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

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

خطة 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

1 القسم

المقدّمة

المقدّمة

ترتبط البنى التحتية للمعلومات الحيوية في دولة الإمارات العربية المتحدة مع العديد من قطاعات البنية التحتية، كما تدعم العديد من العمليات والابتكارات الأساسية في القطاعين العام والخاص. وبصفتها إحدى الدول الرائدة عالمياً في توظيف تقنيات تكنولوجيا المعلومات والاتصالات، تعمل في دولة الإمارات العربية المتحدة العديد من الجهات، مثل: الوزارات والهيئات والمؤسسات والشركات والمواطنين والمقيمين، وهي جميعها معرضة على نحوٍ متزايد للحوادث السيبرانية. وتتضمن هذه الحوادث والتهديدات مجموعة كبيرة من الأحداث الطبيعية والبشرية، والمتعمدة وغير المقصودة، والتي يُمكن أن تمتد عبر العديد من المناطق الإدارية (أي المشتركة بين الإمارات) وعبر مختلف الأنظمة مما يؤثر على الجهات الحكومية والشركات والمواطنين والمقيمين.

وقد أثبتت الأمثلة العالمية مراراً بأن رقعة تأثير الحوادث السيبرانية تزداد باستمرار من حيث النطاق والخطورة، مخترقةً الإجراءات الفردية المتخذة للاستجابة ومسببةً الضرر للخدمات الوطنية الحيوية. ومع انتشار التهديدات وفشل إجراءات الوقاية والحماية أحياناً، يُمكن أن تتصاعد الحادثة بسرعة وتصبح حادثة سيبرانية عالية التأثير. ويستخدم هذا المصطلح لوصف الحوادث التي تتطلب التدخل على المستوى الوطني والتواصل والتنسيق مع العديد من الجهات المعنية لحلها بسرعة وفاعلية بهدف حماية الفضاء الإلكتروني في دولة الإمارات العربية المتحدة وحكومتها وقطاعها الخاص ومواطنيها.

ويدعم كلٌّ من إطار عمل الاستجابة للحوادث السيبرانية وخطة الاستجابة للحوادث السيبرانية تنفيذ الاستراتيجية الوطنية للأمن السيبراني من خلال بناء القدرات الوطنية لإدارة الحوادث وتعزيز مستوى استعداد دولة الإمارات العربية المتحدة وجاهزيتها للحماية من هذه التهديدات واكتشافها والاستجابة لها والتعافي منها بفاعلية.

1.1 الهدف

يقدّم إطار عمل الاستجابة للحوادث السيبرانية الرؤية الاستراتيجية ويساهم في بناء القدرات الوطنية التي تمكّن 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 السيبراني لدولة الإمارات والمساهمة في تعزيز الأمن ورفع مستوى الرفاهية والقدرة التنافسية العالمية للدولة.

أما خطة الاستجابة للحوادث السيبرانية، فتمثّل الخطة الوطنية التشغيلية العامة لإدارة الحوادث السيبرانية في الدولة.

وتهدف إلى تقديم الإرشادات حول الأنشطة المنجزة على نحوٍ جماعي من الجهات المعنية المتأثرة بالمنظومة السيبرانية للدولة، بما يتضمن تلك الموجودة على مستوى الجهة أو القطاع أو على المستوى الإتحادي. وتهدف الخطة الوطنية للاستجابة للحوادث السيبرانية بصورة رئيسية إلى تعزيز الرؤية الاستراتيجية للقدرات الوطنية لتمكينها من إدارة الحوادث السيبرانية على النحو المنصوص عليه في إطار عمل الاستجابة للحوادث السيبرانية ، والتأكد من تحقيق غرضه الاستراتيجي في تمكين دولة الإمارات العربية المتحدة من الحفاظ على استقرار الفضاء السيبراني الخاص بها والاستجابة لحوادث الأمن السيبراني على النحو المحدّد في مخطط التنبيه من الحوادث السيبرانية (الملحق 4.1).

1.2 النطاق ومدى قابلية التطبيق

يسري كل من إطار عمل الاستجابة للحوادث السيبرانية وخطة الاستجابة للحوادث السيبرانية على جميع جهات القطاعين العام والخاص بموجب سياسة حماية البنى التحتية للمعلومات الحيوية داخل حدود الدولة بما يتضمن مياهها الإقليمية ومناطقها الاقتصادية.

1.3 العلاقة بإطار عمل وطني للاستجابة للحوادث السيبرانية

يحدّد إطار عمل الاستجابة للحوادث السيبرانية نموذج الحوكمة وخطوات إدارة الحوادث بهدف الاستجابة بنجاح للحوادث السيبرانية الرئيسية. بينما توفّر خطة الاستجابة للحوادث السيبرانية السياق التشغيلي والتفسيرات المهمة لإطار العمل من خلال تقديم التفاصيل حول أدوار ومسؤوليات مختلف الجهات المشاركة في الاستجابة للحوادث سواءً أثناء حالات الاستقرار أو أثناء حوادث الأمن السيبراني. وتوفّر الخطة أيضاً تفاصيل إضافية حول إجراءات إدارة الحوادث من أجل الحصول على استجابة منسقة ومنظّمة للحوادث السيبرانية المهمة.

2 القسم

الأدوار والمسؤوليات عند الاستجابة للحوادث

يحدّد إطار عمل الاستجابة للحوادث السيبرانية جهتان حوكمة على المستوى الوطني لإدارة الاستجابة للحوادث، وهي: المركز الوطني لعمليات الأمن السيبراني، والمجموعة الوطنية للاستجابة السيبرانية، ويشمل أيضاً مراكز العمليات الأمنية والجهات المشغّلة للبنى التحتية للمعلومات الحيوية ضمن القطاع بصفتها جزءاً لا يتجزأ من إطار عمل الاستجابة للحوادث السيبرانية . وتمتلك جميع هذه الجهات المعنية مسؤوليات محدّدة ضمن الإجراءات المتبعة لإدارة حالات الاستقرار أو الحوادث السيبرانية. وتُوضح هذه المسؤوليات إلى حدٍ أكبر من خلال خطة الاستجابة للحوادث السيبرانية .

2.1 المركز الوطني لعمليات الأمن السيبراني

يقع المركز الوطني لعمليات الأمن السيبراني تحت إدارة مجلس الأمن السيبراني بصفته نقطة التشغيل المركزية (الفنية) للإدارة الوطنية للحوادث السيبرانية في الدولة، حيث ينفذ هذه المهام الأساسية من خلال ما يلي:

2.1.1.1 نشر الوعي السيبراني حول الفضاء الإلكتروني في الدولة من خلال إبراز صورة تشغيلية مشتركة على المستوى الوطني ودمج المعلومات ذات الصلة بين كافة الجهات المعنية (وظيفة مركز الدمج).

2.1.1.2 تنسيق الاستجابة للحوادث السيبرانية على المستوى الفني (وظيفة إدارة الأزمات الفنية).

2.1.1.3 العمل كمركز ارتباط وطني لإدارة الحوادث السيبرانية داخل الدولة، الأمر الذي يسهل التعاون وتبادل المعلومات مع الجهات الموجودة ضمن منظومة العمل في دولة الإمارات والشركاء الرئيسيين الذين لديهم مسؤوليات إضافية للاستجابة للحوادث السيبرانية.

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

2.1 المركز الوطني لعمليات الأمن السيبراني

الدور أثناء حالات الاستقرار

دور المركز الوطني لعمليات الأمن السيبراني أثناء حالات الاستقرار، (المستوى الرابع) يحافظ على الصورة التشغيلية المشتركة وينشر الوعي حول الحالة السيبرانية في الفضاء الإلكتروني في الدولة للجهات المعنية على مستوى الجهة نفسها والقطاع والمستوى الوطني. وتساهم هذه الصورة التشغيلية المشتركة في تمكين مجلس الأمن السيبراني من الدفاع عن الفضاء الإلكتروني وتنظيم أنشطة الاستجابة للحوادث على المستوى الوطني، ولا سيما في أوقات الحوادث السيبرانية المهمة. ويوظف المركز العملية المتبعة للإبلاغ وتبادل المعلومات, وفقا لإطار الاستجابة للحوادث فضلاً عن بناء الصورة التشغيلية المشتركة والحفاظ عليها. ولتنفيذ هذه الوظيفة الأساسية، يمتلك المركز نظام "نقطة الاتصال" الوطني المخصّص لأغراض الإدارة الفنية للحوادث السيبرانية، والذي يكون قناة للإبلاغ وتبادل المعلومات مع فرق الاستجابة لطوارئ الحاسب الآلي ضمن القطاع والجهات المعنية بالبنى التحتية للمعلومات الحيوية. ويُمكن إيجاد قواعد ومتطلبات الإبلاغ وتبادل المعلومات أدناه. و أن المركز الوطني لعمليات الأمن السيبراني يحلل جميع المعلومات المتاحة لتقديم صورة التشغيل المشتركة على الفضاء الإلكتروني لدولة الإمارات.

ينفّذ المركز الوطني لعمليات الأمن السيبراني أثناء حالات الاستقرار، (المستوى الرابع)، من خلال وظيفة إدارة الأزمات الفنية الخاصة به، الأنشطة التي تحدّدها إجراءات إدارة الحوادث السيبرانية، بما يتضمن تسجيل الحوادث والتحقّق منها والتنسيق والتحليل والتنبيه والاحتواء والتخفيف من الأثر واستراتيجيات التعافي، إلى جانب توفير الخبرات الإضافية حسب الحاجة لمعالجة الحادث. وقد يقدّم المركز المساعدة الفنية للجهات المعنية بالبنى التحتية للمعلومات الحيوية للاستجابة للحوادث (المستوى الرابع). وتشمل المساعدة الفنية تعزيز مستوى الوعي بالحالة السيبرانية والتوجيه بشأن أنشطة الاستجابة التي يجب أن تتخذها الجهات ذات الصلة وتوفير الخبرات للاستجابة الفنية (مثل: التخفيف من حدة التهديدات ومعالجة الحوادث) على أساس كل حالة على حدة وحسب الحاجة. ومن أجل تسهيل التعاون وتبادل المعلومات والاستجابة للحوادث، قد يرسل المركز موظفين مختصين إلى الجهات المعنية الرئيسية، بما يتضمن مراكز العمليات الأمنية والجهات المعنية بالبنى التحتية للمعلومات الحيوية على أساس مؤقت أو دائم للحفاظ على العلاقات بها وتعزيز إجراءات الإبلاغ وتبادل المعلومات وتنسيق الإجراءات أثناء الاستجابة للحوادث السيبرانية. وقد تتم أيضاً دعوة مراكز العمليات الأمنية والجهات المعنية بالبنى التحتية للمعلومات الحيوية لإرسال موظفين إلى المركز الوطني لعمليات الأمن السيبراني للاطلاع بأدوار مماثلة.

