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

الإمارات العربية المتحدة
وزارة شؤون مجلس الوزراء
مكتب رئاسة مجلس الوزراء

إطار تبادل المعلومات في الأمن السيبراني

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:	12 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

أدى ازدياد عدد الاتصالات ضمن الفضاء السيبراني إلى تحوّلات كبيرة وظهور اقتصاديات أو وفورات الحجم والكفاءات في جميع أنحاء دولة الإمارات العربية المتحدة والعالم. وصاحب هذا النمو الكبير ارتفاعاً ملموساً في مستوى تعقيد المخاطر الأمنية السيبرانية المشتركة. وكدولة رائدة عالمياً في اعتماد وتطبيق تكنولوجيا المعلومات والاتصالات، تواجه الإمارات العربية المتحدة مجموعة خطيرة من الثغرات المعروفة وغير المعروفة في المجال السيبراني، وبالإضافة إلى ذلك، فقد أصبحت التهديدات (الطبيعية والمصنوعة من قبل الانسان، والمتعمدة وغير المتعمدة) أكثر تنوعاً وقدرة، مما أدى إلى ارتفاع في وتيرة وتعقيد وحجم وتبعات حوادث الأمن السيبراني.

يُمكن ملاحظة نمو متزايد بالوعي حول مخاطر الأمن السيبراني وآثاره المترتبة على الأمن الوطني والعالمي، ولذلك تمثّل تبادل المعلومات في الأمن السيبراني عنصراً مهماً في التخفيف من حدة المخاطر المتعلقة بالأمن السيبراني التي تتعرض لها حكومة دولة الإمارات والبنية التحتية للمعلومات الحيوية فيها.

وضع المجلس إطار العمل هذا لإيجاد إطار وطني لتبادل المعلومات في الأمن السيبراني بهدف إضفاء الطابع المؤسسي على هذه العملية ولتشجيع التعاون وتعزيزه بين مختلف الجهات المعنية. ويتماشى هذا الإطار مع الأولوية الوطنية لدولة الإمارات العربية المتحدة بأن تصبح رائدة عالمية في مجال الأمن السيبراني، كما ستساعد هذه السياسة في تحسين الوضع الأمني للمؤسسات والأفراد داخل الدولة.

1.1 الهدف

يشتمل إطار تبادل المعلومات في الأمن السيبراني الوطني على أساليب ثابتة وقابلة للتكرار فيما يتعلق بنقل المعلومات أو الخبرة في مجال الأمن السيبراني من جهة موثوق بها إلى أخرى. كما يقدّم الإطار وصفاً للمعلومات وأنواعها للجهات الرئيسية المعنية بتبادل المعلومات عن التهديدات، ويعمل على رفع مستوى التعاون بين الجهات المعنية في مجال الفضاء السيبراني من خلال بناء الثقة عبر المنظومة وتقليل مخاطر الأمن السيبراني على المستويات المحلية والإقليمية والوطنية والعالمية.

يتمثّل الهدف من الإطار في تعزيز التبادل الآمن والسريع لمعلومات الأمن السيبراني، مثل: المخاطر، والتهديدات، والثغرات الأمنية، والتدابير المضادة، وأفضل الممارسات والدروس المستفادة. ويركّز على تطوير بيئة لامركزية تتميز بالتوزيع (أو التقسيم) والتنظيم، وذلك لتمكين الجهات المعنية من تبادل المعلومات في الأمن السيبراني عبر منظومة آمنة وموحدة، بما يعزز أمن ومرونة مجال الفضاء السيبراني ،حيث يوظف هذا الإطار الممارسات الموجودة ويطورها، ويحدّد أفضل الممارسات المتبعة في تطبيق قدرات تبادل المعلومات الجديدة داخل الدولة.

1.2 النطاق ومدى قابلية التطبيق

تغطي منظومة تبادل المعلومات في الأمن السيبراني مجموعة كبيرة من الجهات المعنية ابتداءً من المستوى الوطني ووصولاً إلى مواطني الدولة. ويتناول الإطار الوظائف الرئيسية للأمن السيبراني على المستوى الوطني ومستوى الإمارة والقطاع وعبر مجموعات متعددة من الجهات المعنية والأطراف المهتمة. ويُمكن تقسيم قابلية التطبيق كما يلي:

الجهات على المستوى الوطني
يحدّد الإطار العناصر الأساسية للتفاعل بين الجهات الاتحادية المسؤولة عن الأمن السيبراني الوطني وعن مستوى المرونة.

الجهات على مستوى الإمارة
يحدّد الإطار دور كل إمارة، والجهات القيادية فيها المسؤولة عن إدارة ووضع ضوابط تبادل المعلومات في الأمن السيبراني داخل تلك الإمارة.

قطاعات البنى التحتية للمعلومات الحيوية
يحدّد الإطار دور كل قطاع، والجهات القيادية فيه، المسؤولة عن إدارة ووضع ضوابط تبادل المعلومات في الأمن السيبراني.

الجهات الأخرى
يعمل الإطار كدليل توجيهي لجميع الجهات (جهات غير متعلقة بالبنى التحتية للمعلومات الحيوية، والشركات الناشئة، والجهات الأكاديمية، ومقدّمي الخدمات) التي تعمل في دولة الإمارات وذلك لتمكينها من المشاركة في الحوكمة الرشيدة للأمن السيبراني داخل الدولة.

الجمهور العام
يمثّل الإطار مرجعاً لممارسات تبادل المعلومات في الأمن السيبراني في دولة الإمارات العربية المتحدة، ويفصّل دور الأفراد داخل المنظومة المعنية بالجهات المعنية في الدولة.

الشركاء الدوليون
يمثّل الإطار مرجعاً لممارسات تبادل المعلومات في الأمن السيبراني في دولة الإمارات العربية المتحدة، ويحدّد الطريقة التي تستطيع بها هذه الجهات المشاركة بصورة أفضل في عملية تبادل المعلومات في الأمن السيبراني داخل المنظومة المعنية بالجهات المعنية في الدولة.

1.3 المبادئ التوجيهية

صُمّم الإطار بناءً على المبادئ الأساسية المذكورة أدناه حرصاً على إيجاد منظومة شاملة ومتكاملة لتبادل المعلومات في الأمن السيبراني في دولة الإمارات العربية المتحدة.

بناء منظومة مؤمنة

تعزيز الثقة بما يضمن اتخاذ الإجراءات بناءً على معلومات الأمن السيبراني المقدّمة وحمايتها أو مشاركتها على النحو المناسب ضمن أطر وإجراءات تبادل المعلومات.

اللغة المشتركة

تحديد البيانات ووضع ضوابط و أطر موحّدة لتبادل المعلومات مما يُمكّن من أتمتة العمليات وتبادل المعلومات بين المؤسسات وبالتالي تشجيع التعاون المتبادل.

الامتثال للقوانين واللوائح التنظيمية

يتوجب على كافة الجهات مراعاة القوانين واللوائح التنظيمية خلال تبادل المعلومات في الأمن السيبراني لضمان الامتثال للمتطلبات وحماية المعلومات الحساسة من الاختراق.

الوعي السيبراني المشترك

الاستفادة من المعرفة الجماعية، والخبرات، والقدرات التحليلية بهدف تحسين القدرات الدفاعية للعديد من المؤسسات المشاركة ضمن مجتمع محدّد.

2 القسم

إطار تبادل المعلومات في الأمن السيبراني

وُضع إطار تبادل المعلومات في الأمن السيبراني لتمكين مشاركة الأفكار والمعلومات المتعلقة بالأمن السيبراني على نحوٍ شبه فوري بين الجهات المعنية، التي تؤدي بدورها في حماية ورفع مستوى مرونة مجال الفضاء السيبراني. وبشكل عام، ستعزز هذه البيئة مقدار الوعي بأهمية الأمن السيبراني وسترفع من مستوى المرونة والجاهزية، وستعمل على تمكين القدرة على الاستجابة للحوادث السيبرانية بفاعلية وبالوقت المناسب، كما ستتوفّر الدعم المستمر للابتكار والنمو.

