جمعية البر الخيرية بأم الدوم
تحت إشراف وزارة الموارد البشرية
و التنمية الاجتماعية برقم 413

شجرة لا تموت

سياسة الحماية من البرمجيات الضارة

٢٠٢٠ م

الأهداف

الغرض من هذه السياسة هو توفير متطلبات الأمن السيبراني المبنية على أفضل الممارسات والمعايير المتعلقة بحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم الخاصة بـجمعية البر الخيرية بأم الدوم من تهديدات البرمجيات الضارة وتقليل المخاطر السيبرانية الناتجة عن التهديدات الداخلية والخارجية من خلال التركيز على الأهداف الأساسية للحماية وهي: سرية المعلومات، وسلامتها، وتوافرها.

وتهدف هذه السياسة إلى الالتزام بمتطلبات الأمن السيبراني والمتطلبات التشريعية والتنظيمية ذات العلاقة، وهي مطلب تشريعي في الضابط رقم ٢-٣-١ من الضوابط الأساسية للأمن السيبراني (ECC-1:2018) الصادرة من الهيئة الوطنية للأمن السيبراني.

نطاق العمل وقابلية التطبيق

تغطي هذه السياسة جميع أجهزة المستخدمين والخوادم الخاصة بـجمعية البر الخيرية بأم الدوم، وتنطبق على جميع العاملين في جمعية البر الخيرية بأم الدوم.

بنود السياسة

١- البنود العامة

١-١ يجب على جمعية البر الخيرية بأم الدوم تحديد تقنيات وآليات الحماية الحديثة والمتقدمة وتوفيرها والتأكد من موثوقيتها.

١-٢ يجب تطبيق تقنيات وآليات الحماية لحماية أجهزة المستخدمين والأجهزة المحمولة والخوادم من البرمجيات الضارة (Malware) وإدارتها بشكل آمن.

١-٣ يجب التأكد من أن تقنيات وآليات الحماية قادرة على اكتشاف جميع أنواع البرمجيات الضارة المعروفة وإزالتها، مثل الفيروسات (Virus)، وأحصنة طروادة (Trojan Horse)، والديدان (Worms)، وبرمجيات التجسس (Spyware)، وبرمجيات الإعلانات المتسللة (Adware)، ومجموعة الجذر (Root Kits).

١-٤ قبل اختيار تقنيات وآليات الحماية، يجب التأكد من ملاءمتها لأنظمة التشغيل الخاصة بـجمعية البر الخيرية بأم الدوم مثل أنظمة ويندوز (Windows)، وأنظمة يونكس (UNIX)، وأنظمة لينكس (Linux)، ونظام ماك (Mac)، وغيرها.

١-٥ في حال تسبب تحديث تقنيات الحماية بضرر للأنظمة أو متطلبات الأعمال، يجب التأكد من أن تقنيات الحماية قابلة للاسترجاع إلى النسخة السابقة.

١-٦ يجب تقييد صلاحيات تعطيل التثبيت أو إلغائه أو تغيير إعدادات تقنيات الحماية من البرمجيات الضارة ومنحها لمشرفي نظام الحماية فقط.

٢- إعدادات تقنيات وآليات الحماية من البرمجيات الضارة

٢-١ يجب ضبط إعدادات تقنيات الحماية وآلياتها وفقاً للمعايير التقنية الأمنية المعتمدة لدى جمعية البر الخيرية بأم الدوم، مع الأخذ بالاعتبار إرشادات المورد وتوصياته.

٢-٢ يجب ضبط إعدادات برنامج مكافحة الفيروسات على خوادم البريد الإلكتروني لفحص جميع رسائل البريد الإلكتروني الواردة والصادرة.

٢-٣ لا يُسمح للأشخاص التابعين لأطراف خارجية بالاتصال بالشبكة أو الشبكة اللاسلكية لـجمعية البر الخيرية بأم الدوم دون تحديث برنامج مكافحة الفيروسات وضبط الإعدادات المناسبة.

