إضاءات

نشرة توعوية يصدرها معهد الدراسات المصرفية

دولة الكويت - مايو 2019

السلسلة 11 العدد 5

الأمـن السيبرانـي

Cyber Security

مقدمة

أتى مصطلح الأمن السيبراني من لفظ سيبر(Cyber) المنقول عن اليونانية ويعبر عن العالم الافتراضي الذي يحوي كل ما يتعلق بتقنية المعلومات والحاسب الآلي من استخدامات وآليات وتطبيقات وتجهيزات، وترابط فيما بينها من خلال شبكات الحاسب والاتصالات والإنترنت. في العصر الحديث أتى مصطلح الأمن السيبراني من لفظ «سيبر» المنقول عن كلمة cybernetic والتي تعني علم التحكم الآلي في الكائنات الحية والآلات.

إصدارات
مالية ومصرفية

الأمن
السيبراني

محاور العدد:

- تعريف الأمن السيبراني
- الفرق بين الأمن السيبراني وأمن المعلومات
- أهداف الأمن السيبراني
- الجرائم السيبرانية
- أبعاد الأمن السيبراني
- خصائص الأمن السيبراني
- وسائل الحماية غير المادية
- تجنب مخاطر الأمن السيبراني على المجتمع
- تحصين نظم الأمن السيبراني في القطاع المصرفي لدولة الكويت
- فريق عمل أمن المعلومات في القطاع المصرفي
- الخلاصة

تعريف الأمن السيبراني

الإجراء المرتبط بحماية الأنظمة الآلية لشبكة الانترنت وذلك يشمل الأجهزة والبرامج والبيانات، والشبكات والتطبيقات من الهجمات والجرائم السيبرانية والتي تتضمن التعطيل والتخريب أو الدخول غير المشروع أو سرقة معلومات وبيانات لأهداف مالية وغير مالية.

الأمن السيبراني يتمثل في مجموعة من الوسائل التنظيمية والإدارية والتقنية لحماية أجهزة وشبكات الحاسب الآلي ونظم الاتصالات والمعلومات التي يتم تداولها وتخزينها في خوادم داخل أو خارج المؤسسات لمنع الدخول أو الاستخدام غير المصرح به أو الاستغلال وما ينتج عنه من تغيير أو إفشاء أو سرقة للبيانات أو تعطيل للخدمات أو شبكات الاتصال لأهداف غير مشروعة. وفي عصرنا أصبح للأمن السيبراني دور واضح وفعال في حماية الحكومات وأنظمة الدول الحيوية وصد أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة داخليا أو خارجيا لأهداف قد تكون سياسية أو مالية أو عدوانية.

الفرق بين الأمن السيبراني وأمن المعلومات

إن مفهوم الأمن السيبراني وأمن المعلومات متشابهان إلى حد كبير لكنهما غير متطابقين. وإنه لمن المهم فهم الفرق بين الأمن السيبراني وأمن المعلومات وذلك لإزالة اللبس بين المصطلحين بهدف وضع خطة عمل وسياسات واضحة تميز كل مفهوم عن الآخر.

فأمن المعلومات يركز على ثلاثة محاور رئيسية وهي السرية والسلامة وتوفر المعلومات عن طريق تبني المعايير أو المقاييس الأمنية العالمية وأنظمة إدارة أمن ومخاطر المعلومات، كما أنه يتضمن جوانب تقنية عديدة مثل التشفير والتخزين والتأمين الفيزيائي.

أما مفهوم **الأمن السيبراني** فيعني اتخاذ كافة التدابير والاحترازات اللازمة لتأمين البيانات التي يتم تداولها عبر الشبكات الداخلية والخارجية والتي يتم تخزينها خارج المؤسسة أو داخلها بالإضافة إلى تأمين أنظمة وقنوات الاتصالات والخدمات الالكترونية من الاختراقات التي تتم من خلال استخدام ثغرات أو ضعف في أنظمة وأدوات تكنولوجيا المعلومات والاتصالات، أو قصور في الإجراءات التنظيمية.

