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 حماية البريد الإلكتروني

اختر التصنيف

التاريخ: اضغط هنا لإضافة تاريخ

الإصدار: اضغط هنا لإضافة نص

المرجع: اضغط هنا لإضافة نص

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.

# 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.

# 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

الغرض من هذا المعيار هو تحديد متطلبات الأمن السيبراني التفصيلية لتقليل المخاطر السيبرانية الناتجة عن استخدام <اسم الجهة> للبريد الإلكتروني وحمايتها من التهديدات الداخلية والخارجية.

تمت موائمة هذه المعيار مع سياسة حماية البريد الإلكتروني والضوابط والمعايير الصادرة من الهيئة الوطنية للأمن السيبراني والمتطلبات التنظيمية والتشريعية ذات العلاقة.

# نطاق العمل

يغطي هذا المعيار جميع الأصول التقنية والمعلوماتية (شاملة أنظمة البريد الإلكتروني) الخاصة ب<اسم الجهة>، وينطبق على جميع مستخدمي البريد الإلكتروني (الموظفين والمتعاقدين) في <اسم الجهة>.

# المعايير

| ١ | تصفية المحتوى وتحليله (Content Filtering and Analysis) |
|---|---|
| الهدف | ضمان حماية عناوين البريد الإلكتروني من الرسائل الاقتحامية(Spam Emails) والتصيّد الإلكتروني (Phishing Emails) وروابط الإنترنت الضارة والمشبوهة (Malicious URLs) وأي نوع آخر من المحتوى الضار. |
| المخاطر المحتملة | يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على محتوى ضار ومشبوه، وقد تتعرّض <اسم الجهة> لهجمات سيبرانية في حال عدم فحص رسائل البريد الإلكتروني والتأكد من سلامتها. |
| الإجراءات المطلوبة | |
| ١-١ | فحص جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة ب<اسم الجهة> من المحتوى الضار والمشبوه (Malicious Content). |
| ١-٢ | وضع ترميز (Label) على جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة ب<اسم الجهة> بالترميزات الوقائية المناسبة بما يعكس مستوى الحساسية والسريّة بناء على مستوى تصنيف البيانات ووفقًا لنتيجة تحليل المحتوى، أو استخدام إجراء الترميز المعياري (Labeling Standard) المطبّق في <اسم الجهة> وفقًا لسياسة أمن البريد الإلكتروني المعتمدة. من الأمثلة على الترميزات: آمن، وحسّاس، وغيرها. |
| ١-٣ | وضع علامة (Tag) على جميع رسائل البريد الإلكتروني الواردة والصادرة الخاصة ب<اسم الجهة> بالعلامات الوقائية المناسبة لتوضيح الرسائل الخبيثة، الاقتحامية، غير المصرح بها أو استخدام إجراء العلامات المعياري (Tagging Standard) المطبّق في <اسم الجهة> وفقًا لسياسة أمن البريد الإلكتروني المتّبعة فيها. من الأمثلة على |

| | |
|---|---|
| | العلامات: محتوى ضار، ومُرسِل غير مصرّح له، وغير لائق، ورسالة اقتحامية، ورسالة اقتحامية مشتبهة (Suspected SPAM)، وغيرها. |
| ١-٤ | حجب جميع رسائل البريد الإلكتروني الواردة بعلامات وقائية تُشير إلى المحتوى غير المسموح به وفقًا لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة>، على سبيل المثال:<br>• حجب الرسائل الخبيثة وغير المصرّح بها والاقتحامية.<br>• حجر الرسائل الاقتحامية المشتبهة.<br>• السماح بالرسائل الآمنة. |
| ١-٥ | حجب جميع رسائل البريد الإلكتروني الصادرة والمصنفة، بناءً على علامات وقائية تُشير إلى مستوى سريّة رسالة البريد الإلكتروني وذلك وفقًا لسياسة أمن البريد الإلكتروني المتّبعة وسياسة تصنيف البيانات في <اسم الجهة>، على سبيل المثال:<br>• حجب الرسائل الحسّاسة والسريّة.<br>• السماح بالرسائل العامة والخاصة. |
| ١-٦ | حجب رسائل البريد الإلكتروني الاقتحامية التي تتضمّن درجات غير مسموح بها من المخاطر الاقتحامية وفقًا لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة>، على سبيل المثال:<br>• حجب الرسائل شديدة المخاطر.<br>• حجر (أي إيقاف وصولها إلى بريد المستخدم إلى حين التأكد من سلامة محتواها) الرسائل متوسطة المخاطر.<br>• السماح بالرسائل منخفضة ومعدومة المخاطر. |
| ١-٧ | حجب رسائل البريد الإلكتروني الواردة التي تحتوي على روابط إنترنت ونطاقات ضارة ومشبوهة (Malicious URLs and Domains) ومحاولات تصيّد وما إلى ذلك. |
| ١-٨ | استبدال عناوين الويب النشطة (Active Web Addresses) المُدرجة في نص رسالة البريد الإلكتروني بعناوين أخرى. |
| ١-٩ | حجب رسائل البريد الإلكتروني الواردة التي تحتوي على محتوى تفاعلي ( Active Content) في نص الرسالة الإلكترونية أو حذفه منها. |
| ١-١٠ | حجب رسائل البريد الإلكتروني الواردة والصادرة التي تحتوي على ملفات أو محتويات حجمها أكبر من الحجم المسموح، أو ذات صيغة او نوع غير معتمد حسب سياسات <اسم الجهة>، أو تأجيلها حتى يتم التحقق من الملف من قبل الموظف المسؤول وفقًا للسياسة المتبعة. |