وسيمكّن هذا الإطار الجهات من فهم ما يلي:

- لماذا نحتاج إلى تبادل المعلومات في الأمن السيبراني (مثال: المزايا)؟
- لماذا نحتاج إلى تبادل المعلومات في الأمن السيبراني (مثال: أنواع المعلومات)؟
- من يحتاج إلى تبادل المعلومات في الأمن السيبراني (مثال: الجهات المعنية المشاركة)؟
- كيف ينبغي تبادل المعلومات (مثال: منصة تبادل المعلومات)؟

2.1 نظرة عامة على إطار تبادل المعلومات في الأمن السيبراني

في سبيل إيجاد بيئة لامركزية، مقسّمة ومنظّمة تمكّن الأفراد عبر مجتمع متنوع من الجهات المعنية من تبادل المعلومات في الأمن السيبراني، من خلال تحقيق التكامل بين الأفراد، والعمليات، والتكنولوجيا اللازمة.

- **الأفراد:** آليات الحوكمة ومجموعات العمل الضرورية لتمكين إقامة علاقات موثوق بها، ولتوجيه عملية اتخاذ القرارات السريعة والمنظّمة والموزّعة اللازمة لحماية الفضاء السيبراني.
- **العملية:** قوانين التبادل، بما يتضمن توضيح معايير وأدوار الجهات المعنية داخل المؤسسات المشاركة وخارجها، والتي تحدّد أيضاً الضوابط التالية (مثال: اتفاقيات عدم الإفصاح عن المعلومات، واتفاقيات صلاحية تبادل المعلومات (ISAA)، ومواثيق الحوكمة لمجموعات عمل تبادل المعلومات وغيرها).
- **التكنولوجيا:** الأدوات، والأنظمة، والبروتوكولات التي توفّر منصات آمنة تعمل على تمكين المرونة والسرعة في تبادل المعلومات وحماية المعلومات الحيوية.

2.1 نظرة عامة على إطار تبادل المعلومات

وبالتالي فإن إطار العمل يتكون من ستة عناصر أساسية تتمحور حول الأفراد والعملية والتكنولوجيا:

عناصر إطار تبادل المعلومات

الأفراد
- الجهات المعنية
- مجتمع تبادل المعلومات

التكنولوجيا
- آلية تبادل المعلومات

العملية
- أنواع المعلومات
- نماذج تبادل المعلومات
- أساليب تبادل المعلومات

2.2 عناصر إطار تبادل المعلومات

الأفراد

2.2.1 الجهات المعنية

يؤثر الأفراد أو الأنواع المختلفة من المؤسسات بحكم اختلاف منظورهم واهتماماتهم واحتياجاتهم إلى حدٍ كبير على تركيبة نظام تبادل المعلومات، وقد يكون لكل من هؤلاء درجات متفاوتة من القدرات، كما أنهم يواجهون أنواع مختلفة إلى حدٍ كبير من التهديدات، ويمتلكون أيضاً دوافع مختلفة عند التعامل مع معلومات الأمن السيبراني.

وفيما يلي الجهات المعنية وأدوارها في منظومة تبادل المعلومات في الأمن السيبراني:

الجهات على المستوى الوطني

تمتلك هذه الجهات مهام اقتصادية وأمنية ترتكز حول واجبها في الدفاع عن أنظمتها ومعلوماتها المصنفة وغير المصنفة، ومحاربة الجرائم السيبرانية، والمساعدة في الحد من المخاطر الأمنية السيبرانية على المواطنين والمقيمين والزوّار في دولة الإمارات العربية المتحدة.

الجهات على مستوى الإمارة

تضع هذه الجهات التوجهات التنظيمية المحدّدة للإمارة بما يتماشى مع قوانين الأمن السيبراني لدولة الإمارات العربية المتحدة، وتعمل عن كثب مع الجهات الوطنية لتوفير نصائح أمنية متخصّصة للجهات التي تتعامل مع حوادث الأمن السيبراني وتعميم التحذيرات الأولية الاستباقية.

وتقدّم الجهات، مثل: هيئة أبوظبي الرقمية ومركز دبي للأمن الإلكتروني، معلومات تتعلق بالتهديدات للجهات الأخرى داخل الإمارات.

البنية التحتية للمعلومات الحيوية

تحتاج قطاعات البنية التحتية للمعلومات الحيوية، والجهات التابعة لها إلى تبادل المعلومات حول الثغرات الأمنية والتهديدات وأفضل الممارسات داخل القطاعات، وعبرها للمساعدة في إعداد ملف مخاطر وطني.

2.2 عناصر إطار تبادل المعلومات

الأفراد

2.2.1 الجهات المعنية

الجهات الأخرى

المؤسسات الخاصة

تهتم الشركات الخاصة بالحفاظ على أمن المعلومات الحساسة، مثل: بيانات العملاء، والأسرار التجارية، ومعلومات العقود، والمعلومات الشخصية وحقوق الملكية الفكرية الأخرى.

شركات تكنولوجيا المعلومات

تهتم الشركات التي توفّر منتجات وخدمات تكنولوجيا المعلومات بالحفاظ على أمن وسلامة ما تقدّمه، لذا فهي تتبادل المعلومات حول الثغرات الأمنية الموجودة في منتجاتها أو خدماتها، حتى تتمكّن الشركات الأمنية من معالجتها، أو قد تعمل هذه الشركات على إنتاج ونشر تحديثات للبرمجيات لتعالج هذه الثغرات الأمنية.

شركات أمن تكنولوجيا المعلومات

تشتمل شركات أمن تكنولوجيا المعلومات على مزوّدي برامج مكافحة الفيروسات، وخبراء الأدلة الجنائية الحاسوبية، ومختبري الاختراقات، وتعمل هذه الشركات على جمع معلومات الأمن السيبراني، كما أنها توفّر خدمات مبنية على تلك المعلومات إلى جهات أخرى في المنظومة.

الجمهور العام

الباحثون في مجال الأمن

يتعقّب الباحثون في مجال الأمن حملات البرمجيات الخبيثة والهجمات المستهدفة ويكتشفون نقاط ضعف في البرامج، والأجهزة والخدمات وذلك من خلال الدراسات الأكاديمية، أو الأعمال، أو عبر الجهود التعاونية والتطوعية أو لإشباع فضول شخصي، وقد يبلغون الجهات المختصة للمساعدة على الحد من التهديدات ومعالجة نقاط الضعف، أو قد ينشروا ما وجدوه علناً.

2.2 عناصر إطار تبادل المعلومات

الأفراد

2.2.2 أطر وضوابط تبادل المعلومات في الأمن السيبراني

يختلف نطاق تبادل المعلومات ويتراوح في حجمه، حيث من الممكن أن يتم على مستوى صغير متمثّل بمجموعات محلية من الباحثين الذين يلتقون ويتواصلون بانتظام لمناقشة التهديدات والثغرات الأمنية، وقد يصل في بعض الأحيان إلى مستويات عالية قد تتضمن تبادل المعلومات الاستخبارية بين حكومات الدول.

وبالتالي، فإن للجهات المعنية دورٌ مهم في تشكيل أطر وضوابط لتبادل المعلومات. تتكون عملية تبادل المعلومات عادةً من مجتمع من الأفراد والمؤسسات، بحيث يجري الاختيار بناءً على خبراتهم وقدراتهم على إحداث التغيير.