أهداف الأمن السيبراني

- ضمان استمرارية عمل أنظمة وشبكات وخدمات نظم المعلومات.
- حماية الأنظمة التشغيلية من أي محاولة للاختراق.
- اتخاذ الإجراءات الاحترازية لحماية المواقع الإلكترونية وقنوات الدفع الإلكتروني بما يضمن الاستمرارية والكفاءة في تنفيذ جميع العمليات التي يقوم بها مستخدمو الإنترنت.
- اتخاذ التدابير اللازمة لحماية المستخدمين من المخاطر المحتملة عند استخدام الإنترنت.
- تعزيز وحماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات وخصوصية شخصية.

الجرائم السيبرانية

يمكن تعريف الجرائم السيبرانية بالسلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية وأجهزتها الطرفية وخدماتها والتي قد تطال الثقة أو المال أو السمعة أو الأمن والاستقرار.

ومن أبرز مخاطر الجرائم السيبرانية انتحال الشخصيات (Identity theft) حيث يتم الحصول على المعلومات والبيانات بطرق غير شرعية بسبب وجود ثغرات في نظم وضوابط الحماية للأنظمة والشبكات أو قصور في الإجراءات التنظيمية لدى الجهات المستهدفة سواء كانت (حكومية، بنوك، متاجر.. إلخ) والتي تمكن المحتال من تجميع المعلومات اللازمة لتنفيذ الجرائم مثل السرقة والابتزاز وغيرها من الجرائم.

كذلك عند طرح موضوع الجرائم السيبرانية يجب الانتباه إلى اختلافات الدوافع، النوع، وكذلك اتجاه الفعل الجرمي، فهناك ما هو مرتبط بالبيانات العامة والبيانات الخاصة والشخصية الفردية، وهناك ما هو مرتبط بالنظم والتطبيقات الإلكترونية.

وقد ساهم تطور التجارة الإلكترونية والتكنولوجيا بشكل مباشر في ازدياد حجم هذه الجرائم. ونظراً لقلة النصوص القانونية الخاصة بتلك الجرائم وجدت المحاكم صعوبة في تكييف النصوص القانونية لتجريم مثل هذه الأفعال غير المقبولة والّتي قد يكون موضوعها أدوات معلوماتية وهمية (برامج خفية أو أفعال غير ملموسة). فالنص الجزائي يفسر على سبيل الحصر طبقا لإرادة المُشرع ويُحظر استخدام القياس في هذا السياق، عملاً بمبدأ لا جريمة ولا عقوبة إلا بنص أو بناءً عليه.

كما أن مصطلح جرائم الإنترنت وفقاً للاتفاقية الأوروبية بِشأن الجريمة السيبرانية التي عقدت في

بودابست في 23 نوفمبر/تشرين الثاني 2001، تناول الأعمال غير الشرعية المرتبطة بأجهزة الحاسوب والشبكة العنكبوتية. في المقابل تعتبر إزالة المعلومات بواسطة أجهزة الحاسوب من دون استخدام الشبكة العنكبوتية جريمة من جرائم الإنترنت بناءً على الاتفاقيات الدولية كاتفاقية المجلس الأوروبي (2005). ويمكن ذكر العديد من أنواع الجرائم السيبرانية ومنها:

1 -الجرائم المرتبطة بالبيانات والتي تتمثل في الدخول غير المصرح به لأجهزة الحاسب الآلي، وينتج عن ذلك اختراق البيانات الشخصية وانتهاكها وحيازتها. وتعتبر حيازة البيانات الشخصية في هذه الحال غير شرعية.

2 - الجرائم المتعلقة بالنظم وأجهزة الحاسب الآلي التي تؤدي إلى التعدي على سلامة تلك الأجهزة عن طريق إتلافها أو تخريبها أو إساءة استخدامها.

3 - تطوير البرمجيات والروابط التخريبية التي تتلف نظام الحاسب الآلي أو ملحقاته الطرفية من خلال التزوير أو الاختراق أو الاحتيال.

