الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية

هيئة السوق المالية
Capital Market Authority

إخلاء مسؤولية

تود هيئة السوق المالية التنبيه إلى أن هذه الوثيقة لا تعدّ بديلاً عن أي أنظمة أو تشريعات معمول بها في المملكة العربية السعودية، وعند وجود تعارض بين ما ورد في هذه الوثيقة وبين أي من تلك التشريعات، فإن المرجعية تكون لها. ويقع على مؤسسات السوق المسؤولية في تطبيق واتباع التشريعات والأنظمة المعمول بها والتي تسهم في تعزيز الأمن السيبراني وتخفيف أثر التهديدات الأمنية الإلكترونية.

الملخص التنفيذي

تسعى هيئة السوق المالية من خلال برنامج "تطوير القطاع المالي" (أحد برامج تحقيق رؤية المملكة 2030 الاثني عشر المعتمدة من مجلس الشؤون الاقتصادية والتنمية) إلى جعل السوق المالية السعودية السوق الرئيسية في الشرق الأوسط، ومن أهم الأسواق المالية في العالم، وأن تكون سوقاً متقدمةً وجاذبةً للاستثمار المحلي والأجنبي بما يمكّنها من أداء دور محوري في تنمية الاقتصاد وتنويع مصادر دخله. ويندرج تحت المحور الثالث من محاور الخطة الاستراتيجية "تعزيز الثقة" الهدف الاستراتيجي الثامن وهو تعزيز الاستقرار في السوق المالية، الذي يرفع من ثقة المشاركين بالسوق ويسهم في إيجاد بيئة استثمار جاذبة تدعم نمو الاقتصاد الوطني. وتعمل هيئة السوق المالية مع الجهات التنفيذية المختلفة على التنسيق وتبادل المعلومات بما يعزز الاستقرار في السوق المالية ويحد من المخاطر المرتبطة بمعاملات الأوراق المالية، وبما يعزز أمن وسلامة المعلومات والبيانات المالية، واستمرارية أعمال الجهات المشاركة في السوق. كذلك تندرج ضمن الهدف المذكور مبادرة تعزيز الأمن السيبراني التي تهدف إلى توفير بنية تحتية آمنة وشفافة ودعم الأمن المعلوماتي لضمان استقرار البنية التحتية وسلامتها.

ووفقاً لنظام السوق المالية الصادر بالمرسوم الملكي رقم (م/30) بتاريخ 1424/6/2هـ، تم تطوير هذه الوثيقة لتحديد الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية، المبنية على أفضل الممارسات والمعايير العالمية والمحلية؛ لتقليل مخاطر الهجمات والتهديدات الإلكترونية على الأصول المعلوماتية والتقنية لمؤسسات السوق المالية بما يعزز الاستقرار الإلكتروني الأمني في السوق المالية ويحدّ من المخاطر ذات الصلة.

المحتويات

المحتويات

جدول الأشكال

1. التمهيد

1.1 تعريف الأمن السيبراني

يعرّف المعهد الوطني للمعايير والتقنية (NIST) الأمن السيبراني بأنه "عملية حماية المعلومات عن طريق منع الهجمات من خلال كشفها والتصدي لها". وعلى غرار المخاطر المالية والمخاطر ذات الصلة بالسمعة، يمكن لمخاطر الأمن السيبراني أن تؤدي إلى ارتفاع التكاليف والتأثير في العائدات. كذلك من شأنها الإضرار بقدرة المؤسسة على الابتكار واكتساب العملاء والمحافظة عليهم.

أما **المنظمة الدولية للمعايير (ISO)** فترى أن الأمن السيبراني أو الفضاء السيبراني يتمثل في الحفاظ على السرية والسلامة وتوافر المعلومات في الفضاء السيبراني. ويُعرّف "الفضاء السيبراني" بدوره بأنه "البيئة الناتجة عن تفاعل الأفراد مع البرمجيات والخدمات المتاحة عبر الإنترنت عن طريق الأجهزة التقنية والشبكات المتصلة به، والتي ليس لها وجود مادي".

وقد قامت **الهيئة الوطنية للأمن السيبراني (NCA)** بإصدار الضوابط الأساسية للأمن السيبراني باعتبارها الحد الأدنى من متطلبات الأمن السيبراني التي يجب على الجهات الوطنية الالتزام بها. وتهدف الضوابط الأساسية للأمن السيبراني إلى تقليل المخاطر السيبرانية من التهديدات الداخلية والخارجية المختلفة التي تؤثر في الجهات الوطنية. إن الضوابط الأساسية للأمن السيبراني هي ضوابط إلزامية ويتعين على جميع الجهات الوطنية - الداخلة ضمن نطاق انطباقها- أن تنفذ المتطلبات اللازمة لتحقيق الالتزام المستمر بها.

وفي حالة اعتماد الاتفاقيات أو الالتزامات الدولية التي تتضمن متطلبات ذات صلة بالأمن السيبراني على الصعيد المحلي، فيجب أن تلتزم الجهة بهذه المتطلبات.

2.1 أهداف الأمن السيبراني

- **تتضمن الأهداف العامة للأمن السيبراني التالي:**

- **السرية:** اتخاذ التدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات الحساسة والسرية.
- **سلامة المعلومة:** الحماية ضد تعديل المعلومات أو تخريبها بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non- Repudiation) والموثوقية.
- **توافر المعلومة:** ضمان الوصول إلى البيانات والمعلومات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.

2. المقدمة

أُعِدّت هذه الوثيقة بالاستعانة والاسترشاد بعدد من الأطر التنظيمية والمعايير القياسية المحلية والدولية والتي كان من ضمنها ضوابط الهيئة الوطنية للأمن السيبراني (NCA)، وإطار الأمن السيبراني لمؤسسة النقد العربي السعودي (**SAMA**)، وضوابط المعهد الوطني للمعايير والتقنية (NIST)، والمنظمة الدولية للمعايير (ISO).

1.2 الهدف

يهدف الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية (ويشار إليها لاحقاً بـ"الدليل الاسترشادي") إلى تحديد الضوابط المتعلقة بالأمن السيبراني لمؤسسات السوق التي تساعد على تحسين إدارة مخاطر الأمن السيبراني من خلال تبني أفضل الممارسات العالمية وتشريعات الأمن السيبراني المحلية.

2.2 نطاق العمل

يوضح **الدليل الاسترشادي** الضوابط المتعلقة بالأمن السيبراني لمؤسسات السوق السعودية الخاضعة لمتابعة وإشراف هيئة السوق المالية.

3.2 قابلية التطبيق

تعد هذه الوثيقة استرشادية على جميع مؤسسات السوق المالية. ولهيئة السوق المالية الحق في فرض هذه الوثيقة على أي جهة خاضعة لمتابعة وإشراف هيئة السوق المالية.

4.2 المراجعة والتحديث

تضطلع هيئة السوق المالية بالمراجعة الدورية للدليل الاسترشادي وفقاً للمستجدات والمتطلبات التنظيمية ذات العلاقة، وتحديثها متى تطلب الأمر ذلك.

.3

استعراض الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية

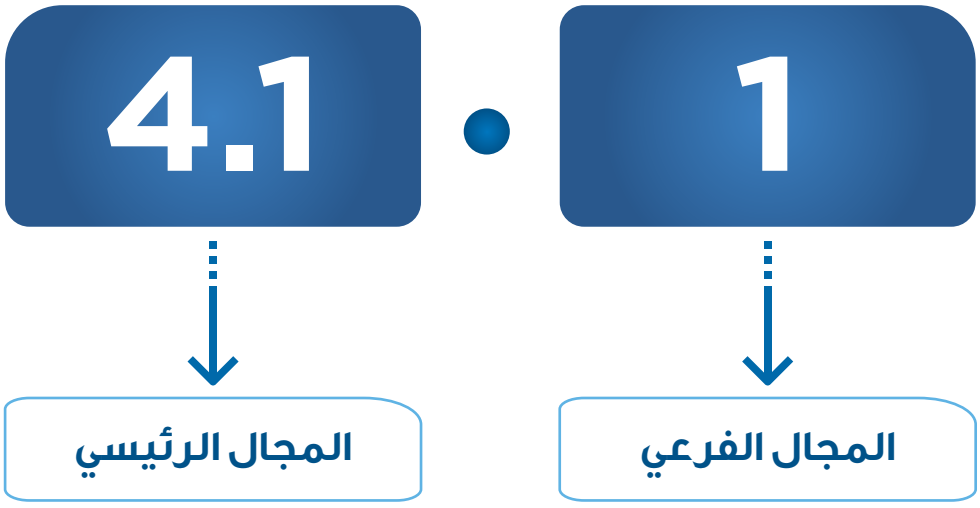
1.3 المجالات الأمنية

- **يتمحور الدليل الاسترشادي حول أربعة مجالات رئيسة:**

- حوكمة الأمن السيبراني.
- إدارة مخاطر الأمن السيبراني والمراجعة والتدقيق.
- ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية.
- أمن الطرف الخارجي المتعلق بالأطراف الخارجية.

- سيتم التطرق للعديد من المجالات الفرعية لكل مجال رئيسي، حيث سيتم تحديد الهدف الأمني لكل مجال فرعي وضوابطه الأساسية.

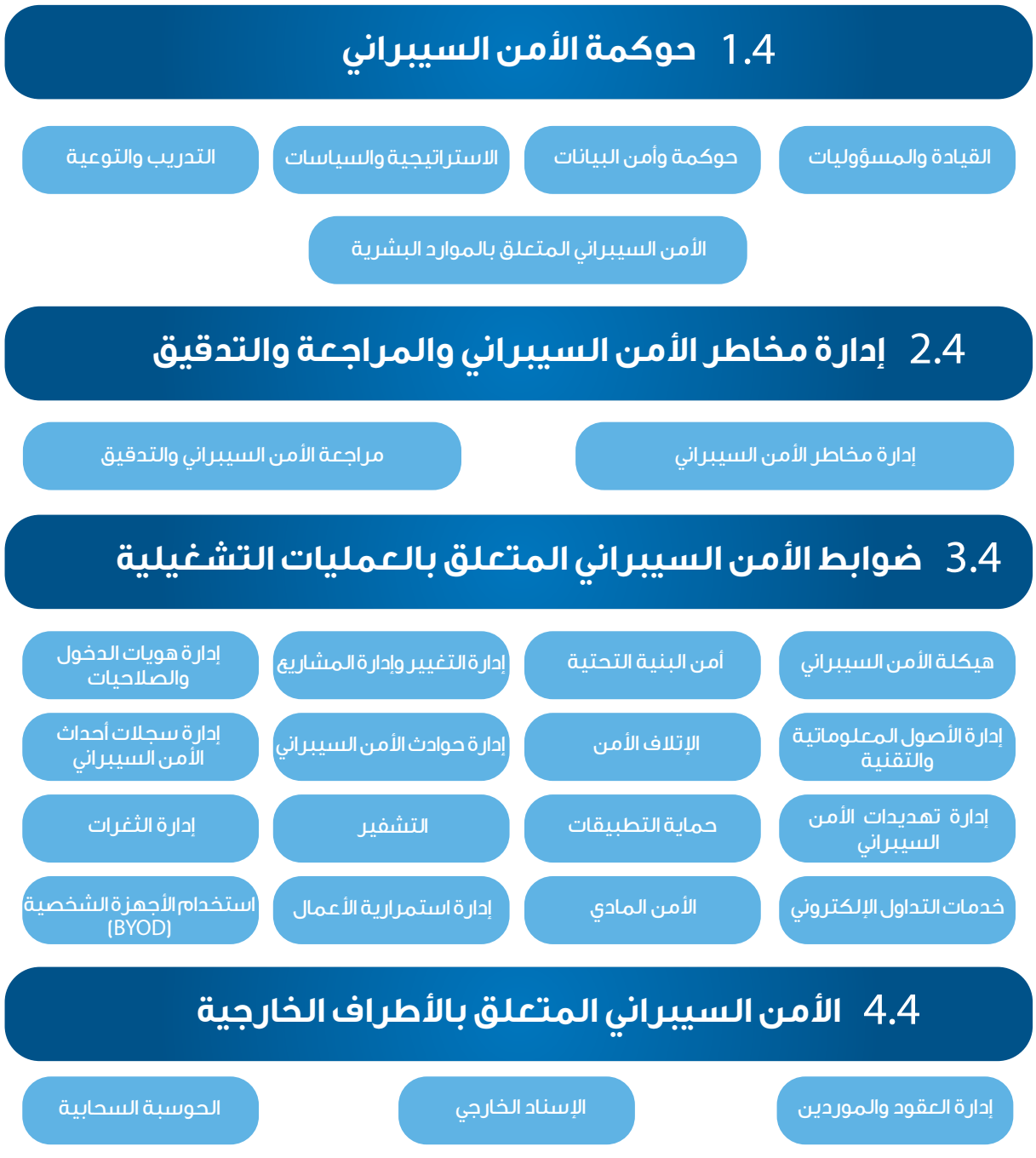
- يصف " الهدف" الناتج المتوقع من تحقيق ضوابط الأمن السيبراني.
- وتحتوي "الضوابط الأساسية" على ضوابط الأمن السيبراني التي يجب الالتزام بها.



