2019

تصنيف حوادث الأمن السيبراني

المحامي الدكتور محمد الذنيبات

الاستاذ المحامي رائد أو العثم

محمود القضاة

تصنيف حوادث الأمن السيبراني

2019

تهدف هذه الورقة إلى تقديم مقترح يتناول تصنيفًا بسيطًا يراعي الطبيعة التقنية والفنية لحوادث الأمن السيبراني على المستوى الاستراتيجي والاجتماعي والسياسي والإقتصادي في الأردن. مستندين – في هيكلية الورقة وموضوعها – على " Cybersecurity Incident Taxonomy " لسنة 2018 [1]، و" تصنيف المركز الوطني الامريكي للأمن السيبراني [2] " وعلى قانون الأمن السيبراني الأردني لسنة 2019.

تستهدف هذه الورقة الخبراء القانونيين في المملكة الأردنية الهاشمية والعرب عموما، بالإضافة إلى خبراء الأمن السيبراني والباحثين فيه على الصعيدين المحلي والعربي.

تكمن الغاية من إعداد وتقديم مقترح التصنيف هذا إلى أن يتم استخدامه/الاستعانة به لغرض أنشطة تنسيق الاستجابة للحوادث على المستوى الوطني والعربي. بالاضافة إلى تفعيل دور المركز الوطني للأمن السيبراني من خلال تفعيل دوره الوظيفي والتنسيقي والرقابي المتمثل باستلام وتنقيح "الإخطارات المتصلة بحوادث الأمن السيبراني " والمرتبط " بإتخاذه التدابير والاجراءات اللازمة للوقاية والتعامل مع مخاطروحوادث الأمن السيبراني ".

استندت هذه الورقة في جانبها القانوني إلى قانون الأمن السيبراني الأردني لسنة 2019 بالاضافة إلى الدراسة التحليلية النقدية لقانون الأمن السيبراني الأردني (والتي عمل عليها الدكتور محمد الذنيبات في دراسة متخصصة تناول فيها الاطار المفاهيمي والموضوعي للقانون).

يكمن نطاق هذا التصنيف في حوادث الأمن السيبراني التي: " تؤثر على أمن الشبكات ونظم المعلومات، في أي قطاع من قطاعات المجتمع ". لتشمل بذلك الحوادث التي لها تأثير كبير على الخدمات: (الأساسية والرقمية – الاتصالات الإلكترونية – الثقة وتحديد الهوية ...).

وتتمثل أهميته في التعرف على التهديدات والمخاطر والحوادث السيبرانية الأمر الذي من شأنه تحديد أسس واليات الوقاية (استباقيا) و/أو المعالجة/التعاطي مع الحوادث السيبرانية بصورة تضمن حماية الأمن الوطني ومصالح الدولة والهيئات والشركات والافراد. بالاضافة إلى توفير الادوات والاجهزة وتأهيل الكوادر البشرية لمواجهة هذه التهديدات والمخاطر والحوادث.

[1] Cybersecurity Incident Taxonomy, http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

[2] NCCIC Cyber Incident Scoring System, https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

التنظيم القانوني لتصنيف حوادث الأمن السيبراني في الأردن

حدد مجلس الوزراء الموقر الأسباب الموجبة لقانون الأمن السيبراني في كتابه المرسل الى مجلس الأمن الموقر بتاريخ 2019/6/17، والذي تناول فيه الإطار العام للأسباب التي دعت إلى ضرورة توفير حماية قانونية للأمن السيبراني (والفضاء السيبراني) على الصعيد الوطني. وما يعنينا ويتصل بموضوع هذه الورقة الأسباب التالية:

- حماية المملكة من تهديدات حوادث الأمن السيبراني
- رفع مستوى الأمن الوطني العام والشامل للمؤسسات والافراد وتطوير قدرات ردع ومراقبة وانذار واستجابة لحوادث الأمن السيبراني والتخفيف من الاضرار الناجمة عنها
- خلق بيئة أمنة وجاذبة للاستثمار ومحفزة للاقتصاد الوطني خاصة في ظل تسارع التطور في أنظمة المعلومات والبنى التحتية وتنامي حجم الخدمات الحكومية
- لمراقبة الفضاء السيبراني الوطني ورصده وتوثيق حوادث الأمن السيبراني

