الأمن السيبراني للمؤسسات المالية الأصغر حجمًا

قائمة التدقيق الخاصة بمجلس الإدارة: قيادة الأمن السيبراني

أساسيات إدارة المخاطر السيبرانية

- ☐ كمجموعة، قوموا على أساس دوري بتقييم ما إذا كان مجلس الإدارة يمكن أن يجيب بشكل إيجابي عن الأسئلة التالية:
  - هل تلبي مؤسستك المتطلبات القانونية والتنظيمية ذات الصلة، مثال، النظام الأوروبي العام لحماية البيانات (GDPR)؟
  - هل حددت مؤسستك عدد الهجمات السيبرانية التي تعرضت لها واختبرت مرونتها المالية؟
  - هل تمتلك مؤسستك خطة تحسين لضمان أن الهجمات تقع ضمن معدل المخاطر المتفق عليه؟
  - هل يُناقش مجلس الإدارة بانتظام معلومات دقيقة وواضحة وقابلة للتنفيذ متعلقة بالمرونة السيبرانية للمؤسسة المدعومة من الإدارة؟
  - هل لدى مؤسستك خطط استجابة للحوادث خضعت مؤخرًا لاختبار تجريبي، بما في ذلك على مستوى مجلس الإدارة؟
  - هل أدوار الأشخاص الرئيسيين المسؤولين عن إدارة المخاطر السيبرانية واضحة ومتماشية مع خطوط الدفاع الثلاثة؟
  - هل أجريت تصديقًا وتأكيدًا مستقلين لوضع المخاطر السيبرانية لمؤسستك، على سبيل المثال، عبر الاختبار أو التصديق أو التأمين؟
- ☐ إذا لم تستطع الإجابة بشكل إيجابي عن واحد أو أكثر مما سبق، فتعاون مع المدير التنفيذي ومدير أمن المعلومات وموظفي المؤسسة المعنيين و/أو الجهات الخارجية لحل المشكلة.

الإشراف

- ☐ تأكد من أن مجلس الإدارة على دراية بدوره باعتباره صاحب المسؤولية النهائي للمخاطر والمرونة السيبرانية لمؤسستك.
  - ☐ فوض أمر الإشراف إلى لجنة مجلس إدارة معينة إذا لزم الأمر.
- ☐ قم بتعيين مسؤول شركة واحد، عادةً مدير أمن المعلومات (CISO) المعين، ليكون مسؤولاً عن الإبلاغ عن قدرة مؤسستك على إدارة المرونة السيبرانية والتقدم في تنفيذ أهداف المرونة السيبرانية.
  - ☐ تأكد من أن هذا المسؤول يتمتع بتواصل منتظم مع المجلس، وسلطة كافية، وإتقان للموضوع المعني، والخبرة والموارد اللازمة لتنفيذ هذه المهام.
- ☐ حدد مدى تحمل مؤسستك للمخاطر سنويًا؛ مع ضمان الاتساق مع استراتيجية شركتك ومعدل المخاطر.
- ☐ احرص على أن يتم إجراء مراجعة مستقلة للمرونة السيبرانية لمؤسستك سنويًا.
- ☐ اعمل على دمج المرونة السيبرانية وتقييم المخاطر في استراتيجية الأعمال الشاملة لمؤسستك، وإدارة المخاطر، ووضع الميزانية، وتخصيص الموارد.
- ☐ قم بالإشراف على ابتكار خطط المرونة السيبرانية وتنفيذها واختبارها وتحسينها بصورة مستمرة، لضمان توافقها في جميع أنحاء مؤسستك وأن مدير أمن المعلومات (CISO) أو الموظف الآخر المسؤول يقدم تقارير عنها بصفة منتظمة إلى مجلس الإدارة.
- ☐ راجع أدائك لما ورد أعلاه بشكل دوري وفكر في طلب مشورة مستقلة للتحسين المستمر.