الشكل 1 نظام الترقيم

استعراض الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية

ويوضح الشكل أدناه الهيكل العام للدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية، ويشير إلى كل من المجالات الأساسية والفرعية للأمن السيبراني.



الشكل 2 الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية

تصنيف الوثيقة: عام

استعراض الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية

2.3 التقييم الذاتي والمراجعة والتدقيق

يخضع تنفيذ الدليل الاسترشادي في مؤسسة السوق لتقييم ذاتي دوري بناءً على الاستبانات ونماذج التقييم الذاتي وفق الآلية التي تراها الهيئة مناسبة.

4. المجالات الأمنية

1.4 حوكمة الأمن السيبراني

تقع كامل المسؤولية عن الأمن السيبراني على عاتق مجلس إدارة مؤسسة السوق، ويمكن لهذا المجلس تفويض صلاحيات الأمن السيبراني إلى لجنة معنية بالأمن السيبراني أو لجنة إشرافية. وتتضمن مسؤوليات لجنة الأمن السيبراني تحديد حوكمة الأمن السيبراني ووضع استراتيجية الأمن السيبراني لمؤسسة السوق بالإضافة إلى تحديد سياسات الأمن السيبراني وضمان تنفيذ تلك السياسات.

1.1.4 القيادة والمسؤوليات

الهدف: تحديد الهيكل التنظيمي للأمن السيبراني والأدوار والمسؤوليات وتوثيقها وتنفيذها واعتمادها من قبل مجلس إدارة مؤسسة السوق.

المجالات الأمنية

الضوابط الأساسية :

1. إنشاء إدارة معنية بالأمن السيبراني مستقلة عن إدارة تقنية المعلومات مع الأخذ بالاعتبار عدم تعارض المصالح.
2. أن يرأس الإدارة المعنية بالأمن السيبراني موظف سعودي "مؤهل" بدوام كامل، ويُشار إليه باسم مدير إدارة الأمن السيبراني.
3. تخصيص واعتماد ميزانية كافية لتنفيذ مهام وأعمال الأمن السيبراني من قبل مجلس إدارة مؤسسة السوق.
4. مراجعة الأدوار والمسؤوليات المتعلقة بالأمن السيبراني بصفة دورية أو في حالة حدوث تغييرات.
5. إنشاء لجنة معنية بالأمن السيبراني على أن ترتبط بالرئيس التنفيذي للجهة أو من ينيبه مع الأخذ بالاعتبار عدم تعارض المصالح.
6. تضم لجنة الأمن السيبراني مدير إدارة الأمن السيبراني ومديري الإدارات ذات العلاقة.
7. إعداد لائحة عمل لجنة الأمن السيبراني وتوثيقها واعتمادها من صاحب الصلاحية، مع توضيح الأهداف والأدوار والمسؤوليات.
8. تتضمن مسؤوليات لجنة الأمن السيبراني التالي:
    1. مراقبة درجة تَقبُّل مخاطر الأمن السيبراني لمؤسسة السوق ومراجعتها والإبلاغ عنها بشكل دوري أو عند حدوث تغيير جوهري بخصوص معدل تقبل المخاطر؛
    2. المراجعة الدورية لاستراتيجية الأمن السيبراني لضمان دعمها لأهداف مؤسسة السوق؛
    3. اعتماد ونشر وتوفير الدعم اللازم والمراقبة بشأن:
        1. حوكمة الأمن السيبراني؛
        2. استراتيجية الأمن السيبراني؛
        3. سياسات الأمن السيبراني؛
        4. برامج الأمن السيبراني (مثل برامج التوعية، وبرنامج تصنيف البيانات، وخصوصية البيانات، ومنع تسريب البيانات)؛
        5. إدارة مخاطر الأمن السيبراني؛
        6. مؤشرات المخاطر الرئيسة ومؤشرات الأداء الرئيسة للأمن السيبراني.

9. تتضمن مسؤوليات مجلس إدارة مؤسسة السوق – بالإضافة لما تقدم- التالي:
    1. االتأكد من أن المعايير والإجراءات تعكس متطلبات الأمن السيبراني؛
    2. التأكد من قبول العاملين لسياسات الأمن السيبراني والالتزام بها، ودعم المعايير والإجراءات عند إصدارها وتحديثها؛
    3. التأكد من إدراج مسؤوليات الأمن السيبراني في الأوصاف الوظيفية للمناصب ذات العلاقة ووظائف الأمن السيبراني.

المجالات الأمنية

10 تتضمن مسؤوليات مدير إدارة الأمن السيبراني التالي:

1 الرفع إلى لجنة الأمن السيبراني حول أي تطوير وتحديث لما يلي:

1 استراتيجية الأمن السيبراني؛

2 سياسات الأمن السيبراني؛

3 بُنية الأمن السيبراني؛

4 إدارة مخاطر الأمن السيبراني؛

2 ضمان تحديد معايير وإجراءات الأمن السيبراني وتوثيقها واعتمادها وتنفيذها؛

3 ضمان تطوير وتدريب موظفي الأمن السيبراني؛

4 مراقبة أنشطة الأمن السيبراني (مراقبة مركز العمليات الأمنية)؛

5 مراقبة الالتزام بأنظمة وسياسات ومعايير وإجراءات الأمن السيبراني؛

6 الإشراف على التحقيق في حوادث الأمن السيبراني؛

7 الحصول على المعلومات الاستباقية(Threat Intelligence) والتعامل معها؛

8 مراجعة وتدقيق برنامج الأمن السيبراني؛

9 الدعم الفعال للوظائف الأخرى المتعلقة بالأمن السيبراني، بما فيها:

1 تصنيف المعلومات والنظم؛

2 تحديد ضوابط الأمن السيبراني للمشاريع المهمة؛

3 مراجعة ضوابط الأمن السيبراني.

10 تصميم برامج التوعية بالأمن السيبراني وتنفيذها؛

11 القياس والإبلاغ عن مؤشرات المخاطر الرئيسة ومؤشرات الأداء الرئيسة بشأن:

1 استراتيجية الأمن السيبراني؛

2 الالتزام بسياسات الأمن السيبراني؛

3 معايير وإجراءات الأمن السيبراني؛

4 برامج الأمن السيبراني (مثل برامج التوعية، وبرنامج تصنيف البيانات).

11 تتمثل مسؤولية التدقيق الداخلي في مؤسسة السوق في إجراء مراجعة وتدقيق لضوابط الأمن السيبراني على أن تتم بشكل دوري وأن يراعى فيها مبدأ عدم تعارض المصالح.

12 يُناط بجميع موظفي مؤسسة السوق مسؤولية الالتزام بسياسات الأمن السيبراني ومعاييرها وإجراءاتها.

المجالات الأمنية

2.1.4 حوكمة وأمن البيانات

الهدف :

ضمان حماية البيانات والمحافظة على سريتها وتوافرها وسلامتها.

الضوابط الأساسية :

1. تطوير وتصميم برنامج حوكمة البيانات.
2. تحديد مجالات البيانات:
   - مالكو البيانات
   - مديرو البيانات
   - أمناء الحفظ
   - مستخدمو البيانات
   - قواميس البيانات
   - إجراءات الأعمال
   - قوائم البيانات
   - قوائم التقارير
   - الأنظمة والتطبيقات
   - السياسات والمعايير
3. تحديد عناصر البيانات الحساسة داخل مجالات البيانات.
4. تحديد تصنيف البيانات وآلية ترميزها بحسب الأهمية.
5. تحديد خصوصية البيانات والمعلومات.
6. إنشاء منصة مركزية لإدارة التغييرات والتحكم فيها وإتاحة الوصول إلى أصول البيانات الحساسة.
7. تحديد آلية لقياس مستوى حماية البيانات.
8. تحديد وتنفيذ خطط سير العمل بهيكل الحوكمة وأهم عناصر ومجالات البيانات.
9. رصد إجراءات سير العمل ومراقبتها والإبلاغ عنها.

3.1.4 الاستراتيجية والسياسات

الهدف :

تحديد سياسات واستراتيجية الأمن السيبراني وتوثيقها واعتمادها وتنفيذها ونشرها لذوي العلاقة وضمان الالتزام بها.

الضوابط الأساسية :

1. تحديد استراتيجية الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها، وتحديثها بشكل دوري.
2. توافق استراتيجية الأمن السيبراني مع الأهداف العامة لمؤسسة السوق وأي متطلبات تنظيمية ذات العلاقة.
3. تتضمن استراتيجية الأمن السيبراني التالي:
   1. أهمية الأمن السيبراني بالنسبة إلى مؤسسة السوق؛
   2. حالة الأمن السيبراني المستقبلية المتوقعة لمؤسسة السوق إلى أن تصبح قادرة على مجابهة تهديدات الأمن السيبراني؛
   3. وضع خطة زمنية لتنفيذ مبادرات ومشاريع واستراتيجية الأمن السيبراني.

4. تحديد سياسات الأمن السيبراني، وتوثيقها، واعتمادها، ونشرها لذوي العلاقة والأطراف المعنية، وضمان الالتزام بها.
5. مراجعة سياسات الأمن السيبراني بشكل دوري وفقًا لخطة مراجعة مُحددة مسبقًا.
6. دعم سياسات الأمن السيبراني بمعايير تقنية أمنية تفصيلية (على سبيل المثال: معايير كلمة المرور، ومعايير جدار الحماية) مع مراعاة أن تكون مبنية على أفضل الممارسات والمعايير المحلية والدولية؛
7. تتضمن سياسات الأمن السيبراني التالي:
   1. تعريف الأمن السيبراني؛
   2. نطاق وأهداف الأمن السيبراني لمؤسسة السوق؛
   3. دعم الإدارة العليا لبرنامج الأمن السيبراني وأهدافه؛
   4. تعريف المسؤوليات والأدوار للأمن السيبراني؛
   5. الإشارة إلى مرجعية معايير الأمن السيبراني المطبقة؛
   6. تتضمن ضوابط الأمن السيبراني التالي:
      1. تصنيف المعلومات بطريقة توضح أهميتها لمؤسسة السوق؛
      2. تحديد الملكية لأصول المعلومات كافة؛
      3. تقييم مخاطر الأمن السيبراني لأصول المعلومات؛
      4. توعية العاملين في الجهة بالأمن السيبراني؛
      5. الالتزام بالاتفاقيات والالتزامات التنظيمية والتعاقدية؛
      6. الإبلاغ عن اختراقات الأمن السيبراني والثغرات الأمنية المشتبه فيها؛
      7. تطبيق متطلبات الأمن السيبراني على إدارة استمرارية الأعمال.

4.1.4 التدريب والتوعية

الهدف :

تحديد برنامج خاص بالأمن السيبراني لتدريب وتوعية موظفي مؤسسة السوق وعملائها والأطراف الخارجية ذات العلاقة؛ لحماية الأصول المعلوماتية والتقنية لمؤسسة السوق.

الضوابط الأساسية :

1. تطوير برنامج توعية بالأمن السيبراني، واعتماده، وتوثيقه، وتنفيذه؛ لتعزيز الوعي بالأمن السيبراني.
2. يستهدف برنامج التوعية بالأمن السيبراني الحماية من أهم المخاطر والتهديدات السيبرانية، وأن يخاطب مختلف الفئات باستخدام قنوات متعددة.
3. تنفيذ برنامج التوعية بالأمن السيبراني بشكل دوري.

4. يتضمن برنامج التدريب والتوعية الخاص بالأمن السيبراني الحماية من التهديدات السيبرانية شاملاً:
   1. الأدوار والمسؤوليات المتعلقة بالأمن السيبراني؛
   2. معلومات عن حوادث الأمن السيبراني والتهديدات السيبرانية، على سبيل المثال: التصيد الإلكتروني؛
   3. التعامل الآمن مع الأجهزة المحمولة ووسائط التخزين؛
   4. التصفح الآمن للإنترنت؛
   5. التعامل الآمن مع مواقع التواصل الاجتماعي.
5. تقييم برنامج التدريب والتوعية بالأمن السيبراني لقياس مدى فعاليته وتقديم توصيات التحسين اللازمة.
6. توفير التدريب المتخصص واللازم لموظفي الامن السيبراني في الوظائف ذات العلاقة.

