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).