UNITED ARAB EMIRATES
MINISTRY OF CABINET AFFAIRS
PRIME MINISTER'S OFFICE

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

إطار الاستجابة للحوادث السيبرانية

الإصدار 1.0

مايو 2023

تنبيه

اعتُمدت هذه الوثيقة ووافق مجلس الوزراء في دولة الإمارات العربية المتحدة عليها، وهي ملكية حصرية وخاصة للمجلس الأمن السيبراني.

ويحتفظ مجلس الأمن السيبراني بحقه في تعديل، أو إضافة، أو حذف أي بند أو قسم من هذه السياسة.

لا يُمكن استخدام هذه الوثيقة أو أي جزءٍ منها دون الحصول على الموافقة الخطية المسبقة من مجلس الأمن السيبراني.

ضوابط الإصدار

الإصدار	0.1
التاريخ:	11 مايو 2022
جهة الإعداد:	مجلس الأمن السيبراني
التعديل:	وثيقة المسودة الأولية

الإصدار	0.2
التاريخ:	...
جهة الإعداد:	...
التعديل:	...

الإصدار	0.3
التاريخ:	...
جهة الإعداد:	...
التعديل:	...

	جهة المراجعة	جهة الموافقة
المسمى الوظيفي:	xxxxxxxxx	xxxxxxxxx
الاسم:	xxxxxxxxx	xxxxxxxxx
التوقيع:	xxxxxxxxx	xxxxxxxxx
التاريخ:	xxxxxxxxx	xxxxxxxxx

جدول المحتويات

جدول المحتويات

1

القسم

المقدّمة

المقدّمة

يدعم الفضاء السيبراني أنشطة متنوعة في الدولة، بما يشمل الاقتصاد الوطني، والأمن الوطني، والصحة والسلامة العامة، والحياة الثقافية والاجتماعية. توفّر لنا تكنولوجيا المعلومات والاتصالات المتطوّرة المستخدمة في الفضاء السيبراني العديد من الفوائد، مما جعلها هدفاً رئيسياً للتهديدات السيبرانية القادرة على تعطيل أو إتلاف أو تدمير الوظائف والخدمات الحيوية التي تؤثر على أسلوب حياتنا. يُمكن وصف التهديدات السيبرانية على أنها تهديدات ديناميكية دائمة التغيّر، مما يجعل وقوع الحوادث أمراً لا يُمكن تجنبه. ومع ذلك، يُمكن أن تساعد القدرة الفعّالة على الاستجابة للحوادث في تقليل تأثيرها والحد من مدى وقوعها.

وُضع إطار الاستجابة للحوادث السيبرانية وتمت موائمته مع الاستراتيجية الوطنية للأمن السيبراني بهدف تعزيز استعداد دولة الإمارات العربية المتحدة وجاهزيتها لمواجهة التهديدات السيبرانية، وقدرتها على الحماية واكتشافها لهذه التهديدات والاستجابة والتعافي منها بفاعلية. وعليه، يتضمن إطار الاستجابة للحوادث السيبرانية المبادئ التوجيهية، ونموذج حوكمة الاستجابة للحوادث السيبرانية، ومخطط تصنيف الحوادث ومراحل الإدارة ومتطلبات الإبلاغ وتبادل المعلومات، بالإضافة إلى مكونات المراقبة وإدارة الأداء التي تشكّل معاً القدرات الوطنية لإدارة للحوادث السيبرانية. يعمل هذا الإطار جنباً إلى جنب مع خطة الاستجابة للحوادث السيبرانية التي تحدّد القدرات بصورة أكبر من خلال توفير التفاصيل التشغيلية.

وضع المجلس هذا الإطار لبناء القدرات الوطنية في إدارة الحوادث وتحديد مستوى استعداد دولة الإمارات واستجابتها لمواجهة لحوادث السيبرانية المهمة والحماية منها واكتشافها والاستجابة لها والتعافي منها والتعلّم منها باستمرار، ويتماشى هذا الإطار مع الأولويات الوطنية للدولة في أن تصبح رائدة عالمية في مجال الأمن السيبراني، كما سيساعد في تحسين الوضع الأمني للمؤسسات والأفراد داخل الدولة.

1.1 الهدف

يساهم إطار الاستجابة للحوادث السيبرانية في بناء القدرات التي تمكن دولة الإمارات العربية المتحدة ومؤسساتها الحكومية وقطاع البنى التحتية للمعلومات الحيوية من الاستجابة للحوادث السيبرانية المهمة بانتظام، الأمر الذي يساهم في الحد من أثرها وضمان استقرار الفضاء الإلكتروني للدولة والمساهمة في تعزيز الأمن ورفع مستوى الرفاهية والقدرة التنافسية العالمية له.

يعمل إطار الاستجابة للحوادث السيبرانية على ما يلي:

- إضفاء الطابع المؤسسي على القدرات الوطنية وفرضها وبناء مجتمع الاستجابة للحوادث السيبرانية لإدارة الحوادث السيبرانية الخطيرة، بما يشمل رفع استعداد الجهات للرد على الهجمات السيبرانية.
- توحيد مفهوم إدارة الاستجابة للحوادث السيبرانية بين الجهات ذات الصلة على المستوى الإتحادي في الدولة ورفع مستوى الوعي من خلال تنفيذ تمارين الرد على الهجمات السيبرانية بين الجهات بالتنسيق مع الجهات المعنية.
- دمج هذه القدرات في السياق المؤسسي للأمن الوطني للدولة وإدارة الأزمات الوطنية بالتنسيق مع الجهات المعنية.
- تحدد مستوى الوعي بالحالة السيبرانية وتعريف التنسيق اللازم للاستجابة بفاعلية للحوادث السيبرانية.
- رفع مستوى الوعي بقدرات وعمليات إدارة الحوادث السيبرانية الوطنية.
- تحديد عمليات الاستجابة للحوادث على مستوى الجهة ومستوى القطاع والمستوى الإتحادي.

1.2 النطاق ومدى قابلية التطبيق

يسري كل من إطار الاستجابة للحوادث السيبرانية وخطة الاستجابة للحوادث السيبرانية على جميع جهات القطاعين العام والخاص بموجب سياسة حماية البنى التحتية للمعلومات الحيوية داخل حدود الدولة، حيث يأتي هذا النطاق الشامل ومدى قابلية التطبيق الواسعة له من الطبيعة الحتمية للحوادث السيبرانية الحرجة التي قد تعمل على إرهاق قدرات إدارة الحوادث على مستوى الجهة وتمتد عادة لتؤثر على جهات وقطاعات وسلطات متعددة.

1.3 دور الإطار والخطة

يعمل إطار الاستجابة للحوادث السيبرانية على تحديد الإطار المؤسسي والعمليات الرئيسية التي تشكل معاً القدرة الوطنية على الاستجابة للحوادث السيبرانية في الدولة. والذي يمكن من ثبات الوضع المؤسسي نسبياً وذلك للمساهمة في توفير الاستقرار بين الجهات المعنية الرئيسية من أداء أدوارها بفاعلية كونها جزءاً من القدرة الوطنية على الاستجابة للحوادث السيبرانية.

تعمل خطة الاستجابة للحوادث السيبرانية على إضافة سياق تشغيلي وتوفير تفسير واضح للإطار العام، كما تؤدي دوراً حيوياً في توفير المرونة اللازمة لتعزيز القدرات على الاستجابة للحوادث السيبرانية في الدولة. ووفقاً لذلك، يجب مراجعة خطة الاستجابة للحوادث السيبرانية والصادرة من مجلس الأمن السيبراني وتعديلها على وتيرة (سنتين إلى ثلاث سنوات)، للتأكد من أنها تعكس التغييرات المهمة في التكنولوجيا العالمية وبيئات التهديد.