تم إنشاء أطر وضوابط تبادل المعلومات في الأمن السيبراني داخل دولة الإمارات العربية المتحدة بحيث تركّز على نطاق عملية تبادل المعلومات في الأمن السيبراني وهدفها العملياتي. وفيما يلي بعض أنواع هذه المجتمعات:

النطاق الجغرافي

أطر وضوابط تبادل المعلومات في الأمن السيبراني على المستوى الدولي: غالباً ما يكون نطاق التهديدات السيبرانية على المستوى الدولي، ولذلك يجب الحرص على تمكين الجهات المشاركة من تبادل المعلومات عبر الحدود. وتشارك الجهات في منتديات ومجموعات ومجتمعات دولية لتتمكّن من الوصول إلى الخبرات والأفكار الأخرى وتبادل المعلومات في الأمن السيبراني حسب نوعها، وحساسيتها وطريقة تبادلها. ويُمكن تحديد وترشيح أعضاء متخصّصين من القطاع الوطني أو قطاع البنية التحتية للمعلومات الحيوية ومن قادة كل إمارة للمشاركة في مثل هذه المنتديات الدولية.

أطر وضوابط تبادل المعلومات في الأمن السيبراني على المستوى الإقليمي: تعمل مثل هذه المجتمعات على دعم برامج تبادل المعلومات لإتاحة الفرصة أمام القطاعين العام والخاص، والشركات المحلية، والجامعات والخبراء للعمل معاً ومناقشة التهديدات والثغرات الأمنية الموجودة في منطقة الشرق الأوسط.

أطر وضوابط تبادل المعلومات في الأمن السيبراني على المستوى الوطني: يشير الدور التنظيمي والأمني لمجلس الأمن السيبراني والعديد من الجهات الأخرى على المستوى الوطني إلى الحاجة إلى إيجاد برامج تبادل المعلومات على المستوى الوطني، حيث أعدت برامج عديدة تعمل على المستوى الوطني بحيث تشمل جميع الجهات الرئيسية لغايات تمكين الجهة المشاركة الطوعية والإلزامية للمعلومات.

2.2 عناصر إطار تبادل المعلومات

الأفراد

2.2.2 أطر وضوابط تبادل المعلومات في الأمن السيبراني

الهدف العملياتي

أطر وضوابط تبادل المعلومات في الأمن السيبراني الخاص بالقطاعات: نظراً لاحتمال وجود تهديدات داخل قطاع معين، يُعد تبادل المعلومات الخاصة بقطاع محدّد وسيلة مهمة لتبادل المعلومات بين الجهات المسؤولة عن البنية التحتية الحيوية داخل ذلك القطاع.

أطر وضوابط تبادل المعلومات في الأمن السيبراني المشترك بين القطاعات: تتكون هذه المجتمعات من جهات تنتمي إلى عدة قطاعات مختلفة وذلك بهدف تعزيز التعاون ضمن عملية تبادل المعلومات من خلال توظيف موارد مرنة وموثوق بها، بالإضافة إلى بناء شبكة موثوقة من الخبراء لتوقع التهديدات السيبرانية وتخفيفها والاستجابة لها.

أطر وضوابط تبادل المعلومات في الأمن السيبراني ذات الاهتمامات المشتركة: تتكون هذه المجتمعات من عدد من الجهات المعنية، بما يشمل المشاركين من القطاع الخاص بهدف تميكن تبادل المعلومات المتعلقة بأفضل الممارسات المتبعة، أو المعلومات حول إجراءات الاستجابة للحوادث الأمنية.

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

العملية

2.2.1 أنواع المعلومات

عادةً تُشارك تسعة أنواع رئيسية من المعلومات من خلال عمليات تبادل المعلومات. ويوضّح القسم التالي طريقة ارتباطها ببعضها، بالإضافة إلى طريقة الاستفادة منها لتحقيق نتائج محدّدة.

التحليل الاستراتيجي

جمع العديد من أنواع المعلومات وتفسيرها وتحليلها لإعداد المقاييس والتوجهات والتوقعات. وغالباً ما تُدمج مع سيناريوهات التوقعات المحتملة التي تستخدم لتحضير صنّاع القرار في الحكومة أو القطاع الخاص للمخاطر المستقبلية. وتستند هذه المعلومات إلى مجموعة متنوعة تشمل الحوادث، وعمليات إثبات المفهوم، والعقائد المؤسسية، وتقييمات المخاطر ويُمكن مشاركتها على قدر الحاجة إلى المعرفة.

أفضل الممارسات

المعلومات المتعلقة بطريقة إعداد البرامج والخدمات وتقديمها، مثل: ضوابط الأمن، وممارسات التطوير والاستجابة للحوادث، وتصحيح البرامج ومقاييس الفاعلية. وقد تختار الجهات مشاركة هذه المعلومات ضمن أطر وضوابط تبادل المعلومات في الأمن السيبراني.

الوعي بالموقف العام

المعلومات التي تمكّن صنّاع القرار من الاستجابة لحادث ما والتي قد تتطلب تتبعاً في الوقت الفعلي لنقاط الضعف والتهديدات النشطة والهجمات. كما يُمكن أن تحتوي على معلومات حول أهداف الهجمات وحالة الشبكات الحيوية العامة أو الخاصة. وعادة يستنبط هذا النوع من البيانات من الثغرات الأمنية، ومن الحوادث، وعمليات التخفيف، والتهديدات، وغيرها، كما يُمكن مشاركتها مع الجميع.

الحوادث

تفاصيل عن محاولات الهجوم والهجمات الناجحة التي قد تتضمن وصفاً للمعلومات المفقودة والتقنيات المستخدمة والهدف منها وأثرها. ويُمكن أن تتراوح شدة الحادث من هجوم تم صده بنجاح إلى هجوم يسبب خطراً كبيراً على الأمن الوطني. ويُمكن مشاركة هذه المعلومات في مجتمعات تبادل المعلومات في الأمن السيبراني المغلقة، ومع الجهات المنظّمة بحسب الحاجة، أو مع الجهات الأخرى التي قد تكون أهدافاً لهجمات مماثلة.

الثغرات الأمنية

الثغرات الأمنية في البرامج أو الأجهزة أو العمليات التجارية والتي يُمكن استغلالها لأغراض خبيثة. ومن المهم جداً أن تُشارك أي معلومات عن الثغرات الأمنية الموجودة في البرامج والتي تتطلب تصحيحاً فورياً، كما ينطبق الأمر نفسه أيضاً على أي معلومات عن أنماط الهجوم الشائعة. وقد تختار الجهات مشاركة هذه المعلومات ضمن مجتمعات تبادل المعلومات في الأمن السيبراني المغلقة أو علناً.

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

العملية

2.2.1 أنواع المعلومات

آليات الحد من المخاطر

أساليب معالجة الثغرات الأمنية، واحتواء التهديدات أو منعها، والاستجابة للحوادث والتعافي منها. وتتضمن الأشكال الشائعة لمثل هذه المعلومات تصحيحات لسد الثغرات الأمنية وتحديثات مكافحة الفيروسات لوقف الاستغلال، وتوجيهات لإزالة أي نشاطات خبيثة من الشبكات. وقد تختار الجهات مشاركة هذه المعلومات ضمن أطر وضوابط تبادل المعلومات في الأمن السيبراني.

الأساليب والإجراءات

تشكّل الأساليب والإجراءات مفهوماً رئيسياً في الأمن السيبراني والتحليل الذكي للمخاطر، فهي تساعد الجهات على تحديد أنماط السلوك التي يُمكن استخدامها للدفاع عن الاستراتيجيات المحدّدة ومسارات التهديد التي تستخدمها الجهات الخبيثة. وقد تختار الجهات مشاركة هذه المعلومات ضمن أطر وضابط تبادل المعلومات في الأمن السيبراني.