1. يوجد تعريف مفصّل للحوادث السيبرانية في إطار العمل وفي الملحق 4.1 - مخطط التنبيه بالحوادث السيبرانية.

2.1 المركز الوطني لعمليات الأمن السيبراني

وأخيراً، يعمل المركز الوطني لعمليات الأمن السيبراني أيضاً على شكل مركز اتصال وطني لإدارة الحوادث السيبرانية داخل الدولة وبناءً على ذلك، يتعامل مع الشركاء الوطنيين الرئيسيين الذين لديهم أدوار ومسؤوليات إضافية في الاستجابة للحوادث السيبرانية بهدف تسهيل تبادل المعلومات والاستعداد للحوادث السيبرانية والحماية منها والاستجابة لها على جميع المستويات. وفيما يلي توضيح للأدوار والمسؤوليات المطلوبة من أجل التعاون الأمثل (2.5 الشركاء الوطنيون الآخرون المنوطون بأدوار ومسؤوليات متعلقة بالمجال السيبراني).

ولرفع مستوى التعاون، يتعيّن على المركز توفير مجموعة عمل خاصة للاستجابة للحوادث، على أن تجتمع شهرياً لتبادل المعلومات حول التهديدات السيبرانية والثغرات الأمنية وأنشطة الاستجابة والدروس المستفادة. وتضم مجموعة العمل هذه ممثّلين من الجهات المنظّمة ضمن القطاع وفريق الاستجابة لطوارئ الحاسب الآلي، ومراكز العمليات الأمنية العاملة ضمن القطاع والجهات المعنية بالبنى التحتية للمعلومات الحيوية ومديري تكنولوجيا المعلومات والاتصالات ومديري مراكز العمليات الأمنية وفريق الاستجابة لحوادث أمن الحاسب الآلي من الجهات الحكومية والجهات المعنية الأخرى. وستساهم مجموعة العمل في تمكين المركز من إقامة العلاقات المثمرة مع مراكز العمليات وتحسين مستوى الاستجابة المنسقة أثناء الحوادث السيبرانية المهمة.

وبالإضافة إلى وظائفها الأساسية المذكورة أعلاه، قد يقدّم المركز الوطني لعمليات الأمن السيبراني الدعم المباشر لتوفير المعلومات لشركاء محدّدين، بما يتضمن جهات الإدارة العامة، وتنظيم ورش عمل دورية لتسهيل نقل المعرفة لجهات مُختارة وتنفيذ أنشطة التوعية والتدريب الأخرى ذات الصلة.

2.1 المركز الوطني لعمليات الأمن السيبراني

الدور أثناء الحوادث السيبرانية الخطيرة (المستوى الثالث)

من خلال دوره المتمثّل بمركز الدمج، يعمل المركز الوطني لعمليات الأمن السيبراني كنقطة محورية وطنية لإيجاد الوعي بالموقف العام. وبالتالي يمثّل المركز نقطة الاتصال الأساسية على مستوى الجهة والقطاع وعلى المستوى الوطني للإبلاغ عن الحوادث السيبرانية ذات الصلة وتبادل المعلومات كما هو محدّد في متطلبات الإبلاغ وفي الفصل المتعلق بتبادل المعلومات .

ويمثّل ما ورد أعلاه أساس الصورة التشغيلية المشتركة التي يوفّرها المركز. وبناءً على هذا الوعي الشامل بالحالة السيبرانية، يتعيّن على المركز تنفيذ ما يلي:

- تحليل المعلومات المتوفّرة عن الحوادث والتهديدات وتقديم التوصيات لرئيس مجلس الأمن السيبراني بشأن الإعلان عن الحادث السيبراني الخطير (المستوى الثالث)، وعقد اجتماع للمجموعة الوطنية للاستجابة السيبرانية عند الحاجة، فضلاً عن تقديم الاستشارات لرئيس المجموعة الوطنية للاستجابة السيبرانية بشأن تشكيل مجموعة وطنية للاستجابة السيبرانية بناءً على طبيعة الحادث ونطاقه وأثره المحتمل أو الفعلي[2]، والعمل بصفة منسق فني لتلك الهيئات (توفير الإخطارات واللوجستيات، وما إلى ذلك).
- تقديم المشورة وإبلاغ المجموعة الوطنية للاستجابة السيبرانية عند انعقادها بشأن الأثر الحقيقي أو المحتمل للحادث، وإجراءات الاستجابة والتعافي، وتحديثات السياسات الاستراتيجية.
- تنسيق أنشطة الاستجابة وتقديم المساعدة الفنية إلى الجهات المعنية بالبنى التحتية للمعلومات الحيوية والجهات المعنية الأخرى، بما يتضمن الخدمات الوطنية المهمة المعرضة للخطر، وتحديد أولويات الحوادث، وتحديد القدرات، والإبلاغ عن الظروف المتعلقة بالحوادث السيبرانية.
- المشاركة مع شركاء الأمن السيبراني الدوليين عند الإيعاز بذلك (على سبيل المثال: مراكز الأمن السيبراني الدولية وفرق الاستجابة للطوارئ والمؤسسات الأخرى) للمساعدة في التصدي للحوادث.
- توفير أنشطة الاتصالات أثناء الأزمات للحفاظ على ثقة الجمهور وتقديم خدمات الاتصالات العامة في حالات الطوارئ تحت التوجيه والإشراف الاستراتيجي من المجموعة الوطنية للاستجابة السيبرانية والسلطات الوطنية الأخرى ذات الصلة عند اللزوم.

وبهدف ضمان قدرة المركز الوطني لعمليات الأمن السيبراني على تنفيذ مسؤولياته الأساسية المذكورة أعلاه، يعمل المركز بالتعاون مع مجموعة العمل للاستجابة للحوادث على وضع خطة وطنية لإدارة الحوادث واختبارها وتحديثها. ووفقاً لأفضل الممارسات الدولية والمعايير المتبعة في القطاع، يجب أن تتضمن خطة إدارة الحوادث على وثيقة مفصّلة للغاية لإدارة الحوادث التشغيلية، فضلاً عن توثيق الإجراءات المطلوبة لإدارة الحوادث التي تغطي جميع مراحل إدارة الحوادث السيبرانية.

2. على سبيل المثال: إذا كان الحادث مرتبطاً بصورة أساسية بقطاعي النفط والغاز والمرافق، فسيشارك ممثلون من قطاعات البنية التحتية الحيوية في أنشطة المجموعة الوطنية للاستجابة السيبرانية بينما قد تكون مشاركة قطاعات البنية التحتية الحيوية الأخرى محدودة.

3. تتضمن أنشطة اتصالات الأزمات إبلاغ الشركات والمواطنين والمقيمين بالتهديدات التي تتعرض لها البنى التحتية للمعلومات الحيوية، وتقديم المعلومات حول الحادث والتوصية بشأن الخطوات التي يُمكن للجهات المعنية والجمهور اتخاذها لحماية أنفسهم وتقليل أثر الحادث. وتشتمل أنشطة الاتصالات الفعالة أثناء الأزمات على عناصر السرعة والدقة ونقل المعلومات القابلة للتنفيذ أثناء الحادث السيبراني المهم وبعده.

2.2 المجموعة الوطنية للاستجابة السيبرانية

تمثّل المجموعة الوطنية للاستجابة السيبرانية هيئة مسؤولة عن اتخاذ القرارات الاستراتيجية، وهي معنية أيضاً بتنسيق إدارة الحوادث السيبرانية في جميع أنحاء دولة الإمارات، وذلك استجابةً للحوادث السيبرانية الخطيرة بالمستوى "الثالث".

وتنفّذ المجموعة على وجه الخصوص ما يلي:

2.2.1.1 تنظيم الموارد والإجراءات لمساعدة الجهات المالكة للأنظمة التي تحتاج المساعدة في التعامل مع الاستجابة للحوادث، بما يشمل الاحتواء والمعالجة.

2.2.1.2 تحديد الحلول المشتركة للتخفيف من الآثار، وذلك بالاعتماد على المركز الوطني لعمليات الأمن السيبراني للحصول على المشورة الفنية على النحو المحدّد أعلاه.

2.2.1.3 توفير القيادة التنظيمية والإشراف على دورة الإجراءات المتخذة للاستجابة للحوادث.

1. يُرجى الاطلاع على الملحق ج.

2.2 المجموعة الوطنية للاستجابة السيبرانية

العضويات

تتألف المجموعة الوطنية للاستجابة السيبرانية من صنّاع القرارات العامة من الشركاء الوطنيين والجهات المنظّمة والجهات المعنية بالبنية التحتية الحيوية وفقاً لنطاق الحادث.

منظومة المجموعة الوطنية للاستجابة السيبرانية

ستتم دعوة ممثّلين رفيعي المستوى للجهات المنظّمة لقطاع البنية التحتية الحيوية ومراكز العمليات الأمنية والجهات المشغّلة بحسب ما يحدّد في سياسة حماية البنية التحتية للمعلومات الحيوية لدولة الإمارات[4] للمشاركة في المجموعة الوطنية للاستجابة السيبرانية. وقد يتنوّع ممثّلو كل قطاع من قطاعات البنية التحتية الحيوية بناءً على الهيكل التنظيمي لكل قطاع. فإذا كان القطاع يمتلك جهة منظّمة، فيجب أن تعمل هذه الجهة بصفتها أحد ممثّلي القطاع ضمن المجموعة الوطنية للاستجابة السيبرانية.