٢-٤ يجب ضمان توافر خوادم برامج الحماية من البرمجيات الضارة، كما يجب أن تكون البيئة الاحتياطية مناسبة لخوادم برامج الحماية من البرمجيات الضارة المخصصة للمهام والأعمال غير الحساسة.

٢-٥ يجب منع الوصول إلى المواقع الإلكترونية والمصادر الأخرى على الإنترنت المعروفة باستضافتها لبرمجيات ضارة وذلك باستخدام آلية تصفية محتوى الويب (Filtering Web Content).

٢-٦ يجب مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق لجميع تقنيات وآليات الحماية من البرمجيات الضارة.

٢-٧ يجب ضبط إعدادات تقنيات الحماية من البرمجيات الضارة للقيام بعمليات التحقق من المحتوى المشبوه في مصادر معزولة مثل صندوق الفحص (Sandbox).

٢-٨ يجب القيام بعمليات مسح دورية لأجهزة المستخدمين والخوادم والتأكد من سلامتها من البرمجيات الضارة.

٢-٩ يجب تحديث تقنيات الحماية من البرمجيات الضارة تلقائياً عند توفر إصدارات جديدة من المورد، مع الأخذ بالاعتبار سياسة إدارة التحديثات والإصلاحات.

٢-١٠ يجب توفير تقنيات حماية البريد الإلكتروني وتصفح الإنترنت من التهديدات المتقدمة المستمرة (APT Protection)، والتي تستخدم عادةً الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Zero-Day Malware)، وتطبيقها وإداراتها بشكل آمن.

٢-١١ يجب ضبط إعدادات تقنيات الحماية بالسماح لقائمة محددة فقط من ملفات التشغيل (Whitelisting) للتطبيقات والبرامج للعمل على الخوادم الخاصة بالأنظمة الحساسة. (CSCC-2-3-1-1)

٢-١٢ يجب حماية الخوادم الخاصة بالأنظمة الحساسة عن طريق تقنيات حماية الأجهزة الطرفية المعتمدة لدى جمعية البر الخيرية بأم الدوم (End-point Protection). (CSCC-2-3-1-2)

٢-١٣ يجب إعداد تقارير دورية حول حالة الحماية من البرمجيات الضارة يوضح فيها عدد الأجهزة والخوادم المرتبطة بتقنيات الحماية وحالتها (مثل: محدثة، أو غير محدثة، أو غير متصلة، إلخ)، ورفعها إلى مسؤول تقنية المعلومات.

٢-١٤ يجب إدارة تقنيات الحماية من البرمجيات الضارة مركزياً ومراقبتها باستمرار.

٣- متطلبات أخرى

٣-١ يجب على مسؤول تقنية المعلومات التأكد من توافر الوعي الأمني اللازم لدى جميع العاملين للتعامل مع البرمجيات الضارة والتقليل من خطورتها.

٣-٢ يجب استخدام مؤشر قياس الأداء (KPI) لضمان التطوير المستمر لحماية أجهزة المستخدمين والخوادم من البرمجيات الضارة.

٣-٣ يجب مراجعة متطلبات الأمن السيبراني لحماية أجهزة المستخدمين والخوادم الخاصة بـجمعية البر الخيرية بأم الدوم دورياً.

الأدوار والمسؤوليات

١. **راعي ومالك وثيقة السياسة:** مسؤول تقنية المعلومات.

٢. **مراجعة السياسة وتحديثها:** مسؤول تقنية المعلومات.

٣. **تنفيذ السياسة وتطبيقها:** المدير التنفيذي ومسؤول تقنية المعلومات.

الالتزام بالسياسة

١. يجب على مسؤول تقنية المعلومات ضمان التزام جمعية البر الخيرية بأم الدوم بهذه السياسة دورياً.

٢. يجب على كافة العاملين في جمعية البر الخيرية بأم الدوم الالتزام بهذه السياسة.

٣. قد يعرض أي انتهاك لهذه السياسة صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في جمعية البر الخيرية بأم الدوم.

المحتويات