اختر التصنيف

| | |
|---|---|
| ١-١١ | حجب رسائل البريد الإلكتروني المُرسلة إلى قائمة غير معرّفة من عناوين البريد الإلكتروني. |
| ٢ | حماية المصادقة (Secure Authentication) |
| الهدف | ضمان حماية استخدام البريد الإلكتروني من خارج <اسم الجهة> من الوصول غير المصرّح به من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني الخارجي (Email Client). |
| المخاطر المحتملة | يُعرّض الوصول غير المصرّح به إلى البريد الإلكتروني <اسم الجهة> إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات السيبرانية ضد <اسم الجهة> وبنيتها التحتية. |
| الإجراءات المطلوبة | |
| ١-٢ | تطبيق آليات التحقّق من الهوية متعدّد العناصر (Multi-Factor Authentication "MFA") على إمكانية وصول المستخدمين للبريد من خارج الشبكة خلال برنامج قارئ البريد الإلكتروني الخارجي (Email Client) وصفحة موقع البريد الإلكتروني (Webmail)، (مثل: Outlook Web Access "OWA") وتطبيقات الجوال. |
| ٢-٢ | بالإضافة إلى ضرورة إدخال اسم المستخدم وكلمة المرور، يجب على <اسم الجهة> استعمال آليات أخرى للتحقّق من الهوية عند الدخول من خارج الشبكة، مثل: الخصائص الحيوية (Biometrics)، أو جهاز توليد الأرقام العشوائية (Hardware Keys)، أو الرسائل القصيرة المؤقتة لتسجيل الدخول (One-Time-Password). |
| ٣-٢ | ضبط متطلبّات إعدادات كلمات المرور المعقدة للبريد الإلكتروني وفقًا لسياسة إدارة هويات الدخول والصلاحيات المتّبعة في <اسم الجهة>. |
| ٤-٢ | تطبيق تقنيات التشفير، مثل: «أمن مستوى النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks)، لحماية آليات التحقّق من الهوية خلال إرسالها. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (such as cipher suite B) المُوصى بها وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة> والمعايير الوطنية للتشفير. |
| ٣ | حماية محتوى البريد الإلكتروني (Content Protection) |
| الهدف | ضمان حماية رسائل البريد الإلكتروني التي تحتوي على مرفقات من الفيروسات والبرمجيات الضارة والتهديدات المتقدّمة المستمرة والهجمات غير المعروفة مسبقًا وأي نوع آخر من المرفقات الخبيثة. |