إذ يجب مراجعة إطار الاستجابة للحوادث السيبرانية وخطة الاستجابة للحوادث السيبرانية بانتظام للتأكد من أنها لا تزال ذات صلة وتعكس الواقع العالمي والإماراتي. لذا يجب جمع المُدخلات التي تشاركها الجهات المعنية خلال هذه المراجعات لتحسين القدرات إلى حدٍ أكبر، وتبادل الخبرات وضمان مشاركة الجهات الرئيسية.

1.4 المبادئ التوجيهية

يستند إطار الاستجابة للحوادث السيبرانية إلى مبادئ توجيهية معترف بها دولياً -أي مناهج حوكمة محدّدة- تصف السياق الواسع الذي تحدث فيه الاستجابة للحوادث السيبرانية المهمة.

حُدّدت هذه المبادئ بهدف إعداد نهج مشترك بين الجهات المعنية داخل مجتمع الاستجابة للحوادث السيبرانية في دولة الإمارات العربية المتحدة.

تمكين الوعي بالحالة السيبرانية من خلال تبادل المعلومات

- تُمكّن عملية تحقيق الوعي بالحالة السيبرانية على مستوى الجهة من خلال المراقبة المستمرة لأصول المعلومات ومتابعة التهديدات والثغرات الأمنية والحوادث السيبرانية الحالية. أما على مستوى القطاع والمستوى الإتحادي، فيُمكن إيجاد الوعي بالحالة السيبرانية من خلال إيجاد عملية تبادل منظّمة للمعلومات بهدف دعم إيجاد فهم شبه فوري ومعرفة ببيئة الفضاء السيبراني في الدولة، مما يمكّن الجهات المعنية من التحذير من الحوادث الوشيكة أو الجارية والبدء في إجراء أنشطة الاستجابة لها.
- وبالتالي، فإن تبادل المعلومات يُعد أمراً ضرورياً لإيجاد الوعي بالحالة السيبرانية، ولتمكين تبادل البيانات والمعرفة بشأن التهديدات والثغرات الأمنية والمخاطر واستراتيجيات التخفيف وأفضل الممارسات. تشكّل جميع هذه المعلومات حجر الأساس الذي تُبنى عليه إدارة الحوادث السيبرانية على المستوى الوطني، بما يشمل الاستجابة للحوادث في حال وقوع حادث سيبراني مهم.

النهج المبني على المخاطر

- يهدف النهج المبني على المخاطر -كمبدأ إرشادي- إلى ربط مستويات المخاطر (أو مستويات شدة الحادث) بالاستجابات المناسبة، بما يشمل الموارد المُفعلة، كونها طريقة قياسية لإيجاد علاقة متوازنة ومحسوبة بين شدة الحادث والموارد الوطنية. يفعّل النهج القائم على المخاطر من خلال القياس التدريجي للحوادث السيبرانية وفق مخطط شدة الحوادث، على أن يتمثّل الهدف الرئيسي في تخصيص الموارد الكافية حسب مستوى الحادث للتأكد من حله (حشد مستويات الموارد المطلوبة) وتخصيص الموارد بفعالية (حشد الموارد الضرورية فقط).

1.4 المبادئ التوجيهية

المسؤولية المشتركة ("توحيد الجهود")

- يجب أن تعمل الجهات المعنية على مستوى الجهة ومستوى القطاع والمستوى الوطني معاً على أساس "توحيد الجهود"، وذلك لضمان فاعليتهم في الحفاظ على استقرار الفضاء السيبراني لدولة وقدرتهم على الاستجابة للحوادث السيبرانية المهمة. تتحمل الجهات (بما يشمل الجهات المشغّلة للبنى التحتية الحيوية) والقطاعات (بما يشمل الجهات المنظّمة للقطاعات) والجهات المعنية على المستوى الوطني (الوزارات والجهات الحكومية والاتحادية) على نحوٍ جماعي مسؤولية التعاون ضمن إطار يقوده مجلس الأمن السيبراني، وهو الجهة المفوضة على المستوى الوطني والمكلفة بتنسيق إدارة الحوادث السيبرانية في الدولة. ومن المهم أن يكون التعاون متعدد الاتجاهات لتمكين المشاركة الفعّالة للمعلومات والاستجابة السريعة أثناء حالات الأزمات.
- بالإضافة إلى ذلك، يؤكد اتباع نهج حكومي شامل على أهمية التعاون بين مختلف المستويات والجهات الحكومية، خاصة على المستوى الوطني والاتحادي ومستوى الإمارة، بما يُمكّن من الاستجابة للحوادث بفاعلية. يُعد هذا المبدأ مهماً جداً، وذلك لأن الحكومات الحديثة تتكون من طبقات متعددة وتعمل ضمن إطار مبني على مجموعة كبيرة من المسؤوليات والأدوار والأولويات. لذا، يُمكن أن تتسبب العقبات البيروقراطية، وسلاسل القيادة غير الواضحة، وغياب مسؤولية واضحة في أضرار جسيمة في حال وقوع حادث بمستوى حاد، كما يُمكن استغلال هذا المبدأ لمنع وجود الفجوات، ولتجنب ازدواجية الجهود أثناء الاستجابة لحادث معقد.

احترام الجهات المتضررة

- يعمل هذا المبدأ على طمأنة أعضاء المنظومة السيبرانية للدولة، وغيرهم من الجهات المعنية الرئيسية والشركاء من المجتمع بأن مصالحهم ستؤخذ بعين الاعتبار أثناء الاستجابة للحوادث إلى الحد الذي يسمح به القانون. إذ تهدف هذه المبادئ أو الالتزامات إلى تعزيز التعاون بين الجهات الحكومية والقطاع الخاص.
- يُكمِّل نهج "تمكين الاستعادة والتعافي" ما ورد أعلاه، حيث يتمحور هذا النهج حول الحاجة إلى تنفيذ أنشطة استجابة للحوادث تعطي الأولوية لاستعادة الجهة المتأثرة وتعافيها وموازنة الأولويات الحكومية والحاجة إلى العودة إلى العمليات الاعتيادية في أسرع وقت ممكن.

2

القسم

النموذج الوطني لحوكمة الاستجابة للحوادث السيرانية

تعتمد قدرات دولة الإمارات العربية المتحدة على الاستجابة بنجاح للحوادث السيبرانية المهمة على التنسيق المركزي والتنفيذ اللامركزي باتباع نهج شامل على مستوى الوطني. كجزء من جهود بناء هذه القدرات التنسيقية، وأُسّست جهتان تنظيميتان على المستويين الوطني والاتحادي، وهي: المركز الوطني للعمليات الأمنية (السيبرانية)، والمجموعة الاستراتيجية الوطنية للاستجابة السيبرانية، وذلك بالتنسيق مع مجلس الأمن السيبراني بصفته الجهة الوطنية المسؤولة عن إدارة الحوادث السيبرانية. وتتمثّل الوظيفة الاستراتيجية لهذه المؤسسات في تمكين التنسيق اللازم لإدارة الحوادث السيبرانية.

