المبادئ التوجيهية المتعلقة بأمن البنية التحتية للإنترنت في الدول العربية

March 2020

ملخص تنفيذي

مع استمرار العديد من الدول العربية في تحديث وتنويع اقتصاداتها، ومع تركز الاهتمام على الخدمات الرقمية والتجارة والحكومة الإلكترونية، تتزايد فرص وتهديدات الإنترنت على حد سواء[1]. ومع زيادة اعتماد الاقتصاد والمجتمع والبنية التحتية المعلوماتية الحيوية اليوم على الإنترنت، أصبح الحفاظ على استمرار الاتصال بشبكة الإنترنت أمرًا ضروريًا لا غني عنه. وبالتالي أصبح لزاما على مختلف الدول أن تولي اهتماماً ليس فقط للأمن السيبراني، ولكن أيضًا للسياسات والتقنيات وأفضل الممارسات التي تعزز أمن البنية التحتية لشبكة الإنترنت.

يتغير أسلوب التعامل مع الأمن السيبراني؛ حيث لم تعد الأطر الاقليمية الأكثر حداثة للأمن السيبراني تركز على الأمن باعتباره غاية في حد ذاته، بل على جعله وسيلة من شأنها تيسير تحقيق الأهداف الاجتماعية والاقتصادية الشاملة. إن الأمن السيبراني اليوم لا يهدف إلى فرض قيود على البنية التحتية مثل "حفر الخنادق المائية، وفتح الجسور المتحركة"، وإنما يركز على دور الأمن في تيسير وجود اقتصاد رقمي عالمي مترابط متبادل الاعتماد. وبالتالي، فإن العمل التعاوني يعد أفضل السبل لتحقيق ذلك.

تتكون شبكة الإنترنت من شبكات مستقلة تتصل ببعضها البعض باستخدام معايير مفتوحة لضمان إمكانية التشغيل البيني؛ ذلك أن البنية التحتية لشبكة الإنترنت تشتمل على بروتوكولات، وخدمات، وبرامجيات ومعدات حاسوبية، وربط شبكي، وبنية تحتية للاتصالات، ومعلومات، وتدعمها الموارد البشرية. ولما كان الإنترنت "شبكة الشبكات"، فإن اقتصار التركيز على مرونة الشبكة الوطنية لن يكفل استمرار الاتصال بشبكة الإنترنت، وإنما يجب أن تكون مرونة الإنترنت الإقليمية هدفًا في حد ذاته.

1 https://gulfif.org/the-new-battlefront-cyber-security-across-the-gcc/

مبادئ أساسية:

استنادًا إلى توجيهات الخبراء الإقليميين والأطر الدولية والإقليمية بشأن الأمن السيبراني، فقد حددت جمعية الإنترنت (ISOC) المبادئ الأساسية التالية لتأمين شبكة الإنترنت:

- **الوعي:** يتعين على جميع الجهات المعنية في كل من القطاعين العام والخاص فهم المخاطر التي تهدد أمنها، ومدى تأثير تلك المخاطر عليها وعلى الآخرين في النظام البيئي الخاص بالبنية التحتية لشبكة الإنترنت.
- **المسؤولية:** يجب على جميع الجهات المعنية تحمل مسؤولية مواجهة المخاطر الأمنية في إطار أدوارها ومؤسساتها، مع الأخذ في الاعتبار للأثار المترتبة على اتخاذ اجراء ما أو التقاعس عن تنفيذه.
- **التعاون:** يجب إشراك جميع الجهات المعنية، بما في ذلك الأطراف المعنية خارج الحدود، في حوار مستمر حول الأمن السيبراني لمواجهة التهديدات الجديدة والمستمرة مواجهة فعالة.
- **الحقوق الأساسية وخصائص الإنترنت:** يجب على الجهات المعنية عند اتخاذها لأي إجراء لمواجهة المخاطر الأمنية الالتزام بالحقوق الأساسية، وتحري الشفافة، وعدم المساس بخصائص الإنترنت الخاصة بالمشاركة التطوعية، والمعايير المفتوحة والركائز التكنولوجية القابلة لإعادة الاستخدام والنزاهة والقدرة على الابتكار والانتشار العالمي2.

ويجب أن تأخذ السياسات والإستراتيجيات في الاعتبار تأثيرها على البنية الأساسية لشبكة لإنترنت، والتأكد من أنها لا تؤثر سلبًا على الانفتاح، والابتكار، والانتشار العالمي لشبكة الإنترنت.

الوضع الأمني في الدول العربية:

من الملامح الأساسية للوضع الأمني الحالي في الدول العربية:

- عدم تنفيذ الاستراتيجيات الوطنية المتعلقة بالأمن السيبراني في جميع الدول، التي تميل الى افتقارها للموارد، وغالبًا ما تركز على نماذج "السيطرة من القمة إلى القاعدة" أكثر من اتباعها لنهج تعاوني.
- تميل فرق التصدي لحوادث أمن الحاسبات (CSIRTs) إلى التعاون على نحو أقل مع القطاع الخاص والجهات المعنية عن مثيلتها في المناطق الأخرى، مما قد يؤثر في قدرتها على تكوين

2 https://www.internetsociety.org/internet-invariants-what-really-matters

شبكات واسعة من علاقات الثقة. وهناك حاجة إلى تكوين مزيد من العلاقات التعاونية لتحسين عملية تبادل المعلومات، والكشف عن الثغرات، وبناء القدرات، والتصدي للحوادث.

- على الرغم من تراجع أمن ومرونة البنية التحتية للإنترنت في بعض المناطق الأخرى، إلا أن هناك فرص متاحة لخلق منهج تعاوني وتحقيق مزيد من الشراكات التعاونية بين القطاعات المختلفة مما سيتيح للقطاعين العام والخاص سبل التعاون والعمل معًا.

توصيات:

ينبغي على الحكومات وغيرها من الجهات المعنية تمكين المنظمات والمؤسسات من خلق ثقافة تعاونية لأمن البنية التحتية للإنترنت من أجل تحقيق الرخاء الاقتصادي والاجتماعي.

على الصعيد الوطني: ينبغي على الحكومات تعزيز وجود نظام بيئي منفتح وتعاوني ومرن لأمن الإنترنت يتضمن ما يلي:

- تعيين البنية التحتية المعلوماتية المهمة وحمايتها.
- تطوير مرونة البنية التحتية للإنترنت من خلال تيسير نشر المعايير الأمنية وأفضل الممارسات.
- تطوير مرونة البنية التحتية لشبكة الإنترنت من خلال تحقيق ربط أفضل بين الشبكات.
- تيسير عملية تبادل المعلومات وبناء العلاقات بين جميع الجهات المعنية.
- تكوين فرق للتصدي لحوادث أمن الحاسبات على الصعيد الوطني ودعمها.
- الاستفادة من المؤسسات العامة في أن تكون مثالًا يحتذى به.
- تحديد ومواجهة العقبات القانونية التي تحول دون مشاركة المعلومات (بما في ذلك دعم الباحثين في "مجال القرصنة الأخلاقية") وإجراء الأبحاث المتعلقة بالثغرات الأمنية والحوادث والتهديدات.

على الصعيد الإقليمي: ينبغي على الحكومات التعاون مع جميع الجهات المعنية لتعزيز التعاون الإقليمي على النحو التالي:

- تكوين مجموعة إقليمية من الخبراء الأمنيين من الحكومة والمؤسسات التجارية والتقنية والأكاديمية والمجتمع المدني لتقديم إرشادات غير ملزمة للمنطقة حول القضايا الأمنية المتعلقة بالبنية التحتية للإنترنت حسب الضرورة.
- المشاركة في مبادرات الأمن السيبراني الحالية المتعلقة بالاتصالات والتنسيق وتعزيزها، بما في ذلك النظر في إمكانية إنشاء منصة إقليمية لتبادل المعلومات المتعلقة بالتهديدات.

- حشد موارد فرق التصدي لحوادث أمن الحاسبات كلما أمكن مثل تنسيق ومشاركة الدورات التدريبية فيما بينها، وذلك لزيادة المعرفة والخبرة، وتكوين علاقات عبر الحدود بين المتخصصين الذين يبنون جسور الثقة من أجل زيادة التعاون.
- زيادة مرونة الشبكات لمواجهة الهجمات والانقطاع من خلال تيسير التنوع في الربط الشبكي محليًا وإقليميًا ودوليًا.

المحتويات

مقدمة

تزداد تهديدات الأمن السيبراني وحوادثه3، ونظرًا لاندماج الاقتصادات العربية في شبكة الإنترنت العالمية، فقد أصبحت هذه الاقتصادات تتأثر بكل من مخاطر ومنافع شبكة الانترنت. ولذلك أصبح للحكومات دور أساسي يجب أن تؤديه برغم صعوبته؛ إذ بات لزامًا عليها التقليل من المخاطر الناجمة عن التهديدات الموجودة على شبكة الإنترنت والحد منها، مع الحفاظ على ثقة الشعوب في شبكة الإنترنت، والتي إذا انعدمت، فإن اقتصاداتهم ستفقد قدرتها الديناميكية على الابتكار والنمو. ويعد العمل بشكل تعاوني في جميع المجالات الاقتصادية أفضل السبل للحفاظ على الثقة في شبكة الإنترنت وتسخير جميع الموارد اللازمة لحمايتها. ولتحقيق ذلك، فإنه يجب على الحكومات ومقدمي البنية التحتية للإنترنت وغيرهم من الخبراء الأمنيين العمل معًا لتحديد البنية التحتية لشبكة الإنترنت في المنطقة وحمايتها، مع الحفاظ على الخصائص الأساسية لشبكة الإنترنت بوصفها منصة مفتوحة جديرة بالثقة ومؤمنة للجميع.

تستند هذه الوثيقة إلى نتائج التشاور مع الخبراء الإقليميين لتقديم إرشادات بشأن كيفية تأمين البنية التحتية لشبكة الإنترنت تأمينًا تعاونيًا، مع تحري الشفافية اللازمة، وحماية الحقوق والخصائص الأساسية لشبكة الإنترنت. تعتمد هذه المبادئ التوجيهية على أفضل الممارسات المستقاة من الأطر الإقليمية في جميع أنحاء العالم، بما في ذلك توصيات منظمة التعاون الاقتصادي والتنمية (OECD) بشأن مكافحة مخاطر الأمن الرقمي من أجل الرخاء الاقتصادي والاجتماعي، ودليل الممارسات الجيدة لإستراتيجية الأمن السيبراني الوطني الصادر عن الاتحاد الأوروبي، والمبادئ التوجيهية لأمن البنية التحتية لشبكة الإنترنت في إفريقيا، والتي تعد مبادرة مشتركة لجمعية الإنترنت ومفوضية الاتحاد الإفريقي4.

النهج الأمني التعاوني

يدرك النهج الأمني التعاوني لأمن الإنترنت أن البشر في النهاية هم من يحافظون على تماسك الإنترنت. وقد اعتمد تطور الإنترنت على نهج التعاون التطوعي. ولا يزال التعاون والتآزر عاملين أساسيين لازدهاره وإمكاناته. ويؤكد النهج على الخمسة مبادئ التالية:

- المحافظة على الفرص وبناء الثقة.
- المسؤولية الجماعية.
- التكامل التام بين الحلول الأمنية والحقوق والإنترنت المفتوح.
- الحلول الأمنية القائمة على الخبرة، والتي تطورت بتوافق الآراء، ووفقًا لتطورات النظرة المستقبلية.
- استهداف نقطة التأثير القصوى–فكر عالميًا، واعمل محليًا.

https://www.internetsociety.org/collaborativesecurity/

3 https://future.internetsociety.org/2017/introduction-drivers-of-change-areas-of-impact/drivers-of-change/cyber-threats/
4 https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/

لقد اختيرت الأطر الإقليمية لأنها مرنة وعملية؛ ولتوفيرها أفضل الممارسات والمبادئ العالمية ذات الصلة. وتستهدف هذه المبادئ التوجيهية صانعي السياسات والجهات التنظيمية ومديري فرق التصدي لحوادث أمن الحاسبات والمؤسسات التابعة لها في الدول العربية، وكذلك مشغلي البنية التحتية في القطاع الخاص مثل مقدمي خدمات الإنترنت. تناقش هذه المبادئ التوجيهية تحديات الأمن السيبراني والفرص الفريدة التي ركز عليها كل من الخبراء والاستشاريين الإقليميين في الدول العربية.

لماذا يستخدم النهج الأمني التعاوني؟

تضطلع الحكومات بدور رئيس في أن تكون مثالًا يحتذى به، وفي التشجيع على تبادل المعلومات والتعاون على الصعيدين الوطني والإقليمي. ولكن نظرًا لكون الإنترنت شبكة الشبكات دون سيطرة مركزية، تملكها أو تديرها العديد من الكيانات المختلفة، فإنه لا يمكن لكيان واحد المحافظة على أمنها. وقد جاء بناء الإنترنت نتيجة للتعاون والتآزر، وهما أكثر الطرق فعالية لحمايته.