5.1.4 الأمن السيبراني المتعلق بالموارد البشرية

الهدف :

ضمان إدراج مسؤوليات الأمن السيبراني المتعلقة بموظفي مؤسسة السوق في عقود الموظفين.

الضوابط الأساسية :

1. تحديد ضوابط الأمن السيبراني المتعلقة بعملية الموارد البشرية وتوثيقها واعتمادها وتنفيذها.
2. مراقبة مدى فعالية ضوابط الأمن السيبراني ضمن عملية الموارد البشرية وقياسها، وتقييمها بشكل دوري.
3. تتضمن ضوابط الأمن السيبراني المتعلقة بعملية الموارد البشرية التالي:
   1. مسؤوليات الأمن السيبراني، وبنود عدم الإفصاح، والمحافظة على سرية المعلومات "Non-Disclosure Clauses" في عقود الموظفين (أثناء العلاقة الوظيفية وبعد انتهائها)؛
   2. التوعية بالأمن السيبراني في بداية عمل الموظفين وخلاله؛
   3. قابلية تطبيق الإجراءات التأديبية؛
   4. إجراء المسح الأمني "Screening" للموظفين وذلك من خلال جهات مخوله بإجراء المسح الأمني؛
   5. متطلبات ضوابط الأمن السيبراني بعد انتهاء/إنهاء العلاقة الوظيفية للموظف، مثل:
      1. إلغاء صلاحيات الدخول؛
      2. إعادة أصول المعلومات المخصصة (على سبيل المثال: بطاقة الدخول، والأجهزة المحمولة، وجميع المعلومات الإلكترونية والمادية).

2.4

إدارة مخاطر الأمن السيبراني والمراجعة والتدقيق

تتمثل إدارة المخاطر في تحديد المخاطر، وتحليلها، والاستجابة لها، ومراقبتها، واستعراضها باستمرار. ولإدارة مخاطر الأمن السيبراني، يجب على مؤسسة السوق القيام بما يلي:

- تحديد مخاطر الأمن السيبراني؛
- تحليل احتمالية وقوع مخاطر الأمن السيبراني والتأثير المترتب عليها؛
- الاستجابة لمخاطر الأمن السيبراني؛
- مراقبة معالجة مخاطر الأمن السيبراني، واستعراض فعالية المراقبة.

ويجب أن يخضع الالتزام بضوابط الأمن السيبراني إلى إجراءات المراجعة والتدقيق الدوري.

1.2.4 إدارة مخاطر الأمن السيبراني

الهدف :

تحديد منهجية إدارة مخاطر الأمن السيبراني وتوثيقها واعتمادها وتنفيذها بهدف حماية سرية وسلامة وتوافر الأصول المعلوماتية والتقنية لمؤسسة السوق، وضمان توافق منهجية إدارة مخاطر الأمن السيبراني مع منهجية إدارة مخاطر مؤسسة السوق.

الضوابط الأساسية :

1. تحديد منهجية إدارة مخاطر الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها، ومراجعتها بشكل دوري.
2. تهدف منهجية إدارة مخاطر الأمن السيبراني إلى حماية سرية وسلامة وتوافر أصول المعلومات.
3. يجب أن تتوافق منهجية إدارة مخاطر الأمن السيبراني مع منهجية إدارة مخاطر مؤسسة السوق المعتمدة.
4. توثيق منهجية إدارة مخاطر الأمن السيبراني، وتحديد المخاطر، وتحليلها، والاستجابة لها، ومراقبتها، ومراجعتها.
5. تتضمن منهجية إدارة مخاطر الأمن السيبراني الأصول المعلوماتية والتقنية مؤسسة السوق، بما في ذلك – على سبيل المثال لا الحصر–:
   - إجراءات العمل؛
   - تطبيقات الأعمال؛
   - مكونات البنية التحتية؛
   - الموظفون.

إدارة مخاطر الأمن السيبراني والمراجعة والتدقيق

6. تنفيذ إجراءات تقييم مخاطر الأمن السيبراني في المراحل التالية:
   1. في مرحلة مبكرة من المشروع؛
   2. قبل إجراء أي تغيير جوهري في البنية التقنية؛
   3. قبل الحصول على خدمات طرف خارجي؛
   4. قبل إطلاق منتجات وتقنيات جديدة.
7. تحديد مخاطر الأمن السيبراني وتوثيقها في سجل موحد يحتوي على جميع الأصول المعلوماتية والتقنية لمؤسسة السوق.
8. توثيق قائمة خيارات معالجة المخاطر (أي قبول المخاطر أو تجنبها أو نقلها أو الحد منها بتطبيق ضوابط الأمن السيبراني).
9. إعطاء الأولوية القصوى لمخاطر الأمن السيبراني عالية الخطورة، ورصدها عن كثب، وإعداد تقارير دورية بالإجراءات المُتخذة للحد من آثارها.

2.2.4 مراجعة الأمن السيبراني والتدقيق

الهدف :

تحديد الية المراجعة والتدقيق والتقييم الدوري لضوابط الأمن السيبراني المتعلقة بأصول مؤسسة السوق المعلوماتية والتقنية؛ للتأكد من أن ضوابط الأمن السيبراني لدى الجهة مطبقة وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

الضوابط الأساسية :

1. إجراء مراجعة وتدقيق لتطبيق ضوابط الأمن السيبراني بشكل دوري.
2. توثيق نتائج المراجعة والملاحظات المكتشفة والإجراءات الموصى بها، ومن ثم إبلاغ صاحب الصلاحية بها.
3. مراجعة الأمن السيبراني من قبل أطراف مستقلة عن إدارة الأمن السيبراني وفقاً للمعايير العامة المقبولة للمراجعة والتدقيق وبما يتماشى مع الدليل الاسترشادي للأمن السيبراني لمؤسسات السوق المالية.
4. مراجعة تطبيق ضوابط الأمن السيبراني وفقًا لدليل وخطة المراجعة والتدقيق الداخلي المعمول بها في مؤسسة السوق.

3.4

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

- **يجب على مؤسسة السوق ضمان تحديد ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية والإجراءات الداعمة لأصول المعلومات الخاصة بها، وتوثيقها، واعتمادها، وتنفيذها؛ من أجل حماية عمليات وتقنيات أصول معلومات مؤسسة السوق وموظفيها وعملائها وأي أطراف خارجية تابعة لها.**

- **كذلك يجب مراقبة الالتزام بضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية وتقييم فعاليتها بشكل دوري لتحديد المراجعات المحتملة للضوابط.**

1.3.4 هيكلية الأمن السيبراني

الهدف :

تحديد هيكلية الأمن السيبراني وتوثيقه واعتماده ومتابعته ومراجعته حيث تقوم مؤسسة السوق بتوضيح متطلبات الأمن السيبراني داخل المؤسسة ومعالجة مبادئ تصميم الشبكة والتطبيقات من أجل تعزيز الأمن السيبراني.

الضوابط الأساسية :

1. تحديد هيكلية الأمن السيبراني "Cyber security Architecture"، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها.
2. أن تتضمن هيكلية الأمن السيبراني التالي:
   1. التخطيط الاستراتيجي وتحديد ضوابط الأمن السيبراني وفقاً لمتطلبات العمل وذلك من خلال مهندسين مؤهلين للأمن السيبراني؛
   2. اتباع مبادئ التصميم اللازمة لتطوير وتطبيق ضوابط الأمن السيبراني (مثل "Security-by-design")؛
   3. المراجعة الدورية لهيكلية الأمن السيبراني.

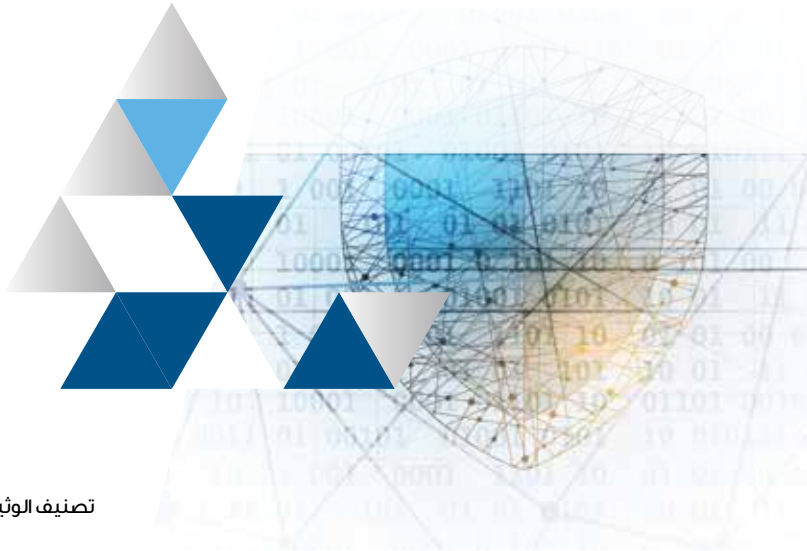
ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

2.3.4 أمن البنية التحتية

الهدف :
تحديد ضوابط الأمن السيبراني للبنية التحتية وتوثيقها واعتمادها وتنفيذها؛ ومراقبة الالتزام بهذه ضوابط وتقييم مدى فعاليتها داخل مؤسسة السوق بشكل دوري.

الضوابط الأساسية :

1. تحديد ضوابط الأمن السيبراني للبنية التحتية، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها. كذلك يجب تقييم هذه المعايير بشكل الدوري.
2. تغطي ضوابط الأمن السيبراني للبنية التحتية مراكز البيانات الرئيسية ومواقع بيانات التعافي من الكوارث.
3. تغطي ضوابط الأمن السيبراني للبنية التحتية جميع مكونات البنية التحتية (مثل أنظمة التشغيل، والخوادم، والأجهزة الافتراضية، وجدران الحماية، وأجهزة الشبكة، ونظام الحماية المتقدمة لاكتشاف الاختراقات "IDS"، ونظام الحماية المتقدمة لاكتشاف ومنع الاختراقات "IPS"، والشبكة اللاسلكية، والاتصالات الخارجية، وقواعد البيانات، وملفات المشاركة وأجهزة الحاسوب المكتبية والمحمولة والأجهزة اللوحية).
4. تتضمن ضوابط الأمن السيبراني للبريد الإلكتروني التالي:
    1. نظام التصفية الخاص بمكافحة الرسائل الإلكترونية التطفلية "Anti-spam Filtering"؛
    2. التحقق من الهوية متعدد العناصر "Multi-Factor Authentication" للدخول للبريد الإلكتروني والدخول عن بُعد؛
    3. النسخ الاحتياطي وأرشفة البريد الإلكتروني؛
    4. توثيق مجال البريد الإلكتروني بالطرق التقنية (مثل طريقة إطار سياسة المرسل "Sender Policy Framework").



ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

2.3.4 أمن البنية التحتية

5 تتضمن ضوابط الأمن السيبراني للبنية التحتية التالي:

1 تطبيق ضوابط الأمن السيبراني (على سبيل المثال: المراقبة والاحتفاظ بسجلات الأحداث، ومنع تسرب البيانات، وإدارة هويات الدخول والصلاحيات، والصيانة عن بُعد)؛

2 مبدأ الفصل بين المهام (مدعوماً بمصفوفة صلاحيات موثقة)؛

3 حماية البيانات والتعامل معها وفقاً لنظام التصنيف المتفق عليه (بما في ذلك خصوصية بيانات العميل، وتجنب الوصول غير المصرح به وتسرب البيانات المتعمد وغير المتعمد)؛

4 استخدام البرامج المعتمدة والمرخصة والبروتوكولات الآمنة؛

5 العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن؛

6 الحماية من البرمجيات الضارة والفيروسات (السماح بقائمة تطبيقات محددة "Whitelisting" والحماية من التهديدات المتقدمة والمستمرة "APT Protection")؛

7 إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات؛

8 الحماية من هجمات حجب الخدمة الموزعة "DDOS"، وأن يشمل:

1 استخدام خدمات التنقية "Scrubbing Services"؛

2 مواصفات عرض النطاق "Bandwidth" المتفق عليه؛

3 المراقبة على مدار الساعة طوال أيام الأسبوع ٢٤/٧ بواسطة مركز العمليات الأمنية "SOC"، ومزود الخدمة، ومزود خدمات التنقية "Scrubbing Provider"؛

4 اختبار تنقية حجب الخدمة الموزعة "DDOS Scrubbing" مرتين في السنة بحد أدنى؛

5 تنفيذ خدمات الحماية من حجب الخدمة الموزعة "DDOS" لمراكز البيانات الرئيسية وكذلك مراكز البيانات الاحتياطية في حالة الكوارث "Disaster Recovery"؛

9 تأمين الاتصال بالإنترنت والتصفح بما في ذلك تقييد الوصول للمواقع المشتبه فيها وخوادم التخزين ومواقع الوصول عن بُعد؛

10 أمن نظام أسماء النطاقات "DNS"؛

11 مزامنة التوقيت "Clock Synchronization" مع مصدر دقيق وموثوق به؛

12 إجراءات النسخ الاحتياطي واستعادة البيانات؛

13 التقييد الحازم لاستخدام وسائط التخزين الخارجية؛

14 المراجعة الدورية لمدى الالتزام بضوابط الأمن السيبراني.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

3.3.4 إدارة التغيير وإدارة المشاريع

الهدف :
تحديد منهجية وإجراءات إدارة التغيير وإدارة المشاريع وتوثيقها واعتمادها وتنفيذها؛ لضمان اتباع نهج موحد موثق ومعتمد لإدارة المشاريع وعند إجراء أي تغييرات على الأصول المعلوماتية والتقنية.