2.1 النموذج

يوجد مصالح مشتركة بين الجهات والهيئات المذكورة أعلاه في ضمان الاستجابة الوطنية للحوادث السيبرانية بفاعلية. ووفقاً لذلك، يجب أن تتعاون الجهات المعنية فيما بينها لتحقيق هذا الهدف المشترك، وذلك لإيجاد حلول جماعية للاستجابة للحوادث والمشكلات المعقدة المتعلقة بالأمن السيبراني. ويجب على الجهات المعنية الفردية الالتزام بالأدوار والمسؤوليات المحدّدة في الإطار الوطني لحوكمة الأمن السيبراني، وذلك للتخفيف على نحوٍ جماعي من آثار الحوادث السيبرانية المهمة على الأمن الوطني والحفاظ على استقرار منظومتها السيبرانية.

يتوجب على نموذج إدارة الحوادث السيبرانية والجهات المعنية فيه تحقيق ما يلي:

- خلق مستوى الوعي بحالة الفضاء السيبراني الوطني والحفاظ عليه بهدف تحديد الحوادث وتحليلها على نحوٍ استباقي.
- اتخاذ القرارات في الوقت المناسب للتخفيف من آثار الحوادث السيبرانية المهمة واستعادة استقرار العمليات بسرعة.
- تعزيز التعاون وضمان الجاهزية في الوقت المحدد وتسهيل تبادل المعلومات والتعلّم والتحسين المستمر.

2.1 النموذج

يوضّح القسم التالي الجهات والهيئات ومسؤولياتهم:

2.1.1 مجلس الأمن السيبراني

- يمثّل مجلس الأمن السيبراني الجهة المسؤولة للدفاع عن الفضاء السيبراني للدولة وتأمينه، حيث تشمل مسؤولياته تنسيق الاستجابة للحوادث السيبرانية المهمة. ويعمل المجلس على المستوى التكتيكي من خلال المركز الوطني للعمليات الأمنية الذي يوفّر وعياً بالحالة السيبرانية ويدعم المجتمع الوطني للاستجابة للحوادث السيبرانية بالقدرات اللازمة، كما ينفذ مهامه على الصعيد الاستراتيجي من خلال العمل كجهة منسّقة بين المجموعة الوطنية للاستجابة السيبرانية والمجلس الوطني للاستجابة للحوادث كما هو مطلوب.
- تحت إشراف مجلس الأمن السيبراني، يُعد المركز الوطني للعمليات الأمنية الجهة الأساسية المسؤولة عن الاستجابة التكتيكية للحوادث في الدولة، وعليه، تم تكليفه بالمسؤوليات التالية:

2.1.1.1 الإشراف على أنشطة الاستجابة في "حالة الاستقرار" واتخاذ القرارات المتعلقة بتصعيد مستويات الحوادث من "المستوى الرابع " إلى "المستوى الثالث"، كما يقدّم النصح والمشورة إلى رئيس مجلس الأمن السيبراني بتصعيد الحادث إلى " والمجموعة الاستراتيجية الوطنية للاستجابة السيبرانية ".

2.1.1.2 إدارة الاستجابة التكتيكية للحوادث عند مستويات التنبيه "المرتفعة" و"الحادة" و"الكارثية".

2.1.1.3 خلق صورة تشغيلية مشتركة والحفاظ عليها بصفته نقطة تكامل جميع المعلومات السيبرانية الوطنية (البيئة الاتحادية) المقدّمة من الحكومة والجهات المشغّلة للبنى التحتية الحيوية والجهات المعنية الأخرى، فيما يتعلق بالتهديدات والثغرات والحوادث وأنشطة التخفيف أو الاستجابة، كما يعمل على توفير المعلومات اللازمة عن الحوادث السيبرانية وأنشطة الاستجابة للقيادة الوطنية والجهات المعنية.

2.1.1.4 تقديم الاستشارات والمعلومات الفنية والتشغيلية للمجموعة الوطنية للاستجابة السيبرانية لمزامنة العمليات والسياسات والإجراءات المتخذة للاستجابة للحوادث السيبرانية.

2.1 النموذج

2.1.2 المجموعة الوطنية للاستجابة السيبرانية

- المجموعة الوطنية للاستجابة السيبرانية هي هيئة استراتيجية معنية بمهام التنسيق واتخاذ القرارات، حيث يشكّلها مجلس الأمن السيبراني ويتولى أيضاً رئاستها. وتشُكّل المجموعة الوطنية للاستجابة السيبرانية بناءً على المشورة المقدّمة من المركز الوطني للعمليات الأمنية وقرار رئيس مجلس الأمن السيبراني.
- وتتألف المجموعة من أعضاء من الجهات المعنية إلى جانب مراكز العمليات الأمنية والجهات المشغّلة للبنى التحتية للمعلومات الحيوية في القطاعات ذات الصلة.

2.1 النموذج

2.1.3 مراكز العمليات الأمنية في القطاع والجهات المشغّلة للبنى التحتية للمعلومات الحيوية

تُعد مراكز العمليات الأمنية في القطاع (المستوى الوطني) والجهات المشغّلة للبنى التحتية للمعلومات الحيوية (بما يشمل جهات القطاع الخاص ذات الصلة) مكونات أساسية للمنظومة السيبرانية لدولة الإمارات العربية المتحدة، كما أنها أهداف محتملة للهجمات السيبرانية، حيث تؤدي هذه الجهات المعنية دوراً مهماً في جهود الاستجابة السيبرانية الوطنية. ووفقاً لذلك، تُعد هذه الجهات:

2.1.3.1 مسؤولة عن الإدارة وبالتالي المالكين الوحيدين للحوادث منخفضة المستوى ("المستوى الرابع")، كما أنها مسؤولة عن اتباع أفضل الممارسات القياسية في المجال، بما يشمل توفير القدرات الداخلية الكافية واللازمة لإدارة الحوادث.

2.1.3.2 مسؤولة عن الإيفاء بمتطلبات الإبلاغ الإلزامية والطوعية عن الحوادث، والمساهمة في الصورة التشغيلية المشتركة التي يبنيها المركز الوطني للعمليات الأمنية.

2.1.3.3 مسؤولة عن وضع خطط الاستجابة السيبرانية الخاصة بقطاعات البنية التحتية للمعلومات الحيوية وتنفيذها.

2.2 التكامل مع إدارة الأزمات الوطنية لدولة الإمارات العربية المتحدة

يُمكن أن تؤدي الحوادث السيبرانية إلى تبعات مادية محتملة أو فعلية، لذا يحرص المجلس على تبادل المعلومات المتعلقة بالحوادث المهمة مع الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث والسلطات الأخرى ذات الصلة، كما أنه يوفّر الدعم للهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث في تنفيذ مسؤولياتها المتمثّلة في إدارة الطوارئ المادية حسب الحاجة. وبالمثل، يُمكن أن تتسبب حالات الطوارئ المادية والكوارث بتبعات وخيمة ذات صلة بالأمن السيبراني، لذا ستقدّم الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث الدعم للمجلس في تنفيذ مسؤولياته المتمثّلة في إدارة الحوادث السيبرانية. كما يجب أن يتعاون كلٌ من المجلس والهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث خلال "الحالات المستقرة" لتنسيق جهود التخطيط.

3

القسم

مخطط التنبيه بالحوادث السيبرانية

يعمل المخطط الوطني للتنبيه بالحوادث السيبرانية كمنبّه وآلية تحذير على المستوى الوطني. وتنقل هذه الآلية المعلومات الحالية عن الحوادث السيبرانية ومستوى أثرها إلى قطاعات البنية التحتية للمعلومات الحيوية، والجهات والمؤسسات الحكومية للدولة.