نهج جديد لأمن البنية التحتية للإنترنت

كان هناك تطور على مدار العقد الماضي في النهج الأساسي المتبع تجاه الأمن السيبراني؛ إذ لم يعد ينظر إلى الأمن بوصفه هدفًا نهائيًا في حد ذاته، بل بوصفه وسيلة من شأنها أن تيسر ممارسة الأنشطة الاجتماعية والاقتصادية. وهناك الآن اعتراف واسع بأن نهج "الخنادق والجسور المتحركة" – وذلك ببناء أسوار أعلى حول الأنظمة والخدمات– لن يفلح في دعم اقتصاد عالمي مترابط يعتمد بعضه على بعض. ويتجلى هذا النهج الجديد في الأطر والإستراتيجيات الوطنية الأكثر نجاحًا حيث يكون الانفتاح والتعاون هما الأساس الذي يجب الاعتماد عليه.

ما الذي تركز عليه هذه المبادئ التوجيهية؟ وما الذي تغفله؟

تركز هذه المبادئ التوجيهية على كيفية تحديد البنية التحتية للإنترنت، وعلى حمايتها والمحافظة عليها في ظل البيئة الحالية المليئة بالتهديدات؛ فخدمات مهمة مثل المرافق والنظم الصحية صارت بحاجة اليوم لإنترنت آمن وفعال. تركز هذه المبادئ التوجيهية على أمن البنية التحتية للإنترنت، وليس الأمن السيبراني ككل.

لا تتعامل المبادئ التوجيهية مباشرة مع الأمن القومي والهجمات الإلكترونية التي تجيزها الدول والحروب الإلكترونية والجرائم الإلكترونية، وإنما مثل تلك القضايا تتعامل معها في الأساس مواثيق دولية مختلفة نذكر منها، على سبيل المثال، اتفاقية بودابست لمكافحة الجرائم الإلكترونية. بيد أن تنفيذ هذه المبادئ

التوجيهية المتعلقة بأمن البنية التحتية للإنترنت سيزيد من قدرة الاقتصاد ككل على التصدي لمجموعة كبيرة من التهديدات والهجمات.

وفي حين أن هذه المبادئ التوجيهية لا تمثل حلًا نهائيًا لجميع القضايا، إلا أن نهجها التعاوني يعد خطوة أولى أساسية نحو بنية تحتية لشبكة الإنترنت تتميز بالمرونة والأمن والأمان.

1 الصورة العامة للتهديدات الأمنية والإمكانيات في الدول العربية

تتشابه طبيعة التهديدات الشائعة في الدول العربية وأنواعها تشابهًا جوهريًا مع تلك المنتشرة في جميع أنحاء العالم. هذه التهديدات والهجمات السيبرانية المتزايدة تحركها جهات حكومية فاعلة، والأنشطة الإجرامية الموجهة ماليًا والنضال الالكتروني (hacktivism) والإرهاب. وعلى الرغم من تأخر هذه المنطقة عمومًا عن أوروبا وآسيا ومنطقة المحيط الهادئ فيما يتعلق بالقدرات والتنسيق5، إلا أنها تتحرك سريعًا لتلحق بالركب. هذا وتشمل الملاحظات الإقليمية العامة ما يلي:

- **التهديدات الجيوسياسية الخطيرة**

تختلف الصورة العامة للتهديدات عن صورتها في المناطق الأخرى؛ وذلك مع وجود قدر كبير من التهديدات الصادرة عن جهات حكومية خارجية فاعلة6، وتدني مستوى الاستعداد7. وفيما يبدو فهناك بلدان أخرى، مثل السودان ومصر والعراق وليبيا، مستهدفة بسبب الضعف العام في أمن شبكاتها.

- **اختراقات البيانات – انخفاض معدلات الإبلاغ وارتفاع التكاليف**

هناك انخفاض نسبي في معدلات الإبلاغ عن الاختراقات الأمنية وتلك المتعلقة بالبيانات8، الأمر الذي يؤدي إلى عدم وضوح كل من أعداد الاختراقات المحتملة ونطاقها الفعلي. ترتفع تكلفة الاختراقات، لتنضم كل من المملكة العربية السعودية ودولة الإمارات العربية المتحدة إلى الولايات المتحدة باعتبارها أكثر ثلاث دول في العالم تحملًا لتكلفة اختراقات البيانات، إذ بلغ متوسط تكلفة معالجة آثار الاختراق الواحد أكثر من 5 ملايين دولار أمريكي9. وإلى جانب ذلك، تشير المدد الزمنية الطويلة نسبيًا اللازمة لمعالجة الاختراقات إلى أن الحوافز لتبادل المعلومات والكشف عن الثغرات تفتقر للتوجيه الجيد لدى الجهات المعنية محليًا على النحو المطلوب. وخلافًا للمناطق الأخرى، حيث تميل اختراقات البيانات إلى التعلق

5 https://www.pwc.com/m1/en/publications/documents/middle-east-cyber-security-survey.pdf
6 https://gulfnews.com/world/gulf/saudi/gulf-states-at-risk-of-cyber-attacks-1.1985345
7 http://www.eiu.com/industry/article/806588464/cyber-attacks-is-the-gcc-prepared/2018-04-03
8 http://www.securitymea.com/2019/07/01/darkmatter-group-releases-mena-cybersecurity-report/

9 https://www.ibm.com/security/data-breach

بالبيانات الشخصية والمالية، فإن الاختراقات في الشرق الأوسط غالبًا ما تتعلق بالأسرار التجارية وأسرار الدولة 10.

- **فرق التصدي لحوادث أمن الحاسبات: الفرق الناشئة والتي تقودها الدولة بصورة أساسية**

في حين أن معظم البلدان قد أنشأت مراكز لتعزيز القدرات الأمنية السيبرانية، ومكافحة الحوادث والتهديدات المباشرة، إلا أن هذه المراكز تميل إلى كونها أقل تعاونًا مع القطاع الخاص والجهات المعنية الأخرى مقارنة بمثيلتها في المناطق الأخرى. الأمر الذي أدى إلى وجود تحديات أمام بناء العلاقات والكشف عن الثغرات. ولذا فقد بدأت بعض البلدان في تكوين فرق في قطاعات بعينها للتصدي لحوادث أمن الحاسبات مثل قطاعي الاتصالات والطاقة.

لا تزال المهارات قيد التطوير، ولا سيما المهارات المتقدمة

لا تزال قدرة الأمن السيبراني على المستوى المتقدم، أي التعليم الجامعي وما بعد الجامعي المتخصص، عند مستوى منخفض نسبيًا. وعلى الرغم من توفير معظم دول المنطقة لتدريب مهني على الأمن السيبراني، إلا أن مستواه أقل بكثير من مستوى إتاحته في مناطق أخرى مثل أوروبا أو آسيا ومنطقة المحيط الهادئ11.

تشير مشاوراتنا التي أجريناها في العديد من الدول العربية إلى أن هناك درجة كبيرة من الوعي بهذه القضايا، ودافع قوي لمعالجتها من خلال زيادة تطوير العلاقات الوطنية والإقليمية اللازمة والحوكمة والقدرة التشغيلية.

2 العناصر الأساسية للبنية التحتية لشبكة الانترنت

يتكون الإنترنت من شبكات مستقلة تتصل ببعضها البعض باستخدام معايير مفتوحة لضمان إمكانية التشغيل البيني. وكذلك تمثل البنية التحتية لشبكة الإنترنت العناصر التي تشكل وتعين على نقل البيانات القابلة للاستخدام عبر تلك الشبكات. ونظرًا لاعتماد معظم اقتصاد الدول ومجتمعاتها وخدماتها الأساسية حاليًا على الإنترنت، فقد أصبح المحافظة على إمكانية الاتصال يمثل أولوية قصوى.

10 https://infowatch.com/sites/default/files/report/analytics/a_study_of_data_leaks_in_the_middle_east_in_2017-2018_.pdf
11 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

وفيايلي العناصر الأساسية الستة للبنية التحتية لشبكة الإنترنت:

البروتوكولات والخدمات

البروتوكولات هي معايير فنية تتيح لمختلف أنظمة الحواسب إمكانية التواصل مع بعضها البعض. وتمثل مجموعة TCP/IP12 التي تشكل أساس الإنترنت مثالًا رئيسًا على تلك البروتوكولات.

إن الخدمات في هذا السياق تمثل الخصائص الوظيفية التي تجعل من الإنترنت أداة جذابة ومفيدة من خلال تيسير عملية تبادل المحتوى عبر الإنترنت. وتتضمن خدمات البنية التحتية لشبكة الإنترنت العَنْوَنَة– وهو النظام العالمي لتحليل أسماء النطاقات الذي يستخدم نظام أسماء النطاقات (DNS)– والذي يتيح لنا التنقل بين صفحات الإنترنت. وهي تشمل أيضًا وظائف مثل التوجيه، واستخدام بروتوكول البوابة الحدودية (BGP)، وخدمات التطبيقات مثل الشبكة العنكبوتية العالمية. وتختلف خدمات البنية التحتية لشبكة لإنترنت عن خدمات المستخدم التي تتصدر خدمات البنية التحتية مثل المتصفحات ومحركات البحث ومواقع التواصل الاجتماعي.

تمثل البروتوكولات والخدمات عناصر أساسية لضمان أمن البنية التحتية لشبكة الإنترنت؛ فبدونها لا يمكننا إرسال البيانات واستقبالها أو التنقل بين صفحات الإنترنت للوصول إلى المعلومات ومشاركتها أو التواصل مع بعضنا البعض.

السياق العربي: يعد اختطاف النطاقات أحد الأخطار الأمنية التي تهدد البروتوكولات والخدمات، والتي كان آخرها حملة "السلحفاة البحرية" (Sea Turtle)، خلال المدة من 2017 إلى 2019، والتي بدا أنها تستهدف مؤسسات القطاعين العام والخاص في الشرق الأوسط وشمال إفريقيا. فقد وصل المهاجمون إلى سجلات أسماء نظام النطاقات الخاصة بمؤسسات معروفة وغيرها لتوجيه المستخدمين إلى خوادم تقع تحت سيطرتهم. وهكذا تعرض مستخدمو المواقع الإلكترونية للتضليل وكان من بينها المواقع التابعة "لمؤسسات عسكرية وأجهزة الأمن الوطنية ووزارات الخارجية وشركات الطاقة في ليبيا ومصر والإمارات العربية المتحدة وقبرص ولبنان والعراق والأردن وتركيا وأرمينيا وسوريا وألبانيا"13.

البرمجيات والمعدات الحاسوبية

تتضمن البرمجيات في هذا السياق أنظمة التشغيل والبرامج الثابتة. وتنطوي منتجات البرمجيات على ثغرات أمنية يجب معالجتها من خلال التحديث المنتظم وتصحيح الأخطاء وغيرها من الوسائل.

12 تعمل مجموعة مهندسي شبكة الإنترنت (IETF)، وهي منظمة للمعايير المفتوحة، على تنظيم وتطوير بروتوكول التحكم بالنقل (TCP) وبروتوكول الإنترنت (IP).

https://en.wikipedia.org/wiki/Internet_protocol_suite

13 https://www.infosecurity-magazine.com/news/dns-hijackers-target-middle-east-1-1/

وأما فيما يتعلق بمصطلح المعدات الحاسوبية، فيقصد به الآلات أو التوصيلات السلكية مثل أجهزة الشبكات (المفاتيح، وأجهزة التوجيه، وجدران الحماية، والبوابات)، والخوادم، وأجهزة المستخدم النهائي (الحواسب الشخصية، والأجهزة اللوحية، والهواتف النقالة).

السياق العربي: من الهجمات الشائعة هجمات الفدية (Ransomware) التي تستند عادة إلى مشكلات تحديث البرامج. وتعد المملكة العربية السعودية والإمارات العربية المتحدة أكثر الدول العربية تعرضًا لذلك النوع من الهجمات14. وفيما يخص المعدات الحاسوبية، فإن الثغرات الأمنية في أجهزة المستخدم تمثل مشكلة، ولا سيما في حالات هجمات التصيد الالكتروني (Phishing attacks) على هواتف المسؤولين المصابة لجمع سجلات المكالمات والتسجيلات الصوتية والمعلومات المتعلقة بموقع الجهاز والرسائل النصية15.

ما هي نقاط تبادل الإنترنت؟

تعد نقطة تبادل الإنترنت موقعًا ماديًا تتصل فيه شبكات الحاسوب المختلفة، مثل مقدمي خدمات الإنترنت، ومقدمي المحتوى، وشبكات توصيل المحتوى (CDN)، والحكومات، والشبكات البحثية. وكذلك تتبادل تلك الشبكات فيها أيضًا محتوى الإنترنت المحلي مع بعضها البعض عبر منصة مشتركة. وهي جزء لا يتجزأ من النظام البيئي المتعلق بشبكة الإنترنت.

ولمزيد من المعلومات، يرجى الاطلاع على الرابط التالي:

https://www.internetsociety.org/issues/ixps/

الربط الشبكي

الإنترنت "شبكة الشبكات"، ومن ثم فإن التقنيات والخدمات التي توفر الربط الشبكي لتلك الشبكات تمثل عناصر بالغة الأهمية. وأحيانًا ما تتوافر هذه التقنيات والخدمات عن طريق نقاط لتبادل الإنترنت (IXPs) – وهي منشأة تلتقي فيها شبكات الحاسوب المختلفة (IP networks) لتبادل المحتوى المحلي مع بعضها البعض من خلال مبدل للشبكات. ويشكل كل من مقدمي خدمة الإنترنت ونقاط تبادل الإنترنت جزءًا لا يتجزأ من البنية التحتية لشبكة الإنترنت. ويعد ضمان الربط الشبكي16 بين الشبكات عنصرًا أساسيًا في إكساب البنية التحتية لشبكة الإنترنت المرونة اللازمة.