يمثّل مجلس الأمن السيبراني الجهة المسؤولة عن المجموعة الوطنية للاستجابة السيبرانية، وبالتالي هو المسؤول عن اعتماد تشكيلتها. ويمثّل المركز الوطني لعمليات الأمن السيبراني الجهة المسؤولة عن التنسيق الفني، ويكون مديره عضواً في المجموعة الوطنية للاستجابة السيبرانية.

ويجب أن يكون أعضاء المجموعة الوطنية للاستجابة السيبرانية صنّاع القرارات العامة في مؤسساتهم ويتمتعون بخبرات كبيرة في المجالات ذات الصلة، بالإضافة إلى امتلاكهم القدرة على توظيف موارد مؤسساتهم ضمن عملية إدارة الحوادث السيبرانية على المستوى الوطني. وبالإضافة إلى ذلك، يُتوقع من ممثّلي قطاع البنى التحتية الحيوية أن يمثّلوا قطاعهم كاملاً في المجموعة الوطنية للاستجابة السيبرانية، وامتلاك القدرة على توفير المعلومات حول الأثر المتوقع أو الفعلي للحوادث السيبرانية المهمة في قطاعهم.

4. يُرجى الاطلاع على الملحق ج.

2.2 المجموعة الوطنية للاستجابة السيبرانية

الدور أثناء حالات الاستقرار

أثناء حالات الاستقرار، تجتمع المجموعة الوطنية للاستجابة السيبرانية على أساس ربع سنوي لتحديد آثار التغيرات الحاصلة على المشهد السيبراني في دولة الإمارات، ولمراجعة وتقييم عمليات الحوكمة المتبعة وإدارة أداء القدرات الوطنية للاستجابة للحوادث وضمان توظيف الدروس المستفادة من الحوادث.

ويجري رئيس المجموعة الوطنية للاستجابة السيبرانية، مستعيناً بمُدخلات المركز الوطني لعمليات الأمن السيبراني، تقييماً للدروس المستفادة من الاختبارات والأنشطة والحوادث السابقة ويراقب تنفيذ الأنشطة التصحيحية، وذلك لضمان التصرف بناءً على الدروس المستفادة. ويجري المركز، مستعيناً بمجموعة العمل للاستجابة للحوادث، تحليلاً للفجوات ويعرض الدروس المستفادة أمام المجموعة. وتتخذ المجموعة القرارات ذات الصلة ثم تراقب تنفيذ الخطط المطلوبة لتناول الفجوات والدروس المستفادة. ويتوقع من أعضاء المجموعة تقديم تحديثات منتظّمة حول كيفية تنفيذ خطط العمل، وتوظيف الدروس المستفادة في كل قطاع على حد سواء.

وتساهم الاجتماعات الدورية أثناء حالات الاستقرار في ترسيخ مستوى التعاون والتنسيق بين أعضاء المجموعة وتعزيز جاهزية المجموعة للاستجابة بسرعة في حال وقوع الحوادث السيبرانية الخطيرة. وبالإضافة إلى ذلك، قد تشارك المجموعة في الأنشطة الوطنية والقطاعية المصممة لاختبار خطط وقدرات الاستجابة السيبرانية والتجهز للحوادث السيبرانية المهمة. وسيضمن رئيس المجموعة تخصيص الموارد اللازمة لدعم كافة أنشطة المجموعة.

2.2 المجموعة الوطنية للاستجابة السيبرانية

الدور أثناء الحوادث السيبرانية الخطيرة (المستوى الثالث)

إذا وصلت مؤشرات الحوادث إلى حدها الأقصى وفقاً لمخطط التنبيه بالحوادث السيبرانية، يُعلن رئيس المجموعة الوطنية للاستجابة للحوادث السيبرانية وقوع حادث سيبراني خطير وبمستوى تنبيه "الثالث"، وذلك بناءً على توصيات المركز الوطني لعمليات الأمن السيبراني.

وفي حال الإعلان عن حادث بالمستوى "الثالث"، يتخذ رئيس المجموعة القرار بشأن تشكيلة المجموعة ويعقد اجتماعاً مخصّصاً (حضوري أو افتراضي أو مدمج) ويطلب تحضير الخطط والطلبات الأولية أو المجدولة من أجل الحصول على المعلومات من أعضاء المجموعة. ويقدّم المركز الوطني لعمليات الأمن السيبراني المساعدة من خلال توفير الخبرات الفنية والتنسيق. ومن جانبهم، يوفّر أعضاء المجموعة المعلومات بسرعة والمشاركة في أنشطة المجموعة للمساعدة في جهود الاستجابة للحوادث السيبرانية.

وأثناء الحوادث السيبرانية الخطيرة، يتولى أعضاء المجموعة مسؤولية التعرّف على الحوادث السيبرانية الحالية في مجالاتهم وتمثيل مؤسساتهم في الحوارات القائمة المتعلقة بإيجاد الحلول وتخصيص الموارد والقدرات المطلوبة. ويشارك أعضاء المجموعة الوطنية للاستجابة السيبرانية في تحديد الأهداف والأولويات للاستجابة للحوادث السيبرانية والاتفاق على خطة موثّقة لمعالجة الحادث والعمل معاً لتنفيذها عند حدوث الحوادث السيبرانية المهمة. وتُعتبر المجموعة الوطنية للاستجابة السيبرانية قد أكملت العمل على أنشطتها عند:

1) تحقيق الأهداف المنصوص عليها في خطة معالجة الحوادث السيبرانية وعودة مستوى التنبيه للحادثة السيبرانية إلى المستوى الرابع أو المستوى الطبيعي

2) تقوم المجموعة بالتصعيد وإعلان حدوث حادث سيبراني بالمستوى الثاني من قبل مجلس الأمن السيبراني بعد التشاور مع الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث في حال تعدي الحدود ذات الصلة أو مؤشرات الحوادث بحسب مخطط التنبيه بالحوادث السيبرانية.

2.3- مراكز العمليات الأمنية في القطاع والجهات المشغّلة للبنى التحتية للمعلومات الحيوية

تمثّل مراكز العمليات الأمنية في القطاع والجهات المعنية بالبنى التحتية للمعلومات الحيوية جهات معنية رئيسية في المنظومة السيبرانية في دولة الإمارات، وبالتالي تمثّل عناصر أساسية لقدرات الاستجابة للحوادث السيبرانية. وتؤدي هذه الجهات المعنية دوراً رئيسياً في حالات الاستقرار وأثناء المشاركة في جهود الاستجابة الوطنية للحوادث السيبرانية المهمة. وتُوضّح قائمة البنى التحتية للمعلومات الحيوية في سياسة حماية البنى التحتية للمعلومات الحيوية المعد من قبل مجلس الأمن السيبراني.

الدور أثناء حالات الاستقرار

تحافظ مراكز العمليات الأمنية في القطاع والجهات المعنية بالبنى التحتية للمعلومات الحيوية على قدراتها الخاصة بالاستجابة للحوادث والاستفادة منها بصورة مستقلة أثناء حالات الاستقرار، وبالتعاون مع المركز الوطني لعمليات الأمن السيبراني أثناء الحوادث بالمستوى الرابع و الثالث. وتتولى هذه الجهات المسؤولية الأساسية الإلزامية وغيرها من المهام التطوعية المتمثّلة بالإبلاغ المعلومات ومشاركتها كما هو محدّد في الخطة

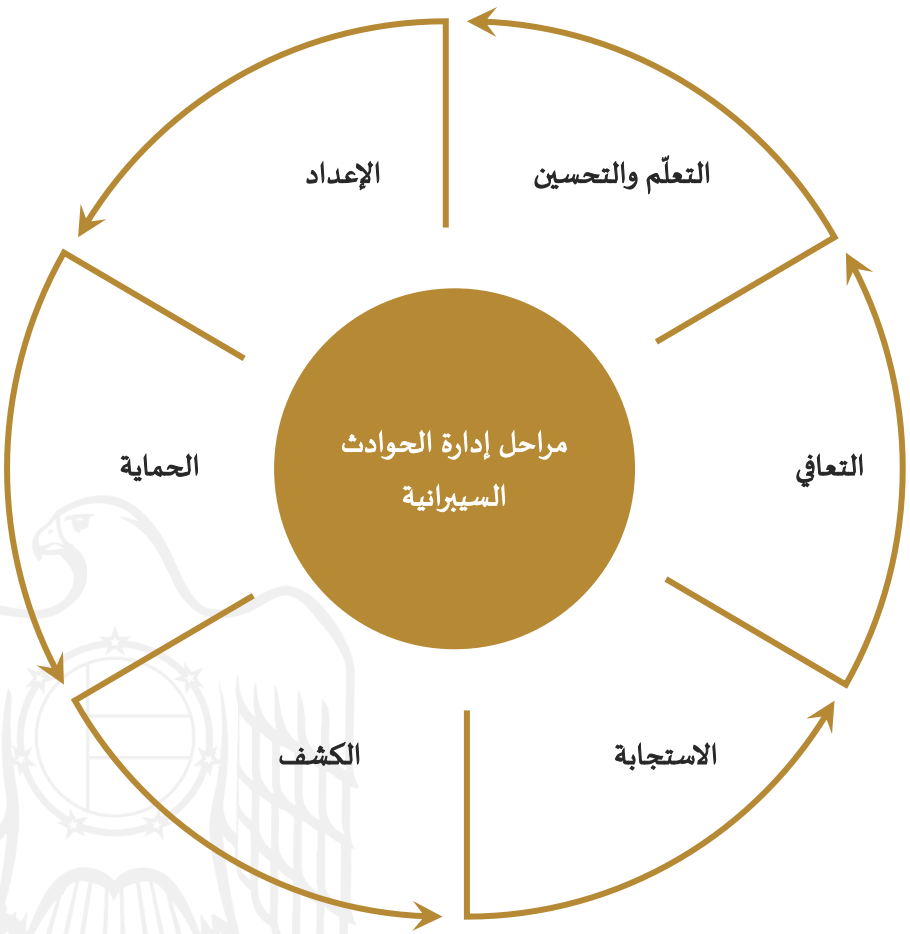
الدور أثناء الحوادث السيبرانية الخطيرة

أثناء وقوع الحوادث السيبرانية المهمة، تتعاون مراكز العمليات الأمنية في القطاع والجهات المعنية بالبنى التحتية للمعلومات الحيوية وتوظف مواردها الخاصة بالتنسيق مع المركز الوطني لعمليات الأمن السيبراني وفي نفس الوقت تشارك في جهود الاستجابة للحوادث السيبرانية.