البقاء على اطلاع

- ☐ عندما ينضم فرد جديد إلى مجلس الإدارة، تأكد من أنه يتمتع بمهارات ومعرفة مناسبة ومحدثة لفهم المخاطر التي تمثلها التهديدات السيبرانية وإدارتها.
- ☐ اطلب المشورة المنتظمة من الإدارة فيما يتعلق بتعرض مؤسستك للمخاطر الحالية والمستقبلية، والمتطلبات التنظيمية ذات الصلة، والمعايير الصناعية والاجتماعية لمعدل المخاطر الذي تتبناه. خطط للمشاركة في:
  - جلسات إحاطة منتظمة بشأن الواجبات التي تنشأ عن اللوائح والتشريعات الجديدة،
  - التخطيط المشترك لمجلس الإدارة واللجنة التنفيذية والزيارات إلى الأقران والقادة أصحاب أفضل الممارسات في مجال الأمن السيبراني،
  - جلسات الإحاطة الأمنية بشأن بيئة التهديد،
  - وتبادل المعلومات على مستوى مجلس الإدارة بشأن الإدارة والإبلاغ.
- ☐ أوضح للإدارة أنها مسؤولة عن الإبلاغ عن تقييم كمي ومفهوم للمخاطر والتهديدات والأحداث السيبرانية كعنصر دائم في جدول أعمال اجتماعات مجلس الإدارة.
- ☐ راجع بانتظام مع الإدارة والموظفين الآخرين المعنيين التطورات المتعلقة بالتحديات النظامية المستمرة مثل نقاط ضعف سلسلة التوريد، والتبعيات المشتركة، والفجوة في تبادل المعلومات بين مجالس الإدارة بشأن إدارة المخاطر السيبرانية.

تمهيد السبيل

- ☐ تأكد من أن الموظفين على جميع المستويات يدركون أن كلاً منهم لديه مسؤوليات مهمة لضمان المرونة السيبرانية لمؤسستك.
- ☐ قم بالإشراف على دور الإدارة في تعزيز ثقافة المخاطر لمؤسستك والحفاظ عليها. قيّم بانتظام فعالية ثقافة المخاطر لمؤسستك، مع الوضع في الاعتبار تأثير الثقافة على السلامة والقدرة وإجراء التغييرات عند الضرورة.
- ☐ وضح أنك تتوقع من جميع الموظفين التصرف بنزاهة والإبلاغ الفوري عن أية عملية عدم امتثال ملحوظة داخل مؤسستك أو خارجها.

الأمن السيبراني للمؤسسات المالية الأصغر حجمًا

قائمة التدقيق الخاصة بالمدير التنفيذي: قيادة الأمن السيبراني

الإدارة

- ☐ قم بتعيين مدير أمن للمعلومات (CISO) في حالة عدم وجود من يشغل المنصب.
- ☐ ضع سياسة أمن سيبراني على مستوى المؤسسة وحافظ عليها، واجعلها تعتمد على المخاطر وتستمد معلوماتها من المعايير والإرشادات الدولية والمحلية والخاصة بالمجال.
- ☐ حدد الأدوار والمسؤوليات لجميع الموظفين المشاركين في الأمن السيبراني. اعمل مع مدير أمن المعلومات لتحديد أدوار الأمن السيبراني المناسبة وحقوق الوصول لجميع مستويات الموظفين.
- ☐ قم بإنشاء أو تحديد قنوات اتصال واضحة بين أي وحدات منفصلة أو موظفين يتعاملون مع جوانب مختلفة من الأمن السيبراني.
- ☐ تأكد من أن مدير أمن المعلومات لديه خط اتصال واضح ومباشر لإطلاعك ومجلس الإدارة على التهديدات في الوقت المناسب.
- ☐ احتفظ بمناشدة منتظمة لمدير أمن المعلومات أو الموظفين الفنيين الآخرين لإحاطة الإدارة العليا.
- ☐ تحقق من أن سياسات الأمن السيبراني ومعاييره وآلياته موحدة في جميع أنحاء المؤسسة.