تتيح نقاط تبادل الإنترنت تبادل محتوى الإنترنت محليًا وليس عبر الشبكات الدولية، فتقلل من حالات تأخر الشبكة، وتخفض تكاليف الوصول إلى الإنترنت للمستخدمين النهائيين من خلال تخفيض تكاليف

14 https://gulfnews.com/technology/uae-is-second-most-targeted-country-in-middle-east-and-africa-for-ransomware-1.2020895
15 https://www.cybersecurity-review.com/news-may-2018/phishing-spy-campaign-targets-top-mideast-officials/
16 https://www.internetsociety.org/policybriefs/internetinterconnection/

التشغيل لدى مقدم خدمات الإنترنت[17]‘[18]. وعلى الرغم من أن نقاط تبادل الإنترنت تساعد في الربط الشبكي من خلال التعامل مع محتوى الإنترنت تعاملًا أكثر كفاءة على الصعيد المحلي، إلا أنها لا تستطيع معالجة نقص المسارات المادية البديلة اللازمة لنقل البيانات، ولهذا فكليهما مهم. وبالإضافة إلى نقاط تبادل الإنترنت، فإن تنوع الربط على المستوى الدولي وثراءه يعد أيضًا أمرًا ضروريًا.

أمن التوجيه[19]

إن توجيه بروتوكول الإنترنت (IP routing) هو ما يجعل الإنترنت يعمل من خلال التأكد من ذهاب حزم البيانات إلى المكان المخصص لها عند الانتقال بين شركات الاتصالات؛ إذ يمكن لحوادث التوجيه[20]، سواء من خلال أخطاء التهيئة أو الهجمات الالكترونية الخطيرة، أن تؤدي إلى خسائر اقتصادية حقيقية من خلال منع الوصول إلى الخدمات الأساسية. وكذلك يمكنها تحويل حزم البيانات عبر شبكات خبيثة، مما يتيح الفرصة للتجسس عليها. إن حوادث مثل اختطاف التوجيه وتسريباته، وتزوير عناوين بروتوكولات الإنترنت هي عمليات عالمية النطاق؛ تؤدي فيها مشكلات التوجيه لدى أحد المشغلين إلى التأثير على غيره من المشغلين الآخرين.

تعد المعايير المتفق عليها بشكل متبادل لأمن التوجيه (MANRs[21]) مبادرة عالمية، تدعمها جمعية الإنترنت، والتي تقدم إصلاحات مهمة للحد من تهديدات التوجيه الأكثر شيوعًا، علمًا أن هناك إصدارات من تلك المبادرة لمشغلي الشبكات ونقاط تبادل الإنترنت، وقد أوردنا وصفها بمزيد من التفصيل في الملحق 3.

السياق العربي: لا تزال الدول العربية تمتلك عددًا صغيرًا نسبيًا من نقاط تبادل الإنترنت، علمًا أنه ليس من الواضح ما إذا كان جميعها يعمل. وهناك حاليًا خمسة عشر نقطة لتبادل الإنترنت في الدول العربية موزعة بين تسع دول[22]، منها ثماني نقاط تعمل حسبما يبدو. وهذا بالإضافة إلى تواجد نقاط لتبادل الإنترنت في مصر والكويت ولبنان وفلسطين والمملكة العربية السعودية والإمارات العربية المتحدة. وثمة مجال كبير لزيادة عدد نقاط تبادل الإنترنت ونطاق تغطيتها لتحسين الربط الشبكي على النحو الأمثل. أما فيما يتعلق بأمن التوجيه، فقد وقع 14 ألف حادث توجيه على مستوى العالم في عام 2017[23]، بيد أنه لا يُعتقد حاليًا أن الدول العربية وقعت ضحية لهجوم كبير منظم. ومع ذلك، يبدو أن هناك احتمالات

17 https://www.internetsociety.org/policybriefs/ixps/
18 https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/
19 https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/
20 https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/
21 https://www.manrs.org/
22 “Middle East & North Africa Internet Infrastructure” report to be published, December 2019: https://www.internetsociety.org/regions/middle-east/
23 https://www.internetsociety.org/blog/2018/01/14000-incidents-2017-routing-security-year-review/

متزايدة على لجوء الجهات الحكومية الفاعلة بالمناطق الأخرى إلى عمليات اختطاف التوجيه المتعمد لإعادة توجيه محتوى الإنترنت على نحو خبيث بهدف التجسس عليها. وقد يتزايد خطر هذا النوع من الهجمات في المنطقة العربية، غير أنه في حالة تبنى عدد كبير من مشغلي الشبكات لمبادرة المعايير المتفق عليها بشكل متبادل لأمن التوجيه، فسيقل ذلك الخطر الذي يهدد المنطقة.

البنية التحتية للاتصالات

يقصد بها الأصول المادية الأساسية اللازمة لتشغيل الإنترنت مثل: الكابلات ووسائل الربط (اللاسلكية: ميكروويف، تلفزة كبلية، قمر صناعي– السلكية: نحاسية، نطاق التردد العريض)، ومباني (مرافق تشمل مراكز البيانات أو نقاط إنزال الكابلات البحرية) وكذلك إمدادات الطاقة، وأنظمة التبريد، والأمن المادي.

السياق العربي: يبدو أن "المسار أقل مرونة" مما هو مطلوب للشبكات الإقليمية المرنة، أي أنه إذا كان هناك مسار مادي واحد فقط لدخول وخروج محتوى الإنترنت من وإلى البلد أو المنطقة، فهذا يعد جانبًا من جوانب الإخفاق. لقد تسببت حوادث الكابلات البحرية في وقوع أعطال بإمكانية الاتصال بالبنية التحتية لشبكة الإنترنت على مستوى المنطقة ومن الأمثلة المهمة على تلك الحوادث القطع الذي وقع في الكابلات عام 2013 بالقرب من محافظة الإسكندرية بجمهورية مصر العربية، مما تسبب ذلك في حدوث بطء في سرعة الإنترنت بجميع أنحاء الشرق الأوسط24. هذا النوع من الحوادث يوضح أهمية الحاجة إلى وجود مرونة لمسار التوجيه الخاص بحركة البيانات، لكي لا تتركز حركة البيانات في عدد صغير من نقاط الاختناق الإقليمية. ولما كان الإنترنت عبارة عن "شبكة الشبكات"، فإن التركيز فقط على مرونة الشبكة الوطنية لن يكفل استمرار الاتصال، ومن ثم يجب أن تكون المرونة الإقليمية للإنترنت هدفًا. إن وجود بنية تحتية قوية للإنترنت تعني وجود مسارات مادية كافية لحركة البيانات في شبكة الإنترنت من وإلى دول أخرى في المنطقة والعالم، ولا سيما حينما يصبح المسار غير متاح بسبب كوارث طبيعية أو خطأ أو هجوم بشري.

المعلومات

تشتمل المعلومات على البيانات المتعلقة بالأنظمة (مثل: قوائم جرد البرمجيات والمعدات الحاسوبية والبنية التحتية)، والبنية المادية للشبكة (الترتيب المادي لعناصر الشبكة)، وتهيئة النظام، ومعلومات التشغيل.

السياق العربي: يتصف مستوى تبادل المعلومات والإبلاغ عن اختراقات البيانات بالانخفاض النسبي، فضلًا عن أن معالجتها يستغرق أوقات طويلة بشكل غير معتاد. إن انخفاض مستوى الإبلاغ عمومًا عن

24 https://gigaom.com/2013/03/27/undersea-cable-cut-near-egypt-slows-down-internet-in-africa-middle-east-south-asia/

تلك الاختراقات يشير إلى وقوعها في جميع أنظمة تكنولوجيا المعلومات والاتصالات دون أن تكتشف25.

الموارد البشرية

تتألف الموارد البشرية من الأفراد الذين يمثلون مصدر قوة لأمن البنية التحتية للإنترنت، بما في ذلك المسؤولين والمشغلين وفرق الدعم والمطورين والمديرين والمراجعين والمستخدمين النهائيين. ويعد الأفراد– ومهاراتهم وقدراتهم، وعلاقاتهم الرسمية وغير الرسمية، والشعور بالتمكين للعمل حسب الحاجة أثناء الحوادث الأمنية– جزءًا أساسيًا من البنية التحتية لشبكة الإنترنت. فالأشخاص المدربون جيدًا والمؤثرون يساعدون على رفع مستوى أمن الأنظمة التي يشغلونها ويستخدمونها. إن الكفاءة والتفهم والدعم من الإدارة، والتزام الموظفين باتباع الإجراءات (وخاصة كبار الموظفين)، والموثوقية لدى الجميع تعد من العوامل المهمة التي يجب تطويرها تطويرًا استباقيًا. هذا وترتبط بالموارد البشرية مجموعة من الترتيبات الإدارية، سواء الرسمية أو غير الرسمية، التي تضع التنظيم الخاص بأمن البنية التحتية لشبكة لإنترنت. ويشمل ذلك مسارات ومسؤوليات واضحة للإبلاغ، والحوافز المشجعة على التعاون، والتشجيع على المشاركة الفعالة والملائمة للمعلومات بين فرق التصدي لحوادث أمن الحاسبات وجهات أخرى في مجتمع الأمن المحلي.

السياق العربي: مثلما هو الحال في المناطق الأخرى، فإن هناك فجوة في المهارات الأمنية26؛ إذ تميل الدول العربية إلى امتلاك أعداد أقل من خبراء الأمن السيبراني المعتمدين، وقد تتركز هذه المهارات في بعض البلدان في العمالة الوافدة27. هناك احتياجات متباينة للمهارات والخبرات على مستوى المبتدئين وفي المناصب الأعلى. الأمر الذي يشير إلى أن هناك حاجة لمزيد من التثقيف بشأن الأمن السيبراني على المستويين الثاني والثالث وضرورة أن يكون هناك تطوير مستمر. ويمكن كذلك توفير المزيد من المعرفة والتدريب المتخصصين خلال التدريب المهني المستمر المتعلق بأنشطة فرق التصدي لحوادث أمن الحاسبات وغيرها من المبادرات القطاعية.

3 مبادئ أمن البنية التحتية لشبكة الانترنت

يحدد هذا الجزء المبادئ الأساسية اللازمة لتأمين البنية التحتية لشبكة الإنترنت. وقد نقلت هذه المبادئ العامة بتصرف عن المبادئ التوجيهية التي وضعتها جمعية الإنترنت استنادًا إلى خبرة أعضائها، وأفضل الممارسات الحالية في جميع أنحاء العالم28. وكذلك تستند إلى التوصيات وأفضل الممارسات التي

25 http://www.securitymea.com/2019/07/01/darkmatter-group-releases-mena-cybersecurity-report/
26 https://thearabweekly.com/skills-gap-exacerbates-cybersecurity-problem-middle-east-faces-threats
27 https://www.fircroft.com/blogs/security-in-the-digital-age-a-report-on-the-middle-east-cyber-72474105124
28 المبادئ التوجيهية لأمن البنية التحتية لشبكة الإنترنت في إفريقيا؛ مبادرة مشتركة بين جمعية الإنترنت ومفوضية الاتحاد الإفريقي؛

اعتمدتها منظمات مثل منظمة آيكان (ICANN)، ومجموعة مهندسي شبكة الإنترنت (IETF)، والاتحاد الدولي للاتصالات (ITU)، والمعهد الوطني للمعايير والتكنولوجيا في أمريكا (NIST)، ووكالة الاتحاد الأوروبى لشؤون أمن الشبكات والمعلومات (ENISA)، والإتحاد الإفريقي[29]، ومنظمة التعاون الاقتصادي والتنمية (OECD)[30]. نقلت هذه المبادئ بتصرف بعد التشاور مع الخبراء والمسؤولين في الدول العربية.

الوعي

يجب على الجهات المعنية في كل من القطاعين العام والخاص إدراك المخاطر الأمنية المعرضين لها، وكذلك كيفية تأثرهم هم والآخرين في النظام البيئي الخاص بالبنية التحتية لشبكة الإنترنت بهذه المخاطر. ويجب على كل شخص مسؤول عن جزء من أجزاء البنية التحتية لشبكة الإنترنت أن يدرك المخاطر التي تواجهه، وأن يتصدى لتلك المخاطر حسبما يقتضي عمله، وذلك لتقليل التأثير إلى أدنى حد على نفسه وعلى غيره في النظام البيئي الخاص بالبنية التحتية للإنترنت في المنطقة العربية.

المسؤولية

يجب أن تتحمل كل جهة من الجهات المعنية مسؤولية مكافحة المخاطر الأمنية حسبما تقتضي وظائفها ومؤسساتها. ونظرًا للطبيعة المترابطة للإنترنت حيث يعتمد الكل بشكل أساسي على بعضه البعض، فإنه يجب على كل مؤسسة النظر في الآثار المحتمل أن تنعكس على الجهات المعنية الأخرى نتيجة أفعالها أو تقاعسها.