3 القسم

خطة الاستجابة للحوادث السيبرانية

تساهم خطة الاستجابة للحوادث السيبرانية في توجيه أنشطة الجهات المعنية بإطار عمل الاستجابة للحوادث السيبرانية الصادر من مجلس الأمن السيبراني، وذلك من خلال مختلف مراحل إدارة الحوادث السيبرانية، بما يتضمن الانتقال من حالة الاستقرار إلى الحادث السيبراني وعودةً إلى حالة الاستقرار. وتساهم خطوات ومراحل إدارة الحوادث السيبرانية في تحديد الأدوار والمهام والمسؤوليات الرئيسية لكل جهة. ويتطلب التنفيذ الفعّال لخطة الاستجابة للحوادث السيبرانية إدماج وتنسيق خطط وسياسات وقدرات إدارة الحوادث السيبرانية التابعة للجهات المعنية سواءً على مستوى الجهة أو القطاع أو على المستوى الوطني. وسيساهم هذا الإدماج في تسريع الاستجابة وتعزيز مستوى تنظيمها على المستوى الوطني لمواجهة الحوادث السيبرانية المهمة.



1. مراحل إدارة الحوادث السيبرانية

3.1 الإعداد

نظراً إلى الطبيعة الديناميكية والمتسارعة لبيئة التهديدات السيبرانية، فإنه لا يُمكن منع كافة الحوادث. وبالتالي يُعد الاستعداد المسبق والتجهيز جانباً أساسياً للحصول على أفضل وأسرع استجابة للحوادث وللتعافي منها بفاعلية. وبناءً على ذلك، تهدف هذه المرحلة إلى بناء قدرات (الأفراد والعمليات والتكنولوجيا) الاستجابة للحوادث السيبرانية، بما يتضمن الإبلاغ وتبادل المعلومات التي تساهم في تعزيز الوعي بالأوضاع السيبرانية.

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

المهام العامة

- توفير القدرات، التي تلبي معايير القطاع فريق الاستجابة لحوادث أمن الحاسب الآلي ومركز العمليات الأمنية (أو ما يعادلها)، لإدارة الحوادث السيبرانية.
- إقامة العلاقات مع الجهات التشغيلية ذات الصلة (مثل: مراكز العمليات الأمنية في القطاع، وفريق الاستجابة لطوارئ الحاسب الآلي، والمركز الوطني لعمليات الأمن السيبراني) لتلبية متطلبات الإبلاغ وتبادل المعلومات وإتاحة إمكانية الدخول إلى المعلومات القطاعية التي تساهم في تعزيز مستوى الوعي بالأوضاع السيبرانية على المستوى الوطني وتقديم المساعدة الفنية.
- المشاركة في الأنشطة المعنية باختبار قدرات وسياسات وخطط وإجراءات الاستجابة للحوادث السيبرانية وتنفيذها (بما يتضمن الحوادث السيبرانية عالية المستوى التي قد تترتب عليها تبعات مادية).

الأفراد

- ربط أفراد الاستجابة للحوادث السيبرانية مع أفراد استمرارية الأعمال وإدارة حالات الطوارئ (الأقسام).
- الاستثمار في التطوير المهني لأفراد الاستجابة للحوادث السيبرانية، بما يتضمن تدريب الأعضاء على إطار عمل الاستجابة للحوادث السيبرانية وخطة الاستجابة للحوادث السيبرانية ، وغيرها من الخطط والإجراءات والتقنيات الداعمة على المستوى الوطني ومستوى القطاع ومستوى الجهة.
- إجراء الدورات التدريبية للمستخدمين النهائيين لنشر التوعية حول الأمن السيبراني.
- ضمان استقلالية طاقم إدارة الحوادث لتجنب حصول التضارب في المصالح.

3.1 الإعداد

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

العملية

- تنفيذ وظائف إدارة الأصول والمخاطر بناءً على أفضل الممارسات المتّبعة في القطاع.
- وضع خطط الاستجابة للحوادث الخاصة بكل جهة ومواءمة الإجراءات التشغيلية مع إطار عمل الاستجابة للحوادث السيبرانية وخطة الاستجابة للحوادث السيبرانية والخطط الأخرى ضمن القطاع بحسب الحاجة.
- إجراء عمليات التقييم للفجوات وتحديد مستوى الجاهزية دورياً ووضع خارطة طريق لتصحيح الفجوات المحدّدة في قدرات الاستجابة للحوادث السيبرانية.
- ربط استجابات الحوادث السيبرانية مع عمليات إدارة استمرارية الأعمال.

التكنولوجيا

- بناء وتعزيز القدرات التكنولوجية (بما يتضمن الأمن المادي) المطلوبة لإدارة الحوادث وفقاً لمعايير القطاع، وذلك يتضمن تقديم توفير المعلومات حول التهديدات والمراقبة وأنشطة الاستجابة والإبلاغ وتبادل المعلومات (بما يتضمن الأنشطة الآلية).

3.1 الإعداد

مراكز العمليات الأمنية للقطاع، وفريق الاستجابة لطوارئ الحاسب الآلي

المهام العامة

- يسعى مركز العمليات الأمنية جاهداً إلى بناء مجتمع الأمن المحلي، والمساعدة في رفع مستوى الوعي، وتقديم التعليم والتدريب اللازم للمؤسسات التي تحتاجه، وهو معني على وجه التحديد أيضاً بإقامة الشراكات، وتوفير الموارد، وآليات التغذية الراجعة لجميع المؤسسات داخل دولة الإمارات العربية المتحدة.
- يحافظ مركز العمليات الأمنية على القدرات الأساسية ويوفّر الخدمات بحسب ما هو محدّد في السياسة المرجعية لمركز العمليات الأمنية المعد من قبل مجلس الأمن السيبراني.

الأفراد - العملية

- بناء وتعزيز شبكة الاستجابة للحوادث ضمن كل قطاع معني والتنسيق مع الجهات الوطنية ذات الصلة (فريق الاستجابة لطوارئ الحاسب الآلي، والمركز الوطني لعمليات الأمن السيبراني)
- مساعدة الجهات المنظّمة في القطاع والمركز الوطني لعمليات الأمن السيبراني على تقييم الحوادث وإدارتها.
- جمع المعلومات حول مستوى الجاهزية على مستوى القطاع وتطوير المقاييس بما يتماشى مع القطاع ومتطلبات الإبلاغ وتبادل المعلومات.
- الإسهام في وضع خطط وإجراءات إدارة الحوادث السيبرانية الخاصة بالقطاع بموجب مبادئ إطار عمل الاستجابة للحوادث السيبرانية وبما يتماشى مع خطة الاستجابة للحوادث السيبرانية .
- المشاركة في الأنشطة القطاعية المعنية باختبار قدرات وسياسات وخطط وإجراءات الاستجابة للحوادث السيبرانية وتنفيذها (بما يتضمن الحوادث السيبرانية عالية المستوى التي قد تترتب عليها تبعات مادية).

التكنولوجيا

- تطوير الأدوات والمعدات والبنى التحتية التي تساعد على تحديد المعلومات اللازمة لتعزيز الجاهزية للحوادث وجمعها وتحليلها ومشاركتها أو نشرها.

3.1 الإعداد

المركز الوطني للعمليات الأمنية

المهام العامة

- إقامة وتعزيز العلاقات مع الجهات المعنية في الجهة والقطاع وعلى الصعيدين الوطني والدولي.
- إيجاد الصورة التشغيلية المشتركة والحفاظ عليها من أجل نشر الوعي حول الوضع السيبراني على المستوى الوطني.
- توفير القدرات (بما يتضمن الأفراد والعمليات والقدرات) التي تمثّل المركز الرئيسي على المستوى الوطني للاستجابة للحوادث، موفرةً الاستجابات الفنية للجهات المعنية بالبنى التحتية للمعلومات الحيوية والقطاعات المتأثرة، ومقدّمةً الدعم للمجموعة الوطنية للاستجابة السيبرانية في أوقات حصول الحوادث.
- توفير القدرات لمساعدة المجموعة الوطنية للاستجابة السيبرانية ورفدهم بالمتطلبات اللوجستية والإدارية.
- المشاركة في الأنشطة على المستوى الوطني ومستوى الحكومة الاتحادية المعنية باختبار قدرات وسياسات وخطط وإجراءات الاستجابة للحوادث السيبرانية وتنفيذها بالتنسيق مع الجهات المعنية (بما يتضمن الحوادث السيبرانية التي قد تترتب عليها تبعات مادية).
- مراجعة أو تقييم خطط وقدرات الاستجابة للحوادث على مستوى القطاع وتقديم التوصيات من أجل التحسين.

الأفراد

- الاستثمار في التطوير المهني للأفراد لمواكبة آخر التقنيات الناشئة وبيئة التهديدات التي تتغير بسرعة.

العملية

- توفير عملية على المستوى الوطني لدمج أنشطة الإبلاغ وتبادل المعلومات للاستجابة للحوادث السيبرانية، وذلك لخلق صورة تشغيلية مشتركة.
- إعداد العمليات التي تمكّن الاستجابة الوطنية للحوادث السيبرانية.
- إعداد العمليات التي تساعد المجموعة الوطنية للاستجابة السيبرانية للحوادث في تفعيل الاستجابات للحوادث السيبرانية المهمة (التنسيق والجوانب اللوجستية).

التكنولوجيا

- توفير الأدوات والأنظمة والبنى التحتية الداعمة التي تتماشى مع معايير القطاع، وذلك من أجل جمع المعلومات وخلق الصورة التشغيلية المشتركة والاطِّلاع على مسؤوليات إدارة الحوادث السيبرانية.

3.1 الإعداد

المجموعة الوطنية للاستجابة السيبرانية

المهام العامة

- عقد الاجتماعات ربع السنوية لمراجعة حالة الأنشطة وتطبيق الدروس المستفادة وتقييم أداء قدرات إدارة الحوادث السيبرانية على المستوى الوطني.

الأفراد

- تحديد الأعضاء المعنيين الذين يمثّلون المؤسسات المعنية وتزويدهم بالمعلومات المتعلقة بالعملية و إطار عمل الاستجابة للحوادث السيبرانية وخطة الاستجابة للحوادث السيبرانية.