الضوابط الأساسية :

1. تحديد منهجية إدارة التغيير، وتوثيقها، واعتمادها وتنفيذها، ومراقبتها، بالإضافة إلى تقييمها ومراجعتها بشكل دوري.
2. تتضمن منهجية واجراءات إدارة التغيير التالي:
    1. ضوابط الأمن السيبراني للتحكم في التغييرات الطارئة على الأصول المعلوماتية والتقنية، مثل تقييم أثر التغيير وفرز وتصنيف التغييرات ومراجعتها؛
    2. الاختبار الأمني، ويجب أن يتضمن:
        1. اختبار الاختراق "Penetration Testing"؛
        2. مراجعة أمنية للكود المصدري "Security Source Code Review" في حالة تطوير التطبيقات داخليا أو خارجيا (إذا تعذر توفير الكود المصدري "Source Code" للتطبيقات الخارجية، فإن تقرير مراجعة الكود المصدري "Source Code" يُعدّ كافيًا)؛
    3. اعتماد صاحب الصلاحية للتغييرات المعنية؛
    4. الحصول على موافقة إدارة الأمن السيبراني في الجهة قبل تقديم التغييرات المعنية إلى المجلس الاستشاري للتغيير "Change-Advisory Board" للحصول على الموافقة اللازمة؛
    5. مراجعة مدى القبول للتغيير بعد تنفيذ ضوابط الأمن السيبراني ذات الصلة؛
    6. مبدأ فصل المهام "Segregation of Duties"؛
    7. فصل بيئة الإنتاج عن بيئات التطوير والاختبار؛
    8. إجراءات التغييرات والإصلاحات الطارئة؛
    9. إجراءات التراجع واستعادة البيانات والأنظمة للحالة السابقة "Rollback" و "Failback"؛
3. تحديد منهجية إدارة المشاريع، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها. كذلك يجب تقييمها ومراجعتها بشكل دوري
4. تتضمن منهجية إدارة المشاريع متطلبات الأمن السيبراني؛ لضمان تحديد مخاطره ومعالجتها كجزء من المشروع.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

5 تتضمن منهجية إدارة المشاريع التالي:
1 إدراج أهداف الأمن السيبراني ضمن أهداف المشروع؛
2 اعتبار إدارة الأمن السيبراني جزءاً من جميع مراحل المشروع؛
3 تقييم المخاطر في بداية المشروع لتحديد مخاطر الأمن السيبراني ولضمان معالجتها؛
4 توثيق مخاطر الأمن السيبراني في سجل مخاطر المشروع ومتابعتها؛
5 تحديد مسؤوليات الأمن السيبراني وتعيينها؛
6 مراجعة الأمن السيبراني من قبل طرف داخلي أو خارجي مستقل.
6 تتضمن منهجية إدارة المشاريع وإدارة التغيير تقييم الثغرات ومعالجتها، ومراجعة الإعدادات والتحصين وحزم التحديثات.

4.3.4 إدارة هويات الدخول والصلاحيات

الهدف :
تقييد الوصول إلى أصول المعلومات وفقاً لمتطلبات العمل المعنية وبما يتماشى مع مبادئ الحاجة إلى المعرفة والاستخدام "Need-to-Have or Need-to-Know"؛ وذلك لضمان توافر امتيازات وصول كافية ومصرح بها لاعتماد المستخدمين.

الضوابط الأساسية :
1 تحديد سياسة إدارة هويات الدخول والصلاحيات، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها.
2 قياس مدى فعالية ضوابط الأمن السيبراني ضمن سياسة إدارة هويات الدخول والصلاحيات وتقييمها بشكل دوري.
3 تتضمن سياسة إدارة هويات الدخول والصلاحيات التالي:
1 متطلبات العمل للتحكم في الوصول (كمبدأ الحاجة إلى المعرفة والاستخدام " Need-to-Have and Need-to-Know " ومبدأ الحد الأدنى من الصلاحيات والامتيازات "Least Privilege")؛
2 إدارة وصول المستخدمين:
1 أن تغطي جميع العاملين (الموظفين والأطراف الخارجية)؛
2 التحقق من هوية المستخدم؛
3 تتحمل إدارة الموارد البشرية مسؤولية إجراء أي تغييرات على الحالة الوظيفية أو المنصب الوظيفي للموظفين؛

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

4. الحصول على موافقة إدارة الأمن السيبراني في حال إجراء أي تغييرات متعلقة بالموظفين الخارجيين أو الأطراف الخارجية؛
5. الحصول على الموافقة على صلاحيات دخول المستخدم بشكل رسمي وموثق وبما يتوافق مع متطلبات العمل (كمبدأ الحاجة إلى المعرفة والاستخدام "Need-to-Have and Need-to-Know" لتجنب الوصول غير المصرح به وتسرب البيانات المتعمد (وغير المتعمد))؛
6. معالجة أي تغييرات طارئة على صلاحيات الدخول في الوقت المناسب؛
7. مراجعة صلاحيات دخول المستخدم والملفات الشخصية بشكل دوري؛
8. مراجعة طلبات دخول المستخدم المقدمة والمعتمدة والمعالجة، وإعداد طلبات الإلغاء ذات الصلة.
3. أن تكون إدارة دخول المستخدم مزودة بأنظمة الأتمتة؛
4. توحيد أنظمة إدارة هويات الدخول والصلاحيات؛
5. التحقق من الهوية متعدد العناصر للدخول إلى الأنظمة والحسابات الحساسة؛
6. تتضمن ضوابط إدارة الصلاحيات المهمة والحساسة وإدارة الدخول عن بُعد التالي:
1. التخصيص والاستخدام المقيد للدخول عن بُعد وللحسابات ذات الصلاحيات المهمة والحساسة، وتحديداً:
1. استخدام آلية التحقق من الهوية متعدد العناصر لجميع عمليات الدخول عن بُعد؛
2. استخدام آلية التحقق من الهوية متعدد العناصر للحسابات ذات الصلاحيات المهمة والحساسة على الأنظمة الحساسة بناءً على تقييم المخاطر؛
2. المراجعة الدورية للمستخدمين ذوي الحسابات المهمة والحساسة وحسابات الدخول عن بعد؛
3. المساءلة في حال المخالفات؛
4. استخدام حسابات الأنظمة المهمة والحساسة يشمل:
1. التقييد والمراقبة؛
2. المحافظة على سرية كلمات المرور؛
3. تغيير كلمات المرور بشكل دوري.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

5.3.4 إدارة الأصول المعلوماتية والتقنية

الهدف :
تحديد عملية إدارة الأصول المعلوماتية والتقنية وتوثيقها واعتمادها وتنفيذها ونشرها ومراقبتها بهدف الحصول على سجل دقيق موحد ومحدث للأصول؛ وذلك لدعم مؤسسة السوق في الحصول على قائمة جرد دقيقة وحديثة.

الضوابط الأساسية :
1. تحديد عملية إدارة الأصول المعلوماتية والتقنية، وتوثيقها، واعتمادها، وتنفيذها، ومراقبتها، وتقييمها بشكل دوري.
2. تتضمن عملية إدارة الأصول المعلوماتية والتقنية – على سبيل المثال لا الحصر– التالي:
   1. سجل موحد يشمل الأصول المعلوماتية والتقنية خلال دورة حياتها كاملة؛
   2. ملكية الأصول المعلوماتية والتقنية؛
   3. تصنيف الأصول المعلوماتية والتقنية، وترميزها والتعامل معها؛
   4. الاحتفاظ بنسخ احتياطية من سجلات الأصول بشكل صحيح وتخزينها في مكان آمن.
3. تحديد سياسة الاستخدام المقبول، وتوثيقها، واعتمادها، وتنفيذها، ونشرها، وتقييمها بشكل دوري.

6.3.4 الإتلاف الآمن

الهدف :
التخلص من أصول المعلومات الخاصة بمؤسسة السوق بشكل آمن إذا لم تعد هناك حاجة إليها؛ وذلك لضمان حماية عمل مؤسسة السوق وعملائها ومعلوماتها الحساسة من التسرب أو الإفصاح غير المصرح به عند التخلص منها.

الضوابط الأساسية :
1. تحديد معايير وإجراءات الإتلاف الآمن، وتوثيقها، واعتمادها، وتنفيذها.
2. تشمل معايير الإتلاف الآمن النسخ الرقمية والورقية وإعادة استخدام الأصول.
3. مراقبة الالتزام بمعايير وإجراءات الإتلاف الآمن.
4. قياس مدى فعالية ضوابط الأمن السيبراني للإتلاف الآمن، وتقييمها بشكل دوري.
5. التخلص من أصول المعلومات إذا لم تعد هناك حاجة إليها وفقًا للمتطلبات التشريعية والتنظيمية ذات العلاقة، وبما يتماشى مع لوائح خصوصية البيانات؛ لتجنب الوصول غير المصرح به وتسرب البيانات المتعمد وغير المتعمد.
6. إتلاف المعلومات الحساسة باستخدام تقنيات معينة لجعل المعلومات غير قابلة للاسترداد (على سبيل المثال: المسح الآمن "Secure Wiping"، المغنطة "Degaussing").
7. ضمان التزام مقدمي خدمات الأطراف الخارجية بمعايير وإجراءات الإتلاف الآمن، كذلك قياس مدى الفعالية وتقييمها بشكل دوري.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

7.3.4 إدارة حوادث الأمن السيبراني

الهدف :

تحديد عملية إدارة حوادث الأمن السيبراني التي تتوافق مع إدارة حوادث مؤسسة السوق وتوثيقها واعتمادها وتنفيذها لتحديد حوادث الأمن السيبراني والاستجابة لها والتغلب عليها. كذلك قياس مدى فعالية هذه العملية وتقييمها بشكل دوري؛ وذلك لضمان تحديد حوادث الأمن السيبراني ومعالجتها في الوقت المناسب للحد من التأثير السلبي المحتمل في مؤسسة السوق.

الضوابط الأساسية :

1. تطوير عملية إدارة حوادث الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها، ومواءمتها مع عملية إدارة حوادث مؤسسة السوق.
2. تضمين خطة التعافي من الكوارث سيناريوهات مختلفة لحوادث الأمن السيبراني.
3. قياس مدى فعالية ضوابط الأمن السيبراني في عملية إدارة حوادث الأمن السيبراني، وتقييمها بشكل دوري.
4. تضمين ضوابط عملية إدارة حوادث الأمن السيبراني التالي:
   1. تأسيس فريق مسؤول عن إدارة حوادث الأمن السيبراني؛
   2. توافر موظفين مؤهلين ومدربين بشكل جيد؛
   3. منطقة محظورة مخصصة لأماكن عمل فريق الاستجابة للطوارئ لحوادث الأمن السيبراني "CERT"؛
   4. وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد؛
   5. تصنيف حوادث الأمن السيبراني؛
   6. معالجة حوادث الأمن السيبراني في الوقت المناسب ومتابعة التقدم ومراقبته؛
   7. حماية الأدلة والسجلات ذات الصلة؛
   8. التحليل الجنائي للحوادث السيبرانية؛
   9. الاحتفاظ بسجل حوادث الأمن السيبراني.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

10 التنسيق مع هيئة السوق المالية قبل أي تفاعل إعلامي يتعلق بالحادثة الأمنية.