التعاون

لا بد من إشراك جميع الجهات المعنية، بما في ذلك الجهات العابرة للحدود، في حوار مستمر حول الأمن السيبراني لمواجهة التهديدات الجديدة والمستمرة مواجهة فعالة. ويشمل ذلك المشاورات الرسمية وغير الرسمية، وإقامة علاقات تعاونية بين القطاعين العام والخاص. علمًا أنه لا يمكن تحقيق أمن البنية التحتية لشبكة الإنترنت من خلال أي منظمة من المنظمات وحدها، وأن نموذج "السيطرة من القمة إلى القاعدة" لن يحقق التعاون وتدفقات المعلومات اللازمين لتحقيق المرونة اللازمة إقليميًا.

الحقوق الأساسية وخصائص الإنترنت

https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/

29 اتفاقية الاتحاد الأفريقي في مجال الأمن السيبراني وحماية البيانات الشخصية
https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

30 منقول بتصرف عن مكافحة مخاطر الأمن الرقمي من أجل الرخاء الاقتصادي والاجتماعي: توصيات منظمة التعاون الاقتصادي والتنمية والوثيقة المرافقة.

يجب أن تلتزم الجهات المعنية بالحقوق الأساسية في جميع الإجراءات التي تتخذها لمكافحة المخاطر الأمنية، وأن تتحرى الشفافية، وألا تمس خصائص الإنترنت الخاصة بالتعاون الطوعي والمعايير المفتوحة وركائز التكنولوجية القابلة لإعادة الاستخدام والنزاهة والقدرة المطلقة على الابتكار والانتشار العالمي31.

ويجب أن تشتمل السياسات والإستراتيجيات على النظر في تأثيرها على البنية الأساسية لشبكة لإنترنت، والتأكد من أنها لا تؤثر سلبًا على الانفتاح، والابتكار، والانتشار العالمي لشبكة الإنترنت.

31 https://www.internetsociety.org/internet-invariants-what-really-matters

4 التطورات الحالية في الدول العربية

تتعامل العديد من الدول العربية مع أمن البنية التحتية لشبكة الإنترنت بوسائل مختلفة مثل الإستراتيجيات الوطنية وتكوين فرق للتصدي لحوادث أمن الحاسبات. وجدير بالذكر أن القدرات والنهج الوطنية والإقليمية لا تزال قيد التطوير؛ ذلك أن جميع الدول لم تتبنى أو تنفذ استراتيجيات وطنية للأمن السيبراني. وكذلك لم تحقق فرق التصدي لحوادث أمن الحاسبات عمومًا أقصى قدر ممكن من فرص التعاون.

وأما فيما يخص المرحلة التالية اللازمة لتأمين البنية التحتية لشبكة الإنترنت، فإنها تتمثل في الانتقال من حيز الاهتمام الذي يرتكز إلى حد كبير على الدولة إلى نهج تعاوني وتآزري بالكامل. ولكن على الرغم من الحاجة إلى فعل الكثير، فقد شهدت العديد من الدول "انتصارات سريعة" حققت فيها المرونة اللازمة على الصعيد الوطني من خلال أنشطة المراكز التعاونية المعنية بمواجهة الحوادث.

4.1 استراتيجيات الأمن السيبراني الوطنية

نفذت العديد من الدول العربية، مثل عمان والأردن والإمارات ومصر، استراتيجيات استباقية للأمن السيبراني للتصدى للوضع الذي يتهددها على نحو استباقي.

تبوأت عُمان المرتبة الرابعة عالميًا في مؤشر قياس جاهزية الدول تجاه الأمن السيبراني العالمي لعام 2017 (GCI) الذي يصدره الاتحاد الدولي للاتصالات، وكذلك المرتبة السادسة عشر في عام 322018. يقيس مؤشر قياس جاهزية الدول تجاه الأمن السيبراني العالمي الردود على الدراسة الاستقصائية وفقًا للمعايير التقنية والتنظيمية والقانونية وبناء القدرات والتعاون. (ويعني المؤشر أيضًا بدراسة السعودية وقطر ومصر والإمارات نظرًا لتحقيقها مستويات "مرتفعة" من الالتزام بالأمن السيبراني). وبالإضافة إلى استضافة عمان للمركز العربي الإقليمي للأمن السيبراني (ITU-ARCC)، فإنها تدعم أيضًا دولًا أخرى في المنطقة وغيرها من المناطق.

انتهت **الأردن** من تنفيذ استراتيجية وطنية للمعلومات والأمن السيبراني امتدت لخمس سنوات (2012 – 2017)33، بالإضافة إلى تكوينها لفريق وطني للاستجابة للطوارئ الحاسوبية في عام 2013. وقد أطلقت الأردن استراتيجيتها الخمسية الثانية34 في عام 2018 لمواكبة التطور السريع للتقنيات الحديثة –

32 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
33 http://nitc.gov.jo/PDF/NIACSS.pdf
34 http://moict.gov.jo/uploads/Public-Consultations/NCSS-DRAFT.pdf

بما في ذلك التشغيل الآلي– وللتصدي للتهديدات المتزايدة والهجمات الإلكترونية التي يتعرض لها القطاعين العام والخاص.

تهدف الاستراتيجية الوطنية للأمن السيبراني35 في **دولة الإمارات العربية المتحدة** إلى إنشاء بنية تحتية إلكترونية آمنة وقوية للمواطنين والأنشطة التجارية. وقد أطلقت الهيئة العامة لتنظيم قطاع الاتصالات، الكيان المسؤول عن قطاع تكنولوجيا المعلومات والاتصالات والتحول الرقمي في البلاد، النسخة المحدثة من الاستراتيجية في عام 2019. وتعتمد تلك الاستراتيجية على خمس ركائز وعدد ستين مبادرة تهدف إلى تعبئة النظام البيئي للأمن السيبراني كاملًا في دولة الإمارات العربية المتحدة. وتهدف الاستراتيجية الجديدة إلى زيادة ثقة المواطنين في العالم الرقمي، وتشجيع الابتكار وريادة الأعمال في مجال الأمن السيبراني، وتمكين الشركات الصغيرة والمتوسطة من حماية نفسها من أكثر الهجمات الإلكترونية شيوعًا، وحماية أصول البنية التحتية للمعلومات المهمة "وتكوين قوة عاملة ذات مستوى عالمي للأمن السيبراني في الإمارات العربية المتحدة" 36.

في عام 2015، أنشأت **جمهورية مصر العربية** المجلس الأعلى للأمن السيبراني ليضم ممثلين عن مختلف الهيئات الحكومية. وأطلقت الدولة الاستراتيجية الوطنية للأمن السيبراني (2018) في ضوء الأهداف الاستراتيجية التي أدت إلى إنشاء المجلس الأعلى للأمن السيبراني (ESCC)، التابع لمجلس الوزراء، ويترأسه وزير الاتصالات وتكنولوجيا المعلومات. وتتكون تلك الاستراتيجية من ستة برامج استراتيجية تشمل برنامج لتطوير الإطار التشريعي الملائم "لأمن الفضاء السيبراني ومكافحة الجرائم السيبرانية وحماية الخصوصية والهوية الرقمية"، والذي سينفذ بالتعاون مع جميع الجهات المعنية مثل الحكومة والقطاع الخاص والمؤسسات الأكاديمية والمجتمع المدني. وهناك برنامج آخر لتكوين فرق للتصدي لحوادث أمن الحاسبات في القطاعات الحيوية. وتركز البرامج الأخرى على تطوير المهارات والقدرات في مجال الأمن السيبراني ودعم البحث والتطوير.

2.4 فرق التصدي لحوادث أمن الحاسبات

فريق التصدي لحوادث أمن الحاسبات، المعروف أيضًا باسم فريق الاستجابة للطوارئ الحاسوبية أو فريق التأهب لحالات الطوارئ الحاسوبية، يعد بمثابة منظمة أو مجموعة من الخبراء المعنية بتلقي الحوادث الأمنية الحاسوبية ودراستها والاستجابة لها. وقد تكون تلك الفرق ذات نطاق جغرافي محدد أو مسؤولة عن قطاع بعينه، ويقودها إما القطاع العام أو القطاع الخاص أو كلاهما. وتؤدي فرق التصدي لحوادث أمن الحاسبات وظيفة حيوية لتبادل المعرفة لضمان الأمن. وجدير بالذكر أن العديد من الدول العربية

35 https://www.tra.gov.ae/userfiles/assets/Lw3seRUaIMd.pdf

36 المصدر نفسه

تدير فرقًا للتصدي لحوادث أمن الحاسبات أو فرقًا للاستجابة للطوارئ الحاسوبية. وهناك بعض الدول تدير أيضًا مراكز تنسيق أوسع نطاقًا للأمن السيبراني، والتي تشتمل مهامها على التواصل، والتدريب المستمر، واعتماد خبراء الأمن السيبراني مثل الباحثين الأمنيين في "مجال القرصنة الأخلاقية"، بالإضافة إلى غيرها من الأنشطة لزيادة القدرات وتنمية وتعميق العلاقات بين الجهات المعنية.

تعد تونس واحدة من أوائل الدول العربية التي كونت فريقًا للتصدي لحوادث أمن الحاسبات في عام 2007، استنادًا إلى قانون السلامة المعلوماتية رقم 5 لعام 2004. وكذلك ينص القانون على الرد على الهجمات أو الاختراقات التي تنطوي على مؤسسات حكومية، ويحدد العلاقة التشغيلية بين الوكالة الوطنية للسلامة المعلوماتية وأي وزارات تتعرض لهجمات37.

وقد تكونت فرق للتصدي لحوادث أمن الحاسبات أيضًا في **الإمارات وتونس ومصر والسودان وسلطنة عمان والسعودية**، حيث تعمل على الارتقاء بمستوى الأمن الشامل للمعلومات على الصعيد الوطني، وحماية البنية التحتية لتكنولوجيا المعلومات جراء المخاطر والتهديدات والهجمات السيبرانية، وكذلك توفير الدعم الفني المباشر للهيئات الحكومية. (فقد أجرى الاتحاد الدولي للاتصالات تقييمات للوقوف على مدى الجاهزية لتكوين فرق للتصدي لحوادث أمن الحاسبات في جزر القمر وجيبوتي وموريتانيا وفلسطين38). ومع ذلك، ففي حين أن فرق التصدي لحوادث أمن الحاسبات القائمة فعليًا غالبًا ما تؤدي عملًا رائعًا، إلا أنها تكاد تفتقر للموارد المالية والتجهيزات والقوى البشرية والمهارات والتمكين لإقامة العلاقات والشبكات التعاونية.

37 https://legislation-securite.tn/fr/node/44031
38 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx

وعلى الرغم من التحديات التي تواجهها تلك الفرق، إلا أنها قد أدت فعليًا دورًا مهمًا في حماية البنية التحتية لشبكة الإنترنت بالمنطقة:

- أنشأت **عمان** فريقها الخاص للتصدي لحوادث أمن الحاسبات في 2010، وتستضيف المركز العربي الإقليمي للأمن السيبراني الذي يهدف إلى تقديم الخدمات والمبادرات إلى المنطقة للارتقاء بمستوى الأمن الإلكتروني من خلال التعاون الإقليمي.
- يعد فريق الاستجابة لحوادث أمن الحاسوب في **الأردن** فريقًا وطنيًا للتصدي لحوادث أمن الحاسبات، والذي أنشأ أيضًا مركزًا جديدًا يضم كفاءات في مجال الأمن السيبراني إلى جانب دوره التشغيلي. وتمتلك الأردن أيضًا مشروع منظومة الأمن السيبراني بالتعاون مع الجيش (JAF-CERT)، وتخطط لإنشاء خدمات مصرفية أو مالية في المستقبل. وتعمل الأردن أيضًا نحو إنشاء منصة وطنية لتبادل المعلومات أو تحديدًا المعلومات المرتبطة بالتهديدات (أي مركز تحليل ومشاركة المعلومات (ISAC)).

كيفية عمل فرق التصدي لحوادث أمن الحاسبات

لقد انتشر مفهوم فرق التصدي لحوادث أمن الحاسبات منذ أواخر الثمانينات في جميع أنحاء العالم بوصفه نموذجًا مهمًا للتعامل مع حوادث مثل البرمجيات الخبيثة، والاختراقات، وهجمات الحرمان من الخدمات (DDOS) وغيرها من تهديدات. عادة ما تعمل فرق التصدي لحوادث أمن الحاسبات يوميًا مع مؤسسات أخرى مثل البنوك والجامعات ومقدمي خدمات البنية التحتية وغيرها من هيئات القطاع الخاص، بغرض تبادل المعلومات والخبرات وتطوير القدرات وبناء العلاقات لمكافحة التهديدات المستمرة والتأهب للاستجابة للحوادث.

عادة ما تكون فرق التصدي لحوادث أمن الحاسبات أثناء الحوادث الخطيرة بمثابة "جهة التنسيق والدعم عند الاستجابة في حالات الحوادث"[1]. ويمكن أن تؤدي القدرة على تبادل المعلومات إلى الحد من عدد الهجمات ونوعها ومدتها وتأثيرها[2].