التهديدات

يُمكن أن تساعد المعلومات حول التهديدات المتخصّصين والجهات على اكتشاف أو ردع الحوادث، والتعلّم من الهجمات، وإيجاد حلول يُمكنها حماية أنظمتهم وأنظمة الآخرين بصورة أفضل. وقد تُعتبر التهديدات على أنها قضايا لم يتم فهمها بعد والتي يُمكن أن يكون لها تداعيات خطيرة محتملة. وقد تختار الجهات مشاركة هذه المعلومات ضمن أطر وضوابط تبادل المعلومات في الأمن السيبراني.

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

العملية

2.2.1 أنواع المعلومات

مؤشرات الاختراق

تشمل هذه مؤشرات الاختراق أجزاءً من بيانات الأدلة الجنائية، مثل: البيانات الموجودة في مُدخلات أو ملفات سجل النظام، والتي يُمكن أن تساعد المتخصّصين والجهات في تحديد الأنشطة الخبيثة المحتملة على نظام أو شبكة، مثل: الملفات الخبيثة أو عناوين البريد الإلكتروني المسروقة أو عناوين بروتوكول الإنترنت المتأثرة أو عينات البرامج الضارة أو معلومات حول منفذي الهجمات. كحد أدنى، يجب مراقبة مؤشرات الاختراق التالية:

- تسجيل الدخول المشبوه
- زيادات في حجم قراءات قاعدة البيانات
- طلبات غير عادية على نظام أسماء النطاقات
- تصحيح غير متوقع للأنظمة
- تغيير على ملفات تعريف الجهاز المحمول
- وجود حزم بيانات في المكان الخطأ
- ظهور سلوك غير بشري في نسبة استخدام الويب
- علامات لنشاط هجمات الحرمان من الخدمة الموزعة DDoS
- حجم استجابات HTML
- وجود عدد كبير من الطلبات لنفس الملف
- نسبة استخدام غير اعتيادية على منافذ التطبيقات
- نسبة استخدام صادرة غير اعتيادية على الشبكة
- تفاوتات في نشاط حساب المستخدم المتميّز
- تفاوتات جغرافية
- تغييرات مشبوهة في السجل أو ملفات النظام

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

العملية

2.2.2 نماذج تبادل المعلومات

يُمكن أن تضم تبادل المعلومات في الأمن السيبراني التبادلات عند الحاجة والتبادلات المبنية على نظام رسمي طويل الأمد. وتعكس الأساليب المتبعة المتغيرات المختلفة، مثل: مستوى الثقة بين الأطراف، والسلطة القانونية للجهات الفاعلة المختلفة، والعلاقات بين الجهات المعنية. ويتمتع كل نموذج بمزايا خاصة به، لذلك يُعد اختيار النموذج المناسب للغرض أمراً مهماً جداً لتحقيق النجاح. ويركّز القسم التالي على نموذجين من نماذج تبادل المعلومات، وهما: المشاركة الطوعية والإفصاح الإلزامي.

نماذج المشاركة الطوعية

يشجع مجلس الأمن السيبراني الجهات التابعة لقطاع البنية التحتية للمعلومات الحيوية والقطاع الخاص على التبادل الطوعي للبيانات ويعتبره أكثر نموذج تبادل أهمية في منظومة الأمن السيبراني. فمن خلال مشاركتها الطوعية لمعلومات الأمن السيبراني تستطيع الجهات الفاعلة تحديد حاجة أو سبب لتبادل البيانات والبدء في مشاركة واستخدام البيانات الإجرائية القيّمة.

تحدّد الجهات مع من تشارك معلوماتها بناءً على نوع المعلومات المعنية والغرض من تبادل المعلومات في الأمن السيبراني، وتكون هذه المشاركة إما بين جهتين أو مجموعة من الجهات.

وتشمل العوامل المؤدية إلى التبادل الطوعي للمعلومات، على سبيل المثال لا الحصر:

- الإسهام في استجابة أو دفاع وطني جماعي.
- حماية العملاء، والعلامات التجارية، والسمعة، والمنتجات.
- إبلاغ السلطات بالحالات والحوادث والتهديدات المحتملة الخطيرة.
- الإبلاغ عن عمليات الاحتيال السيبراني أو النشاط الإجرامي.

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

العملية

2.2.2 نماذج تبادل المعلومات

نموذج الإفصاح الإلزامي

يتعين الامتثال لنظام ضمان أمن المعلومات الساري في الدولة وغيره من الأطر والسياسات الوطنية ذات الصلة، بالإفصاح عن معلومات الأحداث الأمنية للجهات المنظّمة والسلطات الحكومية أو المستثمرين أو الأفراد المتأثرين، بما يشمل العملاء. وتشمل أنواع المعلومات الواجب مشاركتها مع مجلس الأمن السيبراني على سبيل المثال لا الحصر: الحوادث والثغرات والتهديدات ومؤشرات الاختراق.

يُعد الإفصاح الإلزامي عن المعلومات تواصلاً من اتجاه واحد، ولا يركّز فقط على الإبلاغ نفسه بل أيضاً على الطريقة التي ستستخدم بها المعلومات المجمّعة. ويُحدّد نطاق إلزامية تبادل المعلومات في الأمن السيبراني للتأكد من توظيف البيانات المبلغ عنها في عمليات تحسين الأمن والخصوصية بشكل عام داخل الدولة.

ولذلك تأخذ نماذج الإفصاح الإلزامي عن المعلومات في الاعتبار ما يلي:

- نتائج محدّدة بوضوح، مثل: حماية الخصوصية أو السلامة العامة أو تنسيق الاستجابة أو تحسين الدفاعات الأمنية.
- إيجاد توازن بين المخاطر والفوائد المرتبطة بنشر تفاصيل الحادث.
- نُهج مرنة ومقبولة لتبادل المعلومات وفقاً للإطار الزمني المحدّد.

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

العملية

2.2.3 أساليب تبادل المعلومات

تحدّد جميع أطر وضوابط تبادل المعلومات في الأمن السيبراني أنواع المعلومات التي ستشاركها والظروف التي سيتم فيها مشاركتها، والجهات التي ستشارك هذه المعلومات معها بالضبط. وقد تكون أساليب تبادل المعلومات يدوية أو آلية. وفيما يلي أساليب تبادل المعلومات المتبعة داخل الدولة:

التبادلات الرسمية

يخضع تبادل المعلومات لاتفاقيات مستوى الخدمة (SLAs) واتفاقيات عدم الإفصاح عن المعلومات والاتفاقيات الأخرى التي تحدّد مسؤوليات أعضاء مجتمع تبادل المعلومات في الأمن السيبراني والمؤسسات المشاركة. قد يشمل تبادل المعلومات الرسمي أيضاً متطلبات الإفصاح الإلزامي عن المعلومات للجهات المنظّمة والسلطات الحكومية، أو الأفراد المتأثرين، وفقاً لنظام ضمان أمن المعلومات في دولة الإمارات والسياسات والأطر الوطنية الأخرى.

التبادلات القائمة على التصريح الأمني

يمثّل التبادل القائم على التصريح الأمني مجموعة فرعية من التبادل الرسمي، وهو تبادل أضيق من حيث النطاق والمشاركة. وتحتاج برامج تبادل المعلومات، خاصة تلك التي تتضمن أجهزة استخبارية، إلى تبادل معلومات سرية وحساسة أخرى من خلال قنوات محمية، أو بصورة مباشرة مع طرف واحد.

التبادلات عند الحاجة

لا تتطلب أي اتفاقيات رسمية، حيث تنشر جهات مجتمعات تبادل المعلومات في الأمن السيبراني معلومات التهديد على أساس طوعي وعند الحاجة وتكون مسؤولة على نحوٍ فردي عن التأكد من أن المحتوى المقدّم مناسب للمشاركة.