العملية

- إعداد العمليات والبروتوكولات المتبعة لعقد الاجتماعات وإدارة الجوانب اللوجستية بمساعدة المركز الوطني للعمليات الأمنية وتحت قيادة رئيس المجموعة الوطنية للاستجابة السيبرانية.

3.2 الحماية

يُعد اتباع الاستراتيجيات لحماية البنى التحتية للمعلومات الحيوية وتقليص عدد الحوادث جانباً مهماً لإدارة الحوادث. وإذا كانت الضوابط الأمنية غير كافية، قد يزيد حجم الحوادث بصورة تفوق قدرات الاستجابة لها على مستوى الجهة أو القطاع. الأمر الذي قد يؤدي إلى تنفيذ استجابة غير ملائمة، مما قد يفاقم الأثر المترتب على قطاعات البنى التحتية الحيوية في دولة الإمارات. وتوضّح مرحلة الحماية الإجراءات الضرورية للحماية وتقليص عدد الحوادث وتخفيف حدة أثرها قدر المستطاع.

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

المهام العامة

- توفير إطار لإدارة الأصول بما يتوافق مع معايير القطاع، وإدارة الثغرات الأمنية وعمليات زيادة الحماية وتوفير المعلومات حول التهديدات والقدرات الأساسية لمركز العمليات الأمنية، وبما يتضمن المراقبة ومنع عمليات الاختراق وتحديدها.
- إجراء اختبار الاختراق وفقاً لسياسة حماية البنية التحتية للمعلومات الحيوية والمتطلبات الداخلية بعد اتباع أفضل الممارسات القطاعية.
- مواصلة التنسيق مع الجهات المنظّمة للقطاع والمركز الوطني للعمليات الأمنية، وذلك بهدف اكتساب المعرفة حول التغييرات التي تطرأ على السياسة أو الشبكة الوطنية أو التكنولوجيا المستخدمة.

3.2 الحماية

مراكز العمليات الأمنية للقطاع، وفريق الاستجابة لطوارئ الحاسب الآلي

المهام العامة

- مراقبة وتعقب التهديدات، والثغرات الأمنية، والأعطال، وأي محاولات للتسلل، والمساهمة في الحفاظ على الصورة التشغيلية المشتركة على مستوى المركز الوطني للعمليات الأمنية. جمع وتقديم معلومات إضافية من خلال الحصول على البيانات من خلال المراقبة المستمرة، ونتائج تقييم المخاطر، والتحسينات في البنية التحتية والمؤشرات والمقاييس المطوّرة.
- تطوير ومشاركة النصائح والمؤشرات والمحاذير والمعلومات واجراءات التخفيف المُوصى بها باستخدام قنوات الاتصالات المعدّة.
- العمل مع الجهات المعنية في القطاع لتنفيذ عمليات التدقيق الأمنية وعمليات تقييم الثغرات الأمنية، ومستوى الجاهزية والمخاطر وما يتعلق بالبنية التحتية لتحديد نقاط الضعف والثغرات الأمنية (الفنية، والعملية، والموارد البشرية، والقدرات) وتقديم المساعدة المتخصّصة للإصلاح أو التخفيف.
- إجراء الدراسات ونشرها حول أفضل الممارسات لتأمين الشبكات والأنظمة والتطبيقات والتعليم والتدريب وبرامج تعزيز الوعي.
- صياغة وإطلاق أنشطة للتدريب وتبادل المعلومات بهدف إعداد قوى عاملة متخصصة ومدرّبة جيداً في مجال الأمن السيبراني في دولة الإمارات العربية المتحدة.

المركز الوطني للعمليات الأمنية

المهام العامة

- جمع المعلومات من قدرات إدارة الحوادث على مستوى القطاع (مثال: مراكز العمليات الأمنية المتخصّصة بالقطاع وفريق الاستجابة لطوارئ الحاسب الآلي في دولة الإمارات) وفرق الاستجابة للحوادث السيبرانية، ومراكز العمليات الأمنية، و/ أو مراكز العمليات الوطنية. جمع البيانات من خلال أنشطة المراقبة المستمرة للشبكات، وجمع البيانات حول الأنشطة السيبرانية ومراقبتها.
- ضمان حصول الجهات المعنية على معلومات وأخذ إجراءات وقائية وأمنية، وتقديم التوصيات بشأن التغييرات الاستباقية على أصول المعلومات.
- استخدام أدوات التحليل التنبؤي لتحديد وقت أو إمكانية حصول حادث.
- إتاحة المعلومات التنبيهية والتحذيرية وتحديد التغيّرات الخطيرة الناشئة بشكل عام في المجال السيبراني لدولة الإمارات العربية المتحدة.
- تشجيع إجراء عمليات تقييم مستوى الجاهزية والخطورة على مستويي الجهة والقطاع، والتدريب، وتنفيذ تدريبات وتمارين الجاهزية على المستوى الوطني.

3.3 الكشف

تحدّد مرحلة الكشف الأنشطة، والتي تهدف إلى التحديد والتحليل والتحري والتصعيد والإبلاغ عن حادث سيبراني، بالإضافة الى تنظيم استجابة أولية له.

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

المهام العامة

- تُعد الجهات المشغّلة للبنى التحتية للمعلومات الحيوية، ومن خلال استخدامها لقدراتها الأساسية في العمليات الأمنية، على الأغلب أول من يكشف عن الحوادث في شبكاتها وأنظمتها، والتي قد تكون مصدر قلق أو تنبيه لقطاعات البنية التحتية الحيوية أو غيرها ولدولة الإمارات العربية المتحدة، كما لديها معلومات تهديد موثوقة بها تتعلق بنشاط أو حوادث محتملة أو على دراية بالثغرات الأمنية التي تشكّل تهديداً.
- وبمجرد ظهور عامل الشك في موضوع ما أو حالة معينة، تجمع الجهات المعنية معلومات حول النشاط الملحوظ، وتجري تحليلاً لمؤشرات الاختراق، وتبحث عن معلومات مترابطة، وتجري أبحاثاً إضافية لغايات التحقّق؛ والإعلان عن حادث إذا تم التحقّق منه.
- تنفيذ الإجراءات الأولية للاستجابة للحادث (الاحتواء) بناءً على الإجراءات التشغيلية القياسية للجهة، وتحديد الموارد المتأثرة أو التي ستتأثر، بالإضافة إلى تقدير الأثر الحالي والمحتمل للحادث (تقييم الأثر)[5]؛
- وضع أولوية للحادث بناءً على تقييم الأثر وتصنيف الحادث بناءً على الإرشادات والمتطلبات المقدّمة في الملحق 4.1 و وفقا لإطار الاستجابة للحوادث.
- توثيق عملية التحري وجمع الأدلة، بما يتضمن تحضير المعلومات لتستخدم في حالة الحاجة للتصعيد ورفع التقارير.
- الإبلاغ عن الحادث بما يتوافق مع الإرشادات وبناءً على المتطلبات والإجراءات المقدّمة في الملحق 4.1 و وفقا لإطار الاستجابة للحوادث.

3.3 الكشف

مراكز العمليات الأمنية للقطاع، وفريق الاستجابة لطوارئ الحاسب الآلي

المهام العامة

- جمع المعلومات على نطاق القطاع والحفاظ على الوعي بالبيئة السيبرانية وتحليل النشاط الملحوظ على مستوى القطاع، وتحليل مؤشرات الاختراق، والبحث عن معلومات مترابطة، وإجراء بحث إضافي لغايات التحقّق.
- تحليل المعلومات المتوفّرة على مستوى القطاع بناءً على التحليل المختص بالجهة، ودمج معلومات الجهة مع المعلومات الإضافية الواردة عبر قطاع البنية التحتية الحيوية.
- تصنيف الحادث بناءً على الإرشادات وتصعيده إلى المركز الوطني للعمليات الأمنية تماشياً مع متطلبات الإبلاغ.
- تنفيذ الإجراءات الأولية المناسبة للاستجابة للحادث (الاحتواء).
- توثيق عملية التحري وجمع الأدلة، بما يتضمن تحضير المعلومات لتستخدم في حالة الحاجة للتصعيد ورفع التقارير.
- الإبلاغ عن الحادث بما يتوافق مع الإرشادات وبناءً على المتطلبات والإجراءات المقدّمة المقدّمة في الملحق 4.1 و وفقا لإطار الاستجابة للحوادث.

3.3 الكشف

المركز الوطني للعمليات الأمنية

المهام العامة

- بناءً على الصورة التشغيلية المشتركة والمعلومات المبلّغ عنها، يجري تحليل النشاط الملحوظ أو المبلّغ عنه، وتحليل مؤشرات الاختراق، والبحث عن معلومات مترابطة، وإجراء بحث إضافي لغايات التحقّق. يبنى التحليل على المستوى الوطني على مُدخلات على مستوى الجهة والقطاع، والتي تكون معززة بمعلومات أخرى متوفّرة لدى المركز الوطني للعمليات الأمنية.
- وضع تقييم عن الحادث وتصنيفه من خلال تحديد فيما إذا استُوفي شرط أو أكثر حسب المخطط الوطني للتنبيه بالحوادث السيبرانية.
  - الإعلان عن حادث "بالمستوى الثالث" إذا تم التحقّق من ذلك؛
  - في حالة الحاجة ، التصعيد عن طريق مدير المركز الوطني للعمليات الأمنية الذي يقدم توصية إلى رئيس المجموعة الوطنية للاستجابة السيبرانية (CSC) لعقد اجتماع المجموعة مع التركيبة ذات الصلة بناءً على طبيعة ونطاق الحادث ؛ أو
  - في حالة الحاجة ، التصعيد عن طريق مدير المركز الوطني للعمليات الأمنية الذي يقدم توصية إلى رئيس مجلس الأمن السيبراني لرفع مستوى الحادث السيبراني إلى المستوى 2 بعد التنسيق والتشاور مع الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث .
  - تنفيذ الإجراءات الأولية للاستجابة للحادث (الاحتواء) ومساعدة مراكز العمليات الأمنية للقطاع والجهات المعنية بالبنية التحتية للمعلومات الحيوية، بما يتضمن توثيق الأنشطة، بالإضافة إلى:
  - قيادة جهود وأنشطة الاستجابة للحادث خلال مستوى تنبيه "مرتفع"
  - أو مساعدة المجموعة الوطنية للاستجابة للحوادث السيبرانية أو المجلس الوطني للاستجابة للحوادث السيبرانية وقيادة الاستجابة الفنية للحادث إذا تم الإعلان عن حادث سيبراني مهم.
- قد يطلب المركز الوطني للعمليات الأمنية من المعنيين معلومات إضافية من خلال إصدار طلبات معلومات موثّقة أو تقديم معلومات إضافية للمعنيين وذلك بعد بروتوكول إشارة المرور المعروف دولياً.

