

الأمن السيبراني للمؤسسات 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 بمناقشة منتظمة لمدير أمن المعلومات أو الموظفين الفنيين الآخرين لإحاطة الإدارة العليا.
- تحقق من أن سياسات الأمن السيبراني ومعايير 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،
 - تقييم الأموال وتخصيصها للاستثمار في الأمن ومعالجة الفجوات القائمة،
 - 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.
- دمج تقييم الأمن السيبراني للمؤسسة عند النظر في تنفيذ عمليات الدمج والاستحواذ.
- قم بمراجعة سنوية لسياسات الأمن السيبراني الخاصة بالمؤسسة.
- شجع الموظفين الفنيين على المشاركة في تبادل المعلومات الطوعية حول التهديدات والحوادث المتعلقة بالأمن السيبراني.