التبادلات القائمة على الثقة

المجموعات القائمة على الثقة هي مجموعات مغلقة تتكون من جهات لديها اهتمامات مشتركة داخل مجال الأمن السيبراني، حيث تعمل هذه الجهات على تبادل المعلومات فيما بينها في حال وجود قضايا أمنية مشتركة. ولا توجد أي اتفاقيات أو عقود رسمية تحكم تبادل المعلومات بين الأعضاء، ولكن من الممكن أن يتم التبادل وفق أنظمة مخصّصة، مثل: بروتوكول إشارات المرور (TLP).

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

العملية

2.2.3 أساليب تبادل المعلومات

بروتوكول التبادل الآلي الموثوق به للمعلومات الاستخبارية (TAXII)

يُعد بروتوكول التبادل الآلي الموثوق به للمعلومات الاستخبارية (TAXII) الطريقة المفضّلة لتبادل المعلومات الممثّلة باستخدام لغة الهيكل المنظّم لمشاركة معلومات التهديد (STIX)، مما يمكّن المؤسسات من مشاركة معلومات التهديد السيبراني المنظّمة بطريقة آمنة وآلية.

بروتوكول إشارات المرور

يشمل بروتوكول إشارات المرور (TLP) مجموعة من التقسيمات المستخدمة لضمان تبادل المعلومات الحساسة مع الجمهور المناسب. ويستخدم هذا البروتوكول نظاماً من الألوان التي تحدّد الأطراف التي يسمح بتبادل المعلومات معهم، مما يبيّن هدف مصدر المعلومة ويحد من مخاوف الانكشاف. ويعمل بروتوكول إشارات المرور أيضاً على تسريع عملية تبادل المعلومات نظراً لأن المستلمين يعرفون الجهات المسموح تبادل المعلومات معها دون الحاجة إلى الرجوع إلى مصدر المعلومة للحصول على إذن. ويُرجى الرجوع إلى الملاحق.

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

التكنولوجيا

2.2.4 آلية تبادل المعلومات

يُمكن توظيف عدة آليات في عملية تبادل المعلومات بناءً على طبيعة المعلومات والجهات الفاعلة المعنية والقضايا المطروحة. ولتحديد الآلية الأنسب، يجب النظر في مستويات الأتمتة المطلوبة وصيغة المعلومات المتبادلة.

من شخص لآخر

آلية التبادل الأساسية والأكثر فاعلية هي من شخص لآخر (حضورياً أو عبر وسائل الاتصال المرئي)، وفي الكثير من الحالات توجد آليات غير رسمية للتبادل، تحدث أثناء المحادثات غير الرسمية. ويحتاج مجتمع تبادل المعلومات في الأمن السيبراني إلى قنوات اتصال مشفرة معدة لاستخدام هذه الآلية المهمة للتبادل.

من آلة إلى آلة

يساعد استخدام آليات التبادل الآلية في تقليل تكاليف الموارد البشرية، ويُمكن المؤسسات من تبادل معلومات التهديد على نطاق أوسع. يُمكن إنشاء موجز بيانات آلي يُمكن قراءته آلياً لمعلومات التهديد والأمن باستخدام الأدوات المعتمدة في المجال، مثل: الهيكل المنظّم لمشاركة معلومات التهديد (STIX) وبروتوكول التبادل الآلي الموثوق به للمعلومات الاستخبارية (TAXII). وبالتالي، يُمكن تبادل المعلومات عبر القطاعات والمجموعات المختلفة بسرعة شبه فورية تقريباً.

الهيكل المنظّم لمشاركة معلومات التهديد (STIX)

الهيكل المنظّم لمشاركة معلومات التهديد (STIX): لغة موحّدة تم تطويرها بواسطة MITER واللجنة الفنية للتحليل الذكي لمخاطر الإنترنت التابعة لمنظمة أواسيس (OASIS) وذلك لوصف معلومات التهديد السيبراني. صُمّم الهيكل المنظّم لمشاركة معلومات التهديد (STIX) بحيث يُمكّن المستخدمين من وصف المعلومات التالية المتعلقة بالتهديدات:

- الدوافع والمحفزات
- الإمكانات
- القدرات
- الاستجابة

صُمّم هيكل (STIX) بهدف تحسين العديد من القدرات المختلفة، مثل: التحليل التعاوني للتهديدات، والتبادل الآلي لمعلومات التهديد، والكشف الآلي، والاستجابة، وغيرها.

2.2 عناصر إطار تبادل المعلومات في الأمن السيبراني

التكنولوجيا

2.2.4 آلية تبادل المعلومات

ويهدف بروتوكول (TAXII) إلى تقديم المساعدة في أتمتة عمليات أطر وضوابط تبادل المعلومات في الأمن السيبراني الحالية والمساعدة في إنشاء مجتمعات جديدة للمشاركة من خلال تبسيط الجوانب التقنية لتبادل معلومات التهديد السيبراني. وتتضمن نماذج المشاركة التي يدعمها TAXII ما يلي (على سبيل المثال لا الحصر):

المصدر: المُشترِك

يجمع مصدر واحد المعلومات وينشرها للمجتمع، وتكون عادةً على شكل خدمة مراقبة التهديدات والثغرات الأمنية. ويُعد هذا النموذج شائعاً للتنبيهات الواردة من بعض المصادر الموثوقة.

النظام المحوري

النظام المحوري هو النموذج الذي تقوم فيه جهة واحدة على جمع المعلومات من عدة جهات أخرى، حيث تمر المعلومات المشاركة عبر المحور ثم توزّع على الجهات الأخرى.

جهة إلى جهة

تُشارك المعلومات مباشرةً مع جهة واحدة أخرى، وعادةً ما تكون هذه المعلومات مشفرة، حتى لا تتمكن جهات أخرى من اعتراضها.

القسم 3

الأدوار والمسؤوليات المنوطة بالجهات المعنية

يتمثّل الهدف من إطار تبادل المعلومات في الأمن السيبراني الوطني في إعلام وتطبيق وتوجيه أنشطة الجهات المعنية الرئيسية عبر الفضاء السيبراني، بما يتضمن الوزارات ، والجهات، وقطاعات الصناعة، والمؤسسات على المستوى الوطني. وتقود الجهات المعنية الرئيسية تنفيذ العمليات والإجراءات والقدرات الخاصة بتبادل المعلومات في الأمن السيبراني الوطني.

يتعيّن على الوزارات والهيئات والمؤسسات الحكومية التي تستخدم أنظمة حيوية، بما يشمل الأنظمة التي تدعم احتياجات الجهات الحكومية وصنّاع القرار والتي تُعتبر "مهمة جداً" مشاركة معلوماتهم كما هو موضّح أدناه:

مجلس الأمن السيبراني

يتحمل مجلس الأمن السيبراني مسؤولية الدفاع عن الفضاء السيبراني لدولة الإمارات العربية المتحدة وتأمينه، فهو يؤدي دوراً رائداً في تطوير البيئة وتعزيزها وإضفاء الطابع المؤسسي عليها، وكما يعمل على بناء ثقافة الثقة ويحافظ عليها مما يعزز الحاجة إلى المشاركة بمسؤولية. ويشجع المجلس جميع الجهات المعنية على المشاركة، كما يؤدي دوراً فعّالاً في دمج القدرات الحالية لرفع الكفاءات والحد من ازدواجية الجهود. ويشمل دور مجلس الأمن السيبراني المسؤوليات التالية:

