطية واستعادتها واختبرها، واختبر بيانات النسخ الاحتياطي بشكل دوري للتحقق من صلاحيتها.
- ضع اتفاقيات وإجراءات لإجراء العمليات التجارية في منشأة/موقع بديل.
- صمم قناة توزيع واضحة لجميع العملاء.

ممارسة التمارين الرياضية

⇒ نظم تدريبات صغيرة على وضعية سطح الطاولة مع جميع الموظفين أو الممثلين من جميع مستويات الموظفين بما في ذلك المديرون التنفيذيون للمؤسسة، وموظفو العلاقات العامة/الاتصالات، وفرق الشؤون القانونية والامتثال.
⇒ حدد تمارين وضعية سطح الطاولة على مستوى المجال وشارك فيها بصورة مثالية، وذلك في إطار ما يتعلق بمؤسستك.
⇒ ضع عملية لضمان دمج الدروس المستفادة من التدريبات ومعالجتها في إستراتيجية الأمن السيبراني الخاصة بشركتك.