وتكمن الغاية من المخطط في نقل المعلومات بصورة مكثّفة للجهات المعنية عبر أربعة مستويات تنبيهية (المستوى الرابع، والمستوى الثالث، والمستوى الثاني، و المستوى الأول). ويأخذ مستوى التنبيه بعين الاعتبار النشاط السيبراني الفعلي وإمكانية تطوّره وأثره على قطاعات بنية المعلومات الحيوية وفعاليته أمام قدرات الاستجابة. وبصفة عامة جميع المراحل التنبيهية مصمّمة للمساهمة في تعزيز الوعي بالحالة السيبرانية بشكل عام من خلال تقديم مؤشرات إلى حالة الحادث السيبراني وأثره على الدولة.

1. المقدّمة | 2. النموذج الوطني لحوكمة الاستجابة للحوادث | 3. مخطط التنبيه بالحوادث السيبرانية | 4. مراحل إدارة الحوادث السيبرانية
متطلبات الإبلاغ وتبادل المعلومات (البيئة الاتحادية) | 6. أنشطة المراقبة وإدارة الأداء | 7. التنفيذ | 8. الملاحق

الجدول 1: مستوى التنبيه للحوادث السيبرانية على الصعيد الوطني

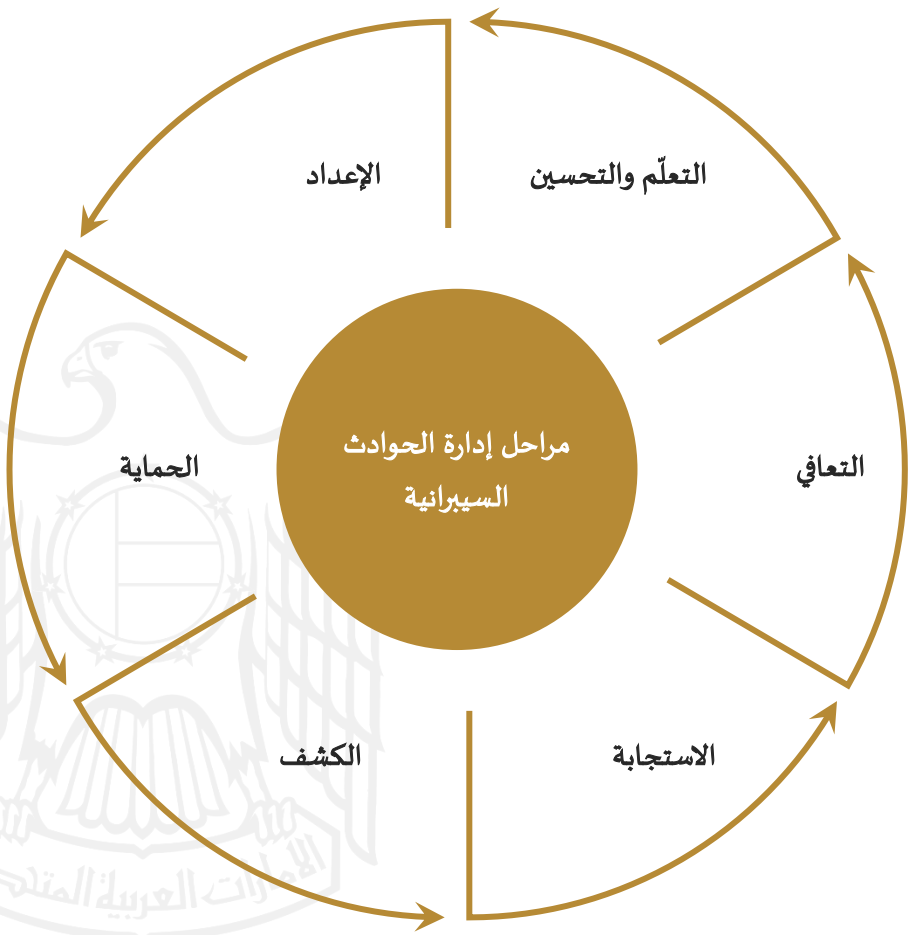
	مستوى التنبيه	النشاط	الأثر المترتب
حادث سيبراني خطير	المستوى الأول أعلى مستوى أثر	• يوجد تهديد أو نشاط سيبراني خبيث من شأنه تعطيل أو تدمير أو خفض قدرات البنية التحتية للمعلومات الحيوية و/ أو الأنظمة الحكومية. • وقع الحادث أو وقوعه وشيكاً أو لا يزال مستمراً.	• تدمير كلي أو شبه كلي محتمل أو ملحوظ أو خفض قدرات أو اختراق للبنية التحتية للمعلومات الحيوية عبر قطاع واحد أو أكثر. • تدمير أو خفض حقيقي وواسع النطاق للقدرات، وقد يكون محتمل أو ملحوظ، مما يهدد استمرار عمل الحكومة أو قطاع البنية التحتية للمعلومات الحيوية. • قد يتم تعليق العمليات والوظائف العادية إلى أجل غير مسمى. • سيتم إدارة الأثر المحتمل من قبل الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث.
	المستوى الثاني أثر عالي المستوى	• وجود تهديد أو زيادة فعلية في الأنشطة السيبرانية الخبيثة الموجهة ضد الخدمات الحيوية الوطنية. • وجود تدخل أو استغلال معروف أو متوقع للبنية التحتية للمعلومات الحيوية التي توفّر خدمة وطنية مهمة.	• احتمالية حدوث أو حدوث خفض كبير للقدرات أو تعطل أو إتلاف أو تضرر أو جميعها للبنية التحتية للمعلومات الحيوية عبر قطاع واحد أو أكثر. • سيتم إدارة الأثر المحتمل من قبل الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث.
	المستوى الثالث أثر متوسط	• وجود مستوى مرتفع من التهديدات أو الأنشطة السيبرانية الخبيثة. • وجود تدخل معروف أو متوقع أو هجوم مركّز.	• اختراق محتمل أو فعلي أو خفض من قدرات الخدمات في واحد أو أكثر من قطاعات البنية التحتية للمعلومات الحيوية. • احتمالية وقوع انخفاض في القدرات أو حدوث التعطل أو الضرر أو احتمالية وقوع أي مما سبق. • سيتم إدارة الأثر المحتمل من قبل المركز الوطني للعمليات الأمنية والمجموعة الوطنية للاستجابة السيبرانيةإذا تطلبت الحاجة.
حالة الاستقرار	المستوى الرابع أثر منخفض	تمثّل تهديدات النشاط السيبراني الخبيث مصدراً للقلق عام فقط.	• لا تتأثر قطاعات البنية التحتية للمعلومات الحيوية أو الأنظمة الحكومية بأي شكل من الأشكال. • تستطيع الجهة المالكة أو الجهة المشغّلة المسؤولة التعامل مع الأثر المحتمل.

4

القسم

مراحل إدارة الحوادث السيبرانية

يهدف القسم التالي إلى توجيه الأنشطة ومساعدة الجهات المعنية بالبنى التحتية للمعلومات الحيوية، والجهات المنظّمة للقطاعات، ومراكز العمليات الأمنية، والشركاء الوطنيين في إيجاد فهم مشترك للأنشطة الواجب تنفيذها كجزء من مراحل إدارة الحوادث السيبرانية. يجب على كل مؤسسة النظر في أنشطتها في سياق بيئتها التشغيلية المحدّدة، وبنية تكنولوجيا المعلومات والاتصالات والوضع العام للمخاطر وبناء قدرات استجابة للحوادث مصممة وفقاً لما سبق بما يتماشى مع إطار المعايير الأساسية لمركز العمليات الأمنية. سيعمل مجلس الأمن السيبراني مع الجهات المنظّمة للقطاعات ومراكز العمليات الأمنية لضمان توافق خطط إدارة الحوادث السيبرانية على مستوى القطاع والمستوى الإتحادي. تهدف مراحل إدارة الحوادث السيبرانية الموضّحة أدناه إلى تحديد نهج مشترك وبناء توافق عام في قدرات الجهات المعنية المتعلقة بالاستجابة للحوادث داخل المنظومة السيبرانية لدولة الإمارات العربية المتحدة.