1. قيادة منظومة تبادل المعلومات في الأمن السيبراني الوطني.
2. جمع أنواع مختلفة من المعلومات من مصادر متعددة.
3. دمج هذه المعلومات وتحليلها، ومن ثم تحويلها إلى صيغ يسهل فهمها (أي تنفيذ التحليل الاستراتيجي والتكتيكي الذي يُوزّع على الجهات المنظّمة للقطاعات والجهات المشغّلة للبنى التحتية للمعلومات الحيوية والمؤسسات الحكومية) وتوزيعها عبر قنوات النشر المناسبة.
4. توفير الموارد المطلوبة لتطوير آليات تبادل المعلومات في الأمن السيبراني والعمليات والتكنولوجيا لحماية المعلومات من الاستخدام غير المصرح به.
5. تعزيز الشراكات والأنشطة الأخرى مع الدول والمؤسسات الدولية لتسهيل تبادل المعلومات على أساس المصالح المشتركة، بما يشمل تحديد المعلومات الدبلوماسية السرية والحساسة التي سيتم مشاركتها والطرق المتبعة في المشاركة والإجراءات المترتبة عليها.
6. تبادل المعلومات العلنية مع الشركاء الدوليين الذين يدعمون تطور المعرفة بالتكنولوجيا، ويسهلون إعداد الإجراءات والعمليات والقدرات المشتركة للأمن السيبراني.
7. إدارة الوصول إلى منصة تبادل المعلومات في الأمن السيبراني، أي نظام الأنظمة (system of systems) الذي يتيح تبادل المعلومات في الوقت المناسب وبأمان بين الجهات المعنية المشاركة داخل دولة الإمارات العربية المتحدة.
8. دعوة الجهات للمشاركة في منصة تبادل المعلومات في الأمن السيبراني، والنظر في الترشيحات الصادرة من جهات أخرى ترغب في المشاركة، ومن ثم الموافقة على هذه الترشيحات.
9. اعتماد ربط أنظمة وشبكات تبادل المعلومات في الأمن السيبراني المعتمدة من قبل مجلس الأمن السيبراني مع الجهات المشاركة.

3.1 الجهات على المستوى الوطني

تعتبر الجهات الحكومية التي تعمل على المستوى الوطني، مثل: الوزارات والهيئات والمؤسسات الحكومية، التي تشغل أنظمة حيوية في منظومة تبادل المعلومات في الأمن السيبراني الوطني وتتعاون جميعها معاً لتعزيز فهم بيئة تهديد الأمن السيبراني الوطنية.

1. تبادل المعلومات حول الحوادث والتهديدات ونقاط الضعف مع مجلس الأمن السيبراني لتقديم معلومات إضافية حول وضع التهديد الوطني.
2. مشاركة التحليل الاستراتيجي وأفضل الممارسات والتنبيهات والتحذيرات الواردة والتدابير والدروس المستفادة مع مجلس الأمن السيبراني.
3. إصدار طلبات المعلومات للحصول على معلومات إضافية من المؤسسات العاملة في القطاعات العامة والخاصة والحكومية الأخرى في دولة الإمارات العربية المتحدة، إذا لزم الأمر، والرد على طلبات المعلومات المماثلة عند استلامها.

3.1 الجهات على المستوى الوطني

الجهات الرئيسية على مستوى الإمارات

تعتبر الجهات الرئيسية التي تعمل على مستوى الإمارات من الجهات الرئيسية المشاركة في منظومة تبادل المعلومات في الأمن السيبراني الوطني وتتعاون جميعها معاً لتعزيز فهم بيئة تهديد الأمن السيبراني الوطنية.

1. تبادل المعلومات مع مجلس الأمن السيبراني حول حالة الأمن السيبراني في جميع أنحاء الإمارة (بناءً على تقارير محدّدة من قبل الجهات الحكومية) لبناء الوعي بالموقف العام وتسهيل الاستجابة المنسّقة في دولة الإمارات العربية المتحدة.
2. مشاركة المعلومات الواردة (على سبيل المثال: المخاطر الاستراتيجية) و/ أو الاستجابة للحوادث الخاصة بالإمارة (على سبيل المثال: البيانات الخاصة بالحوادث) مع الإمارات الأخرى ومجلس الأمن السيبراني لتسهيل تبادل المعلومات في الأمن السيبراني المشترك بين القطاعات.
3. فيما يلي الجهات الرئيسية على مستوى الإمارات:
   - هيئة أبوظبي الرقمية
   - مركز دبي للأمن الإلكتروني
   - دائرة عجمان الرقمية
   - حكومة الشارقة الرقمية
   - حكومة الفجيرة الإلكترونية
   - الحكومة الإلكترونية في رأس الخيمة
   - حكومة أم القيوين الإلكترونية

3.1 الجهات على المستوى الوطني

قطاعات البنى التحتية للمعلومات الحيوية

تُعد قطاعات البنية التحتية للمعلومات الحيوية من الجهات الرئيسية المشاركة في أطر وضوابط تبادل المعلومات في الأمن السيبراني الخاصة بالقطاع و/ أو مجتمعات تبادل المعلومات في الأمن السيبراني المشترك بين القطاعات. كما يُعد تبادل المعلومات في الأمن السيبراني بين قطاعات البنية التحتية الحيوية أمراً ضرورياً لمواجهة التهديدات المتطورة التي تواجه هذه القطاعات وتعزيز المرونة. وتعمل القطاعات كوسطاء للمعلومات حيث توفّر صورة أشمل على المستوى الوطني ومستوى الجهات.

1. وضع خطط تبادل المعلومات في الأمن السيبراني الخاصة بالقطاع والتي تتمحور حول النقاط القابلة للاستغلال أو الثغرات الأمنية الخاصة بالقطاع.
2. تبادل المعلومات مع الجهات المنظّمة للقطاعات (أو المؤسسات القطاعية الأخرى) لتسهيل فهم وتقييم المخاطر على مستوى القطاع.
3. تبادل المعلومات مع الجهات المنظّمة للقطاعات حول وضع الأمن السيبراني عبر القطاع (بناءً على التقارير الصادرة عن الجهات). وبالإضافة إلى ذلك، تقوم الجهات بالإبلاغ عن الحوادث إلى مراكز الاستجابة للحوادث الخاصة بكل قطاع لبناء الوعي بالموقف العام وتسهيل الاستجابة المنسّقة.
4. تبادل المعلومات التي حصل عليها الجهة المنظّمة للقطاعات للقطاع (على سبيل المثال: المخاطر الاستراتيجية) و/ أو الاستجابة لحوادث القطاع (على سبيل المثال: البيانات الخاصة بالحوادث) مع القطاعات الأخرى لتسهيل تبادل المعلومات في الأمن السيبراني المشترك بين القطاعات.

3.1 الجهات على المستوى الوطني

الجهات الأخرى

يجوز لأي جهة (فرد أو مؤسسة) تتحكم أو تدير موارد المعلومات في دولة الإمارات العربية المتحدة المشاركة في تبادل المعلومات في الأمن السيبراني. وتؤدي جميع هذه الجهات دوراً كبيراً في ضمان الأمن السيبراني لدولة الإمارات العربية المتحدة، وهي مدعوة للمشاركة في إطار تبادل المعلومات في الأمن السيبراني الوطني. ويُمكن لأي جهة ضمن سلسلة التوريد الخاصة بالبنية التحتية للمعلومات الحيوية أن تعتبر نفسها جزءاً من منظومة تبادل المعلومات في الأمن السيبراني الوطني.

1. تحديد احتياجات المعلومات المطلوب مشاركتها والالتزام بأي متطلبات إبلاغ إلزامية.
2. توفير التكنولوجيا والمرافق والموارد اللازمة لحماية المعلومات الواردة من خلال منصة تبادل المعلومات في الأمن السيبراني التي يعتمدها مجلس الأمن السيبراني.