يعتمد نموذج فرق التصدي لحوادث أمن الحاسبات على التعاون والانفتاح؛ ذلك أن المشاركة السريعة للمعلومات المتعلقة بالثغرات والبرمجيات الخبيثة والهجمات تعد أمرًا ضروريًا لتلك الفرق لكي تعمل بكفاءة. وهكذا حينما يظهر هجوم أو تهديد خطير أو واسع النطاق، فإنه يفترض على فرق التصدي لحوادث أمن الحاسبات أن تكون قادرة أيضًا على التصرف، معتمدة في ذلك على المنظمات الأخرى على الصعيد الوطني وفرق التصدي لحوادث أمن الحاسبات في الدول الأخرى في المنطقة وغيرها من مناطق العالم من أجل الحصول على المعلومات والمساعدة اللازمتين. هذه العلاقات تحتاج إلى وقت واهتمام لبنائها؛ وذلك لأنها تستند إلى المعرفة والثقة. وإذا لم تستثمر الدول مواردها في تنمية المهارات وبناء العلاقات، فمن المرجح أن تكون أقل فعالية في الاستجابة للحوادث الخطيرة.

1 https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams

2 https://www.researchgate.net/publication/319645577_Cyber_Security_Capacity_Does_it_Matter

- يهدف فريق الاستجابة الوطني لطوارئ الحاسب الآلي (aeCERT) في **دولة الإمارات العربية المتحدة** إلى حماية البنية التحتية لتكنولوجيا المعلومات ونشر المعلومات المتعلقة بالتهديدات والثغرات وحوادث الأمن السيبراني. ويقدم كذلك الفريق مجموعة من الخدمات للجهات الحكومية مثل الاستجابة للحوادث، والطب الشرعي الرقمي، وتقييم أوجه الضعف والثغرات، واختبار الاختراق، وحملات التوعية والدورات، وتقييم عمليات الاحتيال الالكتروني39.
- يعمل المركز الوطني للاستعداد لطوارئ الحاسبات والشبكات في **مصر** بكامل طاقته، وتشتمل الإستراتيجية الوطنية للأمن السيبراني (2017–2021)، بوصفها برنامجًا أساسيًا، على نظام وطني متكامل لحماية الفضاء السيبراني وتأمين البنية التحتية لتكنولوجيا المعلومات والاتصالات بالتعاون مع فرق التصدي لحوادث أمن الحاسبات في القطاعات الحيوية على الصعيد الوطني "استنادًا إلى التجربة الرائدة لقطاع تكنولوجيا المعلومات والاتصالات"40.
- يضطلع فريق التصدي لحوادث أمن الحاسبات التابع لحكومة **البحرين** بدور أساسي في تأمين الشبكات الحكومية. وكذلك تخطط البحرين لإنشاء فريق قطاعي للتصدي لحوادث أمن الحاسبات في عام 2020.
- حصلت مجموعة من الفرق ببعض الدول العربية على عضوية منتدى فرق الأمن والاستجابة للحوادث (FIRST)41، وهي مجموعة دولية من فرق التصدي لحوادث أمن الحاسبات التابعة للقطاعين العام والخاص، والتي تكونت لتبادل المعلومات والمعرفة وأفضل الممارسات والتصدي للحوادث. وتشمل الدول العربية المشار إليها سلفًا كل من المغرب وتونس ومصر والسعودية وعمان والإمارات.

وإذا ما قارنا فرق التصدي لحوادث أمن الحاسبات بالدول العربية بمثيلتها في سائر المناطق الأخرى، سنجدها تميل إلى العمل باتباع نهج "السيطرة من القمة إلى القاعدة" تحت قيادة الدولة. هذا، ومن خلال هذا النهج، فقد تواجه الحكومات تحديات تتمثل في مواءمة الحوافز الموضوعة مع الجهات المعنية الأخرى، ولا سيما فيما يتعلق بتبادل المعلومات والكشف عن الثغرات. وهناك بعض فرق التصدي لحوادث أمن الحاسبات التي تسيطر عليها الحكومة نجدها منحازة للأولويات الوطنية الاستخباراتية، لذا فقد تواجه صعوبة في بناء الثقة والتنسيق مع النظراء الحكوميين في الدول الأخرى. ومع ذلك، فهناك اهتمام كبير بمشاركة التجارب والخبرات، ولا سيما بين دول الخليج. فقد أظهرت مشاوراتنا تأييدًا لزيادة

39 https://www.tra.gov.ae/aecert
40http://www.mcit.gov.eg/Upcont/Documents/Publications_12122018000_EN_National_Cybersecurity_Strategy_2017_2021.pdf
41 https://www.first.org/

التعاون الإقليمي بين فرق التصدي لحوادث أمن الحاسبات أو مراكز تنسيق الأمن السيبراني، بما في ذلك مفهوم إنشاء منصة لتبادل المعلومات لحظيًا بشأن التهديدات التي تواجه الدول العربية.

حددت العديد من الحكومات العربية طرقًا مختلفة للتعامل مع الباحثين الأمنيين في مجال "القرصنة الأخلاقية" الذين ينفذون عمليات اختراق أو غيرها من أشكال اختبار النظام أو الشبكة بهدف ضمان أمن الأنظمة المعلوماتية لمنظمة ما42. وتعمل هذه الحكومات على تسخير المهارات والخبرات البشرية المتاحة وتطويرها على نحو يحفز على التعاون والحد من المخاطر. وفي سياق هذا المجال الذي يضم أفضل الممارسات الناشئة، تبادل المشاركون في ورشنا الإقليمية المناهج التي اتبعوها؛

- عقدت **عمان** مسابقة لترتيب المواهب في مجال الأمن السيبراني. وكذلك تعد دليلًا للباحثين المشتغلين في مجال القرصنة الأخلاقية أو "سفراء الأمن السيبراني".
- أصدرت **تونس** تراخيصًا لمزودي خدمات الأمن السيبراني، وعقدت مسابقات الهاكاثون أو نظمت فعاليات لاختبار مدى صمود البنية التحتية للاختراق.
- أصدرت **الأردن** قانونًا للارتقاء بمستوى الثقة من خلال ترخيص خدمات الأمن السيبراني.

وقد شملت الاقتراحات الأخرى مقترحًا بوضع إطار قانوني لتيسير سبل التعاون البحثي مع فرق التصدي لحوادث أمن الحاسبات وأجهزة إنفاذ القانون في مجال اختبار تقييم أوجه الضعف والقصور، وكذلك وضع إطار آخر لتوسيع دور جمعية الإنترنت الوطنية43 أو مجموعات المصالح الخاصة العالمية44 في جذب المتطوعين لأنشطة الأمن السيبراني والتنسيق مع فرق التصدي لحوادث أمن الحاسبات.

يعد هذا المجال مجالًا معقدًا وأحيانًا غامضًا لا تتضح فيه دائمًا النية من وراء الأبحاث المعنية بالكشف عن الثغرات والقدرة على منع الاختراقات. فهناك العديد من الحكومات التي تعمل على تحديد أو اعتماد الباحثين الأمنيين في مجال الأمن الأخلاقي، وتجنب تقويض الأنشطة المفيدة التي من شأنها تحقيق مرونة شاملة وتكوين قاعدة مهارات محلية. ولما كانت علاقات الثقة والمرونة من الأهمية بمكان، فإنه يجب توخي الحذر تجاه عرقلة التعاون مع النظم القانونية المنفتحة عليه.

4.3 التواصل والتعاون على الصعيدين الوطني والإقليمي

لا تزال مبادرات الأمن السيبراني للتواصل والتعاون الوطني في مراحلها الأولية نسبياً في معظم الدول العربية، مثلها في ذلك مثل العديد من المناطق الأخرى في العالم. على الصعيد الدولي، يوجد لدى أقل

42 https://en.wikipedia.org/wiki/White_hat_(computer_security)
43 https://www.internetsociety.org/chapters/
44 https://www.internetsociety.org/sigs

من نصف دول العالم "شراكات وترتيبات تعاونية بين القطاعين العام والخاص"45. ويصف الاتحاد الدولي للاتصالات النهج الذي تتبعه الجهات المعنية المتعددة تجاه الأمن السيبراني على أنه يشمل مبادرات "تمتلك مدخلات من جميع القطاعات والتخصصات (بما في ذلك الاتفاقات الثنائية والمتعددة الأطراف، والمشاركة في المنتديات أو الاتحادات الدولية، والشراكات بين القطاعين العام والخاص، والشراكات بين الأجهزة، وأفضل الممارسات)"46.

ومن الجدير بالذكر أن هناك اتجاه متزايد في البلدان العربية للدخول في المزيد من الشراكات التعاونية على الصعيد الوطني مثلما يتضح في الظهور الأخير للفرق القطاعية المعنية بالتصدي لحوادث أمن الحاسبات. وكذلك تتزايد جهود الاتصال والتعاون الإقليمي، وهناك دافع واضح لتعميق التعاون الإقليمي حيثما كان ذلك مناسبًا ومثمرًا.

5 التوصيات

لا بد على الحكومات أن تحدث من نهجها تجاه أمن البنية التحتية لشبكة الإنترنت من خلال التركيز على الغرض الأساسي من أمن الإنترنت؛ بمعنى أن الأمن لم يعد هدفًا نهائيًا، بل وسيلة لتيسير تحقيق الأهداف الاجتماعية والاقتصادية الشاملة. فالأمن اليوم لا يتعلق ببناء جدران حول البنية التحتية، وإنما يتمثل دوره الآن في تيسير اقتصاد رقمي عالمي مترابط يعتمد بعضه على بعض، بالإضافة إلى المحافظة على الاتصال الإقليمي الذي يعد هدفًا أساسيًا.

ولما كان الإنترنت "شبكة الشبكات"، فإن اقتصار التركيز على مرونة الشبكة الوطنية لن يكفل استمرار الاتصال بشبكة الانترنت، وإنما يجب أن تكون مرونة الإنترنت الإقليمية في حد ذاتها هدفًا وغاية. ولتحقيق ذلك، فإنه يجب على الحكومات المشاركة والتنسيق مع بعضها البعض على الصعيد الإقليمي.

جدول بملخص التوصيات

التوصيات الوطنية	التوصيات الإقليمية
يجب على الحكومات تعزيز نظام بيئي لأمن الإنترنت يتسم بالانفتاح والتعاون والمرونة يتضمن ما يلي:	يجب على الحكومات التعاون مع جميع الجهات المعنية لتعزيز التعاون الإقليمي على النحو التالي: ○ تكوين مجموعة إقليمية من الخبراء الأمنيين من الحكومة والمؤسسات

45 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
46 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

○ تعيين البنية التحتية المعلوماتية المهمة وحمايتها. ○ تطوير مرونة البنية التحتية للإنترنت من خلال تيسير نشر المعايير الأمنية وأفضل الممارسات. ○ تطوير مرونة البنية التحتية لشبكة الإنترنت من خلال تحقيق ربط أفضل بين الشبكات. ○ تيسير عملية تبادل المعلومات، وبناء العلاقات بين الجهات المعنية. ○ تكوين فرق للتصدي لحوادث أمن ● الحاسبات ودعمها على الصعيد الوطني. ○ الاستفادة من المؤسسات العامة في أن تكون مثالًا يحتذى به. ● تحديد ومواجهة العقبات القانونية التي تحول دون مشاركة المعلومات (بما في ذلك دعم الباحثين الأمنيين في "مجال القرصنة الأخلاقية") وإجراء الأبحاث المتعلقة بالثغرات الأمنية والحوادث والتهديدات. ● العمل على تسخير مهارات القرصنة الأخلاقية وتطويرها من خلال عقد مسابقات المواهب والهاكاثون أو عمل أدلة لمجموعات الباحثين المحليين المشتغلين في مجال القرصنة الأخلاقية أو إصدار التراخيص اللازمة لمزودي خدمات الأمن السيبراني.	التجارية والتقنية والأكاديمية والمجتمع المدني لتقديم إرشادات غير ملزمة للمنطقة حول قضايا البنية التحتية لأمن الإنترنت حسب الضرورة. ○ المشاركة في مبادرات الأمن السيبراني الحالية المتعلقة بالاتصالات والتنسيق وتعزيزها، بما في ذلك النظر في إمكانية إنشاء منصة إقليمية لتبادل المعلومات بشأن التهديدات. ○ حشد موارد فرق التصدي لحوادث أمن الحاسبات كلما أمكن مثل تنسيق ومشاركة الدورات التدريبية فيما بينها، وذلك لزيادة المعرفة والخبرة، وبناء علاقات عبر الحدود بين المتخصصين الذين يبنون جسور الثقة من أجل زيادة التعاون. ○ زيادة مرونة المسار والتوجيه لحركة الإنترنت على أساس أنه "شبكة الشبكات" إقليمية لزيادة نقاط الخروج بالشبكة وتقليل نقاط الاختناق الفعلية أو "نقاط التعطل الفردية".

5.2 التوصيات الوطنية

يجب على الحكومات إيجاد بيئة تركز على النظام البيئي لأمن الإنترنت تتسم بالانفتاح والتعاون والمرونة. وكذلك يجب على الحكومات والجهات المعنية الأخرى تمكين المؤسسات والأفراد من خلال تبادل المعلومات، وتعزيز أفضل الممارسات، وأن تكون مثالًا يحتذى به.