6 إبلاغ الهيئة الوطنية للأمن السيبراني وإدارة أمن المعلومات في هيئة السوق المالية فور وقوع أي حادثة أمنية وتحديدها.

7 تقديم تقرير رسمي عن الحادثة الأمنية إلى هيئة السوق المالية بعد استئناف العمليات، بما في ذلك تفاصيل الحادث التالية:

1 عنوان الحادثة الأمنية الإلكترونية؛

2 تصنيف حالة الحادثة الأمنية الإلكترونية (متوسط أو مرتفع)؛

3 تاريخ ووقت وقوع الحادثة الأمنية الإلكترونية؛

4 تاريخ ووقت اكتشاف الحادثة الأمنية الإلكترونية؛

5 أصول المعلومات المعنية؛

6 التفاصيل الفنية للحادثة الأمنية الإلكترونية؛

7 تحليل للأسباب والدوافع؛

8 الإجراءات التصحيحية المنفذة والمخططة؛

9 وصف الضرر (على سبيل المثال: فقد البيانات، وتعطل الخدمات، والتعديل غير المصرح به للبيانات، وتسرب البيانات المتعمد وغير المتعمد، بالإضافة إلى عدد العملاء المتضررين)؛

10 التكلفة الإجمالية المقدرة للحادثة الأمنية الإلكترونية؛

11 التكلفة التقديرية للإجراءات التصحيحية؛

12 يُرسل التقرير إلى البريد الإلكتروني التالي: Cyber.Incidents@cma.org.sa

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

8.3.4 إدارة سجلات أحداث الأمن

الهدف :

تحديد عملية إدارة سجلات أحداث الأمن السيبراني وتوثيقها واعتمادها وتنفيذها لتحليل التسجيل الأمني والتشغيلي والتعامل مع أحداث الأمن السيبراني. كذلك يجب قياس مدى فعالية هذه العملية وتقييمها بشكل دوري؛ لضمان التعرف على الأحداث المشتبه فيها المتعلقة بأصول المعلومات، والاستجابة لها في الوقت المناسب.

الضوابط الأساسية :

1. تحديد عملية إدارة سجلات أحداث الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها.
2. قياس مدى فعالية ضوابط الأمن السيبراني في عملية إدارة سجلات أحداث الأمن السيبراني، وتقييمها بشكل دوري.
3. تحديد معايير مراقبة سجلات أحداث الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها لدعم هذه العملية.
4. تحدد معايير الأحداث الواجب مراقبتها بناءً على تصنيف أصول المعلومات أو ملف المخاطر.
5. مراقبة سجلات أحداث الأمن السيبراني للحسابات ذات الصلاحيات المهمة والحساسة وحسابات الدخول عن بُعد.
6. الاحتفاظ بسجلات أحداث الأمن السيبراني مدة ١٢ شهرًا على الأقل.
7. تتضمن عملية إدارة سجلات أحداث الأمن السيبراني التالي:
    1. تأسيس فريق مسؤول عن المراقبة الأمنية (مركز العمليات الأمنية "SOC")؛
    2. موظفون مواطنون مؤهلون ومدربون بشكل جيد؛
    3. منطقة محظورة مخصصة لأماكن عمل مركز العمليات الأمنية والأنشطة ذات الصلة؛
    4. الموارد اللازمة لأنشطة المراقبة المستمرة للأحداث الأمنية على مدار ٢٤ ساعة طوال أيام الأسبوع؛
    5. الكشف عن الشفرة المصدرية "Code" والبرمجيات الخبيثة ومعالجتها؛
    6. الكشف عن الأحداث الأمنية المشتبه فيها ومعالجتها؛
    7. استخدام حلول لتحليل حزم الشبكات؛
    8. حماية سجلات أحداث الأمن السيبراني؛
    9. المراقبة الدورية للالتزام بمعايير الأمن السيبراني للتطبيقات والبنية التحتية؛
    10. استخدام التحليل الآلي والمركزي للسجلات الأمنية وربط الأحداث أو الأنماط (مثل نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني "SIEM")؛
    11. الإبلاغ عن حوادث الأمن السيبراني؛
    12. اختبار دوري مستقل للتحقق من فعالية مركز العمليات الأمنية "SOC" (على سبيل المثال، "Red Team").

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

8 وفي حالة حدوث حوادث أمن سيبراني كبرى:

1. يشكَّل فريق لإدارة الأزمات يتكون من مسؤول من مجلس إدارة مؤسسة السوق وممثلين عن الإدارة التنفيذية وأفراد مؤهلين للتعامل مع الحوادث.
2. يخضع الإفصاح عن حوادث الأمن السيبراني لمعايير محددة، وأن يشمل الأطراف ذات العلاقة.
3. وضع خطة تحسين وتطوير بعد انتهاء الأزمة، واتخاذ التدابير اللازمة، وتنفيذ التوصيات المعنية بناءً على التقرير.
4. التأكد من انتهاء الحادث مزوداً بجميع الوثائق اللازمة فيما يتعلق بكيفية انتهائه، والدروس المستفادة منه، ومدى الحاجة إلى إجراء تحقيقات إضافية ومراجعات وتقارير ما بعد الأزمة.

9.3.4 إدارة تهديدات الأمن السيبراني

الهدف :

تحديد عملية إدارة تهديدات الأمن السيبراني وتوثيقها واعتمادها وتنفيذها لتحديد وتقييم وفهم الأخطار التي تهدد الأصول المعلوماتية والتقنية لمؤسسة السوق، وذلك باستخدام مصادر متعددة موثوق بها، وقياس مدى فعالية هذه العملية، وتقييمها بشكل دوري.

الضوابط الأساسية :

1. تحديد عملية إدارة تهديدات الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها.
2. قياس مدى فعالية عملية إدارة تهديدات الأمن السيبراني، وتقييمها بشكل دوري.
3. تتضمن عملية إدارة تهديدات الأمن السيبراني التالي:

1. استخدام المصادر الداخلية، مثل التحكم في الدخول والتطبيقات، وسجلات البنية التحتية، ونظام الحماية المتقدمة لاكتشاف الاختراقات "IDS"، ونظام الحماية المتقدمة لاكتشاف ومنع الاختراقات "IPS"، والأدوات الأمنية ونظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني "SIEM"، وكذلك الإدارات الداعمة (على سبيل المثال: القانونية والمراجعة والتدقيق وقسم الدعم الفني والبحث الجنائي وإدارة مكافحة الاحتيال وإدارة المخاطر والالتزام)؛
2. استخدام مصادر خارجية موثوق بها وذات صلة للمعلومات الاستباقية، مثل الجهات الحكومية ذات العلاقة ومقدمي الخدمات الأمنية؛
3. منهجية محددة لتحليل المعلومات المتعلقة بالتهديد بشكل دوري؛
4. التفاصيل المتعلقة بالتهديدات المحددة، مثل طريقة العمل والجهات الفاعلة والدافع ونوع التهديدات؛
5. مشاركة المعلومات الاستباقية ذات الصلة مع الجهات المعنية.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

10.3.4 ◄ حماية التطبيقات

الهدف :
تحديد ضوابط الأمن السيبراني للتطبيقات وتوثيقها واعتمادها وتنفيذها ومراقبة الالتزام بهذه المعايير وقياس مدى فعالية هذه الضوابط وتقييمها بشكل دوري.

الضوابط الأساسية :

1. تحديد ضوابط الأمن السيبراني للتطبيقات، وتوثيقها، واعتمادها، وتنفيذها.
2. مراقبة الالتزام بضوابط الأمن السيبراني لحماية التطبيقات.
3. قياس مدى فعالية ضوابط الأمن السيبراني للتطبيقات، وتقييمها بشكل دوري.
4. اتباع المنهجية المعتمدة الخاصة بدورة حياة تطوير النظام الآمن "SDLC" عند تطوير التطبيقات.
5. تتضمن ضوابط الأمن السيبراني لحماية التطبيقات التالي:
   1. استخدام معايير التطوير الآمن للتطبيقات "Secure Coding Standards"؛
   2. ضوابط الأمن السيبراني المُطبقة (مثل "Configuration Parameters"، والأحداث التي يتعين مراقبتها والاحتفاظ بها [بما في ذلك الوصول إلى النظام والبيانات]، وإدارة الهويات، وصلاحيات الدخول)؛
   3. استخدام مصادر ومكتبات موثوق بها ومعتمدة؛
   4. استخدام مبدأ المعمارية متعددة المستويات "Multi-tier Architecture"، ونظام التحقق من الهوية متعدد العناصر "Multi-Factor Authentication"، وجدار الحماية لتطبيقات الويب "Web Application Firewall" وبروتوكولات آمنة؛
   5. تنفيذ اختبارات الاختراق لجميع الخدمات المقدمة خارجياً (عن طريق الإنترنت) سنوياً بحد أدنى.
   6. أمن التكامل بين التطبيقات؛
   7. سياسة الاستخدام المقبول؛
   8. مبدأ فصل المهام "Segregation of Duties" (مدعوماً بمصفوفة صلاحيات موثقة)؛
   9. حماية البيانات والتعامل معها وفقاً لنظام التصنيف المعمول به في الجهة (بما في ذلك خصوصية بيانات العميل، وتجنب الوصول غير المصرح به وتسريب البيانات المتعمد أو غير المتعمد)؛
   10. إدارة الثغرات وحزم التحديثات والإصلاحات الأمنية؛
   11. إجراءات النسخ الاحتياطي واستعادة البيانات؛
   12. مراجعة الالتزام بالأمن السيبراني بشكل دوري.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

11.3.4 التشفير

الهدف :
تحديد استخدام حلول التشفير داخل مؤسسة السوق وتوثيقها واعتمادها وتنفيذها؛ لضمان حماية الوصول إلى المعلومات الحساسة وسلامتها.

الضوابط الأساسية :
1. تحديد معايير التشفير، وتوثيقها، واعتمادها، وتنفيذها.
2. مراقبة الالتزام بمعايير التشفير.
3. قياس مدى فعالية ضوابط الأمن السيبراني الخاصة بالتشفير، وتقييمها بشكل دوري.
4. أن يتضمن معيار التشفير التالي:
   1. استعراض عام لحلول التشفير المعتمدة والقيود المطبقة عليها (تقنيا وتنظيمياً)؛
   2. الحالات التي ينبغي بموجبها تطبيق حلول التشفير المعتمدة؛
   3. إدارة مفاتيح التشفير، بما في ذلك إدارة دورة حياتها وأرشفتها واستعادتها؛
   4. تشفير البيانات أثناء النقل والتخزين بناءً على تصنيفها وبحسب أفضل الممارسات والمعايير والمتطلبات التشريعية والتنظيمية ذات الصلة.

12.3.4 إدارة الثغرات

الهدف :
تحديد عملية إدارة الثغرات الأمنية وتوثيقها واعتمادها وتنفيذها لتحديد الثغرات الأمنية في التطبيقات والبنية التحتية والتخفيف من آثارها، وقياس مدى فعالية هذه العملية، وتقييم تأثيرها بشكل دوري.

الضوابط الأساسية :
1. تحديد عملية إدارة الثغرات، وتوثيقها، واعتمادها، وتنفيذها.
2. قياس فعالية عملية إدارة الثغرات، وتقييمها بشكل دوري.
3. تتضمن عملية إدارة الثغرات التالي:
   1. جميع الأصول المعلوماتية والتقنية؛
   2. إجراء فحص الثغرات بشكل دوري؛
   3. تصنيف الثغرات الأمنية؛
   4. تحديد جداول زمنية لمعالجة الثغرات بناءً على تصنيفها؛
   5. تحديد الأولويات للأصول المعلوماتية والتقنية المصنفة؛
   6. إدارة حزم التحديثات الأمنية وأساليب تطبيقها.
   7. التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

13.3.4 خدمات التداول الإلكتروني

الهدف :

تحديد ضوابط الأمن السيبراني لخدمات التداول الإلكتروني وتوثيقها واعتمادها وتنفيذها ومراقبتها، وقياس فعالية هذه الضوابط وتقييمها بشكل دوري؛ لضمان سرية معلومات العملاء.

