هذا المربع مخصّص لأغراض توجيهية. احذف جميع المربعات التوجيهية بعد تعبئة النموذج. يجب تحرير البنود الملوّنة باللون الأزرق بصورة مناسبة. ويجب إزالة التظليل الملون بعد إجراء التعديلات.

أدخل شعار الجهة بالضغط على الصورة الموضحة.

نموذج معيار أمن الخوادم

استبدل <اسم الجهة> باسم الجهة في مجمل صفحات الوثيقة. وللقيام بذلك، اتبع الخطوات التالية:

- اضغط على مفتاحي "Ctrl" و"H" في الوقت نفسه.
- أضف "<اسم الجهة>" في مربع البحث عن النص.
- أدخل الاسم الكامل لجهتك في مربع "استبدال" النص.
- اضغط على "المزيد" وتأكّد من اختيار "Match case".
- اضغط على "استبدل الكل".
- أغلق مربع الحوار.

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

إخلاء المسؤولية

طُور هذا النموذج عن طريق الهيئة الوطنية للأمن السيبراني كمثال توضيحي يمكن استخدامه كدليل ومرجع للجهات. يجب أن يتم تعديل هذا النموذج ومواءمته مع أعمال <اسم الجهة> والمتطلبات التشريعية والتنظيمية ذات العلاقة. كما يجب أن يُعتمد هذا النموذج من قبل رئيس الجهة أو من يقوم/تقوم بتفويضه. وتخلي الهيئة مسؤوليتها من استخدام هذا النموذج كما هو، وتؤكد على أن هذا النموذج ما هو إلا مثال توضيحي.

اختر التصنيف

الإصدار <١,٠>

اعتماد الوثيقة

الدور	المسمى الوظيفي	الاسم	التاريخ	التوقيع
اختر الدور	<أدخل المسمى الوظيفي>	<أدخل الاسم الكامل للموظف>	اضغط هنا لإضافة تاريخ	<أدخل التوقيع>

نسخ الوثيقة

النسخة	التاريخ	عُدِّلَ بواسطة	أسباب التعديل
<أدخل رقم النسخة>	اضغط هنا لإضافة تاريخ	<أدخل الاسم الكامل للموظف>	<أدخل وصف التعديل>

جدول المراجعة

معدل المراجعة	التاريخ لأخر مراجعة	تاريخ المراجعة القادمة
مره واحدة كل سنة	اضغط هنا لإضافة تاريخ	اضغط هنا لإضافة تاريخ

اختر التصنيف

الإصدار <١,٠>

قائمة المحتويات

الغرض ٤
نطاق العمل ٤
المعايير ٤
الأدوار والمسؤوليات ٨
التحديث والمراجعة ٨
الالتزام بالمعيار ٨

اختر التصنيف

الإصدار <١,٠>

الغرض

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية المتعلقة بإدارة وحماية الخوادم الخاصة ب<اسم الجهة> لتقليل المخاطر السيبرانية وحمايتها من التهديدات الداخلية والخارجية.

تمت موائمة هذا المعيار مع سياسة أمن الخوادم والضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

نطاق العمل

يغطي هذا المعيار جميع الأصول التقنية والمعلوماتية (شاملة الخوادم وأنظمة التشغيل) الخاصة ب<اسم الجهة>، وينطبق على جميع العاملين (الموظفين والمتعاقدين) في <اسم الجهة>.

المعايير

١	الوصول الآمن (Secure Access)
الهدف	ضمان حماية الخوادم ووظائفها من الوصول غير المصرح به.
المخاطر المحتملة	الوصول غير المصرّح به إلى الخوادم يعرض <اسم الجهة> لمخاطر عالية قد تؤدي إلى تسريب البيانات أو سرقتها أو تعطيل الخدمات أو انتهاكات أمنية تسمح لمنفذيها باستخدامها لشن المزيد من الهجمات السيبرانية ضدها وضد بنيتها التحتية.
الإجراءات المطلوبة	
١-١	حصر الوصول إلى الخوادم على مشرفي الخوادم فقط وذلك من خلال منح حق الوصول لحسابات المشرفين المختلفين وبروتوكول الإنترنت لأجهزة المستخدمين باستخدام قوائم التحكم بالوصول (ACLs).
١-٢	تعطيل الحسابات الافتراضية (Default Accounts) أو غير التفاعلية أو غير اللازمة.
١-٣	ضبط وإعداد وقت انتهاء الجلسة وحد إغلاق الجلسة عند عدم الاستخدام وفقًا معيار إدارة هويات الدخول والصلاحيات المعتمد لدى <اسم الجهة>.
١-٤	ضبط وإعداد كلمات مرور مُحمِّل تشغيل (Bootloader) نظام الإدخال/الإخراج الأساسي (BIOS).
١-٥	تقييد وصول المشرفين والمشغلين إلى الخوادم الحساسة وحصره على أجهزة الحاسب ذات الصلاحيات الهامة والحساسة (PAWs) وتشفير عمليات الوصول الخاصة بهم.