الجمهور العام

من المهم أن يفهم عامة الأفراد في الإمارات العربية المتحدة دورهم في تأمين الفضاء السيبراني الشخصي والمهني، وتطبيق الممارسات الجيدة للحفاظ على الأمن السيبراني (cyber hygiene) في جميع الأوقات لدعم إعداد منظومة سيبرانية أكثر أمناً ومرونة. تشمل مسؤوليات الجمهور العام ما يلي:

1. متابعة معلومات التهديد السيبراني التي تشاركها الجهات على المستوى الوطني.
2. الإلمام بمعلومات الأمن السيبراني المنشورة على منصات التواصل الاجتماعي ومواقع الجهات على المستوى الوطني
3. الإبلاغ عن أي تهديدات أو نقاط ضعف أو مخاطر مُحدّدة.

4 القسم

أنشطة المراقبة وادارة الأداء

يحدّد إطار تبادل المعلومات في الأمن السيبراني الوطني تدابير رصد وتقييم التقدّم المحرز نحو الأهداف التالية:

- تعزيز الشفافية والإدارة الفعّالة لإطار تبادل المعلومات في الأمن السيبراني الوطني؛
- قياس نجاح إطار تبادل المعلومات في الأمن السيبراني الوطني من خلال المقاييس القائمة على الأداء
- تقديم إرشادات للتحسين واتخاذ خطوات التدخل اللازمة عند اللزوم.

سيعمل مجلس الأمن السيبراني مع الجهات المعنية المشاركة في منظومة تبادل المعلومات في الأمن السيبراني الوطني للحصول على ملاحظات حول فاعلية الإطار من خلال منتديات تبادل المعلومات في الأمن السيبراني والعمليات والحلول التقنية وأنشطة التنفيذ، وذلك بهدف تعزيز قدرات إطار تبادل المعلومات في الأمن السيبراني الوطني.

تتطور عملية تبادل المعلومات في الأمن السيبراني بمرور الوقت، حيث تتطلب اكتساب ثقة المشاركين في التقنيات والعمليات المستخدمة في تبادل المعلومات في الأمن السيبراني الأساسية. يُعد تتبع التقدّم المُحرز في التنفيذ وقياس فاعلية منظومة تبادل المعلومات في الأمن السيبراني الوطني أمراً بالغ الأهمية لضمان نجاح النظام. وسيعمل مجلس الأمن السيبراني على قياس فاعلية الأداء واصدار التوصيات بشأن التحسينات في نفس الوقت الذي يجري فيه تنفيذ وتعزيز واضفاء الطابع المؤسسي على منظومة تبادل المعلومات في الأمن السيبراني الوطني على المستوى الوطني.

5 القسم

التنفيذ

يُعد التعليم والتوعية والتواصل من العناصر المهمة لإلهام التغيير اللازم بهدف النجاح في تعزيز تبادل المعلومات في الأمن السيبراني. وسيتواصل مجلس الأمن السيبراني مع المشاركين لتعزيز تبادل المعلومات في الأمن السيبراني كونها أولوية وطنية مؤسسية. ووُضعت العمليات والإجراءات والحلول لدعم جمع المعلومات وتحليلها ونشرها واستخدامها عبر الحدود المؤسسية، لذلك سيعمل مجلس الأمن السيبراني على رفع مستوى الوعي بما يعزز الثقة بين المشاركين. وبالإضافة إلى ذلك، سيعمل المجلس مع الجهات المعنية المشاركة لاعتماد الجهود المبذولة من قبل المؤسسات التي تساهم بمعلومات ينتج عنها حلول وروابط سيبرانية مبتكرة بين مصادر المعلومات المختلفة بما يعزز مرونة الفضاء السيبراني.

القسم 6

الملاحق

6.1 الاختصارات

الاختصارات	التعريف
AES	معيار التشفير المتقدّم
CERT	فريق الاستجابة لطوارئ الحاسب الآلي
CII	البنى التحتية للمعلومات الحيوية
CIA	السرّية والتوفّر والسلامة
DES	معيار تشفير البيانات
FDE	تشفير القرص بالكامل
FLE	التشفير على مستوى الملفات
ICT	تكنولوجيا المعلومات والاتصالات
IoC	مؤشرات الاختراق
IP	بروتوكول الإنترنت
ISE	بيئة تبادل المعلومات
ISAC	مراكز تبادل المعلومات والتحليلات
ISC	مجتمع تبادل المعلومات
ISE	بيئة تبادل المعلومات
ISF	إطار تبادل المعلومات
NCIS	تبادل المعلومات في الأمن السيبراني
SIA	جهاز استخبارات الإشارة
SHA	خوارزمية التجزئة الآمنة
TTP	الأساليب والتكتيكات والإجراءات

6.2 الهيكل المنظّم لمشاركة معلومات التهديد (STIX)

يجب أن تكون عمليات تبادل المعلومات في الأمن السيبراني مرنة بحيث توفّر مجموعة متنوعة من وسائل الاتصال. كما تُعد الاستجابة للاحتياجات المتوقعة للجهات المشاركة والمواقف المحتملة أمراً ضرورياً لتمكين عملية جمع معلومات التهديد.

وستعتمد المنهجية في دولة الإمارات على التحديد والمشاركة والتحليل في الهيكل المنظّم لمشاركة معلومات التهديد، والمعروف باسم STIX، والمبني على تسعة مفاهيم رئيسية:

المفهوم	المعلومات المجمّعة	المعلومات المُشاركة
المشاهدات	ستُجمع الخصائص أو الأحداث المتعلقة بتشغيل شبكات الكمبيوتر، مثل: أسماء الملفات وقيم السجل وقوائم مراقبة عنوان بروتوكول الإنترنت والحقول وسجلات الوصول بالإضافة إلى أنماط الخصائص.	يجب أن تتضمن المعلومات المشتركة كائنات فردية أو أنماط كائن أو كائنات متعددة تشير إلى التهديدات المحتملة أو حملات التهديد أو الخصوم.
المؤشرات	نمط محدّد واحد أو أكثر يُمكن ملاحظته والذي يمثّل البيانات الاصطناعية والسلوكيات موضع الاهتمام. والتي تُدمج مع البيانات الوصفية السياقية التي تشير إلى الأثر المحتمل أو مدى مصداقيتها بين المعلومات الضرورية الأخرى.	يستفيد مجتمع تبادل المعلومات في الأمن السيبراني من فهم الأنماط المرصودة في سياق الأمن السيبراني والتي تشير إلى السلوكيات المهمة.

6.2 الهيكل المنظّم لمشاركة معلومات التهديد (STIX)

المفهوم	المعلومات المجمّعة	المعلومات المُشاركة
الحوادث	أنماط المؤشرات، محدّدة زمنياً ضمن تحقيقات الاستجابة. وتشمل هذه الحوادث الأطراف المعنية، ومستويات الثقة، وسجلات الإجراءات، وغيرها.	تساعد أنماط الحوادث في رفع المستوى الأمني لمجتمعات تبادل المعلومات في الأمن السيبراني وتمكنها من فهم بيئة التهديد بصورة أفضل.
الأساليب والإجراءات المعادية	طريقة عمل التهديدات السيبرانية، والتي تشمل تقنيات وتكتيكات خصوم محدّدين، مثل: تحديد البرامج الضارة والأفراد التي يسهل استغلالهم.	بعد أن تنجح الجهة بربط المعلومات التي تم جمعها بخصم معين تشاركها مع مجتمع تبادل المعلومات في الأمن السيبراني.
الأهداف التي يُمكن استغلالها	الثغرات الأمنية في برامج الجهات أو الأفراد التابعين لها، والتي يتم استهدافها لغايات الاستغلال، حيث تُجمع نقاط الضعف، والثغرات الأمنية الشائعة وإرشادات التعامل معها في اليوم الأول.	ويتم الرجوع إلى قائمة الإعدادات المشتركة، وقائمة نقاط الضعف الشائعة، وإطار الإبلاغ عن الثغرات الأمنية الشائعة عند تبادل المعلومات.
الإجراءات المتخذة	التدابير المتخذة لمواجهة التهديدات سواء كانت ناجحة أو غير ناجحة، أو تصحيحية أو وقائية.	سيجري مشاركة الأثر والتكلفة والفاعلية والتوجهات بهدف تحسين أمن مجتمع تبادل المعلومات السيبرانية.