الضوابط الأساسية :

1. تحديد ضوابط الأمن السيبراني لخدمات التداول الإلكتروني، وتوثيقها، واعتمادها، وتنفيذها.
2. مراقبة الالتزام بضوابط الأمن السيبراني لخدمات التداول الإلكتروني.
3. قياس مدى فعالية ضوابط الأمن السيبراني لخدمات التداول الإلكتروني، وتقييمها بشكل دوري.
4. تتضمن ضوابط الأمن السيبراني لخدمات التداول الإلكتروني التالي:
    1. حماية الخدمات الإلكترونية، بما في ذلك وسائل التواصل الاجتماعي.
    2. حماية التداولات عبر الإنترنت والجوال والهاتف من خلال:
        1. استخدام متاجر ومواقع التطبيقات الرسمية والموثوق بها؛
        2. استخدام التدابير الوقائية للكشف عن التطبيقات ومواقع الإنترنت المزيفة وإغلاقها؛
        3. استخدام آليات "Sandboxing"؛
        4. استخدام تقنيات التخزين غير المؤقت "Non-Caching" ؛
        5. استخدام تقنيات الاتصال لتفادي هجمات "Man-in-the-Middle"؛
        6. استخدام آليات التحقق من الهوية متعدد العناصر:
            1. يجب استخدام آلية التحقق من الهوية متعدد العناصر أثناء عملية تسجيل العميل من أجل الاستفادة من خدمات التداول الإلكتروني؛
            2. يجب تطبيق آلية التحقق من الهوية متعدد العناصر على جميع خدمات التداول الإلكتروني المتاحة للعملاء؛
            3. حماية رموز الأمان بكلمة مرور؛
            4. حجب خيار وصول العملاء بعد إدخال ٣ كلمات مرور غير صحيحة متتالية أو أرقام تعريف شخصي "PIN" غير صالحة؛
            5. إجراء عمليات طلب التحقق من الهوية متعدد العناصر وتفعيلها من خلال قنوات اتصال مختلفة؛
            6. تطبيق آلية التحقق من الهوية متعدد العناصر على العمليات التالية:
                1. تسجيل الدخول؛
                2. إعادة تعيين كلمة المرور.
            7. ضمان استمرارية وتوافر لخدمات التداول الإلكتروني؛
            8. يجب أن تنطوي اتفاقية التعاقد بين مؤسسة السوق والعميل على توضيح الأدوار والمسؤوليات والالتزامات لكل من مؤسسة السوق والعملاء فيما يخص متطلبات الأمن السيبراني؛
            9. إشعار هيئة السوق المالية عند بدء خدمة تداول إلكتروني جديدة.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

3 **خدمات الإشعار الفوري عبر الرسائل النصية القصيرة:**

1 يجب أن لا تحتوي الرسائل النصية القصيرة "SMS" على بيانات حساسة (مثل رقم الهوية الوطنية الخاص بالعميل، ورقم المحفظة الاستثمارية)؛

2 يجب إرسال الإشعار عبر الرسائل النصية القصيرة "SMS" إلى رقم هاتف العميل عند طلب آلية جديدة للتحقق من الهوية متعدد العناصر؛

3 يجب إرسال الإشعار عبر الرسائل النصية القصيرة "SMS" إلى رقم هاتف العميل عند تنفيذ جميع عمليات التداول والاكتتاب والاسترداد.

14.3.4 الأمن المادي

الهدف :

الحماية المادية لجميع مرافق مؤسسة السوق لمنع الوصول المادي غير المصرح به وضمان حماية مؤسسة السوق.

الضوابط الأساسية :

1 تحديد ضوابط الأمن المادي، وتوثيقها، واعتمادها، وتنفيذها.

2 مراقبة مدى فعالية ضوابط الأمن المادي، وقياسها، وتقييمها بشكل دوري.

3 ضمان حماية خدمات التداول من التعطل الناجم عن انقطاع التيار الكهربائي.

4 مراقبة أجهزة الإنذار من الحريق على نحو مستمر، واختبارها بصفة منتظمة، وصيانتها وفقًا لمواصفات الشركة المصنعة.

5 العمل على تخفيف أثر مخاطر الكوارث الطبيعية.

6 تتضمن عملية الأمن المادي - على سبيل المثال لا الحصر - التالي:

1 ضوابط الدخول المادي (بما في ذلك أمن الزوار)؛

2 المراقبة والرصد (على سبيل المثال: أنظمة المراقبة "CCTV"، وأجهزة الاستشعار)؛

3 حماية مراكز البيانات وغرف البيانات وإمدادات الطاقة للمرافق المهمة؛

4 الحماية ضد المخاطر البيئية؛

5 حماية أصول المعلومات أثناء دورة حياتها (بما في ذلك النقل، والإتلاف الآمن، وتجنب الوصول غير المصرح به، وتسريب البيانات المتعمد أو غير المتعمد)؛

6 تدريب الموظفين على استخدام طفايات الحريق وغيرها من معدات السلامة.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

15.3.4 إدارة استمرارية الأعمال

الهدف :

تحديد سياسة واستراتيجية وخطط استمرارية الأعمال وتوثيقها واعتمادها وتنفيذها بناءً على تقييم مخاطر الأمن السيبراني وتحليل التأثير في الأعمال "BIA"، ومراقبة الالتزام بهذه الضوابط المحددة، وقياس مدى فاعلية تأثيرها، وتقييمها بشكل دوري؛ لضمان فعالية وجاهزية خطط التعافي من الكوارث وفرق العمل في حال وقوع حادث، ومراجعتها بشكل دوري.

الضوابط الأساسية :

1. تحديد سياسة استمرارية الأعمال، وتوثيقها، واعتمادها، وتحديثها، ونشرها للجهات ذات العلاقة داخل مؤسسة السوق وخارجها.
2. مراجعة سياسة استمرارية الأعمال سنويًا أو عند حدوث تغييرات مهمة.
3. تحديد المعايير والتشريعات واللوائح التنظيمية التي تجب مراعاتها أثناء إعداد سياسة استمرارية الأعمال.
4. إجراء تحليل التأثير في الأعمال "BIA" الذي يمكن من خلاله تحديد جميع العمليات والخدمات المهمة الخاصة بالعمل لمؤسسة السوق.
5. إجراء تحليل التأثير في الأعمال "BIA" سنويًا لتحديد نطاق برنامج إدارة استمرارية الأعمال ولتأكيد أولويات الأعمال ومواردها.
6. إعداد استراتيجية إدارة استمرارية الأعمال التي توضح متطلبات استعادة الأعمال، وتتوافق مع الوقت المطلوب والمتوقع لاستعادة القدرة على العمل المحدد والمعتمد في تحليل التأثير في الأعمال "BIA".
7. إنشاء فريق لإدارة الأزمات، مكون من ممثل عن مجلس الإدارة وممثلين عن الإدارة التنفيذية وأفراد مؤهلين للتعامل مع الحوادث التي تؤثر في استمرارية الأعمال.
8. تتضمن خطة استمرارية الأعمال خطوات واضحة ومحددة يجب اتخاذها في حال وقوع أزمات أو حالات طوارئ، وتفاصيل الاتصال الخاصة بجميع الأفراد المسؤولين، واختبارها بصفة منتظمة، ومعرفة مدى محاكاتها للواقع.
9. اختبار خطط إدارة استمرارية الأعمال وخطط التعافي من الكوارث بشكل دوري أو بعد كل تغيير جوهري لضمان ملاءمتها وتحديثها وتوافقها مع أهداف استمرارية الأعمال.
10. التأكد من أن الموظفين العاملين على إعداد برامج إدارة استمرارية الأعمال مدربون ومؤهلون ويمتلكون الخبرة اللازمة للتعامل مع إدارة مثل هذه الخطط والبرامج.
11. توفير التدريب العام والتوعية اللازمة لجميع الموظفين فيما يتعلق بإدارة استمرارية الأعمال.

ضوابط الأمن السيبراني المتعلق بالعمليات التشغيلية

16.3.4 استخدام الأجهزة الشخصية "BYOD"

الهدف :

تحديد معايير وضوابط الأمن السيبراني لاستخدام الأجهزة الذكية (مثل الهواتف الذكية والأجهزة اللوحية وأجهزة الحاسوب المحمولة) لأغراض العمل؛ بهدف ضمان سرية معلومات مؤسسة السوق وحمايتها.

الضوابط الأساسية :

1. تحديد سياسة الأمن السيبراني المتعلقة باستخدام الأجهزة الشخصية، وتوثيقها، واعتمادها، وتنفيذها.
2. مراقبة الالتزام بسياسة الأمن السيبراني المتعلقة باستخدام الأجهزة الشخصية.
3. قياس مدى فعالية ضوابط الأمن السيبراني المتعلقة باستخدام الأجهزة الشخصية، وتقييمها بشكل دوري.
4. أن تتضمن سياسة استخدام الأجهزة الشخصية التالي:
    1. مسؤوليات المستخدم (بما في ذلك التدريب والتوعية)؛
    2. المعلومات المتعلقة بالقيود المفروضة، والعواقب التي يتعرض لها الموظفون عند تطبيق ضوابط الأمن السيبراني على أجهزتهم الشخصية؛ ومن ذلك على سبيل المثال: عند استخدام الأجهزة المعدلة (برنامج كسر الحماية "Jailbreaking")، أو إنهاء العمل، أو في حالة فقدان الجهاز الشخصي أو سرقته؛
    3. فصل البيانات والمعلومات الخاصة بمؤسسة السوق عن المعلومات الشخصية (مثل "Containerization")؛
    4. قوانين استخدام تطبيقات الهواتف المحمولة الخاصة بمؤسسة السوق أو تطبيقات الهواتف المحمولة العامة المعتمدة؛
    5. استخدام إدارة الأجهزة المحمولة "(Mobile Device Management) (MDM)"؛ لتطبيق ضوابط التحكم في الوصول على الجهاز عن بعد، وآليات التشفير وحذف البيانات والمعلومات المخزنة على الجهاز الشخصي عن بُعد؛

4.4

الأمن السيبراني المتعلق بالأطراف الخارجية والموردين

- **عند الاستعانة بخدمات الأطراف الخارجية، يجب على مؤسسة السوق ضمان تطبيق نفس المستوى من حماية الأمن السيبراني على ذلك الطرف الخارجي، كما هو الحال داخل مؤسسة السوق.**

- **تحديد وتنظيم متطلبات الأمن السيبراني بين مؤسسة السوق والأطراف الخارجية وتوثيقها واعتمادها وتنفيذها ومراقبتها. وتُعرّف الأطراف الخارجية في الدليل الاسترشادي بأنهم موفرو خدمات الإسناد ومقدمو الخدمات الخارجية ومزودو الحوسبة السحابية والبائعون والموردون والجهات الحكومية وما إلى ذلك.**

1.4.4 إدارة العقود والموردين

الهدف :
تحديد ضوابط الأمن السيبراني ضمن عمليات إدارة العقود والموردين وتوثيقها واعتمادها وتنفيذها ومراقبتها.

الضوابط الأساسية :

1 تحديد ضوابط الأمن السيبراني، وتوثيقها، واعتمادها، وتنفيذها، ونشرها ضمن إطار عمليات إدارة العقود والموردين.

2 مراقبة الالتزام بعملية إدارة العقود والموردين.

3 قياس مدى فعالية ضوابط الأمن السيبراني ضمن إطار عملية إدارة العقود والموردين، وتقييمها بشكل دوري.

4 تتضمن عمليات إدارة العقود والموردين التالي:

1 تضمين الحد الأدنى من ضوابط الأمن السيبراني التي يجب تطبيقها في جميع الحالات؛

2 الأحقية في إجراء مراجعة وتدقيق للأمن السيبراني بشكل دوري.

5 تتضمن عملية إدارة العقود التالي:

1 إجراء تقييم لمخاطر الأمن السيبراني كجزء من عملية توقيع العقود مع طرف خارجي (مثل خدمات الإسناد لتقنية المعلومات"Outsourcing" والخدمات المدارة "Managed Services")؛

2 تحديد ضوابط الأمن السيبراني كجزء من عملية الطرح والمناقصة؛

3 تقييم استجابات الموردين المحتملين بناءً على ضوابط الأمن السيبراني المحددة؛

4 اختبار ضوابط الأمن السيبراني المتفق عليها (القائمة على المخاطر)؛

5 تحديد إجراءات الاتصال والتصعيد في حالة وقوع حادثة أمن سيبراني؛

6 تحديد اتفاقية المحافظة على سرية البيانات "Non-Disclosure Clauses".

7 الحذف الآمن من قِبَل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.

6 تتضمن عملية إدارة الموردين إعداد تقارير دورية لمتطلبات ضوابط الأمن السيبراني المتفق عليها في العقود ومراجعتها وتقييمها (في اتفاقية مستوى الخدمة "Service Level Agreement").

الأمن السيبراني المتعلق بالأطراف الخارجية والموردين

2.4.4 الإسناد الخارجي

الهدف :

تحديد ضوابط الأمن السيبراني المنصوص عليها في سياسة وعملية الإسناد الخارجي وتوثيقها واعتمادها وتنفيذها ومراقبتها، وقياس مدى فعالية ضوابط الأمن السيبراني المحددة وتقييمها.