4 - الجرائم التي يتم تنفيذها من خلال شبكة الإنترنت، ومنها على سبيل المثال:

- الجرائم العامة التي تمس بالأشخاص، كالتعدي على البيانات والمعلومات الشخصية، بالإضافة إلى التحريض على القتل أو الانتحار، وجرائم التحرش والتهديد وإرسال معلومات خاطئة بهدف التزوير أو الابتزاز عن طريق البريد الإلكتروني.
- جرائم الأحداث التي تسبب الضرر العاطفي عبر الوسائل التقنية واستغلال القصّر للقيام بأفعال غير مشروعة.
- جرائم ضد الإنسانية مثل نشر العنصرية والكراهية للطرف الآخر.
- الترويج للأعمال والأنشطة غير المشروعة كالمقامرة والمواد المخدرة والتلاعب بالنظم للحصول على الأموال دون وجه حق.
- جرائم الانتحال عن طريق اختراق أدوات التعريف والهوية الشخصية أو كلمات السر وتزويرها وهذا يؤدي إلى الإعتداء على الملكية، واستخدام الاسم أو العلامَة التجارية للغير.
- الجرائم التي تساهم في تعطيل الأنشطة والأعمال الحكومية أو التي تخترق المعلومات السرية التي تخص الدولة والعبث بالأدلة القضائية.

أبعاد الأمن السيبراني

يرتبط الأمن السيبراني بعدة مجالات وأبعاد مختلفة سياسية وعسكرية واقتصادية وقانونية واجتماعية، بهدف تحقيق نظام واضح ومتكامل يعمل على الحفاظ على الأمن القومي للدولة من أية تهديدات سيبرانية محتملة، ويمكن توضيح ذلك من خلال الآتي:

1 - للقوة السيبرانية دور فعال في المجال العسكري وذلك بربط الوحدات ببعضها مما يسمح بتدفق المعلومات بسهولة والقدرة على الوصول للهدف. لكن إن لم تكن مؤمّنة جيداً فقد تتعرض بياناتها للاختراق، كما تكون عرضة للهجمات وتدمير قواعدها وتعطلها مما يتسبب في فقدان السيطرة وضعف الموقف في مواجهة العدو.

2 - نظراً للتطور الإلكتروني الذي يستقطب جميع أطراف المجتمع من خلال التسهيلات وخدمات حفظ البيانات والمعلومات وتخزينها كما في شبكات البنوك والبورصة والأسواق والشركات المالية، إذ أصبح الإنترنت أساس المعاملات المالية والاقتصادية وباتت تشكل محوراً رئيسياً للتطور الاقتصادي في القرن الحادي والعشرين، وهو ما أثار الحديث عن أهمية تحقيق الأمن السيبراني في المجال الاقتصادي.

3 - العلاقة بين القانون والتكنولوجيا علاقة طردية، فالتطورات التكنولوجية المختلفة تفترض مواكبة التشريعات القانونية لها من خلال سن أطر وتشريعات للأعمال القانونية وغير القانونية، ولكن تفتقر النصوص القانونية للتشريعات اللازمة لمواكبة تطور الأمن السيبراني وتقليل جرائمها بالتالي ينتج عن ذلك صعوبة تحديد هوية مرتكبي الجرائم ونظراً إلى أن الجرائم السيبرانية غير مقيدة جغرافيا فيتوجب تفعيل التعاون الدولي لمكافحتها.

خصائص الأمن السيبراني

في معظم الأحيان يتم خلق أسماء وهمية أو انتحال أسماء أشخاص من ذوي الاختصاص أو النفوذ أو العلاقة بأمر معين أو جهة معينة على شبكة الانترنت ومن ثم يتم استخدام هذه الأسماء في التفاعلات أو الحوارات أو العمليات عبر شبكة ومواقع الانترنت لحين تكوين مصداقية وثقة متبادلة ومن ثم يتم إما بث المعلومات المغرضة أو سرقة معلومات لأغراض غير مشروعة.

إن للجرائم السيبرانية خصائص تتميز بها ولا تتوافر في الجرائم التقليدية على سبيل المثال:

- صعوبة ملاحظة الجريمة إلا بعد مرور وقت من وقوعها.
- غياب الدليل الواضح وصعوبة إثباته بالإضافة إلى توفر وسائل تقنية تعرقل الوصول للدليل والبراهين.
- الخبرة والكفاءة العالية للمجرم في مجال الاتصالات والتقنيات الحديثة.
- نقص الخبرة التقنية في اكتشاف الجريمة لدى الأجهزة الأمنية، ونقص التشريعات القضائية.