وإلى جانب دور الحكومات في تيسير تبادل المعلومات وتعزيز أفضل الممارسات، فإنها تضطلع بدور فريد في وضع السياسات، وإظهار روح القيادة في النظام البيئي الخاص بالبنية التحتية للإنترنت. وينبغي على الحكومات أن تضطلع بدور رائد في الارتقاء بالوعي والخضوع للمساءلة، وأن تمعن النظر في الآثار المحتملة للسياسات الجديدة على جميع الجهات المعنية وإشراكها في وضعها. ويجب أن تلتزم السياسات وأي قوانين تسنها الحكومات بالمبادئ الأساسية الأربعة؛ وهي الوعي والمسؤولية والتعاون والحفاظ على الحقوق الأساسية وخصائص الإنترنت.

5-1-1 تعيين البنية التحتية المعلوماتية المهمة وحمايتها

يجب على جميع الجهات المعنية العمل معًا لتعيين وتصنيف الأنظمة والشبكات المترابطة اللازمة لضمان رفاهية المواطنين، وتوفير الخدمات الأساسية، والأداء الفعال للحكومة والاقتصاد. ويعد التعيين الدقيق للأنظمة وتصنيفها أساسًا لنجاح عملية مكافحة المخاطر الأمنية؛ فهذا من شأنه أن يضمن إمكانية تركيز التدابير الأمنية المناسبة على الخدمات والبنية التحتية المعلوماتية المهمة، والحيلولة دون تبديد الموارد في مواضع غير أساسية.

وكذلك يجب على جميع الجهات المعنية إعطاء الأولوية للبنية التحتية المعلوماتية المهمة، وإجراء تقييمات للمخاطر، وتنفيذ السياسات والممارسات الأمنية المناسبة دون الإخلال بالقدرات الوظيفية.

هذا ويمكن لعملية وضع نماذج للتهديدات أن تمثل وسيلة مفيدة لتعيين البنية التحتية المعلوماتية المهمة وحمايتها؛ ذلك لأنها تنظر إلى البنية التحتية من وجهة نظر المهاجم لتحديد أسباب التهديد المرجح استخدامه وأهدافه المحتملة، علمًا أنه يمكن الاطلاع على إرشادات أكثر تفصيلاً حول مشغلي الشبكات في الملحق 3 بهذه الوثيقة.

5-1-2 تطوير مرونة البنية التحتية للإنترنت من خلال تيسير نشر المعايير الأمنية وأفضل الممارسات.

في عالم مترابط بأقاليمه التابعة التي تمتد عبر شبكات ودول وقارات متعددة، يكون من الأهمية بمكان أن يسعى جميع المشاركين جاهدين نحو تطبيق أفضل الممارسات في مجال أمن البنية التحتية لشبكة الإنترنت. وقد تنطبق الإرشادات الموجهة لمشغلي الشبكات في الملحق 3 على كل من مؤسسات القطاعين العام والخاص المسؤولة عن أجزاء من البنية التحتية المعلوماتية المهمة مثل مشغلي نطاقات المستوى الأعلى في ترميز الدولة (ccTLDs) أو الشبكات الحكومية الكبرى.

يستعرض الملحق 3 بهذه الوثيقة إرشادات أكثر تفصيلاً لمشغلي الشبكات، بما في ذلك تطبيق البروتوكولات والممارسات المتعلقة بدقة التوجيه، وأمان أسماء النطاقات والبريد الإلكتروني. ويشتمل الملحق أيضًا على روابط لمزيد من المصادر حول كيفية تطبيق مشغلي الشبكات ونقاط تبادل الإنترنت للمعايير المتفق عليها بشكل متبادل لأمن التوجيه.

يمكن أن تحول العقبات القانونية في بعض البلدان دون تطوير تقنيات أمن التوجيه ونشرها. وفي سبيل إيجاد الجهات المعنية لحلول للعقبات التي تم تحديدها، فإنه يجب عليهم إيلاء اهتمام كبير بتأثيرهم المحتمل على خصوصية الأفراد.

5-1-3 تطوير مرونة البنية التحتية لشبكة الإنترنت من خلال تحقيق ربط أفضل بين الشبكات.

يجب على الحكومات أن تشجع استخدام نقاط تبادل الإنترنت على الصعيد الوطني، وزيادة التعاون والاتصالات بين مختلف الشبكات العربية إقليميًا لتحسين الاتصال البيني بما في ذلك الصلات الدولية. ويجب على مشغلي الشبكات ونقاط تبادل الإنترنت أيضًا تطبيق المعايير المتفق عليها بشكل متبادل لأمن التوجيه47، مما سيساعد ذلك على زيادة التوجيه ومرونة حركة بيانات الإنترنت.

5-1-4 تيسير عملية تبادل المعلومات وبناء العلاقات

على الرغم من إدراك وجود ميل للتعامل مع قضية الأمن بطريقة أكثر مركزية بمعرفة الدولة في تلك الدول، إلا أنه لا تزال هناك فرصة لتعزيز عملية تبادل المعلومات. ذلك أن تطوير عمليتي الإبلاغ عن الاختراقات وتبادل المعلومات من شأنه أن يؤدي إلى تحسين قدرة جميع الجهات المعنية على التصدي للحوادث والاستجابة لها.

ذلك يتطلب تحسين الثقة بين الجهات المعنية، وخاصة عبر إقامة الشراكات بين القطاعين العام والخاص. ويمكن بناء الثقة من خلال الاتصالات الرسمية وغير الرسمية المتكررة، وتحديد الأهداف

47 https://www.internetsociety.org/issues/manrs/

المشتركة والعمل على تحقيقها، وضمان الموثوقية التقنية للمؤسسات والأفراد48. وكذلك يجب أن تستند الثقة إلى الاعتراف بأن الجهات المعنية الآخرى شركاء لهم قيمتهم وأولوياتهم وخبراتهم.

وفي حين أن هذه التيسيرات يمكن أن تتحقق بفضل علاقات الثقة اللازمة لمشاركة المعلومات بشكل فعال، إلا أنها قد تشمل أيضًا سياقًا أوسع نطاقًا من التشاور والحوار بين الحكومة، والفرق الوطنية للتصدي لحوادث أمن الحاسبات، والمجتمع المدني، والوسط الأكاديمي، والمجتمع التقني، والقطاع الخاص. ويمكن لهذه المحادثات، سواء أكانت رسمية أو غير رسمية، أن تحدد المواضع التي يلزم فيها اتخاذ إجراء على الصعيد الوطني مثل الحاجة لبرامج تدريبية جديدة لتخفيف فجوة القدرات في مجالات أمنية معينة، أو تبني ممارسات أمنية حديثة داخل الأجهزة الحكومية.

5-1-5 تكوين فرق للتصدي لحوادث أمن الحاسبات على الصعيد الوطني ودعمها

تضطلع فرق التصدي لحوادث أمن الحاسبات بدور مهم تجاه معالجة قضايا أمن البنية التحتية لشبكة الإنترنت من خلال تعيين الحوادث الأمنية، ومساعدة المؤسسات على حماية أنفسها من الهجمات السيبرانية والتعافي منها. إن تواتر التهديدات السيبرانية وخطورتها يتطلب بناء قدرات فعالة تجاه المراقبة والإنذار والاستجابة لها.

ويجب على الحكومات العمل إلى جانب الجهات المعنية الأخرى مثل المجتمع التقني لتكوين فرق للتصدي لحوادث أمن الحاسبات في حالة عدم وجودها، ودعم تلك التي تعمل بشكل تعاوني لتعزيز الوعي والمسؤولية والتعاون والحقوق الأساسية وخصائص الإنترنت.

ويمكن للحكومات أيضًا أن تشجع العمل الذي تؤديه فرق التصدي لحوادث أمن الحاسبات من أجل الأهداف التالية:

1. ضمان توجيه الحوافز باتجاه زيادة تبادل المعلومات على النحو الأمثل، وزيادة الشفافية فيما يتعلق بالثغرات والهجمات السيبرانية المعروفة.
2. رفع قدرات فرق التصدي لحوادث أمن الحاسبات، ولا سيما تلك الفرق ذات الطبيعة المركزية التي تديرها الدولة، على نشر المعرفة، وبناء علاقات تعاونية، وإتاحة فرص المشاركة للخبراء الإقليميين.

48 https://www.researchgate.net/publication/319645577_Cyber_Security_Capacity_Does_it_Matter

3. الحرص على توفير الموارد الكافية لفرق التصدي لحوادث أمن الحاسبات لدعم جمع المعلومات المتعلقة بالتهديدات وتحليلها، ونشر المعلومات العملية.
4. الحرص على أن تصبح المؤسسات الحكومية مثالًا يحتذى به، واستخدامها لفرق التصدي لحوادث أمن الحاسبات في عمليتي تبادل المعلومات وبناء القدرات.

5-1-6 الاستفادة من المؤسسات العامة في أن تكون مثالًا يحتذى به في مجال الأمن السيبراني

يمكن للحكومات، كونها مالكًا ومشغلًا للنظم والشبكات المعلوماتية، أن تكون مثالًا يحتذى به من خلال تبنيها لأفضل الممارسات، واستخدام التقنيات الأمنية، ومن خلال عمليات الشراء الخاصة بها. ويجب على الحكومات أيضًا النظر في استخدام أدوات مثل الحوافز الاقتصادية، وكذلك تشجيع الصناعة على تحسين الأمن السيبراني بشكل استباقي، وتمكين المواطنين من المطالبة بحلول أمنية أفضل؛ ذلك أن تلك الحلول قد تكون في بعض الأحوال أكثر فعالية من القوانين.

يجب على الحكومات أيضًا إعطاء الأولوية للبنية التحتية الخاصة بشبكة الإنترنت والحفاظ على التواصل القائم عبر الإستراتيجيات الأمنية الوطنية، مع مراعاة أن الهدف العام للأمن يتمثل في خدمة الرخاء الاجتماعي والاقتصادي. ويجب على الحكومات الاضطلاع بدور نشط لتشجيع أجهزتها والأطراف الثالثة الموردة للخدمات الحكومية على استخدام المعايير الأمنية وأفضل الممارسات في بنيتها التحتية.

ويمكن للحكومات أيضًا الاستفادة من موازناتها لضمان تخصيص الموارد المناسبة، مثل المخصصات المالية والموظفين، للإدارات والأجهزة الحكومية للعمل ولتأمين أنظمتها.

5-1-7 تحديد ومواجهة العقبات القانونية التي تحول دون مشاركة المعلومات (بما في ذلك دعم الباحثين الأمنيين في "مجال القرصنة الأخلاقية") وإجراء الأبحاث المتعلقة بالثغرات الأمنية والحوادث والتهديدات.

يمكن أن تمثل العقبات القانونية عائقاً أمام الباحثين الأمنيين وتمنعهم من الكشف عن المعلومات المتعلقة بالثغرات. فالباحثون الأمنيون في "مجال القرصنة الأخلاقية"، المنفذون لعمليات الاختراق وغيرها من الاختبارات للأنظمة والشبكات من خارج المؤسسة، قد يخشون من أن الكشف عن أوجه الضعف والثغرات أو الحوادث أو التهديدات الأمنية المتعلقة بالتوجيه قد يضعهم في مساءلة قانونية. ولذلك ينبغي على الحكومات أن تبدي تقبلًا ودعمًا أفضل للباحثين الأمنيين في "مجال القرصنة الأخلاقية". وذلك يمكن تحقيقه من خلال ما يلي:

- تحديد العقبات القانونية أمام تبادل كل ما يتعلق بالمعلومات والثغرات وتذليلها.

- العمل على تسخير المهارات المتاحة للأشخاص وتطويرها على نحو يحفز على التعاون من خلال، على سبيل المثال، مسابقات المواهب السيبرانية أو الهاكاثون أو مجموعات الباحثين المشتغلين في مجال القرصنة الأخلاقية.
- دراسة وضع أطر للباحثين من أجل التعاون مع فرق التصدي لحوادث أمن الحاسبات بشأن الاختبارات المتعلقة بالكشف عن الثغرات.
-

5.2 التوصيات الإقليمية

5-2-1 المشاركة في مبادرات الأمن السيبراني الحالية المتعلقة بالاتصالات والتنسيق وتعزيزها

تعد علاقات العمل المتبادلة والمبادرات الإقليمية التي تعزز التعاون بين الدول وسيلة أساسية للتشجيع على اتباع نهج تعاوني شامل يعود بالفائدة على الجميع[49]. ويجب على الحكومات المشاركة على نحو استباقي في المنتديات الإقليمية والدولية للتعاون في مجال الأمن السيبراني، وتركيز الجهود على التعاون الشامل، والتنسيق وتبادل المعلومات بين جميع الجهات المعنية التي تدعم الخصائص الأساسية لشبكة الإنترنت.

وبالإضافة إلى التنسيق مع المركز العربي الإقليمي للأمن السيبراني والقمة الإقليمية للأمن السيبراني في الدول العربية، فإنه يجب على الحكومات وغيرها من الجهات المعنية التفكير في المشاركة في المبادرات العالمية؛ ذلك أن المنتديات التالية يمكن أن تساعدهم على تعزيز المعلومات وتبادلها بشأن أمن البنية التحتية لشبكة الإنترنت، وبناء علاقات عبر القطاعات والحدود. فتلك العلاقات والتدفق المعرفي الحديث وأفضل الممارسات المتحققة قد تمثل ضرورة من ضروريات التعامل مع الحوادث الخطيرة مستقبلًا:

- المنتدى العالمي للخبرة السيبرانية (GFCE)
- اللجنة الدولية لاستقرار الفضاء السيبراني (GCSC)
- المركز العالمي لقدرات الأمن السيبراني، أكسفورد (GCSCC)

وكذلك يجب على الحكومات إشراك جميع الجهات المعنية، بما في ذلك تلك العابرة للحدود، لتحديد ما إذا كان من المفيد والعملي تبادل المعلومات محليًا على نطاق أكبر حول التهديدات استنادًا إلى بعض العلاقات الثنائية القائمة للتبادل اللحظي للمعلومات المرتبطة بالتهديدات والثغرات.