الضوابط الأساسية :

1. تحديد ضوابط الأمن السيبراني في سياسة وعملية الإسناد الخارجي، وتوثيقها، واعتمادها، وتنفيذها، ونشرها داخل مؤسسة السوق.
2. قياس ضوابط الأمن السيبراني المتعلقة بسياسة وعملية الإسناد الخارجي، وتقييمها بشكل دوري.
3. أن تشمل عملية الإسناد الخارجي مشاركة إدارة الأمن السيبراني وتقييم مخاطر الأمن السيبراني؛
4. الالتزام بالأنظمة والتشريعات الوطنية ذات العلاقة.
5. يقتصر الإسناد الخارجي لتوفير خدمات مراقبة العمليات الأمنية على مقدمي الخدمة الموجودين بالمملكة العربية السعودية.

الأمن السيبراني المتعلق بالأطراف الخارجية والموردين

3.4.4 الحوسبة السحابية

الهدف :

تحديد ضوابط الأمن السيبراني في استخدام الحوسبة السحابية وعملية الخدمات السحابية والاستضافة وتوثيقها واعتمادها وتنفيذها ومراقبتها، وقياس مدى فعالية ضوابط الأمن السيبراني المحددة وتقييمها.

الضوابط الأساسية :

1. تحديد ضوابط الأمن السيبراني ضمن سياسة الحوسبة السحابية للخدمات السحابية والاستضافة، وتوثيقها، واعتمادها، وتنفيذها، ونشرها داخل مؤسسة السوق.
2. مراقبة الالتزام بسياسة الحوسبة السحابية.
3. قياس ضوابط الأمن السيبراني المتعلقة بسياسة الحوسبة السحابية وعملية الخدمات السحابية والاستضافة، وتقييمها بشكل دوري.
4. تتضمن ضوابط الأمن السيبراني لسياسة الحوسبة السحابية للخدمات السحابية التالي:
    1. عملية اعتماد الخدمات السحابية، وتشمل:
        1. إجراء تقييم لمخاطر الأمن السيبراني تجاه مزود الخدمة السحابية والخدمات السحابية؛
        2. إبرام عقد يشمل ضوابط الأمن السيبراني، وذلك قبل استخدام الخدمات السحابية؛
    2. إجراء تصنيف البيانات قبل استضافتها؛
    3. موقع البيانات، ويشمل الالتزام باستخدام الخدمات السحابية الموجودة في المملكة العربية السعودية؛
    4. قيود استخدام البيانات، وتشمل عدم استخدام مزود الخدمة السحابية بيانات مؤسسة السوق لأغراض أخرى؛
    5. الحماية، ويجب على مزود الخدمة السحابية تطبيق ضوابط الأمن السيبراني ومراقبتها على النحو المحدد في تقييم المخاطر؛ وذلك من أجل حماية سرية بيانات مؤسسة السوق وسلامتها وضمان توافرها؛
    6. فصل البيانات، ويشمل فصل بيانات مؤسسة السوق عن البيانات الأخرى التي يحتفظ بها مزود الخدمة السحابية بشكل ملائم، بحيث يكون مزود الخدمة السحابية قادرًا على تحديد بيانات مؤسسة السوق في جميع الأوقات وتمييزها عن البيانات الأخرى.
    7. استمرارية الأعمال، ويتضمن ذلك تلبية متطلبات استمرارية الأعمال وفقًا لسياسة استمرارية الأعمال المعتمدة لدى مؤسسة السوق؛
    8. أحقية مؤسسة السوق في إجراء مراجعة وتدقيق وفحص للأمن السيبراني لدى مزود الخدمة السحابية؛
    9. الإنهاء، ويشمل:
        1. حقوق مؤسسة السوق في الإنهاء؛
        2. حقوق مؤسسة السوق باستعادة بياناتها من قبل مزود الخدمة السحابية عند الإنهاء في صيغة مناسبة يمكن استخدامها؛
        3. حقوق مؤسسة السوق بالمطالبة بحذف بياناتها من قبل مزود الخدمة السحابية عند الإنهاء بشكل غير قابل للاستعادة.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

إدارة صلاحيات الوصول

Access management

إدارة الوصول هي عملية منح المستخدمين المصرح لهم الحق في استخدام الخدمة، ومنع وصول المستخدمين غير المصرح لهم.

إدارة الهوية

Identity management

عملية التحكم في المعلومات المتعلقة بمستخدمي أجهزة الحاسوب، بما في ذلك كيفية التحقق من الهوية والأنظمة المصرح لهم بالوصول إليها والإجراءات المصرح لهم باتخاذها. وتشمل أيضا إدارة المعلومات المتعلقة بالمستخدم وكيفية الوصول إلى تلك المعلومات وتعديلها ومن يمكنه ذلك.

الأصل

Asset

أي شيء ملموس أو غير ملموس له قيمة بالنسبة إلى الجهة. وهناك أنواع كثيرة من الأصول؛ وبعض هذه الأصول تتضمن أشياء واضحة، مثل: الأشخاص، والآلات، والمرافق، وبراءات الاختراع، والبرمجيات، والخدمات. ويمكن أن يشمل المصطلح أيضاً أشياء أقل وضوحاً، مثل: المعلومات والخصائص (كسمعة الجهة وصورتها العامة، أو المهارة والمعرفة).

هجوم

Attack

أي نوع من الأنشطة الخبيثة التي تحاول الوصول بشكل غير مشروع أو جمع موارد النظم المعلوماتية أو المعلومات نفسها أو تعطيلها أو منعها أو تحطيمها أو تدميرها.

تدقيق

Audit

المراجعة المستقلة ودراسة السجلات والأنشطة لتقييم مدى فعالية ضوابط الأمن السيبراني ولضمان الالتزام بالسياسات والإجراءات التشغيلية والمعايير والمتطلبات التشريعية والتنظيمية ذات العلاقة.

التوافر

Availability

ضمان الوصول إلى البيانات والمعلومات والأنظمة والتطبيقات واستخدامها في الوقت المناسب.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

السرية
Confidentiality
الاحتفاظ بقيود مصرح بها على الوصول إلى المعلومات والإفصاح عنها، بما في ذلك وسائل حماية معلومات الخصوصية.

سلامة المعلومات
Integrity
الحماية ضد تعديل أو تخريب المعلومات بشكل غير مصرح به، وتتضمن ضمان عدم الإنكار للمعلومات (Non- Repudi-ation) والموثوقية.

التأكيد
Assurance
التأكد من تحقيق الأهداف الأمنية الأربعة (السلامة والتوافر والسرية والمساءلة) من خلال تنفيذ محدد. ويشمل التحقق (١) وظيفة تؤدى بشكل صحيح، و(٢) حماية كافية من الأخطاء غير المقصودة (من قبل المستخدمين أو البرامج)، و (٣) مقاومة كافية للاختراق المتعمد أو الالتفاف.

الرئيس التنفيذي
المسؤول التنفيذي الذي يتمتع بسلطة اتخاذ القرارات الرئيسية داخل المنظمة.

لجنة الأمن السيبراني
تهدف إلى مساعدة مؤسسة السوق المالية للحصول على ممارسات الأمن السيبراني الجيدة، الموضوعة من جانب هيئه السوق المالية.

مؤسسات السوق
الجهات المالية التي تخضع لإشراف ورقابة وترخيص هيئة السوق المالية.

إدارة التغيير
تتمثل في تحديد وإجراء التغييرات المطلوبة فيما يتعلق بالرقابة على نظم الأعمال/المعلومات.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

المجلس الاستشاري للتغيير
Change-Advisory Board
هو المجلس الذي يقدم الدعم إلى فريق إدارة التغيير من خلال تقديم التغييرات اللازمة والمساعدة في تقييم التغييرات وتحديد أولوياتها.

الحوسبة السحابية
نموذج للتمكين من الوصول عند الطلب إلى مجموعة مشتركة من موارد تقنية المعلومات (مثل: الشبكات والخوادم والتخزين والتطبيقات والخدمات) التي يمكن توفيرها بسرعة وإطلاقها بالحد الدنى من الجهد الإداري التشغيلي. وتسمح الحوسبة السحابية للمستخدمين بالوصول إلى الخدمات القائمة على التقنية من خلال شبكة الحوسبة السحابية دون الحاجة إلى وجود معرفة لديهم أو تحكم في البنية التحتية التقنية التي تدعمهم.

استمرارية الأعمال
قدرة المؤسسة على مواصلة تقديم خدمات تقنية المعلومات وخدمات الأعمال بمستويات محددة ومقبولة مسبقًا بعد وقوع حادث تخريبي.

إدارة مخاطر المؤسسة
الأساليب والعمليات التي تستخدمها المؤسسة لإدارة المخاطر التي تتعرض لها مهمتها ولإرساء الثقة اللازمة للمؤسسة لدعم المهام المشتركة. وتنطوي على تحديد تبعيات المهام القائمة على قدرات المؤسسة، وتحديد المخاطر وترتيب أولوياتها بسبب التهديدات المحددة وتنفيذ التدابير المضادة لتوفير موقف ثابت للمخاطر واستجابة ديناميكية فعاله للتهديدات النشطة؛ وتقييم أداء المؤسسات ضد التهديدات وتعديل التدابير المضادة بحسب الاقتضاء.

المخاطر السيبرانية
المخاطر التي تمس عمليات أعمال المنظمة (بما في ذلك رسالة المنظمة أو مهمتها أو صورتها أو سمعتها) أو أصول المنظمة أو الأفراد أو المنظمات الأخرى أو الدولة، بسبب إمكانية الوصول غير المصرح به أو الاستخدام أو الإفصاح أو التعطيل أو التعديل أو إتلاف المعلومات و/أو نظم المعلومات.

مؤشرات الأداءِ الرئيسة
KPI
نوع من أدوات قياس مستوى الأداء يقيّم مدى نجاح نشاط ما أو جهة تجاه تحقيق أهداف محددة.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

الاحتمالية
Likelihood
أحد العوامل المرجّحة القائمة على تحليل احتمالية استغلال أحد التهديدات لثغرة أمنية معينة.

سجل المخاطر
Risk register
يتمثل سجل المخاطر في جدول يُستخدم مرجعاً لجميع المخاطر المحددة، ويتضمن معلومات إضافية حول كل خطر على حدة، على سبيل المثال: فئة المخاطر، والجهة المسؤولة عن إدارتها، وإجراءات الحد من آثارها.

الأمن السيبراني
Cybersecurity
يعرَّف الأمن السيبراني بأنه مجموعة من الأدوات والسياسات والمفاهيم الأمنية والضمانات الأمنية والمبادئ التوجيهية ونهج لإدارة المخاطر والإجراءات ودورات التدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية أصول معلومات مؤسسة السوق من التهديدات الداخلية والخارجية.

صمود الأمن السيبراني
Cybersecurity Resilience
القدرة الشاملة للجهة على الصمود أمام الأحداث السيبرانية، ومسببات الضرر، والتعافي منها.

ضوابط الأمن السيبراني
الضوابط الإدارية والتشغيلية والفنية (أي الضمانات أو التدابير المضادة) المنصوص عليها في نظام المعلومات لحماية سرية وسلامة وتوافر النظام ومعلوماته.

فعالية ضوابط الأمن السيبراني
قياس مدى صحة التنفيذ (أي مدى توافق تنفيذ الرقابة مع الخطة الأمنية) ومدى استيفاء الخطة الأمنية للاحتياجات التنظيمية وفقًا للقدرة على تحمل المخاطر الحالية.

برنامج التوعية بالأمن السيبراني
برنامج يشرح قواعد السلوك المناسبة للاستخدام الآمن لأنظمة تقنية المعلومات. ويحتوي البرنامج على سياسات وإجراءات الأمن السيبراني المطلوب اتباعها.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

حوكمة الأمن السيبراني

مجموعة من المسؤوليات والممارسات التي يقوم بها مجلس الإدارة والإدارة التنفيذية بهدف توفير التوجيه الاستراتيجي للأمن السيبراني، وضمان تحقيق أهدافه، والتأكد من إدارة المخاطر السيبرانية بشكل مناسب، والتحقق من استخدام موارد المؤسسة على نحو مسؤول.

سياسة الأمن السيبراني

مجموعه من المعايير الموضوعة لتوفير الخدمات الأمنية. وتحدد هذه المعايير الأنشطة الخاصة بمرافق معالجة البيانات التي يتم إجراؤها للحفاظ على الحالة الأمنية للنظم والبيانات.