4.1 الإعداد

تتضمن مرحلة التحضير كل من القدرات والأنشطة (أي الأشخاص والعمليات والتكنولوجيا) التي تمكن الجهات المعنية من الاستجابة لحادث سيبراني، فتشمل نشاطات التحضير بناء الوعي بالحالة السيبرانية والحفاظ عليه، حيث يعد ذلك من المسؤوليات المشتركة بين الجهات المعنية على مستوى الجهة والقطاع والمستوى الوطني. كما يجب تدريب مجتمع الاستجابة للحوادث السيبرانية مسبقاً وبانتظام على إدارة الحوادث السيبرانية بفاعلية، وذلك لضمان التحديد المسبق لمعظم الحوادث المحتملة والتدرب على معالجتها قبل وقوعها، حيث يمكّن ذلك تنفيذ إجراءات استجابة منسقة في حال وقوع حادث سيبراني خطير. ويعد إجراء تمارين الاستجابة للحوادث المختلفة طريقة جيدة أخرى لتحضير الجهات للتعامل مع حادث حقيقي.

4.2 الحماية

من السهل التعامل مع الحوادث التي لا تحدث أبداً، لذلك فإن حماية البنية التحتية للمعلومات الحيوية من الحوادث مهم جداً في بناء قدرات فعّالة في إدارة الحوادث. وتتضمن مرحلة الحماية تدابير واستراتيجيات وقائية، بالإضافة إلى تحليلات تهدف إلى التنبؤ بوقت وقوع الحادث، وتشمل أيضاً عملية تصميم وتنفيذ الإجراءات اللازمة لحماية الأنظمة من حادث محتمل.

4.3 الكشف

تتضمن مرحلة الكشف تحديد وقوع حدث مثير للاهتمام، والتحقّق فيما إن كان هذا الحدث يُمكن تصنيفه على أنه حادث، وتحليل مستوى الاختراق وتصعيد الحادث (إذا لزم الأمر). في هذه المرحلة، تؤدي الجهات المعنية بالبنية التحتية للمعلومات الحيوية دوراً مهماً على نحوٍ خاص لأنها عادة تكون أول من يكتشف الحوادث المهمة على شبكاتها الخاصة، أو لديها معلومات استخباراتية أو معلومات موثوقة تتعلق بنشاط أو حادث محتمل أو تكون على علم بالثغرات الموجودة. كما تؤدي مراكز العمليات الأمنية التابعة للقطاع دوراً مهماً. خلال هذه المرحلة، يُمكن أن تتخذ الجهات المعنية المتأثرة أيضاً خطوات لتنظيم استجابة أولية.

4.4 الاستجابة

خلال مرحلة الاستجابة، يجري التحقيق بهدف جمع وتحليل الأدلة المرتبطة بالحادث وتحديد مستوى الاختراق والسبب الجذري له وأثره والحصول على أي معلومات أخرى لازمة لتسهيل إجراءات الاستجابة. تُنفّذ إجراءات التخفيف لاحتواء الحادث، وذلك لتقليل الأثر أو التخلص منه أو الحد من الضرر الناجم عن الحادث. كما تجدر الإشارة إلى أن معظم الحوادث السيبرانية هي انتهاكات للقوانين المتعلقة بالجرائم السيبرانية في الدولة، ويُمكن أن تساعد عملية جمع الأدلة الرقمية والتعامل معها على النحو الصحيح في دعم تطبيق القانون والملاحقة القضائية اللاحقة.

4.5 التعافي

تبدأ مرحلة الاستعادة والتعافي فور اكتشاف الحادث وقد تُنفّذ بشكل موازٍ لجهود الاستجابة، فهي تهدف إلى إصلاح الخدمات والعمليات واستعادتها. تشمل هذه المرحلة التواصل مع الجهات المعنية الأخرى فيما يتعلق بإجراءات الاستعادة والتعافي وحالة الخدمات المهمة. وخلال مرحلة الاستعادة والتعافي، تنتقل عمليات الجهات والقطاعات والعمليات الوطنية من حالة الحادث السيبراني الخطير إلى الحالة المستقرة.

4.6 التعلّم والتحسين

يحدث التطوير المستمر طوال مراحل إدارة الحوادث السيبرانية ويركّز على تنفيذ العمليات والأنشطة الفعّالة. وبعد وقوع حادث، يجب على الجهات المعنية العمل على تقليل احتمالية وقوع هجمات في المستقبل من خلال التحقيق الجنائي، وزيادة حماية البنية التحتية ورفع مستوى الوعي بالمخاطر وتدابير التخفيف المحتملة. يُمكن الحفاظ على فاعلية القدرات الوطنية لإدارة الحوادث السيبرانية وتعزيز مستوى جاهزيتها بمرور الوقت، وذلك من خلال تطبيق الدروس المستفادة على مستوى الجهة ومستوى القطاع والمستوى الوطني.

5

القسم

متطلبات الإبلاغ وتبادل المعلومات (البيئة الاتحادية)

يشكّل الإبلاغ وتبادل المعلومات (البيئة الاتحادية) عنصران مهمان في الإطار الوطني للاستجابة للحوادث السيبرانية. ويُمكن أن تتضمن عملية الإبلاغ عناصر طوعية وإلزامية، بينما تُنفّذ عملية تبادل المعلومات يدوياً أو من شخص لآخر أو آلياً (باستخدام الصيغ التي يُمكن قراءتها آلياً). تؤدي جميع الجهات المعنية الرئيسية دوراً مهماً في نظام إدارة الحوادث من حيث الحفاظ على صورة تشغيلية مشتركة ومحدّثة أثناء وقوع حادث سيبراني مهم. لذا يجب إنشاء قنوات محدّدة جيداً وتحديد عمليات الإبلاغ وتبادل المعلومات على نحوٍ مسبق، وذلك لضمان تعزيز القدرة على التعاون التي تركّز على حل أزمات البيئات التكنولوجية شديدة التعقيد. ومن المهم جداً أن تدرك جميع الجهات المعنية مسؤولياتها بوضوح.

لذلك، يجب إنشاء شبكة تتكون من نقاط اتصال معنية والحفاظ عليها بإشراف من مجلس الأمن السيبراني، حيث ستركّز هذه الشبكة على الإبلاغ عن الحوادث السيبرانية وتبادل المعلومات (بما يشمل المعلومات الفنية) من خلال اتباع عملية ومتطلبات محدّدة بوضوح. يتألف أعضاء هذه الشبكة من ممثلي المركز الوطني للعمليات الأمنية، وفريق الاستجابة لطوارئ الحاسب الآلي، ومراكز العمليات الأمنية في القطاع والجهات المشغّلة للبنى التحتية للمعلومات الحيوية. كما تُنشأ شبكة إضافية بقيادة مجلس الأمن السيبراني بحيث تربط ما بين مجتمع إدارة الحوادث السيبرانية الأوسع (الجهات المعنية).