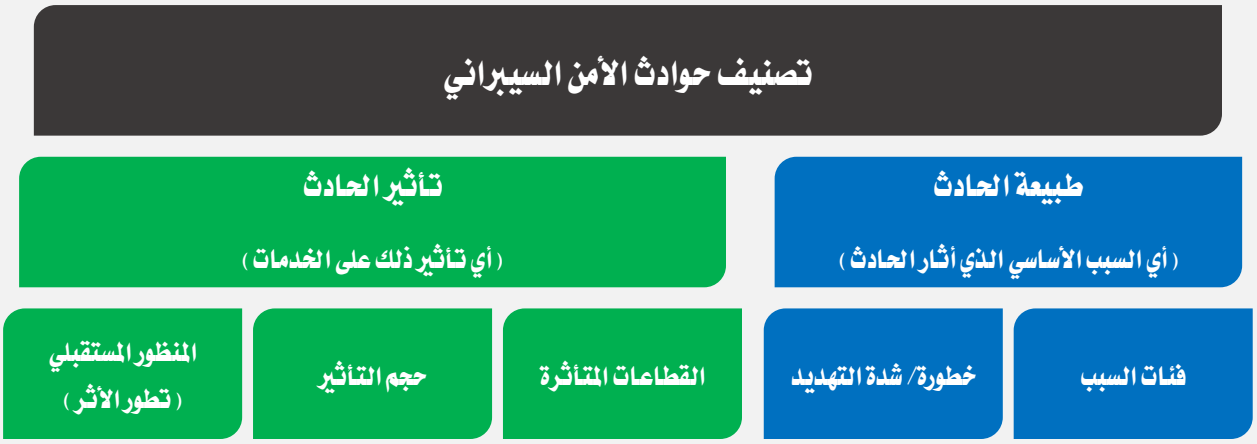
إلا أن المشرع لم يعالج في قانون الأمن السيبراني الأردني المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والأثر والتصنيف. الأمر الذي من شأنه التأثير على ضمان الحماية المقررة أو المرجوة للأمن السيبراني وسلامة الفضاء السيبراني الأردني.

لذا كانت هذه الورقة مدخلا للتعرف على طبيعة تصنيف حوادث الأمن السيبراني واتصالها بقطاعات الخدمات العامة والخاصة، واليات التعامل مع التهديد السيبراني وحوادث الأمن السيبراني ومعالجة اثارها وتأثيرها في هذه القطاعات. ليتم ذلك من خلال تقسيم الورقة - من حيث الموضوع - إلى قسمين، نتناول في القسم الأول الإطار الفني والتقني لتصنيف حوادث الأمن السيبراني، ثم نتناول في القسم الثاني الإطار القانوني لتصنيف حوادث الأمن السيبراني.

القسم الأول: الإطار الفني والتقني

التصنيف (تصنيف حوادث الأمن السيبراني والتهديدات السيبرانية)

تناول التصنيف الأوروبي للأمن السيبراني تصنيف حوادث الأمن السيبراني على جزئين جوهريين، هما:



أولا: طبيعة حادث الأمن السيبراني:

يستخدم الجزء الأول من التصنيف: لتصنيف طبيعة الحادث، أي: (تحديد نوع التهديد الذي أثار الحادث، وشدة هذا التهديد).

1. فئات أصل/مصدر السبب:

يتم استخدام فئة مصدر السبب للإشارة إلى نوع الحدث أو التهديد الذي تسبب في وقوع الحادث. وفي هذا السياق عدد التصنيف الأوروبي هذه الفئات، وتناولها على خمس فئات، كالاتي:

فشل النظام

- إذ يرجع الحادث إلى فشل في النظام، (أي أن السبب راجع إلى مصدر داخلي وليس هناك أسباب خارجية لذلك الفشل). ومثال ذلك: حدوث عطل في الأجهزة أو خلل في البرنامج أو خلل في إحد ى الإجراءات أو ما إلى ذلك.

الظواهر الطبيعية

- إذ يرجع الحادث إلى ظاهرة طبيعية. ومثال ذلك: تسبب عاصفة – أو التوهج الشمسي، أو فيضان، أو زلزال، أو حرائق ... إلخ – في إثارة الحادث.

الأخطاء البشرية	• إذ يرجع الحادث إلى خطأ بشري، أي أن النظام خال من أي خطأ أو عيب ويعمل بشكل صحيح، ولكن تم استخدامه بشكل خاطئ. ومثال ذلك: قيام شخص بخطأ أو إهمال أدى لوقوع لحادث.
الأفعال الخبيثة/الضارة	• إذ يرجع الحادث إلى عمل ضار. ومثال ذلك: تسبب الهجوم الإلكتروني – أو الهجوم المادي أو تخريب للمتلكات أو أي عمل تخريبي أو أي هجوم من الداخل أو سرقة وما يمكن قياسه على ذلك – في إثارة الحادث.
إخفاقات /فشل الطرف الثالث في تقديم خدماته	• إذ يرجع الحادث إلى اخلال أو انقطاع خدمة طرف ثالث (المؤسسات الخدماتية). ومثال ذلك: تسبب انقطاع التيار الكهربائي – أو انقطاع الإنترنت ... الخ – في إثارة الحادث.