تقييم المخاطر وإدارتها

- ☐ قم بإجراء تقييم مخاطر للأمن السيبراني بالتعاون مع مدير أمن المعلومات أو الموظفين الفنيين الآخرين، والذي يجب أن يشمل:
  - وصفًا لأصول مؤسستك ومختلف مستويات الاعتماد على التكنولوجيا،
  - تقييمًا لنضج مؤسستك والمخاطر الكامنة المرتبطة بالتبعيات التكنولوجية لأصولها،
  - 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 الفهم والوعي والحفاظ عليه،
  - إعادة تقييم نضج الأمن السيبراني والمخاطر والأهداف المتعلقة به في مؤسستك باستمرار، و
  - التفكير في الاستعانة بتدابير وقائية مثل شراء تأمين سيبراني.
- ☐ تحليل وتقديم النتائج لأصحاب المصلحة الرئيسيين ومجلس الإدارة.
- ☐ التخطيط للإشراف على أي خطوات لزيادة الاستعداد الإلكتروني ومراقبة التقدم.

الثقافة المؤسسية

- ☐ ناقش المخاطر والأمن السيبراني بانتظام على مستوى القيادة.
- ☐ تأكد من أن التدريب على الأمن السيبراني جزء من تدريب جميع الموظفين الجدد واطلب من جميع الموظفين التوقيع على الوثائق التي توافق على الالتزام بسياسات الأمن السيبراني الخاصة بالمؤسسة.
- ☐ قم بإنشاء تدريب متكرر على الأمن السيبراني لجميع الموظفين.
- ☐ تأكد من مراعاة الأمن السيبراني دائمًا عندما تقوم مؤسستك بتقييم البائعين المحتملين وتبادل البيانات مع الجهات الخارجية.
- ☐ قم بمراجعة سنوية لسياسات الأمن السيبراني الخاصة بالمؤسسة.
- ☐ شجع الموظفين الفنيين على المشاركة في تبادل المعلومات الطوعية حول التهديدات والحوادث المتعلقة بالأمن السيبراني.

الأمن السيبراني للمؤسسات المالية الأصغر حجمًا

قائمة التدقيق الخاصة بمدير أمن المعلومات: حماية مؤسستك

وضع برنامج لأمن المعلومات قائم على المخاطر

- ☐ حدد جميع أنواع المعلومات التي تُخزنها شركتك أو تستخدمها وأدرجها (مثل، أسماء العملاء وعناوين البريد الإلكتروني).
- ☐ اطرح الأسئلة وسجل الإجابات الخاصة بكل نوع من أنواع المعلومات:
  - ماذا سيحدث إذا تم الإعلان عن هذه المعلومات؟
  - ماذا سيحدث لعملي إذا كانت هذه المعلومات غير صحيحة؟
  - ما الذي سيحدث لشركتي إذا لم أتمكن أنا أو عملائي من الوصول إلى هذه المعلومات؟
- ☐ حدد التكنولوجيا المرتبطة بالمعلومات التي حددتها. يمكن أن يشمل ذلك الأجهزة (مثل، أجهزة الكمبيوتر) وتطبيقات البرامج (مثل، البريد الإلكتروني للمستعرض).
  - عند الاقتضاء، قم بتضمين تكنولوجيات من خارج عملك (مثل "السحابة") وأي تقنيات حماية موجودة لديك مثل جدران الحماية.
  - ضمّن الصنع والطراز والأرقام التسلسلية ومعرفات أخرى.
  - تتبع موقع كل منتج. بالنسبة للبرنامج، حدد الجهاز (الأجهزة) الذي تم تحميل البرنامج عليه.
- ☐ راجع بانتظام المعلومات الواردة من CERT وFS-ISAC الوطنية وفصل InfraGard المحلي، وغيرها، حول التهديدات ونقاط الضعف التي قد يواجهها القطاع المالي وتقدير احتمال تأثرك.
- ☐ قم بإجراء فحص أو تحليل لنقاط الضعف مرة واحدة في السنة على الأقل.
- ☐ قم بإنشاء سياسة أمن سيبراني لمؤسستك.
- ☐ 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.