٦-١	تقييد الوصول إلى الخوادم وحصره على المشرفين والمشغلين وذلك عن طريق خوادم الوصول إلى المناطق الآمنة (Jump Servers) أو إدارة الصلاحيات الهامة والحسّاسة (PAM). ١-٦-١ استخدام خوادم منفصلة للوصول إلى المناطق الآمنة (Jump Servers) لمشرفي ومستخدمي النظام. ٢-٦-١ استخدام التحقّق من الهوية متعدّد العناصر من أجل الوصول عبر خوادم الوصول إلى المناطق الآمنة (Jump Server) المستخدمة من قبل مشرفي النظام وذلك من خلال تطبيق قوائم التحكم بالوصول (ACLs). ٣-٦-١ تقييد الوصول إلى خوادم الوصول إلى المناطق الآمنة(Jump Servers) وحصره على المشرفين والمشغلين المصرح لهم فقط. ٤-٦-١ تقييد الوصول إلى الشبكة وحصره على خوادم الوصول إلى المناطق الآمنة (Jump Servers)من خلال تطبيق قوائم التحكم بالوصول(ACLs) . ٥-٦-١ وضع خوادم الوصول إلى المناطق الآمنة (Jump Servers) في منطقة إدارة الشبكة. ٦-٦-١ إلغاء تفعيل خاصية الوصول إلى الإنترنت على خوادم الوصول إلى المناطق الآمنة (Jump Servers). ٧-٦-١ إلغاء تفعيل الخدمات الخطرة وغير اللازمة (مثل إرسال رسائل البريد الإلكتروني واستلامها) على خوادم الوصول إلى المناطق الآمنة (Jump Servers). ٨-٦-١ تفعيل جميع مستويات التسجيل إضافةً إلى سجل التدقيق والسجلات الأمنية محليًا وعلى نظام تسجيل أحداث مركزي.
٢	حماية الخوادم (Server Protection)
الهدف	ضمان حماية الخوادم من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقًا وأي نوع آخر من الهجمات الخبيثة.
المخاطر المحتملة	يمكن أن تؤدي الهجمات الخبيثة الناجحة على الخوادم إلى تعريض <اسم الجهة> لاختراق أمني أو وصول غير مصرح به أو الكشف عن البيانات في حال تركت الخوادم دون حماية.
الإجراءات المطلوبة	
١-٢	ضبط وإعداد حد إغلاق نظام التشغيل ووظائف التطبيقات عن طريق الحد الأدنى من الصلاحيات والامتيازات المطلوب للتشغيل في الظروف الاعتيادية، مثل إلغاء تفعيل تغيير وقت النظام يدويًا، والإغلاق/إعادة التشغيل، وتعديل ملفات النظام، وإنشاء/تعديل/حذف الملفات، وغيرها.
٢-٢	تطبيق خاصية السماح بقائمة محددة من التطبيقات (whitelisting) على الخوادم لتمكين عمل تطبيقات وبرمجيات محددة فقط وفقًا للحاجة.

٢-٣	إعداد أنظمة السماح بقائمة محددة من التطبيقات بحيث لا يمكن للمستخدمين إلغاء تفعيل الأنظمة باستثناء مديري النظام عند أدائهم لمهام إدارية معينة تقتضي إلغاء تفعيل السماح بقائمة محددة من التطبيقات مؤقتًا.
٢-٤	تعريف الملفات التنفيذية المعتمدة (exe وcom وpif وغيرها) ومكتبات البرمجيات (dll وocx وغيرها) والنصوص (ps١ وbat وvbs وغيرها) وبرامج التثبيت (msi وmsp وغيرها) واعتمادها بحيث يتم تنفيذها بواسطة مستخدمين معينين حسب الاحتياجات.
٢-٥	تطبيق خاصية السماح بقائمة محددة من التطبيقات (whitelisting) لاستخدام قواعد التجزئة المشفرة أو قواعد شهادات الناشر أو قواعد المسار للسماح باستخدام التطبيقات أو منعها.
٢-٦	ضبط وإعداد مجلدات التطبيقات وفقًا لتصاريح نظام الملفات لمنع أي تعديل غير مصرح به على المجلد أو تصاريح الملفات.
٢-٧	تمكين وظيفة الحماية على الخوادم لاستخدامها في إجراءات الحد من المخاطر على نظام التشغيل وإجراءات الحد من المخاطر لتطبيقات معينة.
٢-٨	تطبيق نظام الكشف والاستجابة عند النقطة النهائية (Endpoint Detection and Response (EDR)) ونظام كشف الاختراقات القائم على المستضيف (Host-based Intrusion Detection System (HIDS)) ونظام الحماية المتقدمة لاكتشاف ومنع الاختراقات في المستضيف (Host-based Intrusion Prevention System "HIPS") على جميع الخوادم.
٢-٩	استخدام جدار حماية من البرمجيات المستضافة على جميع الخوادم.
٢-١٠	استخدام برامج مكافحة الفيروسات على جميع الخوادم.
٢-١١	استخدام حماية الأجهزة الطرفية (Endpoint Protection) على جميع الخوادم.
٢-١٢	استخدام برامج الحماية من التهديدات المتقدمة المستمرة (APT) على جميع الخوادم.
٢-١٣	استخدام برمجيات التحكم بأجهزة النهاية الطرفية على كافة الخوادم لمنع الاستخدام غير المصرح به للأجهزة.
٢-١٤	استخدام تقنية منع تسّرب البيانات (DLP) عند الضرورة وفقًا للمعايير المذكورة في معيار منع تسرب البيانات المعتمد لدى <اسم الجهة>.
٢-١٥	تطبيق جميع المتطلبات بموجب سياسة الحماية من البرمجيات الضارة المعتمدة في <اسم الجهة>.