5.1 الإبلاغ الفني (البيئة الاتحادية)

يُبلّغ عن البيانات الفنية المتعلقة بالحوادث السيبرانية وتُشارك من خلال اتحاد مراكز العمليات الأمنية على النحو المحدّد في إطار المعايير الأساسية لمركز العمليات الأمنية. تتبع قنوات الإبلاغ نموذجاً هرمياً تُجمع فيه المعلومات ذات الصلة (بما يشمل معلومات التهديد، وإدارة الثغرات، ومؤشرات الحوادث، وغيرها) من الجهات المعنية بالبنية التحتية للمعلومات الحيوية ونقلها إلى مراكز العمليات الأمنية الخاصة بالقطاع، ومن هذه المراكز إلى المركز الوطني للعمليات الأمنية. حُدّدت الأدوار والمسؤوليات ومتطلبات الإبلاغ (بما يشمل الجداول الزمنية للإبلاغ) ضمن إطار المعايير الأساسية لمركز العمليات الأمنية (يُرجى الاطلاع على الملحق). ويتولى مجلس الأمن السيبراني مسؤولية إدارة قنوات الإبلاغ والحفاظ عليها كونه الجهة الوطنية الرئيسية في هذا المجال. ويعمل المجلس أيضاً على إعداد وتنفيذ إطار تبادل المعلومات ذات الصلة لتمكين الأطراف من تحقيق متطلباتهم الخاصة.

يجب بناء إطار إرشادي لتفعيل دور الجهات بهدف تحديد الخطوات (مثل: متطلبات الإبلاغ) والقيود والتبعيات للجهات الفاعلة الرئيسية أثناء الاستجابة للحوادث (مفصّل في الملحق).

5.2 إدارة الأزمات التشغيلية

يجب إنشاء شبكة تتكون من نقاط اتصال محدّدة لأغراض إدارة الأزمات التشغيلية، بحيث تُستخدم خلال الحوادث السيبرانية المهمة التي تتطلب التعاون المتبادل بين الجهات المعنية الرئيسية لتمكين الاستجابة للأزمات بفاعلية؛ سواءً من مجتمع الأمن السيبراني أو على نطاق أوسع يشمل الجهات المعنية في مجالات الأمن والسياسة في الدولة. حيث تهدف هذه الشبكة إلى تمكين الاستجابة من خلال توفير حلقة وصل بين الوزارات ذات الصلة وجهات إنفاذ القانون وجهات إدارة الكوارث، وغيرها من الجهات ذات الصلة، بالإضافة إلى الجهات المعنية بالبنية التحتية للمعلومات الحيوية المتضررة على الصعيد الوطني. ويتولى مجلس الأمن السيبراني مسؤولية إدارة قنوات الإبلاغ والحفاظ عليها كونه الجهة الوطنية الرئيسية في هذا المجال حيث يحتوي الملحق على المزيد من التفاصيل حول شبكة نقاط الاتصال.

5.3 تبادل المعلومات على الصعيد الدولي

عند الاستجابة للحوادث السيبرانية الخطيرة، يتعيّن على مجلس الأمن السيبراني إنشاء سياسات وإجراءات داعمة تحدّد المبادئ التوجيهية للتعامل مع الشركاء الدوليين في إدارة الحوادث السيبرانية وتوزيع معلومات الحوادث السيبرانية، بما يشمل نوع البيانات وآلية تبادل المعلومات، بحيث يتماشى إطار السياسة مع الإطار العام لتبادل المعلومات الخاص بمجلس الأمن السيبراني. وتهدف هذه السياسات إلى التحكّم في إقامة الشراكات الدولية (بما يشمل تبادل المعلومات) من مراكز العمليات الأمنية في القطاع، والجهات المشغّلة للبنى التحتية للمعلومات الحيوية، بحيث تنص على الموافقات اللازمة لإقامة هذا التعاون (من المركز الوطني للعمليات الأمنية أو مجلس الأمن السيبراني أو وزارة الخارجية والتعاون الدولي)، وأي شروط، بما يشمل تقليل البيانات وأي إرشادات بشأن العوائق القانونية أو التصنيفية المحتملة، وغيرها من القضايا المهمة. على المستوى التشغيلي، يجب أن تحدّد السياسات بوضوح متطلبات التوثيق (الأدوار الرئيسية، وجهة الاتصال، والنطاق، ومشاركة البيانات، وغيرها) بالإضافة إلى نظام نقاط التواصل ذي الصلة.

القسم 6

أنشطة المراقبة وإدارة الأداء

تُعد عملية مراقبة النظام لإدارة الحوادث السيبرانية على المستوى الوطني بالغة الأهمية، مع أنها معقدة للغاية، فيجب تطوير وتعزيز عنصر المراقبة كجزء من قدرات إدارة الحوادث في الدولة كونه ضرورياً لبناء إطار وخطة استجابة سيبرانية وطنية قابلة للقياس. وتُعد القدرة على قياس الاستجابة للحوادث ضرورية لبناء المعرفة فهي تعمل كأساس للتحسين والتطوير المستمر. يجب أن تشتمل وظيفة المراقبة على مكونات متعددة، بما يشمل توفير المعرفة بالأصول والمقاييس الرئيسية للحوادث التي تغطي كامل دورة الحادث السيبراني. يقوم مجلس الأمن السيبراني بالتحكّم بقدرة المراقبة، كما يجب تحديد تفاصيلها في خطة الاستجابة للحوادث السيبرانية.

تُعد إدارة الأداء عنصراً رئيسياً آخر في النظام الوطني لإدارة الحوادث السيبرانية، حيث يستخدم نظام الإدارة البيانات التي توفّرها وظيفة المراقبة المذكورة أعلاه ويقارنها بمؤشرات الأداء الرئيسية المحدّدة مسبقاً والتي توفّر أساساً موضوعياً لتقييم أداء القدرات الوطنية في إدارة الحوادث السيبرانية. وفقاً لذلك، يجب أن تتوافق البيانات المجمّعة كجزء من عملية المراقبة بوضوح مع مؤشرات الأداء الرئيسية التي تحدّدها إدارة الأداء. من الناحية النظرية، يُمكن ربط تلك المؤشرات بتقييمات المخاطر ذات الصلة بهدف دعم جهود الحوكمة. ويجب أن يوفّر نظام إدارة الأداء الذي يديره مجلس الأمن السيبراني صورة واضحة عن مدى توفّر القدرة الوطنية للاستجابة للحوادث وكفاءتها في ظل أهدافها الرئيسية؛ والتي تُقاس من خلال مؤشرات الأداء الرئيسية ذات الصلة، مما يوفّر رؤية واضحة لغايات التنفيذ وأساساً متيناً للتحسين المستمر.

ويجب أيضاً تحديد نظام مفصّل للمراقبة وإدارة الأداء بحيث يوفّر المعرفة اللازمة والمقاييس ذات الصلة التي تصف الأداء العام للقدرة الوطنية على الاستجابة للحوادث وذلك من خلال وضع الإجراءات التشغيلية القياسية المفصّلة التي يوفّرها مجلس الأمن السيبراني بصفته الجهة الوطنية الرئيسية في هذا المجال. يجب أن يأخذ مثل هذا النظام في الاعتبار كلاً من الإطار والخطة للاستجابة للحوادث السيبرانية، بالإضافة إلى توفير معايير مفصّلة تدعم القياس المنهجي.