3.4 الاستجابة

يتمثّل الهدف الرئيسي من مرحلة الاستجابة أولاً في احتواء الحادث. ويهدف الاحتواء إلى منع الحادث من إرهاق الموارد، والحد من أثره المترتب، ومنعه من الانتشار، وإتاحة الوقت لتطوير طريقة مخصّصة للإصلاح. وبعد أن تتم عملية الاحتواء بنجاح، يأتي دور مرحلة التخلص من مكونات الحادث، بما يشتمل على حذف البرامج الخبيثة من خلال تحديد جميع الثغرات السيبرانية التي تم اختراقها والحد من وجودها.

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

خلال المرحلة الطبيعية

- الحفاظ على القدرة على تنفيذ العمليات الأساسية، بالإضافة إلى استثمار القدرات المعيارية لمراكز العمليات الأمنية لدى الجهات في تنفيذ عمليات المراقبة والتقييم ورفع التقارير.
- مراقبة التحليل الذكي للمخاطر وتحسين حالات الاستخدام باستمرار.
- تنفيذ إجراءات الاحتواء والتخلص بما يتماشى مع الإجراءات التشغيلية القياسية لدى الجهات وأفضل الممارسات.
- تأمين وتوثيق الأدلة لأغراض التحريات، والإجراءات التصحيحية، والإجراءات التأديبية المحتملة، و/ أو للملاحقة القانونية.

خلال المستوى الرابع

- التنسيق مع مركز العمليات الأمنية للقطاع والمركز الوطني للعمليات الأمنية من خلال إنشاء قنوات تمكّن من التواصل بفاعلية وبالوقت المناسب، ويتضمن ذلك الاستجابة لطلبات الحصول على المعلومات التي تصدر من أقسام مراكز العمليات الأمنية أو من المركز الوطني للعمليات الأمنية للحفاظ على صورة تشغيلية مشتركة ولتحديد استراتيجيات التخفيف.
- تنفيذ إجراءات التخفيف المحدّدة من قبل مركز العمليات الأمنية للقطاع أو المركز الوطني للعمليات الأمنية لخفض أثر الحادث.

بعد الإعلان عن حادث سيبراني خطير، خلال الحوادث السيبرانية من المستوى الثالث

- المحافظة على التواصل الفعّال والسريع مع المركز الوطني للعمليات الأمنية، ومراكز العمليات الأمنية في القطاع ومجموعة الاستجابة السيبرانية الوطنية، ويتضمن ذلك الاستجابة لطلبات المعلومات وتلبية متطلبات الإبلاغ عن الحادث وتبادل المعلومات.
- تقييم استراتيجيات التخفيف من حدة المخاطر وتنفيذها تحت قيادة المركز الوطني للعمليات الأمنية وإشرافه كما تعتمده مجموعة الاستجابة السيبرانية الوطنية.
- الحفاظ على الدعم العاجل للمستقبل المنظور.

3.4 الاستجابة

مراكز العمليات الأمنية للقطاع

بعد الإعلان عن حادث مهم، وخلال المرحلة بمستوى كارثي

- المحافظة على التواصل الفعّال والسريع مع المركز الوطني للعمليات الأمنية، ومراكز العمليات الأمنية في القطاع والمجلس الوطني للاستجابة للحوادث، ويتضمن ذلك الاستجابة لطلبات المعلومات وتلبية متطلبات الإبلاغ عن الحادث وتبادل المعلومات.
- تقييم استراتيجيات التخفيف من حدة المخاطر وتنفيذها تحت قيادة المركز الوطني للعمليات الأمنية وإشرافه كما يعتمده المجلس الوطني للاستجابة للحوادث.
- الحفاظ على الدعم العاجل للمستقبل المنظور.

3.4 الاستجابة

المركز الوطني للعمليات الأمنية

خلال المرحلة الطبيعية

- الحفاظ على صورة تشغيلية مشتركة ومحدثّة وتبادل المعلومات المفيدة من خلال رفع التقارير وتبادل المعلومات عبر شبكات الارتباط.

خلال المستوى الرابع

- تنسيق وتطبيق إجراءات احتواء التهديدات والتخلص منها، والتعاون مع مركز العمليات الأمنية للقطاع ودعم الجهات المعنية بالبنية التحتية للمعلومات الحيوية المتأثرة من خلال تقديم المساعدة الفنية.

بعد الإعلان عن حادث سيبراني خطير، خلال الحوادث السيبرانية من المستوى الثالث

- تسهيل إجراءات مناسبة لتبادل المعلومات وتعزيز التعاون اللازم بين الشركاء من خلال القنوات المعدّة، وطلب الحصول على تحديثات الحالة والحفاظ على الصورة التشغيلية المشتركة حسب مركز العمليات الأمنية، بما يتضمن المحافظة على لوحات المعلومات التنفيذية لمجموعة الاستجابة السيبرانية الوطنية عند انعقادها.
- يعمل مركز العمليات الأمنية وبالتعاون مع الجهات المتأثرة على تقييم وتحليل المعلومات المتوفّرة ووضع خطة استجابة للحوادث الفنية لتطبيق إجراءات الاحتواء والتخفيف على المستوى الوطني بعد أخذ الموافقة من مجموعة الاستجابة السيبرانية الوطنية عند انعقادها.
- تقديم تقارير دورية للحالة وعرض خطة الاستجابة للحوادث أمام مجموعة الاستجابة السيبرانية الوطنية للموافقة عليها عند انعقادها.
- توفير الدعم اللوجستي وتسهيل عملية اتخاذ القرار ودعم أنشطة الرقابة من مجموعة الاستجابة السيبرانية الوطنية عند انعقادها .
- تنفيذ إجراءات التواصل بناءً على خطة الأزمات الوطنية باتباع نهج التواصل المعمول به مسبقاً والمصمّم خصيصاً للحوادث السيبرانية المهمة والمعتمد من مجموعة الاستجابة للحوادث السيبرانية ، وذلك من خلال جمع وتوزيع المعلومات المرصودة (تعديلها إذا لزم الأمر وبعد التعليمات) حول الحادث باستخدام القنوات المناسبة، بما فيها الارتباط مع الوسائل الوطنية والدولية.
- توفير أو إرسال الدعم العاجل ("فرق خاصة") إلى الجهات المتأثرة للمساعدة في الاستجابة للحادث على المستوى المحلي إذا لزم الأمر.

3.4 الاستجابة

المركز الوطني للعمليات الأمنية

خلال المستوى الثاني

- تسهيل إجراءات مناسبة لتبادل المعلومات وتعزيز التعاون اللازم بين الشركاء من خلال القنوات المعدّة، وطلب الحصول على تحديثات الحالة والحفاظ على الصورة التشغيلية المشتركة حسب مركز العمليات الأمنية، بما يتضمن المحافظة على لوحات المعلومات التنفيذية للجهات المعنية.
- يعمل مركز العمليات الأمنية وبالتعاون مع الجهات المتأثرة على تقييم وتحليل المعلومات المتوفّرة ووضع خطة استجابة للحوادث الفنية لتطبيق إجراءات الاحتواء والتخفيف على المستوى الوطني بعد أخذ الموافقة من مجلس الأمن السيبراني والجهات المعنية.
- تقديم تقارير دورية للحالة وعرض خطة الاستجابة للحوادث أمام مجلس الأمن السيبراني والجهات المعنية للموافقة عليها.
- توفير الدعم اللوجستي وتسهيل عملية اتخاذ القرار ومساعدة الرقابة من من مجلس الأمن السيبراني والجهات المعنية.
- تنفيذ إجراءات التواصل بناءً على خطة الأزمات الوطنية باتباع نهج التواصل المعمول به مسبقاً والمصمّم خصيصاً للحوادث السيبرانية المهمة والمعتمد من جلس الأمن السيبراني والجهات المعنية، وذلك من خلال جمع وتوزيع المعلومات المرصودة (تعديلها إذا لزم الأمر وبعد التعليمات) حول الحادث باستخدام القنوات المناسبة، بما فيها الارتباط مع الوسائل الوطنية والدولية.
- توفير أو إرسال الدعم العاجل ("فرق خاصة") إلى الجهات المتأثرة للمساعدة في الاستجابة للحادث على المستوى المحلي إذا لزم الأمر.

3.4 الاستجابة

المجموعة الوطنية للاستجابة السيبرانية

بعد الإعلان عن حادث سيبراني خطير، خلال الحوادث السيبرانية من المستوى الثالث

- عقد اجتماع لمراجعة الإجراءات المعّدة مسبقاً.
- مراجعة وطلب تحديثات لطلبات المعلومات، وتقديم الإحاطات أو الإيجازات من المركز الوطني للعمليات الأمنية وتقييم متطلبات الموارد اللازمة لإدارة الحادث.
- المراجعة، وإذا تطلب الأمر، التعديل والموافقة على خطة الاستجابة للحوادث المعدّة من المركز الوطني للاستجابة إلى الحوادث.
- المراجعة، وإذا تطلب الأمر، التعديل والموافقة على خطة التواصل المتعلقة بالأزمات.
- التنسيق والإشراف على العمليات الوطنية للاستجابة بناءً على دليل خطة الاستجابة للحوادث المُعتمد.
- التنسيق مع الجهات المعنية على المستوى الوطني وتخصيص الموارد الوطنية للتخفيف من الحادث.