| | |
|---|---|
| المخاطر المحتملة | يُمكن أن ينخدع المستخدم برسائل البريد الإلكتروني التي تحتوي على مرفقات خبيثة حيث قد تتعرض <اسم الجهة> لاختراق بياناتها أو الوصول إليها بشكل غير مصرّح به أو كشفها في حال عدم فحص مرفقات البريد الإلكتروني. |
| الإجراءات المطلوبة | |
| ٣-١ | تطبيق وتفعيل تصنيفين لمرفقات البريد الإلكتروني: التصنيف الأول وفقًا لنوع الملف، والتصنيف الثاني وفقًا لمحتوى الملف. |
| ٣-٢ | وضع علامات وقائية (tagging) في المرفقات حسب أنواع المرفقات وصيغتها، على سبيل المثال:<br>• **اللائحة السوداء:** جميع أنواع نسخ البرمجيات القابلة للتنفيذ من ويندوز (Windows PE) وأوامر ماكرو أوفيس (Office Macros) والبرمجيات أو الأوامر النصية (Scripts)، وغيره.<br>• **اللائحة الرمادية:** الأرشيفات متعدّدة المستويات (Multi-Layer Archives) وملفات حماية كلمة المرور وملفات التشفير والملفات التي يزيد حجمها عن الحد الأقصى، وغيرها من الملفات ضمن قائمة الحجر (Quarantine-list)<br>• **اللائحة البيضاء:** ملفات برامج أوفيس القياسية (مثل: docx وpptx وxlsx) وملفات pdf وtxt، والملفات الأرشيفية، وغيرها.<br>• **لائحة المرفقات غير المعروفة:** أنواع وصيغ الملفات غير المعروفة والتي يتعذّر التحقّق منها. |
| ٣-٣ | وضع علامات وقائية (tagging) في المرفقات بعد فحصها من البرمجيات الضارة بإدراج نتائج الفحص، على سبيل المثال:<br>• **ضارة:** تحتوي على فيروس أو برنامج ضار أو تهديد متقدّم مستمر أو غيره.<br>• **آمنة:** تحتوي على ملف مرفق آمن.<br>• **غير معروفة:** أي تعذّر فحصها. |
| ٣-٤ | تحديد أنواع الملفات باستخدام محتواها مثل ترويسة وتذييل الملف ( Footer and Header) وليس من خلال صيغها. |
| ٣-٥ | فحص جميع المرفقات المسموحة والتي تمت تصفيتها للتأكد من خلوها من الملفات الضارة، مثل: الفيروسات والبرمجيات الضارة وأي نوع آخر من الملفات المشبوهة. |
| ٣-٦ | فحص جميع أنظمة وخوادم البريد للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة في المكونات التقنية للبريد الإلكتروني وبوابة البريد (Mail Gateway) وخاصية ترحيل البريد (Mail Relay) أو خادم البريد (Mail Server) قبل أن تصل إلى برنامج قارئ البريد (Email Client). |

| | |
|---|---|
| ٣-٧ | إجراء فحص للتحقّق من عدم وجود أي برمجيات ضارة أو مشبوهة عبر برامج قراءة البريد (Email Clients) باستخدام حل يُقدّمه مورّد أو مزوّد مختلف عن الموجود في البند ٣-٦ مثل إضافة أدوات للحماية من الفيروسات إلى برنامج قارئ البريد. |
| ٣-٨ | فحص جميع المرفقات المسموحة والتي تمت تصفيتها عبر إجراء تحليل ديناميكي للمرفقات باستخدام تقنية الحماية المعزولة (Sandbox) للتحقّق من التهديدات المتقدّمة المستمرة (APT) والبرمجيات الضارة غير المعروفة مسبقًا. |
| ٣-٩ | حجب أو تجريد جميع رسائل البريد الإلكتروني التي تحتوي على ملفات مرفقة ضارة أو مصنفة ضمن اللائحة السوداء وفقًا لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة> ثمّ إضافة عنوان المرسل والنطاق إلى اللائحة السوداء. |
| ٣-١٠ | حجر جميع رسائل البريد الإلكتروني التي تتضمّن ملفات ضمن اللائحة الرمادية إذا كانت آمنة. |
| ٣-١١ | حجر جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة غير معروفة. |
| ٣-١٢ | قبول جميع رسائل البريد الإلكتروني التي تتضمّن ملفات مرفقة آمنة ومسموحة. |
| **٤** | **التحقّق من مرسل البريد الإلكتروني (Email Sender Verification)** |
| الهدف | ضمان الحفاظ على سريّة بيانات البريد الإلكتروني والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة. |
| المخاطر المحتملة | تحمي خاصية التأكّد من سلامة وموثوقية رسائل البريد الإلكتروني <اسم الجهة> من عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الضارة والكشف عن المعلومات المهمّة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدم. |
| الإجراءات المطلوبة | |
| ٤-١ | التحقّق من المُرسِل باختبار قاعدتين من بيانات سمعة المُرسِل (Sender Reputation) على الأقل. |
| ٤-٢ | التحقّق من عنوان المُرسِل مقابل قوائم الرسائل الاقتحامية (Email SPAM lists) المتواجدة على الإنترنت والتي تُحدث يوميًا. |
| ٤-٣ | التحقّق من بروتوكول الإنترنت (Internet Protocol "IP") الخاص بخادم بريد المُرسِل واسم النطاق بمقارنته مع القائمة اللحظية لعناوين الإنترنت العشوائية (Real-time Blackhole Lists). |