6.2 الهيكل المنظّم لمشاركة معلومات التهديد (STIX)

المفهوم	المعلومات المجمّعة	المعلومات المُشاركة
الحملات	مجموعات من الحوادث التي تشير إلى أن منفذ الهجمات يعمل على تحقيق هدف معيّن. وتشمل مجموعات من الحوادث ذات الصلة، ترتبط فيما بينها بأنماط متشابهة.	مجموعات الحوادث وسياقها الذي يشير إلى ارتباطها ببعضها، بالإضافة إلى إجراءات التخفيف الناجحة.
منفذو الهجمات	توصيفات الجهات الخبيثة التي تم إنشاؤها بناءً على السلوكيات المرصودة، مثل: الدافع المتوقع، والآثار المترتبة، والأساليب والتكتيكات والإجراءات المعادية، والعلاقات مع منفذي الهجمات الأخرى.	توجيهات التعامل مع المشكلة، ومستوى الثقة، ومصدر المعلومات، بالإضافة إلى السياق والبيانات الوصفية اللازمة لتحسين المعرفة بهيكل منفذ الهجمات في مجتمعات تبادل المعلومات.
التقارير	تعد وثائق تقرير الثغرات الأمنية تلقائياً وفقاً لبروتوكول التبادل الآلي الموثوق للمعلومات الاستخبارية (TAXII)، ويُمكن أن توفّر هذه المعلومات طرقاً متعددة لتبادل المعلومات في الأمن السيبراني، من نظير إلى نظير وإلى النظام المحوري.	تجمع التقارير السياق الذي تمت فيه ملاحظة العوامل الأخرى وتحدّد أسباب ضرورة مشاركتها.

وبناءً على ما تقدّم، يجب على أي مجتمع تبادل المعلومات في الأمن السيبراني يعمل داخل الدولة اتباع كل من أساليب توثيق الهيكل المنظّم لمشاركة معلومات التهديد (STIX) وبروتوكول التبادل الآلي الموثوق به للمعلومات الاستخبارية (TAXII) الخاصة بالحوادث السيبرانية. كما يجب فصل معلومات التهديد المجمّعة ومعلومات التهديد التي سيتم مشاركتها، والظروف التي سيتم بموجبها مشاركتها، وتحديد المستلمين المعتمدين لمعلومات التهديد الخاصة بهم وفقاً لبروتوكول إشارات المرور.

كما يتوجب عليهم مراجعة بروتوكول (STIX) وبروتوكول (TAXII) وبروتوكول إشارات المرور لتقييم المعلومات على النحو المناسب، ومن ثم التأكد من تنقيح معلومات التهديد والبيانات الوصفية على نحوٍ جيد.

6.3 بروتوكول إشارات المرور

يُعد بروتوكول إشارات المرور، الذي يبدأ باللون الأحمر وينتهي باللون الأبيض، أفضل طريقة مستخدمة عالمياً لتحديد تقسيمات تبادل المعلومات المناسبة، إذ تحدّد هذه التقسيمات معلومات التهديد التي قد تكون مناسبة للتوزيع و/ أو المعلومات الأخرى غير المناسبة للتوزيع. وسيعد كل مجتمع تبادل معلومات في الأمن السيبراني تقسيمات خاصة به، والتي ستساعد في تبادل المعلومات.

يحدّد بروتوكول إشارات المرور القيود التي تنطبق على معلومات التهديد. ومع ذلك، تمتلك الجهات المشاركة الحرية في تحديد طريقة تبادل المعلومات المناسبة لها، وذلك ينطبّق أيضاً على باقي المعلومات المشتركة. ويُمكن أن تختار الجهات مشاركة أو عدم مشاركة إجراءات التجميع أو التكنولوجيا المستخدمة، وذلك يعتمد على مستوى بروتوكول إشارة المرور الذي تم اختياره.

ويجب على الجهات أن تحدّد أنواع التقارير التي ترغب في مشاركتها على كل مستوى، بالإضافة إلى تحديد مستوى تبادل المعلومات المرغوب قبل كتابة التقارير ومشاركتها.

اللون	توقيت الاستخدام	آلية المشاركة
بروتوكول إشارات المرور: اللون الأحمر  يمنع مشاركته أو توزيعه، ويقتصر على المعنيين فقط.	يُستخدم بروتوكول إشارات المرور: اللون الأحمر عندما يكون من غير الممكن اتخاذ أي إجراء فعّال بناءً على المعلومات من قبل أي طرف إضافي، ويُمكن أن تؤثر هذه المعلومات على خصوصية الطرف الأصلي أو سمعته أو عملياته في حالة تم استخدامها بشكل غير صحيح.	لا يجوز للمستلم المباشر مشاركة معلومات بروتوكول إشارات المرور: اللون الأحمر مع أي طرف خارج الاجتماع. أو المحادثة الأصلية. وضمن سياق الاجتماع، على سبيل المثال: تقتصر المعلومات على الحاضرين في الاجتماع عند تفعيل بروتوكول إشارات المرور: اللون الأحمر. وفي معظم الظروف، يجب تبادل هذه المعلومات شفهياً أو شخصياً.
بروتوكول إشارات المرور: اللون الأصفر  توزيع محدود يقتصر على المؤسسات التي يعمل بها المشاركون.	يُستخدم بروتوكول إشارات المرور: اللون الأصفر عندما يكون هناك حاجة إلى دعم إضافي لاتخاذ أي إجراء فعّال. ومع ذلك يترتب عليه مخاطر على الخصوصية أو السمعة أو العمليات إذا تم مشاركته خارج المؤسسات المعنية.	لا يجوز للمستلم المباشر مشاركة معلومات بروتوكول إشارات المرور: اللون الأصفر إلّا مع أعضاء مؤسسته، ومع العملاء الذين يحتاجون إلى معرفة المعلومات لحماية أنفسهم أو منع المزيد من الضرر. **يستطيع مصدر المعلومات إضافة حدود إضافية على نطاق المشاركة، والتي من الواجب الالتزام بها.**

6.3 بروتوكول إشارات المرور

اللون	توقيت الاستخدام	آلية المشاركة
بروتوكول إشارات المرور: اللون الأخضر  مشاركة محدودة، تقتصر على المجتمع.	يُستخدم بروتوكول إشارات المرور: اللون الأخضر عندما تكون المعلومات مفيدة لجميع المؤسسات المشاركة . وزملائهم داخل المجتمع أو القطاع الأوسع.	يُمكن للمستلم مشاركة معلومات بروتوكول إشارات . المرور: اللون الأخضر مع زملائه والمؤسسات الشريكة داخل القطاع أو المجتمع، ولكن لا يسمح بمشاركتها عبر القنوات المتاحة للجمهور. ويُمكن تعميم المعلومات من هذه الفئة على نطاق واسع داخل مجتمع معين، ولا يسمح توزيعها خارجه.
بروتوكول إشارات المرور: اللون الأبيض  لا يوجد أي قيود على المشاركة.	يُمكن استخدام بروتوكول إشارات المرور: اللون الأبيض عندما يترتب على تبادل المعلومات مخاطر قليلة أو معدومة فيما يتعلق بسوء الاستخدام، وفقاً للقوانين والإجراءات المعمول بها للتوزيع العام.	يجوز توزيع معلومات بروتوكول إشارات المرور: اللون الأبيض دون قيود، لكنها تخضع لقوانين حقوق النشر. الاعتيادية.