3.5 التعافي

تشمل مرحلة التعافي التطبيق المناسب لإجراءات المعالجة والاستعادة وتأتي بعد خطة الاستجابة للحوادث في الجهات المعنية بالبنى التحتية للمعلومات الحيوية على المستوى الوطني والتي تأثرت بحادثة ما. المهمة الحالية هي إعادة الأنظمة والعمليات إلى حالتها الطبيعية، وضمان عملها ومعالجة الثغرات السيبرانية المستغلة أو المحدّدة بطريقة أخرى لمنع وقوع حوادث مماثلة. وبالنسبة للحوادث على نطاق واسع، قد تستغرق مرحلة الاستعادة والتعافي أشهراً عدة، وبالتالي يجب أن يتمثّل الهدف الأساسي في تعزيز المستوى الأمني بشكل عام وعلى وجه السرعة نسبياً وعمل تغييرات ذات قيمة عالية لمنع الحوادث في المستقبل.

يجب تنفيذ إجراءات التعافي والاستعادة بطريقة تحفظ تكامل النظام وتساعد في عمليات التحليل العميقة والتحريات حول الحادث، بما يتضمن تلبية متطلبات سلسلة حيازة الأدلة والاحتفاظ بالأدلة الأخرى لتمكين الملاحقة القانونية.

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

المهام العامة

- على الجهات المشغّلة للبنى التحتية للمعلومات الحيوية تلبية جميع المتطلبات فيما يتعلق بمشاركة التقارير والمعلومات، بما يتضمن الاستجابة لطلبات المعلومات وتقديم آخر التحديثات دورياً لمركز العمليات الأمنية للقطاع المعني والمركز الوطني للعمليات الأمنية للمساعدة في عملية إصلاح الصورة التشغيلية المشتركة وتقديم نظرة محدّثة حول تطبيق خطة الاستجابة للحوادث.
- تطبّق الجهات المشغّلة للبنى التحتية للمعلومات الحيوية، مستخدمة قدراتها الأساسية في العمليات الأمنية، إجراءات المعالجة والاستعادة كما هو محدّد في الخطة المتفق عليها للاستجابة للحوادث وبالتعاون مع المركز الوطني للاستجابة للحوادث، و المجلس الوطني للاستجابة للحوادث عند انعقاده والسلطات المعنية، لاستعادة الأنظمة والشبكات المتأثرة إلى حالة الاستقرار الطبيعية.
- على الجهات المشغّلة للبنى التحتية للمعلومات الحيوية الحفاظ على سجل مفصّل حول إجراءات الاستعادة والتعافي، وعليها أيضاً الوفاء بالتزاماتها القانونية أو غيرها من سلسلة حيازة الأدلة الإلزامية، وغيرها من التزامات الاحتفاظ بالأدلة، بما يتضمن عملية التوثيق.
- إعادة توزيع الموارد القادمة من المهام الأقل حيوية لتوفير قدرة إضافية للاستعادة والتعافي إذا لزم الأمر.
- إعداد تقييم أولي بالأضرار يشمل تأكيداً بأن الحادث تمت معالجته، وأن جميع الشبكات والأنظمة تعمل طبيعياً.

3.5 التعافي

مراكز العمليات الأمنية للقطاع

المهام العامة

- مراقبة الشبكات والأصول على مستوى القطاع وجمع المعلومات وإبلاغ المركز الوطني للعمليات الأمنية للمشاركة في إصلاح الصورة التشغيلية المشتركة وحالة تطبيق خطة الاستجابة للحوادث.
- إعداد وتقديم المُدخلات حول الاستعادة والتعافي من الحادث السيبراني للمركز الوطني للعمليات الأمنية لإبلاغ صنّاع القرارات لدى مجموعة الاستجابة السيبرانية الوطنية عند انعقاده والسلطات المعنية والمساعدة في إجراءات التحليل والتعافي والاستعادة على مستوى الجهة والقطاع بما يتضمن توزيع الدعم العاجل المتوفّر.

المركز الوطني للعمليات الأمنية

المهام العامة

- مراقبة إدارة الحوادث وجمع المعلومات والحفاظ على صورة تشغيلية مشتركة محدّثة.
- إدارة ومعاينة التنفيذ لأنشطة الإصلاح والاستعادة التقنية المناسبة بعد خطة الاستجابة للحوادث على المستوى الوطني مع توفير الخبرة الفنية والدعم العاجل للعاملين في مركز العمليات الأمنية للقطاع والبنية التحتية للمعلومات الحيوية أو المؤسسات الحكومية للمساعدة في استعادة الشبكات والخدمات المهمة.
- معالجة الحادث بالشكل المناسب والإبلاغ عن مستوى التنبيه للحادث السيبراني (بما يتضمن التخفيف من التصعيد) على المستوى الوطني وللجهات المعنية.
- الاضطلاع بمهام التواصل حسب الإجراءات التشغيلية القياسية وبعدها خطة اتصال الأزمات
- إعداد تقييم أولي بالأضرار.

3.5 التعافي

المجموعة الوطنية للاستجابة السيبرانية

المهام العامة

- تعمل المجموعة الوطنية للاستجابة للحوادث على تنسيق ومعاينة تطبيق خطة الاستجابة للحوادث على المستوى الاستراتيجي، بما يتضمن تنفيذ إجراءات المعالجة والإصلاح على المستوى الوطني خلال وقوع الحوادث السيبرانية من المستوى "الثالث". ويتضمن ذلك التنسيق مع الجهات المعنية وتقديم الدعم العاجل والوطني.
- نظرة عامة على تطبيق خطة التواصل في الأزمات.
- نظرة عامة على تحضير التقييم الأولي للضرر.

3.6 التعلّم والتحسين

تُعد مرحلة التعلّم والتحسين العنصر الأخير في مرحلة إدارة الحوادث السيبرانية بعد أن معالجة الحادث. وتهدف هذه المرحلة إلى جمع المعلومات وتحليلها لفهم ما حدث، ولماذا حصل ذلك، والخروج بخطة يحدّد فيها توصيات للتحسين والتخفيف وضمان منع حدوث نفس الحادث والتخفيف من الثغرات السيبرانية، وبشكل عام تحسين الوضع الأمني السيبراني لدولة الإمارات العربية المتحدة.

الجهة المعنية بالبنى التحتية للمعلومات الحيوية

المهام العامة

- جمع وتحليل البيانات والعمليات المتاحة بالتعاون مع مراكز العمليات الأمنية في القطاع والمركز الوطني للعمليات الأمنية لتقييم الحادث، وتحديد مستوى وطبيعة الإسناد المطلوب إذا أمكن، والعمل على تطوير وتحديث ملفات تعريف التهديد وإعداد تقرير ما بعد الحادث بصورة توثّق النتائج، بما يتضمن الأثر والتقييم المفصّل بالأضرار، وتحديد العيوب وقياسات التخفيف والتحسينات المتعلقة بالعمليات والتعليمات.
- تطبيق التوصيات الواردة في تقرير ما بعد الحادث لمعالجة الثغرات السيبرانية، وذلك بهدف منع حدوث أعطال وأضرار في المستقبل وزيادة حماية الشبكات والأنظمة المتأثرة.
- المشاركة في الأنشطة المعنية بالدروس المستفادة من خلال مساعدة المركز الوطني للعمليات الأمنية في تحليل وتحديد السبب الرئيسي للحادث السيبراني المؤثر والمساعدة في الملاحقة القانونية عند الحاجة.

3.6 التعلّم والتحسين

مراكز العمليات الأمنية للقطاع

المهام العامة

- إجراء تحليل ما بعد الحادث على مستوى القطاع، بحيث يتضمن معرفة المسبب الرئيسي بعد الحادث من خلال إجراء تقييم مفصّل ما بعد الحادث لتقييم إجراءات الاستجابة ومعرفة نقاط القوة ونقاط الضعف والتعديل وتطوير إجراءات تشغيلية جديدة كجزء من بيئة تعليمية متكيّفة ومستمرة. استخدام بيانات تقرير ما بعد الحادث للمساهمة في تحسين العمليات.
- توجيه ودعم أنشطة نقل المعرفة ما بين الجهات المعنية بالمعلومات الحيوية والجهات المنظّمة والمركز الوطني للعمليات الأمنية، وبما يتضمن تطوير سيناريوهات الحوادث المحتملة لأغراض التدريب في المستقبل.
- إعداد نموذج أثر الحوادث في قطاع معيّن وإجراء تحليل للتوجهات لفهم وتوقع التوجهات المستقبلية والسيناريوهات عالية الخطورة.

المركز الوطني للعمليات الأمنية

المهام العامة

- تنفيذ الأنشطة المتعلقة بالدروس المستفادة بالتعاون مع المجموعة الوطنية للاستجابة السيبرانية والجهات المعنية بحسب ما هو مناسب، وإجراء تحليل ما بعد الحادث على المستوى الوطني، بحيث يتضمن تحليل المسبب الرئيسي بعد الحادث من خلال تقييم عمليات الاستجابة وتعديل العمليات كجزء من بيئة تعليمية متكيّفة ومستمرة.
- قيادة جهود تحديد الإسناد على المستوى الوطني والتعاون مع الجهات المعنية في أنشطة المتابعة، ويتضمن ذلك الملاحقات القانونية حسب الحاجة.
- تسهيل نقل المعرفة بين الجهات العاملة ضمن المنظومة السيبرانية لدولة الإمارات العربية المتحدة، وإصدار التوصيات للجهات المعنية بالبنية التحتية للمعلومات الحيوية، ومراكز العمليات الأمنية للقطاع وصناع السياسات.
- إعداد نموذج أثر الحوادث على المستوى الوطني، ويشمل تقييم الاعتماد المتبادل وتنفيذ تحليل للتوجهات لفهم وتوقع التوجهات المستقبلية وسيناريوهات عالية الخطورة.

3.6 التعلّم والتحسين

المجموعة الوطنية للاستجابة السيبرانية

المهام العامة

- تقييم أداء قدرات الإدارة الوطنية للحوادث السيبرانية، بما يتضمن العمليات والسياسات.
- تنفيذ الأنشطة المتعلقة بالدروس المستفادة بعد حصول حادث سيبراني بالمستوى "الثالث"، وذلك لمراجعة المسبب الرئيسي وأثره الفعلي على العمليات والمنظومة السيبرانية لدولة الإمارات العربية المتحدة.
- تقديم التوصيات بشأن التحسينات أو بالتعديلات على خطة الاستجابة للحوادث السيبرانية، ولسياسات دولة الإمارات العربية المتحدة وإمكاناتها في الاستجابة للحوادث السيبرانية.