التوثيق الرسمي

الوثائق المكتوبة الموافق عليها من القيادة العليا والمعمّمة على الأطراف المعنية.

حادثة

Incident

انتهاك أمني بمخالفة سياسات الأمن السيبراني أو سياسات الاستخدام المقبول أو ممارسات أو ضوابط أو متطلبات الأمن السيبراني.

خطة إدارة الحوادث

توثيق مجموعه من التعليمات أو الإجراءات المحددة مسبقًا للكشف عن الهجمات السيبرانية الخبيثة الموجهة ضد نظام (أنظمه) المعلومات في المنظمة والاستجابة لها والحد من عواقبها.

نظام إدارة سجلات الأحداث ومراقبة الأمن السيبراني

SIEM

نظام يقوم بإدارة وتحليل بيانات سجلات الأحداث الأمنية في الوقت الفعلي لتوفير مراقبة للتهديدات، وتحليل نتائج القواعد المترابطة لسجلات الأحداث، وإعداد التقارير حول بيانات السجلات، والاستجابة للحوادث.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

مركز العمليات الأمنية

SOC

يُعَدّ مركز العمليات الأمنية بمنزلة موقع متخصص (وفريق) يراقب البيانات المتعلقة بالأمن من أنظمة معلومات المؤسسة ويقيّمها (مثل مواقع الإنترنت والتطبيقات وقواعد البيانات والخوادم والشبكات وأجهزة الحاسوب المكتبية والأجهزة الأخرى)، وغالبًا ما يتم تخصيص مركز العمليات الأمنية لأعمال الكشف والتحقيق والاستجابة المحتملة لمؤشرات الانتهاكات الأمنية. ويعمل مركز العمليات الأمنية على نحو وثيق من خلال المعلومات المصنفة المرتبطة بالأمن ويقوم بنشرها في مناطق أخرى من المنظمة (مثل وظيفة الأمن السيبراني وفريق إدارة الحوادث وموفري خدمات تقنية المعلومات).

المعلومات الاستباقية

Threat intelligence

معلومات منظمة حول الهجمات الأخيرة والحالية والمحتملة التي يمكن أن تشكل تهديداً سيبرانياً للجهة.

تهديد

Threat

أي ظرف أو حدث متعلق بنظام المعلومات وله تأثير سلبي في أعمال مؤسسة السوق (بما في ذلك مهمتها أو وظائفها أو مكانتها أو سمعتها) أو أصولها التنظيمية أو أفرادها مستغلا النظم المعلوماتية عن طريق الوصول غير المصرح به إلى المعلومات أو تدميرها أو كشفها أو تعديلها و/أو الحرمان من الخدمة، وأيضاً، قدرة مصدر التهديد على النجاح في استغلال إحدى الثغرات الخاصة بنظام معلومات معين.

الأدلة الجنائية

جمع البيانات المتعلقة بالحاسوب والاحتفاظ بها وتحليلها لأغراض التحقيق بطريقه تحافظ على سلامة البيانات.

التشفير

هي القواعد التي تشتمل على مبادئ ووسائل وطرق تخزين ونقل البيانات أو المعلومات في شكل معين؛ وذلك من أجل إخفاء محتواها الدلالي، ومنع الاستخدام غير المصرح به أو منع التعديل غير المكتشف، بحيث لا يمكن لغير الأشخاص المعنيين قراءتها ومعالجتها.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

التهديدات المتقدمة المستمرة

APT

الحماية من التهديدات المتقدمة التي تستخدم أساليب خفية تهدف إلى الدخول غير المشروع إلى الأنظمة والشبكات التقنية ومحاولة البقاء فيها أطول فترة ممكنة عن طريق تفادي أنظمة الكشف والحماية. وهذه الأساليب تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Malware Day-Zero) لتحقيق هدفها.

نظام الحماية المتقدمة لاكتشاف الاختراقات

IDS

يتمثل نظام الحماية المتقدمة لاكتشاف الاختراقات (IDS) في الأجهزة أو البرمجيات التي تجمع المعلومات من مختلف المناطق داخل جهاز حاسوب أو الشبكة لتحديد وتحليل الخروقات الأمنية المحتملة التي تشمل كل محاولات التسلل (الهجمات من خارج المنظمات) وسوء الاستخدام (الهجمات من داخل المنظمات).

نظام الحماية المتقدمة لاكتشاف ومنع الاختراقات

IPS

هو نظام يمكنه اكتشاف الاختراقات (IPS) ومنعها واكتشاف أنشطة التسلل ومحاوله إيقافها بشكل مثالي قبل تحقيق أهدافها.

أحضر الجهاز الخاص بك

BYOD

يشير مصطلح "BYOD" إلى الأجهزة المملوكة شخصيًا (أجهزة الحاسوب المحمولة، والأجهزة اللوحية، والهواتف الذكية) التي يُسمح للموظفين والمتعهدين باستخدامها لتنفيذ وظائف العمل.

الدوائر التلفزيونية المغلقة

CCTV

تتمثل الدوائر التلفزيونية المغلقة في استخدام كاميرات الفيديو لنقل إشارة إلى مكان معين على مجموعة محدودة من الشاشات.

تطبيقات الأعمال

أي تطبيق يستخدمه العاملون لأداء وظائف الأعمال المختلفة في الجهة.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

مصفوفة الصلاحيات

مصفوفة تحدد الحقوق والأذونات التي يحتاج إليها دور معين من أجل الوصول إلى المعلومات. وتحدد المصفوفة كل مستخدم، والمهام والأعمال التي يقوم بها، والأنظمة المتأثرة.

تصنيف البيانات

تحديد مستوى حساسية البيانات أثناء إنشائها أو تعديلها أو تعزيزها أو تخزينها أو نقلها. وبعد ذلك، يحدد تصنيف البيانات مدى الحاجة إلى التحكم في البيانات أو تأمينها، ويشير أيضًا إلى قيمتها من حيث الأصول التجارية.

قائمة التطبيقات المصرحة

Application Whitelisting

قائمة للتطبيقات ومكونات التطبيق (المكتبات، ملفات التكوين، ...إلخ.) المصرح لها أن تكون موجودة أو نشيطة على الخادم وفق أساس محدد. وتهدف تقنيات قائمة التطبيقات المصرح لها إلى إيقاف تشغيل البرمجيات الضارة وغيرها من البرامج غير المصرح بها، على عكس التقنيات الأمنية، مثل برنامج مكافحة الفيروسات، الذي يستخدم قوائم سوداء لمنع النشاط السيئ المعروف والسماح بجميع التقنيات الأخرى. وقد تم تصميم تقنيات القائمة البيضاء للسماح بالنشاط المعروف وحظر جميع الأنشطة الأخرى.

كسر حماية نظام التشغيل

Jailbreaking

أحد أشكال زيادة الامتيازات على الجهاز، بحيث يزيل قيود البرامج التي تفرضها الشركة المصنّعة للبرمجيات، وغالبا ما يؤدي إلى امتيازات غير محدودة على الجهاز.

البرمجيات الضارة

Malware

برنامج يصيب الأنظمة بطريقة خفية في الغالب لانتهاك سريه أو سلامة أو توافر بيانات الجهاز المستهدف أو التطبيقات أو نظم التشغيل ذات الصلة أو إزعاج أو تعطيل الجهاز المستهدف.

إدارة الأجهزة المحمولة

MDM

إدارة الأجهزة المحمولة (MDM) أحد المصطلحات الخاصة بهذا القطاع فيما يتعلق بإدارة الأجهزة المحمولة.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

الأجهزة المحمولة

وسائط التخزين القابلة للنقل/ حزم الأقراص المحمولة (مثل الأقراص المرنة، والأقراص المضغوطة، ومحركات أقراص USB المحمولة، ومحركات الاقراص الثابتة الخارجية، وبطاقات الذاكرة المحمولة الأخرى أو محركات الاقراص التي تحتوي على ذاكرة).

أجهزة الحوسبة والاتصالات المحمولة المزودة بإمكانيه تخزين المعلومات (على سبيل المثال: الحاسوب المحمول، والمساعد الرقمي الشخصي، والهواتف الخلوية، والكاميرات الرقمية، وأجهزه التسجيل الصوتي).

التحقق من الهوية متعدد العناصر

MFA

أن يتم التحقق من هوية المستخدم باستخدام عاملين أو أكثر. وتشتمل عوامل التحقق من الهوية على "أولًا" شيء يعرفه المستخدم فقط (مثل كلمه المرور/رقم التعريف الشخصي)، "ثانيًا" حيازة أي شيء يملكه المستخدم (مثل جهاز تعريف التشفير أو رمز الأمان)، أو "ثالثًا" سمة حيوية متعلقة بالمستخدم نفسه (مثل المقاييس الحيوية "البيومترية").

الثغرات الأمنية

Vulnerability

أي نوع من نقاط الضعف في نظام الحاسب الآلي، أو برامجه أو تطبيقاته، أو في مجموعة من الإجراءات، أو في أي شيء يجعل الأمن السيبراني عرضة للتهديد.

إدارة الثغرات الأمنية

هي ممارسة دورية لتحديد الثغرات الأمنية، وتصنيفها، ومعالجتها.

حزم التحديثات والإصلاحات

Patch

تحديث أنظمة التشغيل أو التطبيقات أو أي برامج أخرى يتم تطويرها خصيصاً لتصحيح مشاكل معينة في البرنامج ويشمل الثغرات.

اختبار الاختراق

Penetration Test

اختبار نظام حاسب آلي أو شبكة أو تطبيق موقع إلكتروني أو تطبيق هواتف ذكية للبحث عن ثغرات يمكن أن يستغلها المهاجم.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

الأجهزة الشخصية

الأجهزة التي لا تملكها أو تصدرها المنظمة مثل الهواتف الذكية.

الأمن المادي

الحماية المادية للمرافق التي تستضيف أصول المعلومات من الأحداث الأمنية المقصودة وغير المقصودة.

رقم التعريف الشخصي

PIN

كلمة مرور تتكون من أرقام فقط.

التأثير في الأعمال

BIA

تحديد الأنشطة الهامة والأولويات الخاصة بالمؤسسة، إضافة إلى تحديد مدى الاعتمادية بين الأنشطة المختلفة، والحد الأدنى من الموارد اللازمة للتعافي، ومدى التأثير الذي يمكن ان يسببه تعطل الاعمال.

حسابات حساسة ومهمة

Privileged Accounts

حسابات أنظمة المعلومات التي تتمتع بتصاريح معتمدة لأداء وظائف متعلقة بالأمن غير مسموح للمستخدمين العاديين بالقيام بها.

المعلومات الحساسة

Sensitive Information

هي المعلومات التي يؤدي فقدانها، أو ما يتعلق بذلك من سوء الاستخدام أو الوصول غير المصرح به أو التعديل، إلى وجود تأثير سلبي في الشؤون التنظيمية أو خصوصية الأفراد. بالإضافة إلى ذلك، تتمثل المعلومات الحساسة أيضًا في المعلومات التي تُعَدّ حساسة وفقًا لسياسة تصنيف البيانات التنظيمية.

Sandboxing

بيئة تنفيذ مقيدة يتم التحكم فيها لمنع البرمجيات الضارة المحتملة من الوصول إلى أي موارد للنظام باستثناء الموارد المصرح لها.

الملحقات

المصطلحات والتعريفات

يوضح الجدول أدناه بعض المصطلحات وتعريفاتها الواردة في هذه الوثيقة

دورة حياة تطوير البرمجيات

SDLC

تصف دورة حياة تطوير البرمجيات نطاق الأنشطة المرتبطة بنظام ما، بما في ذلك بدء النظام وما يتعلق به من تطوير واقتناء وتنفيذ وتشغيل وصيانة إلى التخلص منه وهو الأمر الذي يحفز بدء نظام آخر.

المعايير الأمنية لشفرة البرامج والتطبيقات

Secure Coding Standards

ممارسة تطوير برمجيات وتطبيقات الحاسب الآلي بطريقة تحمي من التعرض غير المقصود لثغرات الأمن السيبراني المتعلقة بالبرمجيات والتطبيقات.

اتفاقية مستوى الخدمة

Service Level Agreement

هي اتفاقية تفاوض بين طرفين أحدهم يكون العميل والأخر هو مزود الخدمة، والتي توضح الخدمات التي يجب تقديمها من قبل مزود الخدمة والمعايير التي يجب استيفائها لتقديم الخدمة.

المعهد الوطني للمعايير والتقنية

NIST

المعهد الوطني الأمريكي للمعايير والتقنية (www.nist.gov)