| ٥ | التحقّق من سلسلة الثقة المتعلقة بالبريد الإلكتروني (Email Chain of Trust Verification) |
|---|---|
| الهدف | ضمان الحفاظ على سريّة بيانات البريد الإلكتروني والتأكّد من سلامتها وموثوقيتها لحمايتها من الوصول غير المصرّح به والكشف عن المعلومات الحسّاسة. |
| المخاطر المحتملة | قد يؤدي عدم التأكد من سلامة وموثوقية رسائل البريد الإلكتروني إلى عمليات تزوير البريد الإلكتروني والرسائل الإلكترونية الخبيثة والكشف عن المعلومات المهمة والحسّاسة والوصول غير المصرّح به إلى الرسائل الإلكترونية الخاصة بالمستخدمين. |
| الإجراءات المطلوبة | |
| ٥-١ | إنشاء وتسجيل إطار سياسة المُرسِل (Sender Policy Framework "SPF") والبريد المُعرَّف بمفاتيح النطاق (Domain Key Identified Mail "DKIM") ومصادقة الرسائل والإبلاغ عنها ومطابقتها (Domain-based Message Authentication, Reporting and Conformance "DMARC") استنادًا إلى النطاق. |
| ٥-٢ | التحقّق من المُرسِل وفق نظام مصادقة هوية مُرسِل الرسائل (SenderID) وسجلات إطار سياسة المُرسِل (SPF) واتخاذ الإجراء المناسب وفقًا لسياسة أمن البريد الإلكتروني المتّبعة في <اسم الجهة>. |
| ٥-٣ | التحقّق من المُرسِلين وفق البريد المُعرَّف بمفاتيح النطاق (DKIM) التي يستخدمونها.<br>• رفض الفشل في البريد المُعرَّف بمفاتيح النطاق. |
| ٥-٤ | ضبط إطار سياسة المُرسِل (SPF) على السجلات الخارجية المقابلة لنظام أسماء النطاقات (External DNS Records) لكل أسماء النطاقات التي تملكها <اسم الجهة> للسماح فقط بسجلات تبادل البريد (Mail Exchange Records) في الخوادم التي صرّحت لها <اسم الجهة> بإرسال الرسائل الإلكترونية نيابةً عنها. |
| ٥-٥ | ضبط سجلات البريد المُعرَّف بمفاتيح النطاق(DKIM) لتوقيع محتوى رسائل البريد الإلكتروني(Email Digital Signing) الخاصة ب<اسم الجهة> وذلك بتحديد مفاتيح عامة تشفيرية للتواقيع (Public Key Cryptography). |
| ٥-٦ | ضبط «مصادقة الرسائل والإبلاغ عنها ومطابقتها استنادًا إلى النطاق» (DMARC) لأتمتة تطبيق الإجراءات المناسبة بشأن الأخطاء المرصودة في نظام مصادقة هوية مُرسِل الرسائل وسجلات إطار سياسة المُرسِل والبريد المُعرّف بمفاتيح النطاق وفقًا لسياسة حماية البريد الإلكتروني المتبعة في <اسم الجهة>. على سبيل المثال:<br>• **رفض/حجر** الفشل الجزئي (Relaxed Fail) في البريد المُعرَّف بمفاتيح النطاق (DKIM) وسجلات إطار سياسة المُرسِل (SPF). |