5-2-2 حشد موارد فرق التصدي لحوادث أمن الحاسبات إقليميًا

49 https://www.oecd-ilibrary.org/science-and-technology/the-promotion-of-a-culture-of-security-for-information-systems-and-networks-in-oecd-countries_232017148827

يجب على فرق التصدي لحوادث أمن الحاسبات في جميع أنحاء المنطقة حشد مواردهم كلما أمكن؛ إذ يمكنهم، على سبيل المثال، التنسيق أو حتى إتاحة الدورات التدريبية لفرق التصدي لحوادث أمن الحاسبات الأخرى. وهذا من شأنه زيادة المعرفة والخبرة في جميع أنحاء المنطقة، وكذلك بناء علاقات عابرة للحدود بين المختصين الذين يبنون العلاقات ويمدون جسور الثقة من أجل تحقيق قدر أكبر من التعاون.

5-2-3 زيادة مرونة المسار الإقليمي لحركة بيانات الإنترنت

ولما كان الإنترنت "شبكة الشبكات"، فإن اقتصار التركيز على مرونة الشبكة الوطنية لن يكفل استمرار الاتصال بشبكة الإنترنت، وإنما يجب أن تكون مرونة الإنترنت الإقليمية في حد ذاتها هدفًا وغاية. فحوادث الكابلات البحرية وما ترتب عليها من انقطاع الاتصال بالإنترنت وتعطل بنيته التحتية على صعيد المنطقة[50] قد أظهر ضرورة وجود مرونة في مسار توجيه حركة بيانات شبكة الإنترنت على نحو لا يجعل حركة البيانات متركزة في عدد صغير من نقاط الاختناق الإقليمية (أو نقاط تعطل فردية).

يجب على الحكومات أن تعمل إلى جانب الجهات المعنية الأخرى على أساس أن الإنترنت "شبكة الشبكات" إقليمية، وذلك لزيادة الربط الشبكي الثري والمتنوع على الصعيدين الوطني والدولي بغرض التقليل من نقاط الإخفاق الفردية ومشكلات عنق الزجاجة.

يجب على جميع الجهات المعنية العمل أيضًا نحو تحقيق مزيد من التعاون العابر للحدود بين مشغلي الشبكات ونقاط تبادل الإنترنت عبر الدول العربية لتنسيق وتبادل المعرفة والاستجابة للحوادث.

شكر وتقدير

وضعت هذه المبادئ التوجيهية بالتشاور مع خبراء الأمن السيبراني في الدول العربية وخارجها، وأعضاء جمعية الإنترنت بما في ذلك فروع المؤسسة في المنطقة والذين قاموا بمراجعة هذه المبادئ التوجيهية.

تود جمعية الإنترنت أن تتوجه بالشكر للمؤسسات التالية وأعضائها لدعمهم للعملية التحضيرية والتشاورية:

معهد تشاتام هاوس، المعهد الملكي للعلاقات الدولية، لاستضافته لورشة العمل التشاورية (مايو 2019)

المملكة العربية السعودية، لاستضافتها ورشة العمل التشاورية (يونيو 2019)

دولة الكويت، لاستضافتها ورشة العمل التشاورية (سبتمبر 2019)

سلطنة عمان، لاستضافتها ورشة العمل التشاورية (نوفمبر 2019)

The Internet Society is grateful to regional experts for their active participation in this process and valuable contributions, including the following institutions:

50 https://gigaom.com/2013/03/27/undersea-cable-cut-near-egypt-slows-down-internet-in-africa-middle-east-south-asia/

كما تود جمعية الإنترنت أن تعبر عن امتنانها للخبراء الإقليميين والمؤسسات التالية لمشاركتهم الفاعلة في هذه العملية ولمدخلاتهم الهامة في هذه الوثيقة:

- وزارة الاقتصاد الرقمي والريادة وهيئة تنظيم الاتصالات بالمملكة الهاشمية الأردنية
- هيئة تنظيم الاتصالات في دولة الإمارات المتحدة.
- هيئة تنظيم الاتصالات في سلطنة عمان.
- هيئة تنظيم الاتصالات في دولة البحرين.
- جهاز تنظيم الاتصالات في جمهورية مصر العربية.
- هيئة تنظيم الاتصالات وتكنولوجيا المعلومات في دولة الكويت
- وزارة الاتصالات وتكنولوجيا المعلومات في دولة فلسطين
- جمعية الإنترنت، فرع الجمعية بالسودان
- الوكالة التونسية للإنترنت في دولة تونس

كما نود أن نتوجه بالشكر للمدخلات الكريمة لأعضاء جمعية الانترنت نيرمين السعدني، كريستين رانيجير، رايان بولاك، سالي ونتورث، أولاف كولكمان، سلام ياموت، ماكس ستوشي وأندريه روباشفسكي، لما قدموه من قيادة وأراء ونصح، وماريا فاريل (مستشارة) لمراجعتها لتلك المبادئ التوجيهية.

الملحق 1: المنهجية والموارد

خضعت هذه المبادئ التوجيهية لتغييرات وتعديلات لتلائم الاحتياجات المحددة للدول العربية، مستفيدين في ذلك من أفضل الممارسات والآراء الواردة في الأطر والآليات التي تشمل ما يلي:

- توصيات منظمة التعاون الاقتصادي والتنمية بشأن مكافحة مخاطر الأمن الرقمي من أجل الرخاء الاقتصادي والاجتماعي والوثيقة المصاحبة (2015)51.
- دليل الممارسات الجيدة لإستراتيجية الأمن السيبراني الوطني الصادر عن الاتحاد الأوروبي52.
- اتفاقية الاتحاد الإفريقي بشأن الأمن السيبراني وحماية البيانات الشخصية (2014)53.
- المبادئ التوجيهية لأمن البنية التحتية لشبكة الإنترنت في إفريقيا، والتي تعد مبادرة مشتركة لجمعية الإنترنت ومفوضية الاتحاد الإفريقي54.

وفيما يلي مصادر جمعية الإنترنت التي قد تكون مفيدة لصانعي السياسات:

- Collaborative Security: An approach to tackling Internet Security issues55
- Policy Brief: Botnets (2015)56
- Routing Security for Policymakers57
- An Overview of Internet Content-Blocking58
- Policy Brief: Internet Exchange Points (IXPs) (2015)59

51 http://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf
52 https://www.enisa.europa.eu/publications/ncss-good-practice-guide
53 *https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf*
54 https://www.internetsociety.org/resources/doc/2017/internet-infrastructure-security-guidelines-for-africa/
55 https://www.internetsociety.org/collaborativesecurity/approach/
56 https://www.internetsociety.org/policybriefs/botnets/
57 https://www.internetsociety.org/resources/doc/2018/routing-security-for-policymakers/
58 https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

والنسخة العربية:

https://www.internetsociety.org/wp-content/uploads/2017/03/ISOC-ContentBlockingOverview_ar.pdf
59 https://www.internetsociety.org/policybriefs/ixps/

الملحق 2: المصطلحات المتعلقة بالإنترنت وأمنه

لا تعد هذه التعريفات مسردًا متكاملًا، بالإضافة إلى أنها ليست تعريفات رسمية وموثوقة، وإنما الغرض منها تقديم تعريف مبسط للمصطلحات.

هجمات

قد يستخدم المهاجمون مجموعة متنوعة من الأدوات والبرامج النصية والبرامج لشن هجمات على الشبكات وأجهزتها، ولخداع الموظفين أو البائعين أو منعهم من الوصول إلى الشبكة سواء في الموقع أو عن بعد. وعادةً ما يكون الهجوم موجهًا في أجهزة الشبكة إلى نقاط النهاية مثل الخوادم وأجهزة الكمبيوتر المكتبية. ويحدث الهجوم السيبراني إذا ما نجح المهاجم في اختراق عناصر التحكم الأمني.

الاختراقات

في سياق الشبكات، "تؤدي الاختراقات الأمنية على نحو غير مقصود أو غير قانوني إلى التدمير أو الفقدان أو التغيير أو الإفشاء أو الوصول غير المصرح به إلى البيانات الشخصية المنقولة أو المخزنة أو المعالجة بطريقة أخرى عند توفير" 60 خدمات الاتصالات الإلكترونية.

النهج الأمني التعاوني

يدرك النهج الأمني التعاوني لأمن الإنترنت أن البشر في النهاية هم من يحافظون على تماسك الإنترنت. وقد استند تطور الإنترنت إلى التعاون والتآزر الطوعي. ولا يزال التعاون والتآزر عاملين أساسيين لازدهاره وإمكاناته. ويؤكد النهج على الخمسة مبادئ التالية:

- المحافظة على الفرص وبناء الثقة.
- المسؤولية الجماعية.
- التكامل التام بين الحلول الأمنية والحقوق والإنترنت المفتوح.
- الحلول الأمنية القائمة على الخبرة، والتي تطورت بتوافق الآراء، ووفقًا لتطورات النظرة المستقبلية.
- استهداف نقطة التأثير القصوى–فكر عالميًا، واعمل محليًا 61.

فرق التصدي لحوادث أمن الحاسبات

منظمة أو مجموعة من الخبراء التي تتلقى الحوادث الأمنية الحاسوبية وتدرسها وتستجيب لها. وقد تكون تلك الفرق ذات نطاق جغرافي محدد أو مسؤولة عن قطاع بعينه، ويقودها كل من القطاع العام والقطاع

60 https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/

61 https://www.internetsociety.org/collaborativesecurity/

الخاص أو أحدهما. وتؤدي فرق التصدي لحوادث أمن الحاسبات وظيفة حيوية لتبادل المعرفة لضمان الأمن.

البنية التحتية المعلوماتية المهمة

الأنظمة والشبكات المترابطة، التي سيكون لتعطيلها أو تدميرها تأثيرًا خطيرًا على صحة المواطنين أو سلامتهم أو أمنهم أو رخائهم الاقتصادي، أو توفير الخدمات الأساسية، أو الأداء الفعال للحكومة والاقتصاد.

هجمات الحرمان من الخدمات

هجمات الحرمان من الخدمات هي "محاولة لجعل خدمة الكترونية ما غير متوفرة عن طريق إغراقها بسيل من البيانات الالكترونية من مصادر متعددة"62.

نظام أسماء النطاقات

"نظام تسمية هرمي لا مركزي للحواسب أو الخدمات أو المصادر الأخرى المتصلة بشبكة الإنترنت. هذا النظام يربط مختلف المعلومات بأسماء النطاقات المخصصة لكل كيان من الكيانات المشاركة، الأهم من ذلك، أنه يترجم أسماء النطاقات المحفوظة بيسر أكبر إلى عناوين الآي بي IP الرقمية اللازمة لإيجاد وتحديد خدمات وأجهزة الكمبيوتر بالإضافة إلى البروتوكولات الشبكية الأساسية"63.

الخصائص الأساسية لشبكة الإنترنت

"الخصائص التي مكّنت الإنترنت من أن يكون منصة للابتكار تتسم ظاهريًا بعدم المحدودية. وحددت ليس تقنيته فحسب، وإنما شكله أيضًا من ناحية التأثير العالمي والبنى الاجتماعية"64.

وتشمل تلك الخصائص المحددة ما يلي:

- التعاون الطوعي
- المعايير المفتوحة
- ركائز التكنولوجيا القابلة لإعادة الاستخدام
- النزاهة
- القدرة المطلقة على الابتكار
- الانتشار العالمي

62 http://www.digitalattackmap.com/understanding-ddos/
63 https://en.wikipedia.org/wiki/Domain_Name_System
64 https://www.internetsociety.org/internet-invariants-what-really-matters

نقاط تبادل الإنترنت

نظام يسمح للعديد من الشبكات المتصلة بالإنترنت بتبادل البيانات مع بعضها بعض في نقطة التقاء مشتركة، ومن ثم استبعاد الحاجة إلى بناء روابط ثنائية منفصلة مع كل شبكة من الشبكات المحلية.

البنية التحتية لشبكة الإنترنت

العناصر التي تشكل وتمكّن من نقل البيانات عبر شبكة مترابطة من بين شبكات. وتشتمل هذه العناصر على بروتوكولات وخدمات وبرمجيات ومعدات حاسوبية وربط شبكي وبنية تحتية للاتصالات ومعلومات، وقوى بشرية.

مقدم خدمات الإنترنت

الشركة أو المؤسسة التي توفر للأفراد والمؤسسات والشركات وغيرها إمكانية الوصول إلى شبكة الإنترنت والانتفاع بها. وبالإضافة إلى توصيل المستخدمين، فكثيرًا ما يتيح مقدمو خدمات الإنترنت خدمات أخرى مثل البريد الإلكتروني واستضافة المواقع لعملائهم.