7

القسم

التنفيذ

يقود مجلس الأمن السيبراني تنفيذ وتفعيل إطار الاستجابة للحوادث السيبرانية بصفته الجهة الوطنية الرئيسية في هذا المجال بالتشاور مع الجهات المعنية الرئيسية في المنظومة السيبرانية للدولة. وعليه، ستستغرق هذه العملية وقتاً عند تطبيقها على مستوى الجهة ومستوى القطاع والمستوى الوطني حيث تستمر العمليات والإجراءات في التطور مع استمرار جاهزية القدرات وبيئات التهديد في التغيّر. يجب وضع إجراءات الدعم والقدرات والأدوات والنظم والمحافظة عليها وتحديثها. يعمل المجلس مع الجهات المعنية عبر مجتمع الاستجابة للحوادث السيبرانية لتنفيذ إطار الاستجابة للحوادث السيبرانية بهدف بناء قدرات تشغيلية كاملة والاستمرار في رفع مستوى جاهزيتها.

8

القسم
الملاحق

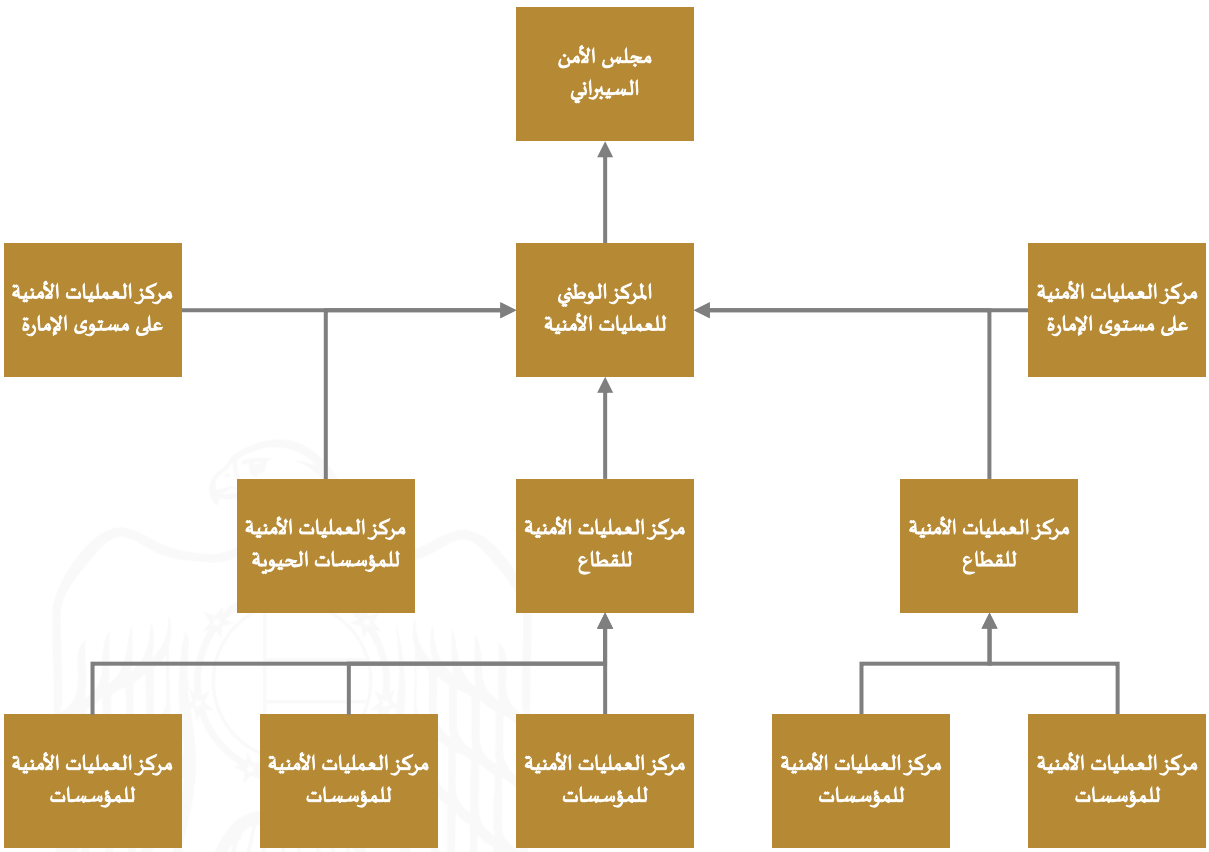
8.1 الإبلاغ وتبادل المعلومات: البيئة الاتحادية والمتطلبات وشبكة نقاط الاتصال

يشكّل الإبلاغ وتبادل المعلومات عنصران مهمان لتمكين القدرة الوطنية للاستجابة للحوادث السيبرانية. لذا يجب تحديد دور الجهات المعنية وقنوات تبادل المعلومات الفنية والتشغيلية والعمليات ذات الصلة بشكل صارم وبوضوح، وذلك لدعم الأداء الفعّال لقدرات الاستجابة للحوادث السيبرانية في حالة الأزمات. وثمّة أسلوبان مختلفان للإبلاغ وتبادل المعلومات، لكل منهما وظائف وأشكال مختلفة.

8.1 الإبلاغ وتبادل المعلومات: البيئة الاتحادية والمتطلبات وشبكة نقاط الاتصال

8.1.1 الإبلاغ الفني (البيئة الاتحادية)

يُبلّغ عن البيانات الفنية المتعلقة بالحوادث السيبرانية وتُشارك من خلال اتحاد مراكز العمليات الأمنية على النحو المحدّد بالتفصيل في إطار المعايير الأساسية لمركز العمليات الأمنية. تتبع قنوات الإبلاغ نموذجاً هرمياً تُجمع فيه المعلومات ذات الصلة (بما يشمل معلومات التهديد، وإدارة الثغرات، ومؤشرات الحوادث، وغيرها) من الجهات المعنية بالبنية التحتية للمعلومات الحيوية ونقلها إلى مراكز العمليات الأمنية الخاصة بالقطاع، ومن هذه المراكز إلى المركز الوطني للعمليات الأمنية.



الصورة 1-أ: البيئة الاتحادية (إطار المعايير الأساسية لمركز العمليات الأمنية)

8.1 الإبلاغ وتبادل المعلومات: البيئة الاتحادية والمتطلبات وشبكة نقاط الاتصال

8.1.1 الإبلاغ الفني (البيئة الاتحادية)

يجب أن تحتوي جميع تقارير الحوادث على بيانات قياسية حول:

- درجة الأولوية المحلية
- مستوى الفئة المخصّص
- العنوان
- الوصف
- الوضع الراهن
- الخلل في البيانات

ويجب إيصال جميع هذه التنبيهات مع اختتام عملية التحري، كما يجب رفع التقارير بالتحديثات بشكل وتكرار مناسبين. ويُراعى عند حساب وقت التنبيه أنه يحسب بالاعتماد على وقت الإعلان عن وقوع الحادث كما يلي:

متطلبات الإبلاغ الخاصة بالجهات المعنية بالبنية التحتية للمعلومات الحيوية

الفئة	متوسط وقت التنبيه
المستوى 4 حوادث على المستوى المحلي	1440 دقيقة
المستوى 3 حوادث بمستوى مرتفع	60 دقيقة

يُحدّد الوقت المتوقع للتحديث للجهات المعنية بالبنية التحتية للمعلومات الحيوية على النحو التالي:

الفئة	متوسط وقت التنبيه
المستوى الرابع (اللون الأخضر)	1440 دقيقة
المستوى الثالث (اللون الأصفر)	120 دقيقة
المستوى الثاني (اللون البرتقالي)	60 دقيقة
المستوى الأول (اللون الأحمر)	شبه فوري

يجب على مراكز العمليات الأمنية التابعة للقطاع ومركز العمليات الأمنية الوطني تحديد قواعد الإجراءات التشغيلية القياسية للبيئة الاتحادية. بالإضافة إلى ذلك، لتعزيز قدرات المركز الوطني للعمليات الأمنية على الكشف، يجب إعداد الإجراءات التشغيلية القياسية لتحدّد متطلبات الجهات الخاصة بالبنية التحتية للمعلومات الحيوية بهدف تحديد نطاق مؤشرات الحوادث والمعلومات الأخرى ذات العلاقة التي يجري مشاركتها (على سبيل المثال: جدار الحماية الخاص بالشبكة الفرعية، والبروكسي التوجيهي، وتحليل اسم النطاق، وما إلى ذلك). يجب أن تتوافق الإجراءات التشغيلية القياسية التي أعدّها المركز الوطني للعمليات الأمنية مع المعايير الأساسية لمركز العمليات الأمنية. ويتولى مجلس الأمن السيبراني (عبر المركز الوطني للعمليات الأمنية) مسؤولية إدارة قنوات الإبلاغ والحفاظ عليها كونه الجهة الوطنية الرئيسية في هذا المجال.