| | |
|---|---|
| | ملاحظة: الفشل الجزئي (Relaxed Fail) يسمح بمرور الرسائل الواردة من النطاقات الفرعية، والفشل الكامل(Strict Fail) يمنع ذلك. |
| ٦ | حماية أنظمة البريد الإلكتروني (Email Systems Security) |
| الهدف | ضمان حماية وأمن البنية التحتية الأساسية لخدمة البريد الإلكتروني بما في ذلك خوادم البريد وبواباته وقواعد بياناته وحلوله الأمنية. |
| المخاطر المحتملة | من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية البنية التحتية لخدمة البريد الإلكتروني في <اسم الجهة> إلى استغلال المهاجمين لنقاط الضعف الكامنة في أنظمة البريد الإلكتروني واستغلال ثغراتها للوصول غير المصرّح به إلى شبكة <اسم الجهة> وبياناتها. |
| الإجراءات المطلوبة | |
| ١-٦ | إجراء اختبارات أمنية دورية (مثل: فحص الثغرات الأمنية وتنفيذ عمليات اختبار الاختراق) وفقًا للسياسات والإجراءات ذات العلاقة في <اسم الجهة>. |
| ٢-٦ | مراجعة وتطبيق حزم التحديثات والإصلاحات دوريًا على أنظمة البريد الإلكتروني وفقًا لسياسة إدارة التحديثات والإصلاحات المعتمدة لدى <اسم الجهة>، وضمان تحديث جميع الأنظمة. |
| ٣-٦ | حذف أو إلغاء تفعيل التطبيقات والخدمات غير الضرورية أو غير اللازمة من أنظمة البريد الإلكتروني، مثل: خدمات الطباعة وبروتوكول الاتصال عن بعد غير الآمن (Telnet)، وغيرها. |
| ٤-٦ | ضبط إعدادات وتحصين (Secure Configuration and Hardening) أنظمة البريد الإلكتروني على مستوى التطبيقات وقاعدة البيانات والتشغيل كل ثلاثة أشهر وفقًا لمعيار أمن الخادم ومعيار أمن قاعدة البيانات المعتمدين لدى <اسم الجهة>. |
| ٥-٦ | تقييد الوصول (Restrict Access) إلى أنظمة البريد الإلكتروني ليكون مسموح به فقط لمدراء أنظمة البريد الإلكتروني (Mail System Administrators). |
| ٦-٦ | حذف أو إلغاء تفعيل الحسابات الافتراضية أو غير التفاعلية أو غير اللازمة. |
| ٧-٦ | إلزام مدراء الأنظمة ومُشغّلي أنظمة البريد الإلكتروني باستخدام آلية التحقّق من الهوية متعدّد العناصر للوصول إلى أنظمة البريد الإلكتروني. |
| ٨-٦ | استخدام مبدأ الحماية الذي يمنح مدراء ومُشغّلي أنظمة البريد الإلكتروني ( Email System Administrators and Operators) الحد الأدنى من صلاحيات الوصول (Least-Privilege Principle) إلى مختلف أنواع أنظمة البريد الإلكتروني. |

| | |
|---|---|
| ٦-٩ | تقييد الوصول الشبكي إلى أنظمة إدارة البريد الإلكتروني على المنطقة الشبكية التي تتواجد فيها والمنطقة الشبكية الخاصة بالإدارة (Management Zone). |
| ٦-١٠ | حذف أو إلغاء تفعيل خصائص تطبيق البريد الإلكتروني وملفات الإعدادات غير الضرورية أو غير اللازمة. |
| ٦-١١ | حجب إمكانية الوصول (Restrict Access) إلى مجلدات الشبكة ( Network File Shares) والملفات غير الضرورية أو غير اللازمة. |
| ٦-١٢ | استخدام ضوابط الأجهزة الطرفية (Peripheral Device Controls) وحجب الوصول إلى وسائل التخزين القابلة للإزالة مثل الأقراص المتحركة (CD) والأقراص المدمجة (DVD) وذاكرة التخزين (USB). |
| ٦-١٣ | تثبيت برامج أنظمة البريد الإلكتروني على خوادم استضافة مخصصة لها. |
| ٦-١٤ | ضبط رسائل خدمة برتوكولات نقل البريد (مثل: بروتوكول إرسال البريد البسيط "SMTP"، وبروتوكول مكتب البريد "POP"، وبروتوكول الوصول إلى رسائل الإنترنت "IMAP"، وغيرها) لمنع الكشف عن معلومات إصدار البرنامج أو نظام التشغيل (Exchange Version). |
| ٦-١٥ | تفعيل أوامر البريد غير الخطرة فقط وذلك لتفادي الأوامر الخطرة مثل (VRFY وEXPN). |
| ٦-١٦ | تفعيل سجلات الأحداث (Event Logging) في أنظمة البريد الإلكتروني وسجل التدقيق (Audit Log) الواجب إرسالهما إلى نظام مركزي لإدارة سجلات الأحداث وفقًا لسياسة ومعيار إدارة سجلات الأحداث ومراقبة الأمن السيبراني المعتمدين لدى <اسم الجهة>. |
| ٦-١٧ | إنشاء البنية التحتية لخدمة البريد الإلكتروني باستخدام مبدأ المعمارية متعددة المستويات (Multi-Tier Architecture) المحمية باستخدام طبقتين مختلفتين من جدار الحماية (Firewalls)، وتحديدًا، إدراج بوابة أمن البريد الإلكتروني (Mail Gateway) في منطقة الإنترنت المحايدة (DMZ)، وخوادم تطبيقات البريد الإلكتروني في منطقة الإنتاج (Production Zone)، وخوادم قواعد بيانات البريد الإلكتروني في المنطقة الموثوقة (Trusted Zone) أو منطقة قاعدة البيانات (Database Zone). |
| ٦-١٨ | حماية صفحة موقع البريد الإلكتروني خلف جدار حماية تطبيق الويب ( Web Application Firewall "WAF"). |
| ٦-١٩ | تعطيل خاصية الترحيل المفتوح (Open Mail Relay). |