وسائل الحماية غير المادية

وهي الوسائل التي تتعلق بالحماية داخل الشركات والمؤسسات العامة والخاصة، وتتمثل بالسياسة الأمنية الداخلية المتبعة للوقاية من الأخطار الناجمة عن استعمال الحواسيب وربطها بالشبكة، على سبيل المثال:

1 - نشر التوعية اللازمة بمفهوم الأمن السيبراني والمخاطر المصاحبة لاستخدام شبكة الانترنت وأجهزة الحاسب الآلي وأجهزة الاتصالات وتثقيف المستخدمين بمبادئ حفظ وحماية البيانات.

2 - حث الأفراد والموظفين في الوزارات والمؤسسات على اتباع الإرشادات المتعلقة بأمن المعلومات والإبلاغ الفوري عن أي عمل أو فعل غير اعتيادي على الشبكة أو أي محاولة اتصال بواسطة روابط غير معروفة أثناء استعمال الحاسب الآلي أو الأنظمة التشغيلية الملحقة.

تجنب مخاطر الأمن السيبراني على المجتمع:

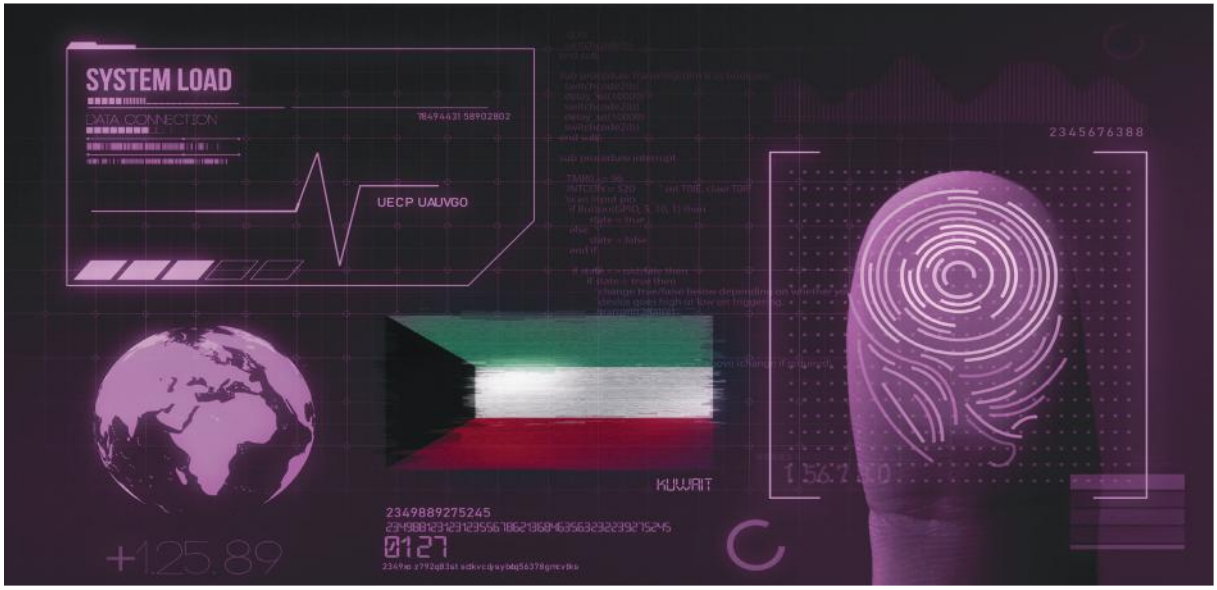
من أهم الخطوات اللازمة للحد من مخاطر الأمن السيبراني على المجتمع هي نشر الوعي والثقافة السيبرانية وإيجاد سبل الحماية الملائمة للفضاء السيبراني العربي ومنها:

1 - المساهمة في تغطية كل ما يستجد عن الأمن والسلامة في مجال الأمن السيبراني على جميع المستويات منها: المستوى التجاري، والاقتصادي، والأكاديمي، والاجتماعي، والقانوني، والتنظيمي.

2 - بناء قاعدة بيانات للأطر التشريعية والتنظيمية السائدة في الدول العربية الخاصة بإدارة التعاملات عبر شبكة الانترنت وسن التشريعات والعقوبات اللازمة لمنفذي الجرائم السيبرانية ووضع ضوابط قانونية صارمة.

3 - أهمية التعاون بين كافة المؤسسات خاصة العسكرية والتكنولوجيا لزيادة كفاءة القدرات والحفاظ على سرية المعلومات.