2. شدة التهديد:

يتم استخدام شدة التهديد للإشارة – من منظور تقني – إلى التأثير المحتمل والمخاطر المرتبطة بالتهديد. ليصار إلى قياس حدة ودرجة التهديد للحادث من خلال التعرف على مصدر السبب (سواء أكان فشل في النظام أو بفعل بشري أو بفعل هجوم سيبراني ...) وتقييم أثره على القطاعات المتأثرة، من خلال مقاييس تبين حدة /شدة الخطورة أو التهديد:

أ. شدة عالية/مرتفعة، التأثير المحتمل مرتفع. (مرتفع)

ب. شدة متوسطة، التأثير المحتمل متوسط. (متوسط)

ج. شدة منخفضة، التأثير المحتمل منخفض. (منخفض)

كما نوه التصنيف الاوروبي الى أن على الجهات المعنية مراعاة بعض العوامل لدى تقييم شدة التهديد، ومن هذه العوامل:

أ. دراسة المخاطر بالنسبة للدولة أو الشركات أو الافراد.

ب. حجم الجهد المطلوب أو التكاليف اللازمة للتخفيف أو للحماية أو لمعالجة التهديد أو الخطر.

ج. مقدار الأضرار المحتملة للدولة أو الشركات أو الأفراد، والتي يمكن أن يكون سببها التهديد.

د. قياس حجم ومعدل انتشار التهديد (عدوانيته).

ه. استمرارية الهجمات (العدد والتكرار ...).

و. أهمية الأنظمة التي يحتمل تأثرها بالتهديد أو الحادث. وغيرها من العوامل المتعلقة بتقييم شدة تأثير التهديد.

ثانيا : تأثير/ أثر حادث الأمن السيبراني

يستخدم الجزء الثاني من التصنيف لتصنيف تأثير الحادث، (أي تأثيره على الخدمات، في أي قطاع من قطاعات الاقتصاد وا لمجتمع).

1. القطاعات المتأثرة

يتصل دراسة أثر حوادث الأمن السيبراني بتأثيرها على الخدمات التي تقدمها القطاعات العامة - أو الخاصة - في الفضاء السيبراني. ومن القطاعات الهامة – على سبيل المثال - التي يجب أن تكون محلا للاعتبار لدى النظر في أثر حوادث الأمن السيبراني القطاعات التالية :

أ. **الخدمات المتصلة بالقطاعات السيادية.**

ب. **الخدمات العامة.**

ج. **الخدمات الحكومية.**

د. **الخدمات ذات الطابع الحساس (خدمات الثقة وتحديد الهوية).**

ه. **الخدمات الرقمية.**

و. **خدمات الاتصالات.**

2. شدة التأثير/الأثر

يتم قياس شدة التأثير للتعرف على وتقييم الأثر الناجم عن الحادث في ا لمجتمع والاقتصاد...الخ. الامر الذي يتطلب الأخذ في العوامل التي يجب مراعاتها عند تقييم شدة التأثير:

أ. **المخاطر على صحة وسلامة السكان ، ومثال ذلك: التأثير على خدمات الطوارئ**

ب. **التأثير على الاقتصاد وا لمجتمع ، ومثال ذلك: التسبب في خسائر كبيرة**

ج. **الأضرار والتكاليف للمواطنين و/أو المنظمات/المؤسسات/الشركات المتضررة**

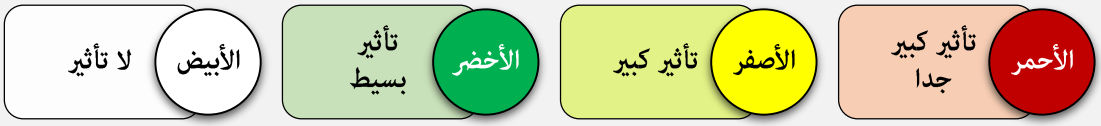
د. **اضطراب الحياة اليومية**

ه. **الآثار المتتالية في القطاعات الحرجة**

و. **تأثير وسائل الإعلام والتغطية**

ز. **التأثير السياسي والأهمية**

يتبع التصنيف الأوروبي في قياس التأثير/الأثر النظام التالي:



كما أصدرت مراكز الأمن السيبراني الفيدرالية في الولايات المتحدة الأمريكية مخططا يتناول شدة الحوادث السيبرانية [3]، اعتمدت فيه العناصر التالية:

التعريف العام	
المستوى 5 – حالة طوارئ – (أسود)	• يشكل تهديداً وشيكًا لتوفير خدمات البنية التحتية الحيوية واسعة النطاق، أو الاستقرار الحكومي الوطني، أو لحياة الأشخاص الأمريكيين
المستوى 4 – شديد – (أحمر)	• من المحتمل أن ينتج عنه تأثير كبير على الصحة أو السلامة العامة أو الأمن القومي أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية.
المستوى 3 – مرتفع – (البرتقالي)	• من المحتمل أن ينتج عنه تأثير واضح على الصحة أو السلامة العامة أو الأمن القومي أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية أو ثقة الجمهور.
المستوى 2 – متوسط – (الأصفر)	• قد يؤثر على الصحة العامة أو السلامة أو الأمن القومي أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية أو ثقة الجمهور.
المستوى 1 – منخفض – (أخضر)	• من غير المحتمل التأثير على الصحة أو السلامة العامة أو الأمن القومي أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية أو ثقة الجمهور.
المستوى 0 – خط الأساس – (أبيض)	• حدث لا أساس له أو غير منطقي.

3. التوقعات/النظرة المستقبلية للحادث (تطور الأثر)

ويراد بها النظرة المستقبلية للحادث وقياس تطوره (التكهنات/التوقعات)، للساعات/الأيام القادمة، مع مراعاة التأثير على الخدمات – على المجتمع و / أو الاقتصاد، وفق التصنيف التالي:

أ. (تحسن في الوضع). من المتوقع أن تنخفض شدة التأثير في الساعات/الأيام القادمة.

ب. (أن يكون الوضع مستقرا). من المتوقع أن تظل شدة التأثير كما هي خلال الساعات/الأيام القادمة.

ج. (أن يحصل تفاقم في الوضع). من المتوقع أن تزداد شدة التأثير في الساعات/الأيام القادمة.

[3] Cyber Incident Severity Schema,
https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf

القسم الثاني: الإطار القانوني

تكمن الغاية من بيان الإطار الفني والتقني – القسم الأول – في الاستناد اليها في صياغة ووضع الأحكام والضوابط والمعايير القانونية، والتي تمثل الركيزة والمرجع الأساس للجهات المعنية في المملكة (المجلس الوطني والمركز الوطني للأمن السيبراني) لضمان حماية الأمن السيبراني الوطني.

وبالرجوع إلى ما سبق بيانه، وباستقراء قانون الأمن السيبراني الأردني، نجد أن القانون لم ينظم المسائل التقنية والفنية لحادث الأمن السيبراني من حيث الطبيعة والأثر والتصنيف (كما تم تناوله في القسم الأول من الورقة).

ومن خلال النظر في الإطار التقني والفني لتصنيف حادث الأمن السيبراني، يتبين لنا أن على المشرع الأردني الأخذ في الاعتبار ضرورة معالجة هذه الجوانب في إطار قانوني. <u>الأمر الذي سيساعد الدولة في</u>:

ضمان حماية أمن المملكة السيبراني وسلامة الفضاء السيبراني الوطني

تسهيل اجراءات التحقيق والمراقبة والتحري والتنسيق (من خلال الاستعانة بمعايير ومؤشرات التصنيف للتعرف على طبيعة وأثر وحجم التهديدات والحوادث السيبرانية).

العمل على حصر المستلزمات المادية - (الادوات والاجهزة ...) - المطلوبة لمواجهة حوادث الأمن السيبراني والاستعداد لها والوقاية منها ومن أثرها.

ولإستكمال الاطار القانوني لما سبق ذكره، نورد المقترحات القانونية المتصلة في الجوانب التقنية والفنية لتصنيف حادث الأمن السيبراني، وفق الاتي:

أ. المقترحات العامة

1. بيان وتنظيم حوادث الأمن السيبراني بصورة دقيقة وواضحة تراعي الطبيعة الفنية والتقنية لها، وتراعي تصنيفها واليات التعامل معها (من حيث طبيعة وحجم الخطر والتأثير والقطاعات المتأثرة بالحوادث ...).

إذ أن المشرع لم يتناول هذه المسائل في القانون، إنما اكتفى في المادة (9) بتنظيم إطار عام (غير واضح) يبين الإختصاص الهيكلي (الاداري) للمجلس الوطني للأمن السيبراني في تحديد حوادث الأمن السيبراني وصلاحيات المركز الوطني للأمن السيبراني في الاستجابة لها!