| | |
|---|---|
| ٦-٢٠ | ضبط تشفير نقل البريد الإلكتروني باستخدام تقنيات التشفير، مثل: «أمن طبقة النقل» (Transport Layer Security) و«الشبكات الخاصة الافتراضية» (Virtual Private Networks) لحماية رسائل البريد الإلكتروني خلال إرسال الرسائل. واستخدام أحدث بروتوكولات التشفير وخوارزميات التشفير المدعومة (Cipher Suites) المُوصى بها (مثل التشفير بمجموعة Suite B) وفقًا لمعيار التشفير المعتمد لدى <اسم الجهة>. |
| ٦-٢١ | تفعيل تقنية (STARTTLS) لتشفير الاتصال بين خوادم البريد الإلكتروني (email gateways) لمنع هجمات (man-in-the-middle) غير النشطة. |
| ٦-٢٢ | ضبط مجموعات مواصفات الارتداد لبيانات البريد (Mail Bounce Profiles)، على سبيل المثال:<br>• الارتداد القوي لرسائل البريد الإلكتروني المرسلة إلى عناوين بريد غير موجودة أو منتهية الصلاحية أو غير مفعّلة. |
| ٧ | برنامج قارئ البريد الإلكتروني (Email Client Security) |
| الهدف | ضمان حماية استخدام البريد الإلكتروني من خلال صفحة موقع البريد الإلكتروني (Webmail) أو برنامج قارئ البريد الإلكتروني (Email Client). |
| المخاطر المحتملة | من الممكن أن يؤدي عدم اتخاذ أي إجراء لحماية برنامج قارئ البريد الإلكتروني إلى مخاطر كبيرة قد تؤدي إلى سرقة المعلومات وانتحال الشخصيات مما يتيح استخدامها في تنفيذ المزيد من الهجمات الضارة ضد موظفي <اسم الجهة> وبنيتها التحتية. |
| الإجراءات المطلوبة | |
| ٧-١ | استخدام برنامج قارئ بريد إلكتروني محدث ومدعوم بالكامل. |
| ٧-٢ | منع تشغيل صفحة موقع البريد الإلكتروني على المتصفحات غير المرخصة. |
| ٧-٣ | تعطيل التطبيقات الإضافية أو المكونات غير الضرورية أو غير المسموح بها لبرنامج قارئ البريد الإلكتروني. |
| ٧-٤ | منع تشغيل لغات البرمجة النصية في برنامج قارئ البريد الإلكتروني. |
| ٧-٥ | ضبط تكامل برنامج قارئ البريد الإلكتروني مع أنظمة حماية الأجهزة كمضاد الفيروسات والبرمجيات الضارة. |

| ٨ | النسخ الاحتياطية والأرشفة (Backup and Archival) |
|---|---|
| الهدف | ضمان سلامة بيانات البريد الإلكتروني وتوافرها وقابلية استعادتها وحمايتها من فقدانها أو تخريبها. |
| المخاطر المحتملة | في حال حذف بيانات البريد الإلكتروني والرسائل الإلكترونية أو العبث بها أو فقدانها بالخطأ أو تخريبها أو تعرّضها لهجوم إلكتروني، لن تتمكّن <اسم الجهة> من استرداد بيانات بريدها الإلكتروني وسجل اتصالاتها مما يؤثّر على أنشطة أعمالها الاعتيادية. |
| الإجراءات المطلوبة | |
| ١-٨ | تطبيق النسخ الاحتياطي والأرشفة لبيانات البريد الإلكتروني بما يتوافق مع المعايير التقنية والأمنية المذكورة في معيار إدارة النسخ الاحتياطية والتعافي من الكوارث المعتمد لدى <اسم الجهة> لمقاومة الهجمات السيبرانية. |

## 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>.