١٠ مجالات لتحسين جاهزية الأمن السيبراني

حماية البيانات هي دورة مستمرة
تكون البيانات عند الإنشاء والنقل والتخزين عرضة لمخاطر مثل اللوصول غير المصرح به أو التعديل أو الحذف أو أنواع أخرى من التهديدات مثل برامج الفدية. فأحرص على تطبيق تدابير الحماية والضمانات اللازمة لمنع فقدان/اختراق البيانات والحفاظ على ثالوث أمن المعلومات "CIA Triad".

ضبط إعدادات المراقبة الأمنية ومراجعة السجلات الالكترونية
المراقبة الأمنية ومراجعة السجلات في النظام (الكمبيوتر أو الجدار الناري أو التطبيق) بشكل دوري يساعدك في فهم أداء النظام والتشغيل القائم، حيث تعد هذه إحدى الخطوات الاستباقية لتحديد والكشف عن المؤشرات التي تدل على أن النظام قد يتعرض للهجمات أو الاختراق وبالتالي يمكنك استخدام تلك المعلومات بشكل فعال في التحقق من أسباب الاختراق أو التفاعل السريع مع التنبيهات للردع من احتمالية نجاح الهجمة.

الاستثمار في جاهزية الأمن السيبراني (إدارة الاستجابة للحوادث وعملية الاستجابة)
من المهم أن تبني القدرة على التعرف وردع التهديدات السيبرانية الاستجابة للحوادث وأن تكون تلك الجاهزية جزء من سياسة الأمن السيبراني الخاصة بالمنشأة. خطط مسبقًا ووفقًا للضوابط الأساسية للأمن السيبراني لوضع خطة للاستجابة لحوادث الأمن السيبراني والتعاون المطلوب مع الموردين والجهات الوطنية المسؤولة.

إدارة الهوية والدخول
تأكد من آلية التحقق من هويات المستخدمين والتحكم في حقوق الوصول وعمليات دخول المستخدمين للنظام، وقم بمراجعة أنشطة الدخول للموظفين وذلك لحماية البيانات والأجهزة. ضع في اعتبارك أيضًا صلاحيات الوصول والاتصال التلقائي من الأنظمة ذاتها إلى البيانات واحرص على إجراء تغييرات بداخل الأنظمة الأخرى من خلال ضبط الإعدادات.

أمن سلسلة التوريد
كن مدركاً للمخاطر المحتملة في أمن سلسلة التوريد وقم تحويل المخاطر الى فرص من خلال الحفاظ على علاقة عمل وثيقة مع البائعين والموردين من خلال الزيارات المتكررة والاتصالات لتبادل أفضل ممارسات الأمن السيبراني في عملية الشراء أو مشاريع التطوير.

إدارة الثغرات الأمنية / نقاط الضعف
حافظ على أمان البنية التحتية التقنية من هجمات الاستغلال المعروفة وأحرص على الالتزام وتطبيق المعايير أو أي متطلبات تنظيمية. من المهم إعطاء الأولوية للتعامل مع الثغرات الأمنية ذات الأهمية البالغة (تصنيف CVSS) بالإضافة الى التعرف وتحديد الأنظمة الحيوية الحساسة وأي نقاط ضعف من شأنها أن تؤثر على المؤسسة .

إدارة الأصول
تأكد من التعرف وتحديد وتتبع الأنظمة والبيانات التي تمتلكها المؤسسة بالإضافة الى المخاطر أو الثغرات الأمنية المحتملة التي تؤثر على كل منها، ودورها في العمل.

المشاركة والتدريب
يبدأ الأمر ببناء ثقافة إيجابية لـ مخاطر الأمن السيبراني في المؤسسة، حيث يعتبر "الأمن السيبراني" مسؤولية الجميع. تعد ثقافة المخاطر مؤشر رئيسيا على مدى انتشار السياسات وممارسات إدارة المخاطر في المؤسسة. فأحرص على تمكين الموظفين بالمهارات وتزويدهم بالمعرفة من خلال التوعية والتدريب الفعال.

بُنية آمنة، وضبط الإعدادات بشكل آمن
اتبع النهج الدفاعي المتعمق لتتضمن هندسة البنية التحتية مناطق الأمن بالشبكة والاعدادات المطلوبة لجميع الأنظمة والأجهزة في المؤسسة. كما أن هنالك مفهوم آخر يجب مراعاته في هذا النهج ألا وهو إتباع منهجية" التصميم الآمن" والذي سيساعد بشكل استباقي في الحماية من التهديدات السيبرانية.

إدارة مخاطر الأمن السيبراني
تُطبق جميع برامج الأمن السيبراني الناجحة نهجًا قائمًا على المخاطر مصممًا وفقاً للاحتياجات التنظيمية المحددة ونقاط الضعف التشغيلية.