التوجيه

يحدد التوجيه كيفية انتقال البيانات من نقطة ما في الشبكة أو الشبكات إلى نقطة أخرى. وتسمى العقد الشبكية التي تتخذ قرارات التوجيه بالموجهات التي يجري بينها تبادل معلومات إمكانية الوصول (أي ما إذا كان بالإمكان الوصول إلى شبكة معينة من خلال إحدى العقد). وهناك نوعان من البروتوكولات المستخدمة في تبادل المعلومات هما: بروتوكول التوجيه الداخلي المستخدم بين الموجهات داخل الشبكة (مثل بروتوكول المسار الأقصر أولًا (OSPF) أو بروتوكول الربط بين الأنظمة الوسيطية (IS-IS) أو بروتوكول توجيه المعلومات (RIP))، وبروتوكول التوجيه الخارجي المستخدم بين الشبكات، أو الأنظمة المستقلة (AS)، والذي يسمى أيضًا ببروتوكول البوابة الحدودية (BGP) الذي من بين ثغراته عدم توفيره لوسيلة يمكن من خلالها التحقق من صحة المعلومات المتبادلة. علمًا أن اتمام عملية التحقق من صحة المعلومات يتطلب استخدام مزيد من الأدوات والممارسات.

الجهات المعنية

الأفراد أو الجماعات أو المؤسسات أو الكيانات أو المجتمعات ذات المصلحة أوالاهتمام بالإنترنت. وتشمل الجهات المعنية كل من الحكومات والقطاع الخاص والمجتمع المدني والوسطين الأكاديمي والتقني.

الملحق 3: إرشادات لمشغلي الشبكات

ركزت هذه الوثيقة بدرجة كبيرة على الخطوات التي يجب على الحكومات اتخاذها. ولما كان القطاع الخاص الذي يعمل في صناعة الاتصالات هو المتحكم عمومًا في قدر كبير من البنية التحتية لشبكة الإنترنت، فإن الإرشادات التالية تركز على ما يتعين على مشغلي الشبكات القيام به.

1 مقدمو خدمات الإنترنت/ على مستوى المشغل

يؤدي مشغلو الشبكات دورًا مباشرًا في تأمين البنية التحتية لشبكة الإنترنت نظرًا لكونهم الجهات المسؤولة عن تشغيل الشبكات في قارة إفريقيا. إن التأثيرات المترتبة على وجود ضعف أمني في شبكة أحد المشغلين لا تقتصر على تلك الشبكة فحسب، وإنما تمتد لتشمل أيضًا الشبكات الأخرى في إفريقيا، وتلك الموجودة في جميع أنحاء العالم.

1-1 وضع ضوابط أمنية أساسية

تتطلب مواجهة التحديات المتعلقة بأمن البنية التحتية لشبكة الإنترنت تعاونًا والتزامًا من جميع الجهات المعنية. ففي عالم مترابط بأقاليمه التابعة التي تمتد عبر شبكات ودول وقارات متعددة، يكون من الأهمية بمكان أن يلتزم جميع المشاركين بالحد الأدنى من الضوابط الأمنية أو الضوابط الأساسية التي سرعان ما سيتجاوزها الكثيرون، وسيعتمد عليها آخرون.

أمن نظام التوجيه واسم النطاق

يجب على مشغلي الشبكات التصدي لانتشار معلومات التوجيه غير الصحيحة، ومنع تبادل البيانات باستخدام عناوين آي بي IP المصدر المنتحلة، وتيسير الاتصالات التشغيلية والتنسيق عالميًا بين مشغلي الشبكات، وتيسير التحقق من صحة معلومات التوجيه على نطاق عالمي. فغالبًا ما يستخدم انتحال عنوان الآي بي IPأو تزوير عنوان المصدر في هجمات الحرمان من الخدمات لجعل الحلول الدفاعية أكثر صعوبة.

ويجب على مشغلي الشبكات تمكين التحقق من صحة الامتدادات الأمنية لنظام اسم النطاق (DNSSEC)[65] من خلال محللات أنظمة أسماء النطاقات لديهم لضمان سلامة وموثوقية عمليات أنظمة أسماء النطاقات. ويجب على مشغلي سجلات أنظمة أسماء النطاقات، ومشغلي خوادم أنظمة أسماء النطاقات الموثوقة، ومسجلي النطاق، دعم الامتدادات الأمنية لنظام اسم النطاق وتنفيذ الممارسات الأمنية السائدة مثل التحكم في الوصول والثغرات وإدارة التصحيح.

يجب على مشغلي الشبكات أيضًا دمج أفضل الممارسات الحالية المتعلقة بأمن التوجيه والمرونة ضمن عمليات إدارة الشبكة لديهم. وتحدد المبادرة العالمية للمعايير المتفق عليها بشكل متبادل لأمن التوجيه[66] حزمة مختصرة من الإجراءات الأساسية والمهمة التي تضمن مرونة نظام التوجيه العالمي وأمنه. وقد اضطلع بوضع المعايير المتفق عليها بشكل متبادل لأمن التوجيه أعضاء من مجتمع مشغلي الشبكات بدعم من جمعية الإنترنت.

تقترح المعايير المتفق عليها بشكل متبادل لأمن التوجيه خطوات بسيطة على مشغلي الشبكات لتحسين أمان الإنترنت وموثوقيته إلى حد بعيد، علمًا بأن تلك المعايير كانت قد وضعت في الأساس من أجل مشغلي الشبكات، إلا أن نقاط تبادل الإنترنت تعد شريك هام لديه مجموعة منفصلة من الإجراءات المتعلقة بالمعايير المتفق عليها بشكل متبادل لأمن التوجيه. ولمزيد من المعلومات، يرجى زيارة الموقع التالي: https://www.manrs.org/

الأمن الشبكي

إن التأمين المنفصل للشبكات يعد أمرًا ضروريًا لحماية كل شبكة وغيرها من الشبكات في النظام البيئي للإنترنت. وهذا يتضمن تصفية البيانات الاحتيالية وحركة الهجمات الحجمية، سواء أكانت الواردة أو الصادرة، من شبكاتها. وفي حين أن حركة البيانات الاحتيالية والهجمات الصادرة قد تؤدي إلى إلحاق الضرر بسمعة عنوان الآي بي ip الخاص بشبكة المنشأ، إلا أنه كثيرًا ما تسفر عن تأثيرات سلبية ومباشرة بدرجة أكبر على الشبكات الأخرى في النظام البيئي للإنترنت.

توفر مجموعة أدوات مكافحة البريد الإلكتروني التطفلي التي وضعتها جمعية الإنترنت [16] أفضل الممارسات لصانعي السياسات، ومشغلي الشبكات، والمستخدمين لتأمين شبكاتهم تأمينًا أفضل من تهديد البريد الإلكتروني التطفلي. وكذلك توفر مجموعة الأدوات روابط لمصادر خارجية حول البريد الإلكتروني التطفلي ومكافحة بيانات الإنترنت غير المرغوب فيها. تنصح مدونة قواعد السلوك الخاصة بأداة التأمين (Anti-bot) التي وضعتها مجموعة (M^{3}AAWG) [17] لمقدمي خدمات الإنترنت بالانخراط في

65 https://www.internetsociety.org/deploy360/dnssec/basics/
66 https://www.manrs.org

مجالات التعلم والكشف والإبلاغ والعلاج والتعاون. وجدير بالذكر أن مدونة قواعد السلوك تعزز المبادئ الأساسية وهي الوعي والمسؤولية والتعاون ودعم الحقوق الأساسية وخصائص الإنترنت.

الممارسات الأمنية الأساسية

يجب استخدام البروتوكولات الآمنة التالية في المنتجات والخدمات التي تدعم البنية التحتية لشبكة الإنترنت: بروتوكول طبقة المنافذ الآمنة (TLS)[67]، وهو بروتوكول تشفير يجب استخدامه لحماية خدمات الويب. يقوم بروتوكول طبقة المنافذ الآمنة بترميز البيانات المتبادلة خلال عمليات بروتوكول نقل النص الفائق(HTTP) ويحدد على نحو ترميزي أحد الأطراف المشاركة أو أكثر في العملية؛ وذلك لأن الخصوصية والهوية يعدان عنصران أساسيان من عناصر البنية التحتية الآمنة لشبكة الإنترنت.

يجب على مشغلي خدمات البريد الإلكتروني نشر معايير وممارسات أمان البريد الإلكتروني المناسبة مثل البريد المعرف بمفاتيح النطاق (DKIM) و نظام التعرّف على هوية المرسِل (SPF) ومصادقة الرسائل المستندة إلى النطاق، والإبلاغ، والمطابقة (DMARC)[68].

يجب على المشغلين أيضًا ضمان إدارة البرامج المهمة للبنية التحتية للإنترنت بشكل فعال يمنع خلق الثغرات الأمنية. ويجب عدم نشر أي برمجيات في البنية التحتية للإنترنت إلا التي تخضع للصيانة بواسطة البائع أو مجتمع المصادر المفتوحة. ويجب على المشغلين استخدام سياسة التصحيح (Patching) التي تعطي الأولوية لتخفيف آثار الثغرات الأمنية في البرمجيات، على الرغم من المخاطر الملازمة لفترة التشغيل. ويمكن أيضًا للمشغلين إنشاء برنامج لإدارة الثغرات الأمنية في البرمجيات يمنح المسؤولية عن التخفيف المستمر لآثار الثغرات في البرمجيات للأفراد أو المؤسسات. ويعد غياب المساءلة المؤسسية عن إدارة ثغرة البرمجيات أحد الأسباب الشائعة لفشل العديد من المؤسسات في تصحيح مشكلات البرمجيات على نحو مناسب.

2-1 خلق التعاون والتآزر والحفاظ عليهما

بالإضافة إلى مشاركة مقدمي خدمات الإنترنت ومشغلي الشبكات في الهيئات الوطنية المعنية المتعددة الموضحة في القسم 3-2-2، فإنهم يتحملون أيضًا مسؤولية التنسيق والتعاون مع بعضهم البعض ومع عملائهم من المؤسسات والجهات المعنية الأخرى. ويجب على مقدمي خدمات الإنترنت ومشغلي الشبكات الالتزام بما يلي:

- التشجيع على التعاون والتآزر بين العملاء من المؤسسات والحكومات المحلية والإقليمية والهيئات التنظيمية في منع وكشف وتخفيف حوادث التوجيه.

67 https://www.internetsociety.org/deploy360/tls/basics/
68 https://www.internetsociety.org/resources/ota/2017/email-authentication-dmarc/

- تيسير سبل الاتصال والتنسيق التشغيلي العالمي بين مشغلي الشبكات.
- المشاركة الفعالة في جمعيات مقدمي خدمات الإنترنت مثل مجموعات ومنتديات مشغلي الشبكات الوطنية والإقليمية.
- إيجاد آليات لتبادل المعلومات مع المقدمين الآخرين فيما يخص حوادث الانقطاع لكي يتم إصلاحها سريعًا والتسريع من عمليات الصيانة.
- التعاون مع هيئات إنفاذ القانون والهيئات التنظيمية أثناء التحقيق في الجرائم السيبرانية أو غيرها من الأنشطة غير المشروعة وملاحقة مرتكبيها.

2 المستوى المؤسسي أو التنظيمي

هناك حاجة لوجود قيادة تنفيذية ومساءلة فيما يخص القضايا السيبرانية. يجب أن يكون القائد التنفيذي في كل مؤسسة مسؤولاً عن أمن معلومات تلك المؤسسة. وانطلاقًا من هذا الدور، فإنه يمكن للقائد التنفيذي تخصيص الموارد اللازمة لخلق وتعزيز الثقافة المؤسسية للأمن السيبراني؛ ذلك أن التأثير القوي للممارسات الأمنية في المؤسسات المستفيدة من تكنولوجيا المعلومات والاتصالات لا ينعكس على تلك المؤسسات فحسب، وإنما يؤثر أيضًا على النظام البيئي الأوسع نطاقًا لشبكة الإنترنت. وبالتالي فإنه من المهم أن تكون هذه المنظمات على دراية بآثار أفعالها (أو تقاعسها) على أمن الآخرين. إن السياسة الأمنية الواضحة والمنفذة والتي تستند على التقييم المتكرر للمخاطر، يجب أن تشتمل على إجراءات محددة منها تطبيق إجراءات أساسية لضمان سلامة الشبكة، وإيجاد منظومة ملائمة من عناصر التحكم، وجود عملية منظمة قادرة على التصدي للحوادث السيبرانية، وإجراء تدريبات دورية، وإقرار أسلوب للفصح عن البيانات ، والحرص على إقامة علاقات مع أصحاب المصلحة الآخرين مثل المسؤولين الحكوميين وفرق التصدي لحوادث أمن الحاسبات.

ويجب على الحكومات الوطنية، وغيرها من أصحاب المصلحة، تمكين المنظمات والمؤسسات من إيجاد ثقافة للأمن السيبراني من أجل الرخاء الاقتصادي والاجتماعي من خلال تبادل المعلومات، وتعزيز أفضل الممارسات، وإيجاد مثال يحتذى به. ويجب إنشاء الهيكل التنظيمي اللازم في المؤسسات المسؤولة عن مبادرات الأمن السيبراني وأنشطته.

ويجب على المنظمات والمؤسسات تطبيق أفضل الممارسات الحالية، وإيجاد ثقافة للأمن السيبراني على المستويين التشغيلي والتنفيذي.