



المركز الوطني للأمن السيبراني
NATIONAL CYBER SECURITY CENTER



مجالات لتحسين جاهزية الأمن السيبراني



لمزيد من المعلومات
امسح هنا!

#الوعي_السيبراني
www.ncsc.gov.bh



حماية البيانات دورة مستمرة



تكون البيانات عند الإنشاء والنقل والتخزين عرضة للمخاطر، مثل: الوصول غير المصرح به أو التعديل أو الحذف أو أنواع أخرى من التهديدات مثل برامج الفدية. احرص على تطبيق تدابير الحماية والضمانات اللازمة لمنع فقدان/اختراق البيانات والحفاظ على ثلوث أمن المعلومات "CIA Triad".

ضبط إعدادات المراقبة الأمنية ومراجعة السجلات الإلكترونية



المراقبة الأمنية ومراجعة السجلات في النظام (الحاسب الآلي أو الجدار الناري أو التطبيق) بشكل دوري يساعدك في فهم أداء النظام والتشغيل القائم، حيث تعد هذه إحدى الخطوات الاستباقية لتحديد وكشف المؤشرات التي تدل على أن النظام قد يتعرض للهجمات أو الاختراق ويمكنك 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 والاستجابة للحوادث وأن تكون تلك الجاهزية جزءًا 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، وراجع أنشطة دخول الموظفين لحماية البيانات والأجهزة. ضع في اعتبارك أيضًا صلاحيات الوصول والاتصال التلقائي من الأنظمة ذاتها إلى البيانات وحرص على إجراء تغييرات بداخل الأنظمة الأخرى من خلال ضبط الإعدادات.

أمن سلسلة التوريد



كن مدركًا للمخاطر المحتملة في أمن سلسلة التوريد وقم بتحويل المخاطر إلى 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 وحرص على الالتزام وتطبيق المعايير أو أي متطلبات تنظيمية. من المهم إعطاء الأولوية للتعامل مع الثغرات الأمنية ذات الأهمية البالغة (تصنيف CVSS) بالإضافة إلى 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 إلى المخاطر أو الثغرات الأمنية المحتملة التي تؤثر على كل منها، ودورها في العمل.

المشاركة والتدريب



يبدأ الأمر ببناء ثقافة إيجابية حول مخاطر الأمن السيبراني في المؤسسة، حيث يعتبر "الأمن السيبراني" مسؤولية الجميع. تعد ثقافة المخاطر مؤشرًا رئيسيًا على مدى انتشار السياسات وممارسات إدارة المخاطر في المؤسسة. فاحرص على تزويد الموظفين بالمهارات والمعرفة من خلال التوعية والتدريب الفعال.

بُنية آمنة، وضبط الإعدادات بشكل آمن



اتبع النهج الدفاعي المتعمق لتضمن هندسة البنية التحتية مناطق الأمن بالشبكة والإعدادات المطلوبة لجميع الأنظمة والأجهزة في المؤسسة، واتباع منهجية "التصميم الآمن" والذي يساعد بشكل استباقي في الحماية من التهديدات السيبرانية.

إدارة مخاطر الأمن السيبراني



تطبق جميع برامج الأمن السيبراني الناجحة نهجًا مصممًا وفقًا للاحتياجات التنظيمية المحددة ونقاط الضعف التشغيلية.