8.1 الإبلاغ وتبادل المعلومات: البيئة الاتحادية والمتطلبات وشبكة نقاط الاتصال

8.1.2 إدارة الأزمات التشغيلية

يجب إنشاء شبكة تتكون من نقاط اتصال محدّدة لأغراض إدارة الأزمات التشغيلية، بحيث تُستخدم خلال الحوادث السيبرانية المهمة التي تتطلب التعاون المتبادل بين الجهات المعنية الرئيسية لتمكين الاستجابة للأزمات بفاعلية. يتمثّل الهدف في عملية إنشاء هذه الشبكة في ربط مجتمع الأمن السيبراني والجهات المعنية الرئيسية في لذات المجال على الصعيد الوطني والمعنية بإدارة الأزمات الأمنية الحقيقية.

ويعمل المركز الوطني للعمليات الأمنية على بناء شبكة ارتباط وإدارتها بالنيابة عن مجلس الأمن السيبراني، بحيث تتألف من أشخاص محدّدين من الجهات الحكومية المعنية .

8.1 الإبلاغ وتبادل المعلومات: البيئة الاتحادية والمتطلبات وشبكة نقاط الاتصال

8.1.2 إدارة الأزمات التشغيلية

تهدف هذه الشبكة إلى تمكين التفعيل المنسق للموارد الوطنية ذات الصلة على أساس نهج حكومي شامل يهدف إلى "توحيد الجهود" فيما يتعلق بإدارة الحوادث السيبرانية على المستوى الإتحادي، بحيث تتضمن الاستعداد، وتعزيز التعاون، وتمكين الاستجابة للأزمات، بالإضافة إلى تنفيذ التدريبات، والتمارين وأنشطة الدروس المستفادة.

يجب أن يضع المركز الوطني للعمليات الأمنية الإجراءات التشغيلية القياسية المهمة وبروتوكولات التواصل تحت إشراف مجلس الأمن السيبراني.

كما يجب إجراء تمارين منتظّمة يعدّها المركز الوطني للعمليات الأمنية وينظمها تحت مظلة مجلس الأمن السيبراني، بهدف تطوير قدرات وطنية متطورة في إدارة الأزمات السيبرانية. من الواجب أيضاً إجراء اختبارات وتقييمات الثغرات والجاهزية، كما يجب معالجة الثغرات المحدّدة. بالاضافة إلى ذلك، يفضّل إجراء التمارين سنوياً على الأقل بالتنسيق مع الجهات المعنية.

8.2 إطار إرشادي لتفعيل دور الجهات (نظرة عامة على التبعيات)

يوفّر الرسم التالي إرشادات إضافية تساعد في فهم إجراءات البيئة الاتحادية (الإبلاغ والتصعيد)، بالإضافة إلى متطلبات الحفاظ على الصورة التشغيلية العامة للدولة التي تُنفّذها من قبل الجهات ذات الصلة في المجال السيبراني وقيادة المركز الوطني للعمليات الأمنية.

تشير الأسهم لاتجاه التصعيد من قبل الجهات ذات العلاقة.

8.2.1 حالة الاستقرار – المستوى الرابع

(المستوى الرابع، متوسط وقت التنبيه 1440 دقيقة)

المستوى الرابع

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

↓ الإعلان عن حادث

مركز العمليات الأمنية للقطاع

8.2 إطار إرشادي لتفعيل دور الجهات (نظرة عامة على التبعيات)

8.2.2 حادث سيبراني خطير – حادث سيبراني بالمستوى الثالث.

(المستوى الثالث، متوسط وقت التنبيه 60 دقيقة)

المستوى الثالث

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

↓

مركز العمليات الأمنية للقطاع

↓ الإعلان عن حادث

المركز الوطني للعمليات الأمنية

↓ عند الحاجة

المجموعة الوطنية للاستجابة السيبرانية

8.2 إطار إرشادي لتفعيل دور الجهات (نظرة عامة على التبعيات)

8.2.3 حادث سيبراني خطير - حادث سيبراني بالمستوى الثاني

(المستوى الثاني، تحديثات كل 60 دقيقة)

المستوى الثاني

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

↓

مركز العمليات الأمنية للقطاع

↓ الإعلان عن حادث

المركز الوطني للعمليات الأمنية

↓ عند الحاجة

المجموعة الوطنية للاستجابة السيبرانية

↓ يتم رفعه إلى المستوى الثاني بواسطة مجلس الأمن السيبراني بعد التنسيق مع الهيئة الوطنية لإدراة الطوارئ والأزمات والكوارث

الهيئة الوطنية لإدراة الطوارئ والأزمات والكوارث

8.2 إطار إرشادي لتفعيل دور الجهات (نظرة عامة على التبعيات)

8.2.4 حادث سيبراني خطير - حادث سيبراني بالمستوى الأول

(المستوى الأول، تحديثات فورية)

المستوى الأول

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

↓

مركز العمليات الأمنية للقطاع

↓ الإعلان عن حادث

المركز الوطني للعمليات الأمنية

↓ عند الحاجة

المجموعة الوطنية للاستجابة السيبرانية

↓ يتم رفعه إلى المستوى الثاني بواسطة مجلس الأمن السيبراني بعد التنسيق مع الهيئة الوطنية لإدراة الطوارئ والأزمات والكوارث

الهيئة الوطنية لإدراة الطوارئ والأزمات والكوارث

↓ يتم رفعه إلى المستوى الأول بواسطة مجلس الأمن السيبراني بعد التنسيق مع الهيئة الوطنية لإدراة الطوارئ والأزمات والكوارث

القيادة العليا

8.3 الاختصارات

الاختصار	الوصف
aeCERT	فريق الاستجابة لطوارئ الحاسب الآلي لدولة الإمارات العربية المتحدة
CERT	فريق الاستجابة لطوارئ الحاسب الآلي
CII	البنى التحتية للمعلومات الحيوية
CIIP	حماية البنية التحتية للمعلومات الحيوية
CSC	مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة
MTTN	متوسط وقت التنبيه
NCEMA	الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث
CIRF	إطار الاستجابة للحوادث السيبرانية
NCRG	المجموعة الوطنية للاستجابة السيبرانية
CIRP	الخطة الاستجابة للحوادث السيبرانية
NCSGF	الإطار الوطني لحوكمة الأمن السيبراني
NCSS	استراتيجية الأمن السيبراني
NSOC	المركز الوطني للعمليات الأمنية السيبرانية
POC	نقطة الاتصال
SOC	مركز العمليات الأمنية
SOP	الإجراءات التشغيلية القياسية