٣	إدارة الخوادم (Central Management)
الهدف	تحديد المتطلبات الأمنية لإدارة الخوادم لضمان إدارة وتشغيل الخوادم بطريقة آمنة وضمان تطبيق وتنفيذ جميع المتطلبات الأمنية.
المخاطر المحتملة	يؤدي الافتقار إلى الإدارة الآمنة وعدم تطبيق المتطلبات الأمنية على الخوادم إلى زيادة احتمالية التعرض للهجمات ووجود الثغرات ونقاط الضعف في بيئة <اسم الجهة>، حيث يمكن استغلال هذه الثغرات في الهجمات أو الاختراقات الخبيثة التي تعرض الخوادم والبيانات في <اسم الجهة> إلى انتهاكات أمنية.
الإجراءات المطلوبة	
١-٣	إعداد خادم الإدارة المركزية أو خادم النطاق ليطبق سياسات الإعدادات والتحصين المعتمدة لدى <اسم الجهة> على جميع الخوادم.
٢-٣	تثبيت أدوات إدارة إعدادات النظام التي تقوم تلقائيًا بتنفيذ وإعادة تثبيت إعدادات الضبط والتهيئة للأنظمة في فترات زمنية محددة ومنتظمة.
٣-٣	تطبيق نظام مراقبة الإعدادات المتوافقة مع بروتوكول أتمتة محتوى الأمن (Security Content Automation Protocol "SCAP") للتأكد من عناصر الإعدادات الأمنية كافة وجدولة الاستثناءات المعتمدة والإبلاغ عن حدوث أي تغييرات غير مصرّح بها.
٤	معايير أخرى (Other Standards)
الهدف	تطبيق جميع المعايير والمتطلبات الأمنية للخوادم لضمان أعلى مستويات الحماية.
المخاطر المحتملة	عدم تطبيق جميع المعايير والمتطلبات الأمنية يعرض <اسم الجهة> إلى زيادة في المخاطر الأمنية للخوادم.
الإجراءات المطلوبة	
١-٤	تطبيق المعايير التالية: ١- معيار أمن البيئة الافتراضية. ٢- معيار التعافي من الكوارث والنسخ الاحتياطية. ٣- معيار التشفير. ٤- معيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني. ٥- معيار الأمن المادي. ٦- معايير الإعدادات الآمنة والتحصين.

الأدوار والمسؤوليات

١- **مالك المعيار:** <رئيس الإدارة المعنية بالأمن السيبراني>.

٢- **مراجعة المعيار وتحديثه:** <الإدارة المعنية بالأمن السيبراني>.

٣- **تنفيذ المعيار وتطبيقه:** <الإدارة المعنية بتقنية المعلومات>.

٤- **قياس الالتزام بالمعيار:** <الإدارة المعنية بالأمن السيبراني>.

التحديث والمراجعة

يجب على <الإدارة المعنية بالأمن السيبراني> مراجعة المعيار سنويًا على الأقل أو في حال حدوث تغييرات في السياسات أو الإجراءات التنظيمية في <اسم الجهة> أو المتطلبات التشريعية والتنظيمية ذات العلاقة.

الالتزام بالمعيار

١- يجب على <رئيس الإدارة المعنية بالأمن السيبراني> التأكد من التزام <اسم الجهة> بهذا المعيار دوريًا.

٢- يجب على كافة العاملين في <اسم الجهة> الالتزام بهذا المعيار.

٣- قد يعرض أي انتهاك لهذا المعيار صاحب المخالفة إلى إجراء تأديبي حسب الإجراءات المتبعة في <اسم الجهة>.