أ. يحدد حادث الأمن السيبراني الذي يشكل خطرا على أمن المملكة وسلامتها بقرار من المجلس بناء على تنسيب رئيس المركز.

ب. يكون المركز مسؤولا عن إدارة وتوجيه الاستجابة لحوادث الأمن السيبراني المشار اليها في الفقرة (أ) من هذه المادة وتلتزم الجهات كافة بالتعليمات والتوجيهات التي تصدر عن المركز.

2. تحديد معايير قياس مناسبة لتكون المرجع الأساس للجهات المعنية (المجلس والمركز الوطني للأمن السيبراني) لتصنيف حوادث الأمن السيبراني على الصعيد الوطني وفق أسس واضحة لا تدع مجالا للاجتهاد أو للتجاوز أو التغول أو التشدد، ولتكون مرجعا واضحا للأفراد والشركات والمؤسسات وكل معني في تقديم خدمات أو استخدام الفضاء السيبراني الوطني (بوضوح وشفافية درء لأي غموض أو ضبابية أو المساس بحقوق المستخدمين أو الحد من تلك الحقوق).
3. تحديد وحصر فئات التأثير المحتملة لتكون المرجع والاداة التي تسمح للمركز الوطني للأمن السيبراني من تقييم شدة المخاطر وأولوية الحوادث وحجمها وأثرها – من منظور وطني.
4. العمل على تدابير واضحة تعنى بحماية الأمن السيبراني الوطني، تراعي فيها الطبيعة الفنية والتقنية لحوادث الأمن السيبراني واثارها على القطاعات العامة والخاصة وتصنيفها.

ب. المقترحات المتخصصة :

1. أن تراعي أسس التصنيف الطبيعة التقنية والفنية للحادث وربطه بالقطاع المتأثر به. ومثال ذلك: أن يعمل المركز الوطني على تصنيف الحوادث وفق طبيعة القطاعات المتأثرة على الصعيد الوطني. لتكون بذلك قد راعت طبيعة عمل هذه القطاعات ومدى أثر التهديد أو الحادث في التأثير على تقديم خدماتها اقتصاديا واجتماعيا. ونقترح – هنا – أن يصار إلى تصنيف القطاعات الأساسية والحيوية في المملكة وفق الاتي:

* الخدمات المتصلة بالقطاعات السيادية. وتشمل (الديوان الملكي والقطاعات العسكرية والامنية والدفاع وما يقاس عليها / يتصل بها)
* الخدمات العامة. وتشمل قطاعات (الطاقة – الصحة – النقل – المالية – المياه – البنية التحتية الرقمية...)
* الخدمات الحكومية. وتشمل (الإدارات العامة...)
* خدمات الهيئات المستقلة. وتشمل (الانتخابات أو حقوق الانسان ...)
* الخدمات ذات الطابع الخاص (خدمات الثقة وتحديد الهوية). وتشمل (سلطات إصدار الشهادات، أو أنظمة الهوية الإلكترونية، أو البطاقات الذكية ...)
* الخدمات الرقمية. وتشمل (الخدمات السحابية، وأماكن الأسواق عبر الإنترنت، ومحركات البحث عبر الإنترنت...)
* خدمات الاتصالات.

وتجدر الاشارة هنا إلى ضرورة العمل على معايير وضوابط من شأنها إزالة أي لبس أو تداخل في الأثر لأي حادث من شأنه المساس في أكثر من قطاع.

2. أن يصار إلى بيان وتحديد أنظمة المعلومات/البنية التحتية الحرجة/الحساسة للدولة (من حيث المفهوم والطبيعة والاثر المحتمل/الناجم عن الحادث السيبراني المتصل بها).

يقصد بأنظمة المعلومات الحرجة/الحساسة: " أنظمة المعلومات التي تتأثر، في حال وقوع حادث [تسلل ، اختطاف التحكم التشغيلي، تحريف/تغيير، انقطاع، توقف، شلل، هجوم أو تدمير]، بصورة تعرض أمن الشبكات [الأمن السيبراني] لخطر كبير وحرج. يمس الأمن الوطني ". وتشمل أنظمة المعلومات الحرجة/الحساسة الاتي:

* أنظمة المعلومات العسكرية والأمنية والدبلوماسية وما يمكن القياس عليها.
* أنظمة المعلومات التي تخزن وتعالج المعلومات المصنفة على أنها أسرار للدولة.
* أنظمة المعلومات التي تخدم تخزين وحفظ البيانات ذات الأهمية الخاصة بالنسبة للدولة أو الشركات أو الهيئات.
* أنظمة المعلومات التي تخدم حفظ وتصنيع وإدارة المرافق المتصلة بالأمن الوطني.
* أنظمة المعلومات الحساسة (الحرجة) التي تخدم تشغيل المؤسسات والهيئات المركزية (للدولة).
* أنظمة المعلومات الوطنية المتصلة بقطاعات الطاقة، والتمويل، والخدمات المصرفية، والاتصالات، والنقل، والموارد الطبيعية والبيئة، والمواد الكيميائية، والصحة، والثقافة، والإعلام.

3. أن يصار إلى وضع أطر عامة في القانون تنظم وتتناول أسباب/مصادر التهديدات والحوادث السيبرانية.

* فشل النظام.
* الأخطاء البشرية.
* الأفعال الضارة.
* الكوارث الطبيعية.
* فشل الطرف الثالث في تقديم خدماته.

4. ضرورة بيان المقصود – من حيث الماهية والطبيعة والغاية – بتقييم الأمن السيبراني في القانون.

يقصد بتقييم الأمن السيبراني:

" نشاط استعراض وتقييم محتويات و عناصر الأمن السيبراني من أجل توفير الأساس/الركيزة لأجل اتخاذ قرار بشأن إنشاء أو تحديث أنظمة المعلومات ".

5. ضرورة بيان المقصود – من حيث الماهية والطبيعة والغاية – بتدقيق الأمن السيبراني في القانون.

يقصد بتدقيق الأمن السيبراني:

" نشاط تحديد حالة الأمن السيبراني الفعلية لأنظمة المعلومات وبنيتها التحتية أو المعلومات المخزنة والمعالجة والمرسلة عليه/عبره، بهدف منع وكشف ومعالجة أي تهديد للأمن السيبراني واقتراح خطط و تدابير من شأنها ضمان التشغيل الطبيعي لهذا النظام ".

6. أن تراعي أسس التقييم الأولويات الوطنية لحماية الأمن السيبراني. ومثال ذلك:

تصنيف حوادث الأمن السيبراني

خط الاساس – (لا تهديد). أو

طفيف – (حادث أولوية طفيفة : وجود إمكانية للتأثير مما يتطلب القيام بالتحري والتدقيق.)

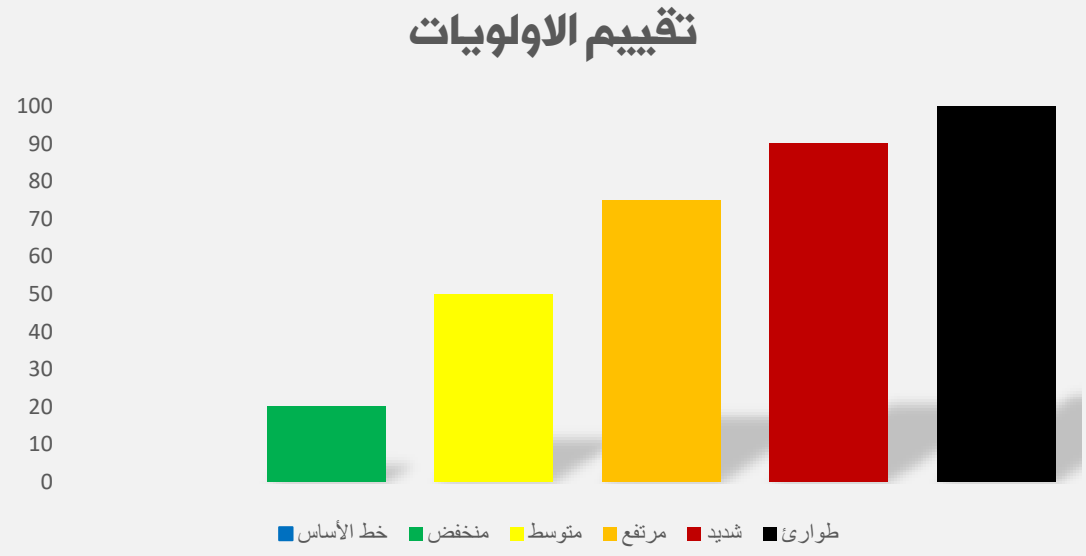
منخفض – (من غير المرجح أن تؤثر الحوادث ذات الأولوية المنخفضة على الصحة العامة أو السلامة أو الأمن الوطني أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية أو ثقة الجمهور).