القسم 4

الملاحق

4.1 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.

4.1 مخطط التنبيه بالحوادث السيبرانية

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 السيبرانية إذا 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.

4.2 نموذج منصة الاستجابة للحوادث لدولة الإمارات العربية المتحدة - السيناريوهات المعتادة للهجمات ودليل المبادئ

يتولى مجلس الأمن السيبراني والمركز الوطني للعمليات الأمنية مهمة قيادة الاستجابة الوطنية للحوادث السيبرانية في دولة الإمارات العربية المتحدة. وفي إطار تنفيذ المسؤولية المنوطة بصفة جهاز وطني رئيسي، يلتزم كلٌ من المجلس والمركز بمهمة بناء مجتمع الاستجابة للحوادث في دولة الإمارات العربية المتحدة استعداداً للحوادث السيبرانية الكبرى وبهدف حماية الأصول السيبرانية الحيوية للدولة. وبالاعتماد على أفضل الممارسات الدولية، تتمثّل إحدى طرق رفع مستوى الاستعداد والجاهزية في إعداد دليل الاستجابة للحوادث، بحيث يهدف هذا الدليل إلى تحديد سيناريوهات الهجوم التي تمت ملاحظتها عالمياً من أجل التخطيط للمستقبل ورفع مستوى الاستعداد وتعزيز عمليات الاختبار والنهج المتبع. وفيما يلي توضيح لنماذج متقدّمة لمنصات الاستجابة للحوادث، فمن الممكن وضع خطط أكثر تفصيلاً وتحسينها خلال التمارين التي تشمل الجهات الفاعلة الرئيسية. ويُمكن لمثل هذه المشاريع أن تساهم إلى حدٍ كبير في رفع مستوى التأهب بشأن الحوادث السيبرانية وزيادة مستوى الوعي بين صنّاع القرارات. ولا تهدف منصة الاستجابة للحوادث إلى الخوض في التفاصيل الفنية ذات المستوى البسيط، بل لنمذجة واختبار الاستجابة الوطنية من منظور حكومي شامل مما يوفّر عملية استجابة موحّدة لحوادث الأمن السيبراني، ويصف العملية من بدايتها إلى نهايتها باستخدام مراحل الاستجابة للحوادث بما يتضمن الإشارة إلى ما إذا كانت المرحلة تشكّل جزءاً تقنياً أو إدارياً من الاستجابة للحوادث.

ومع أن السيناريوهات المذكورة أدناه غير واقعية، إلّا أنها معدّة بناءً على هجمات سيبرانية حقيقية تسببت في خسائر فادحة. ويُمكن أيضاً اعتبار الأدلة الثلاثة أدناه حالات استخدام نموذجية لقدرات الاستجابة الوطنية للحوادث الموضّحة.

4.2 نموذج منصة الاستجابة للحوادث لدولة الإمارات العربية المتحدة - السيناريوهات المعتادة للهجمات ودليل المبادئ

4.2.1 سيناريو الهجوم الأول: محطة تقليدية لتوليد الطاقة تتعرض لهجوم باستخدام برمجيات الفدية

إحدى الجهات المعنية بالبنى التحتية للمعلومات الحيوية (غير حقيقية): محطة توليد طاقة في الإمارات العربية المتحدة

وصف السيناريو: في الساعات الأولى من عطلة عيد الفطر، سجل موظفو محطة توليد الطاقة ومشغلو شبكات الكهرباء الوطنية في الإمارات العربية المتحدة انخفاضاً في الإنتاج من قبل المحطة. وبعد فترة قصيرة تلقى موظفو مركز العمليات الأمنية التابع للبنية التحتية للمعلومات الحيوية لمحطة توليد الطاقة تنبيهات من نظام المعلومات الأمنية وإدارة الأحداث بخصوص تواجد برمجيات خبيثة. وخلال الساعات الثلاث اللاحقة، تعطلت العديد من أنظمة تكنولوجيا المعلومات المهمة أو توقفت تماماً عن العمل.

عملية الاستجابة للحوادث

الكشف

- [الجانب الفني] استناداً إلى تنبيهات نظام المعلومات الأمنية وإدارة الأحداث والتحقيقات الأولية، يعلن مركز العمليات الأمنية الخاص بالبنية التحتية للمعلومات الحيوية لمحطة توليد الطاقة عن وقوع حادث (هجوم برمجيات خبيثة)، ويبدأ في جمع الأدلة (مؤشرات الحادث، والتكتيكات والتقنيات والإجراءات، وتوقيعات الهجوم؛ يُرجى الاطلاع على المعايير الأساسية لمركز العمليات الأمنية فيما يتعلق بالإبلاغ والمشاركة) وثم بدأ في إجراء التحليل الأولي.
- [الجانب الإداري] استناداً إلى تحليلها الأولي والمخطط الوطني للتنبيه بالحوادث السيبرانية، يصنّف مركز العمليات الأمنية الحادث في البداية على أنه "المستوى الثالث" على الأقل، وبالتالي يتم تصعيد الحادث إلى مركز العمليات الأمنية الخاص بالقطاع.

4.2 نموذج منصة الاستجابة للحوادث لدولة الإمارات العربية المتحدة - السيناريوهات المعتادة للهجمات ودليل المبادئ

عملية الاستجابة للحوادث

الاستجابة

- [الجانب الإداري] استناداً إلى المعلومات المتاحة والمخطط الوطني للتنبيه بالحوادث السيبرانية، يعلن مركز العمليات الأمنية عن وقوع حادث "مستوى الثالث".
- [الجانب الفني] يرفع مركز العمليات الأمنية للقطاع (استناداً إلى البروتوكول المحدّد في خطة الاستجابة للحوادث السيبرانية والإجراءات التشغيلية القياسية التفصيلية) التقارير ويشارك المعلومات مع المركز الوطني للعمليات الأمنية الذي يعمل كمركز دمج وطني لإدارة الحوادث السيبرانية ويحافظ على الصورة التشغيلية المشتركة.
- [الجانب الفني] بمساعدة مركز العمليات الأمنية الخاص بالقطاع، يبدأ مركز العمليات الأمنية الخاص بالبنية التحتية للمعلومات الحيوية أنشطة الاستجابة بناءً على الدليل المتوفّر بهدف احتواء الهجوم والتخفيف من حدته.
- [الجانب الفني] يرفع مركز العمليات الأمنية الخاص بالبنية التحتية للمعلومات الحيوية تقريراً وفقاً للمتطلبات (الموضّحة في الملحق (أ) ومتطلبات مركز العمليات الأمنية).
- [الجانب الفني] يبلغ مركز العمليات الأمنية الخاص بالقطاع المركز الوطني للعمليات الأمنية بمعلومات الحادث وفقاً لمتطلبات المشاركة والإبلاغ.
- [الجانب الإداري] يبلغ المركز الوطني للعمليات الأمنية الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث وينسق معها.
- [الجانب الإداري] تقود الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث عملية الاستجابة للحوادث خارج النطاق السيبراني.

التعافي

- [الجانب الفني] بمساعدة مركز العمليات الأمنية الخاص بالقطاع، تنفذ مراكز العمليات الأمنية الخاصة بالبنية التحتية للمعلومات الحيوية خطط استمرارية الأعمال والتعافي من الكوارث بعد النجاح في احتواء الهجوم، كما تنفذ خطة التخلص من المتسبب واسترداد الأصول المتضررة في غضون ساعات قليلة.
- [الجانب الإداري] يعالج مركز العمليات الأمنية الخاص بالقطاع الحادث.

التعلّم والتحسين

- [الجانب الفني] و[الجانب الإداري] تعدّ مراكز العمليات الأمنية الخاصة بالبنية التحتية للمعلومات الحيوية الوثائق التي تشمل الأدلة ذات الصلة، وتجري تحليل ما بعد الحادث وتحدّد الدروس المستفادة (بما يشمل خطوات زيادة الحماية). وتُشارك هذه الوثائق مع مراكز العمليات الأمنية الخاصة بالقطاع.
- [الجانب الفني] و[الجانب الإداري] تشارك مراكز العمليات الأمنية الخاصة بالقطاع الدروس المستفادة مع الأعضاء الآخرين في قطاع البنية التحتية للمعلومات الحيوية عبر القنوات القائمة لمشاركة معلومات الأمن السيبراني (يُرجى الاطلاع على إطار تبادل المعلومات).

4.3 قائمة سياسات ومعايير دولة الإمارات العربية المتحدة المتعلقة بالأمن السيبراني

تشكّل السياسات والمعايير التالية الإطار العام لسياسة حوكمة الفضاء السيبراني لدولة الإمارات العربية المتحدة:

الهيئة/ الجهة	الوثيقة
هيئة تنظيم الاتصالات والحكومة الرقمية	قانون ضمان أمن المعلومات في دولة الإمارات العربية المتحدة.
هيئة تنظيم الاتصالات والحكومة الرقمية	سياسة البنى التحتية للمعلومات الحيوية لدولة الإمارات العربية المتحدة.
هيئة تنظيم الاتصالات والحكومة الرقمية	الإطار الوطني لإدارة مخاطر الأمن السيبراني لدولة الإمارات العربية المتحدة.
هيئة تنظيم الاتصالات والحكومة الرقمية	الاستراتيجية الوطني للأمن السيبراني لدولة الإمارات العربية المتحدة (2019)

4.4 الاختصارات

الاختصارات	الوثيقة
aeCERT	فريق الاستجابة لطوارئ الحاسب الآلي
CII	البنية التحتية للمعلومات الحيوية
CIIP	حماية البنية التحتية للمعلومات الحيوية
CSC	مجلس الأمن السيبراني لدولة الإمارات العربية المتحدة
NCEMA	الهيئة الوطنية لإدارة الطوارئ والأزمات والكوارث
CIRF	اطار الاستجابة للحوادث السيبرانية
NCRG	المجموعة الوطنية للاستجابة السيبرانية
CIRP	الخطة الاستجابة للحوادث السيبرانية
NCSGF	الإطار الوطني لحوكمة الأمن السيبراني
NCSS	الاستراتيجية الوطنية للأمن السيبراني