4 - المساهمة في إعداد خطط وحملات توعوية أمنية لنشر الوعي وتسليط الضوء على الاستخدام الخاطئ لشبكة الانترنت وذلك عن طريق عقد ورش عمل ووضع برامج تدريبية وعمل فعاليات خاصة بأمن المعلومات (عمليات الاختراق الوهمي) وتوزيع مطبوعات وتكثيف الارشادات الدورية.



تحصين نظم الأمن السيبراني في القطاع المصرفي لدولة الكويت

في ضوء حرص بنك الكويت المركزي على تعزيز وسائل الحماية والأمن السيبراني في القطاع المصرفي في دولة الكويت، فقد تم تشكيل فريق متخصص للتفتيش على تكنولوجيا المعلومات لدى البنوك، ويدخل في نطاق فحصه الإجراءات المرتبطة بالأمن السيبراني واستخداماته المختلفة.

والجدير بالذكر أنه تم إلزام البنوك بتطبيق معايير عالمية وممارسات متحفظة للحد من المخاطر المرتبطة بالأمن السيبراني بهدف تعزيز حماية مواقع البنوك الإلكترونية وقنوات الدفع المرتبطة بها لتنفيذ عمليات آمنة بما يضمن استمرارية وتوفر وسرية المعلومات التي يتم التعامل بها.

كذلك هو الحال بالنسبة للخدمات والمنتجات المقدمة من قبل كافة الجهات الخاضعة لرقابة بنك الكويت المركزي لطرحها في السوق المحلي، حيث يتم دراستها ومراجعتها واختبارها وتقييمها أمنيا من قبل المختصين في بنك الكويت المركزي ويتم إعطاء الرأي الفني لقبولها أو تعديلها أو رفضها قبل الموافقة عليها.

فريق عمل أمن المعلومات في القطاع المصرفي

في إطار سعي بنك الكويت المركزي لتعزيز وسائل الحماية والأمن السيبراني في القطاع المصرفي، شكل فريق عمل لأمن المعلومات في القطاع المصرفي برئاسة بنك الكويت المركزي وعضوية البنوك الكويتية وذلك لتنسيق الجهود فيما بين وحدات القطاع المصرفي وكذلك الاستجابة الفعالة لمواجهة أي هجمات سيبرانية أو محاولات لاختراق الشبكات والأنظمة التقنية، بالإضافة إلى تطوير خطط التعافي من الكوارث والتحوط من مخاطر التطور التكنولوجي، وتبادل المعلومات والخبرات لمساندة أعضاء الفريق في إدارة المخاطر في مجال الأمن السيبراني بشكل أفضل.

كما يعكف الفريق حالياً على تجهيز استراتيجية الأمن السيبراني وخطة إدارة الأزمات السيبرانيه وكذلك دليل أمن المعلومات بالإضافة إلى تنفيذ البرامج التدريبية وبرامج المحاكاة للهجمات السيبرانيه، والتي تهدف إلى رفع مستوى جاهزية القطاع المصرفي وتطوير آليات الحماية ومواجهة الهجمات بشكل جماعي.

الخلاصة

للأمن السيبراني أهمية كبيرة لضمان حفظ المعلومات الموجودة على شبكات الإنترنت واستمرارية سير المعلومات بشكل صحيح ومنتظم كما يتيح للمستخدمين إضافة معلوماتهم الشخصية بشكل سري ومحمي بالإضافة إلى ذلك يساهم الأمن السيبراني في حماية أمن الدولة وقواعدها وهيئاتها وذلك عن طريق نشر الوعي الثقافي بين المستخدمين.

المصادر:

1. https://makkahnewspaper.com/article/
2. https://www.almowaten.net
3. https://edu.moe.gov.sa/jeddah/DocumentCentre/Docs
4. http://arabcb.org/initiative/733/
5. https://www.almrsal.com/post/552008

معهد الدراسات المصرفية
INSTITUTE OF BANKING STUDIES

ص.ب: 1080 الصفاة - 13011 الكويت
P.O.Box 1080 Safat 13011 Kuwait
تلفون: 22901100 965+ - فاكس: 22466430 965+
البريد الإلكتروني: cs@kibs.edu.kw - www.kibs.edu.kw

ibs_kuwait IBSKuwait