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،