متوسط – (قد تؤثر الحوادث ذات الأولوية المتوسطة على الصحة العامة أو السلامة أو الأمن الوطني أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية أو ثقة الجمهور).

مرتفع – (من المحتمل أن ينتج عن الحادث ذي الأولوية العالية تأثير واضح على الصحة العامة أو السلامة أو الأمن الوطني أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية أو ثقة الجمهور).

شديد – (من المحتمل أن ينتج عن الحادث ذي الأولوية الشديدة تأثير كبير على الصحة العامة أو السلامة أو الأمن الوطني أو الأمن الاقتصادي أو العلاقات الخارجية أو الحريات المدنية).

طوارئ – (يمثل حادث الأولوية الطارئ تهديداً وشيكًا يمس توفير خدمات البنية التحتية الحيوية/الحساسة بصورة واسعة النطاق أو يمس الاستقرار الوطني أو حياة الأشخاص في المملكة).



7. أن تكون التدابير المتخذة وعمليات الاستجابة للحوادث والتهديدات سريعة ودقيقة، خاصة فيما يتصل بأنظمة المعلومات الحرجة/الحساسة.

تشمل الأنشطة المعنية بالاستجابة والتعامل مع حادث الأمن السيبراني المتصل بأنظمة المعلومات الحساسة بالنسبة للأمن الوطني، الاتي:

* اكتشاف وتحديد حادث الأمن السيبراني
* حماية الموقع وموازنة الأدلة
* حظر وتقييد نطاق الحادث الذي وقع، وتخفيف الخسائر والأضرار الناجمة عنه
* تحديد أهداف وأغراض ونطاق الاستجابة
* التحقق من حادث الأمن السيبراني وتحليله وتقييمه وتصنيفه
* تنفيذ خطط للاستجابة للحادث ومعالجته
* تحديد سبب الحادث وتعقب مصدره
* التحقيق في الحادث والتعامل معه وفقًا للقانون.

8. أن يتبع بالتصنيف إجراءات محدثة ومرنة تواكب التطور التقني لاستخدام الفضاء السيبراني.

وعملا بالمقترحات السابقة، نجد أن للمركز الوطني للأمن السيبراني الاستفادة من تصنيف المركز الوطني الامريكي للأمن السيبراني للأولويات المرتبطة بالقطاعات الهامة والحيوية لدى وقوع الحادث [4]، وتصميم نظام لتقييم أثر الحادث السيبراني مبني على العناصر التالية:

- Functional Impact[5]
- Observed Activity[6]

[4] NCCIC Cyber Incident Scoring System, https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

[5] Functional impact is a measure of the actual, ongoing impact to the organization. In many cases (e.g., scans and probes or a successfully defended attack), little or no impact may be experienced due to the incident. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

[6] Observed activity describes what is known about threat actor activity on the network. These options are normalized upon guidance issued by the Office of the Director of National Intelligence (ODNI) and used by the intelligence community. Although the ODNI guidance document goes into more detail, observed activity is sorted into the following general categories: Prepare, Engage, Presence, and Effect. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

- Location of Observed Activity[7]
- Actor Characterization[8]
- Information Impact[9]
- Recoverability[10]
- Cross-Sector Dependency[11], and
- Potential Impact[12].

بحيث يصار إلى ضبط هذه العناصر في قالب يستطيع في مجمله أن يقيس مدى أثر/تأثير حوادث الأمن السيبراني في المملكة، والاعتماد عليها في وضع اليات واجراءات التعامل واتخاذ التدابير اللازمة لمواجهة التهديدات والحوادث ومخاطرهما على أنظمة المعلومات والبنية التحتية للمؤسسات والشركات والهيئات...

[7] The location of observed activity describes where the observed activity was detected in the network. The options for observed activity are based on a modified version of the Purdue Enterprise Reference Architecture. A flexible set of definitions was chosen for this category because each affected entity will likely have a different perspective on what systems are critical to its enterprise. The location of observed activity is likely to change during the course of an incident and should be updated as new information becomes available. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

[8] One of the greatest challenges in incident response is attributing an incident to a particular actor set and understanding the skill levels and intentions of that actor. NCCIC may leverage its own analytic body of knowledge as well as that of other mission partners to determine an actor's capabilities with regard to specific target systems such as industrial control environments. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

[9] In addition to functional impact, incidents may also affect the confidentiality and integrity of the information stored or processed by various systems. The information impact category is used to describe the type of information lost, compromised, or corrupted. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