تجنب التلف الناجم عن البرمجيات الخبيثة

- ☐ قم بتنشيط جدار الحماية وحدد قوائم التحكم في الوصول (ACLs). قم بتقييد الوصول باستخدام إعداد القائمة البيضاء.
- ☐ استخدم برامج مكافحة الفيروسات والحماية من برامج التجسس على جميع أجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة.
- ☐ طبق أحدث تحديثات البرامج التي تقدمها الجهات المُصنعة والبائعون. "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.
- ☐ 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 USBs من مصادر خارجية أو إعطاء وحدات USB الخاصة 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.
- ☐ فكر في توظيف خدمة اختبار الاختراق لتقييم أمن أصول مؤسستك وأنظمتها.

تدريب الموظفين

- ☐ خطط لتقديم دورات تدريبية إلزامية حول الأمن 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.

☐ خطط لإجراء اختبارات لوعي الموظف وطبقها، وذلك من خلال المحاكاة مثل، إرسال رسائل بريد إلكتروني على غرار التصيد الاحتيالي من حسابات وهمية. قيّم أي أخطاء يقع فيها الموظفون واستخدمها كفرص للتعلم والتحسين.

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 التغيرالمفاجيء 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 كلمة المرور وحماية رقم التعريف الشخصي 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.

☐ استخدم 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.

CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE · SWIFT · SWIFT INSTITUTE · FS-ISAC · Standard Chartered · CYBER READINESS INSTITUTE · GLOBAL CYBER ALLIANCE

- ☐ لا تمنح الموظفين إمكانية وصول إلا إلى أنظمة البيانات المحددة التي يحتاجون إليها لوظائفهم وتأكد من عدم امتلاكهم إمكانية تثبيت أي برنامج دون إذن.
- ☐ قم بإنشاء حسابات مستخدم لكل موظف على أجهزة الكمبيوتر الخاصة بمؤسستك.

تأمين شبكة WI-FI

- ☐ 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. سجل جهاز التوجيه لدى الشركة المُصنعة وسجل الدخول للحصول على التحديثات.

تجنُّب 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).

الأمن السيبراني للمؤسسات المالية الأصغر حجمًا

قائمة التدقيق الخاصة بمدير أمن البيانات: حماية عملائك

تقديم المشورة للعملاء والموظفين بشأن حماية البيانات على المستوى الفردي

- ☐ زود الموظفين والعملاء بالمبادئ التوجيهية الشخصية التالية الواجب اتباعها لحماية بياناتهم بشكل أفضل:
  - استخدم كلمات مرور قوية على جميع الأجهزة الشخصية والمهنية، وفكر في استخدام مدير كلمة المرور.
  - حافظ على تحديث أنظمة التشغيل والبرامج والتطبيقات الأخرى على جميع 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.
  - 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.
  - 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، حاول الحد من 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.
- ☐ اعرض أو اطلب، 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 وإنفاذها على جميع الموظفين، وأنه تتم مراجعتها 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 أمان المحتوى على الموقع الإلكتروني (المواقع الإلكترونية).
- ☐ قم بتمكين تحديد المفتاح العام على الموقع الإلكتروني (المواقع الإلكترونية).
- ☐ تأكد من عدم استخدام تطبيق (تطبيقات) الويب العام أبدًا لملفات تعريف الارتباط بهدف تخزين معلومات العميل الحساسة أو البالغة الأهمية (مثل، كلمات المرور) وأن لها 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،
  - والإبلاغ 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 البيانات وسياسات الأمن الخاصة بالمؤسسة.

إخطار العملاء

- ☐ افهم 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 في أقرب وقت ممكن، وذلك عن طريق تقديم:
  - وصف عام للحادث والمعلومات التي تم اختراقها؛
  - رقم هاتف لتقديم مزيد 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؛
  - وأي معلومات أخرى مطلوبة بموجب اللوائح التي يجب على مؤسستك الامتثال لها.