[10] Recoverability represents the scope of resources needed to recover from the incident. In many cases, an entity's internal computer network defense staff will be able to handle an incident without external support, resulting in a recoverability classification of Regular. An example of a Regular recovery would be a phishing email that was automatically blocked by a mail server. In Extended recoverability cases, significant efforts such as a multi-agency, multi-organizational response task force may be needed for recovery. For example, if an entity requests support from the NCCIC, the incident is by its nature an extended recovery. Lastly, it may not be feasible to recover from some types of incidents, such as significant confidentiality or privacy compromises. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

[11] Cross-sector dependency is a weighting factor that is determined based on cross-sector analyses conducted by the DHS Office of Critical Infrastructure Analysis (OCIA). https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

[12] The potential impact category estimates the overall national impact resulting from a total loss of service from the affected entity. Other existing standards for rating cybersecurity incident risk lack consideration for the unique and diverse critical infrastructure assets of the owners and operators and U.S. Government departments and agencies that NCCIC is tasked with helping to protect. A similar incident at two separate stakeholder facilities might have a significantly different impact to operations at a national level. Therefore, each incident will be scored differently relative to the risk it presents in a nationwide context. https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline

وبعد استعراض الوضع التقني والقانوني لتصنيف حوادث الأمن السيبراني والتهديدات السيبرانية، نجد أنه ومن الضروري لغايات إنفاذ قانون الأمن السيبراني الأردني والعمل على تطبيقه وعلى حماية الأمن السيبراني الوطني، أن تعمل الجهات المعنية على تصنيف حوادث الأمن السيبراني بما يتوافق وطبيعة الفضاء السيبراني الوطني ومتطلبات حماية أمن المملكة (بما في ذلك الافراد والشركات). على أن يتم ذلك من خلال تحديد أسس محددة لتصنيف حوادث الأمن السيبراني ومعايير تراعي طبيعة ووظائف القطاعات الحيوية والبنية التحتية الحرجة لمؤسسات الدولة وهيئاتها ودوائرها.

وفي هذا الصدد، نرى ضرورة العمل على إفراد نصوص قانونية في القانون – وأنظمته وتعليماته في المستقبل – تبين ابتداء المقصود بأنظمة المعلومات/البنية التحتية الحرجة للدولة وتحديد القطاعات الحيوية (والسيادية)، وتنظيم أحكام خاصة هدفها ضمان حماية الأمن السيبراني الوطني وسلامة فضائه السيبراني. بالاضافة إلى بيان وتعريف تقييم وتدقيق الأمن السيبراني – على الصعيد الوطني – وبيان اليات الاستجابة والتعامل، الأمر الذي سيساعد الجهات المعنية من التعاطي مع أي تهديد أو حادث من شأنه المساس أو التأثير في/على هذه القطاعات و/أو أنظمة المعلومات/البنية التحتية. من خلال الارتكاز على أسس ومعايير تصنيف واضحة ومحدثة تواكب التطور التقني والفني لإستخدام الفضاء السيبراني، ولتكون قادرة على تصنيف أي فعل (حادث أو تهديد) وقياس مدى خطورته بكفاءة ودقة، تحقيقا للهدف الاساسي من القانون والمتمثل ب: الوقاية من - أو التعامل مع - الاثار الناجمة عن أي فعل (قد) يمس الأمن السيبراني الوطني (قبل وقوعه أو في حال احتمالية وقوعه أو بعد وقوعه).

إعداد

المحامي الدكتور محمد عبد المجيد الذنيبات – متخصص وباحث قانوني في التجارة والخدمات الالكترونية

الاستاذ المحامي رائد عبد الرزاق أبو العثم – متخصص في الجرائم الالكترونية

السيد محمود عبد الحميد القضاة – خبير في مجال أمن وحماية البيانات (الامن السيبراني)

www.althunibat.com

المراجع

- Cybersecurity Incident Taxonomy, http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf
- NCCIC Cyber Incident Scoring System, https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System#accordion-section-baseline
- Cyber Incident Severity Schema, https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf
- NCISS Incident Scoring Demo, https://www.us-cert.gov/nciss/demo
- DIRECTIVE (EU) 2016/1148, "concerning measures for a high common level of security of network and information systems across the Union", https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
- EU Cybersecurity Act, P8_TA-PROV(2019)0151, http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf
- Vietnamese cybersecurity law, No.: 24/2018/QH14, https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf
- KPMG, "Overview of China's Cybersecurity Law", https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf
- قانون الأمن السيبراني الاردني لسنة 2019.
- الدكتور محمد الذنيبات، "دراسة تحليلية ونقدية لقانون الأمن السيبراني لسنة 2019".