الأمن السيبراني للمؤسسات المالية الأصغر حجمًا

قائمة التدقيق الخاصة بمدير أمن البيانات: حماية الاتصالات للجهات الخارجية

اختيار البائعين مع وضع الأمن السيبراني في الاعتبار

في كل مرة تقوم فيها بتقييم بائع محتمل، راجع الأسئلة التالية:

- ☐ ما الخبرة التي يمتلكها البائع في خدمة عملاء مشابهين لمؤسستك؟
- ☐ هل وثقوا امتثالهم لمعايير الأمن السيبراني المعروفة (مثل إطار عمل NIST أو معيار الأيزو 27001، أو هل يمكنهم تقديم تقرير SOC2)؟
- ☐ أي من بياناتك و/أو أصولك سيحتاجون إلى الوصول إليها لأداء خدماتهم، وهل يطلبون أي وصول غير ضروري ظاهريًا؟
- ☐ كيف يخططون لحماية أصول مؤسستك وبياناتها الموجودة في حوزتهم؟
- ☐ كيف يديرون المخاطر السيبرانية الخاصة بالجهة الخارجية، وهل يمكنهم تقديم معلومات عن أمن سلسلة التوريد الخاصة بهم؟
- ☐ ما خطتهم للتعافي من الكوارث واستمرارية الأعمال في حالة وقوع حادث يؤثر في مؤسستك؟
- ☐ كيف سيحافظون على تحديث مؤسستك من حيث التواصل، والتهديدات، والتغييرات داخل مؤسستهم؟

تحديد المخاطر من خلال الجهات الخارجية

قم بإجراء تقييم للمخاطر السيبرانية للجهة الخارجية، بما في ذلك الخطوات التالية:

- ☐ قم بإنشاء قائمة بالعلاقات مع جميع البائعين، والأصول والبيانات المعروضة في كل منها، وحدثها باستمرار.
- ☐ قم بإجراء مراجعة للبيانات التي يستطيع كل بائع أو جهة خارجية الوصول إليها، مع ضمان التزام كل مستوى من مستويات الوصول بمبدأ "الامتياز الأقل".
- ☐ رتب علاقاتك مع البائع والجهة 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 والامتثال للمعايير ذات الصلة.
- ☐ قم بتطوير خطة للتقييم الأمني المنتظم، مع الأخذ في الاعتبار أنك قد ترغب أحيانًا في إجراء تقييمات موقعية للبائعين الذين لديهم أعلى مخاطر و/أو أكبر وصول إلى بيانات العميل.

إدارة أمن الجهة الخارجية

- ☐ قم بإجراء العناية الواجبة الشاملة. حدد توقعات الأمن السيبراني في جميع 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 للمؤسسات المالية والكيانات الأخرى التي تتعامل معها أو تشارك البيانات معها، مع الأخذ بعين الاعتبار أن البائعين والجهات الخارجية يجب أن يتبعوا أيضًا أي متطلبات أمن سيبراني يجب أن تلبيها مؤسستك.
- ☐ 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.

تبادل المعلومات

- ☐ تأكد من أن لديك قنوات اتصال ونقاط اتصال واضحة للتواصل بشأن المشكلات الأمنية مع بائعي مؤسستك ونظرائها.
- ☐ تحقق من أن لدى مؤسستك إجراءات لضمان تبادل موثوق 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 بشأن ما تخوضه المؤسسات الأخرى مع الجهات الخارجية من حيث التهديدات، ونقاط الضعف، والحوادث، والاستجابات من خلال المشاركة في مؤسسات تبادل المعلومات مثل FS-ISAC والبحث عن مصادر معلومات تهديدات أخرى.

الأمن السيبراني للمؤسسات المالية الأصغر حجمًا

قائمة تدقيق الاستجابة للحوادث

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.
  - ☐ 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 استراتيجية الأمن السيبراني الخاصة بشركتك.

الاستجابة

- ☐ نفذ إجراءات خطة الاستجابة للحوادث للحد من التأثير على العمليات التجارية.
- ☐ 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 آخر 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.
- ☐ تأكد من أن الأنظمة المتأثرة تعمل بشكل طبيعي.
- ☐ 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.