الفصل الثاني

تعاظم أهمية أمن المعلومات[1]

يستعرض هذا الفصل مشهدَ تعاظمِ أهميةِ أمن المعلومات وأمانها في الآونة الأخيرة، وتفاقمَ المهددات وكثرةَ الاختراقات وتواترها على كل الأصعدة، ويأتي على ذكر حالات عالمية مختلفة بوصفها أمثلة لذلك.

1.2 تطور المعلوماتية يرافقها تعاظم أخطار أمنها.

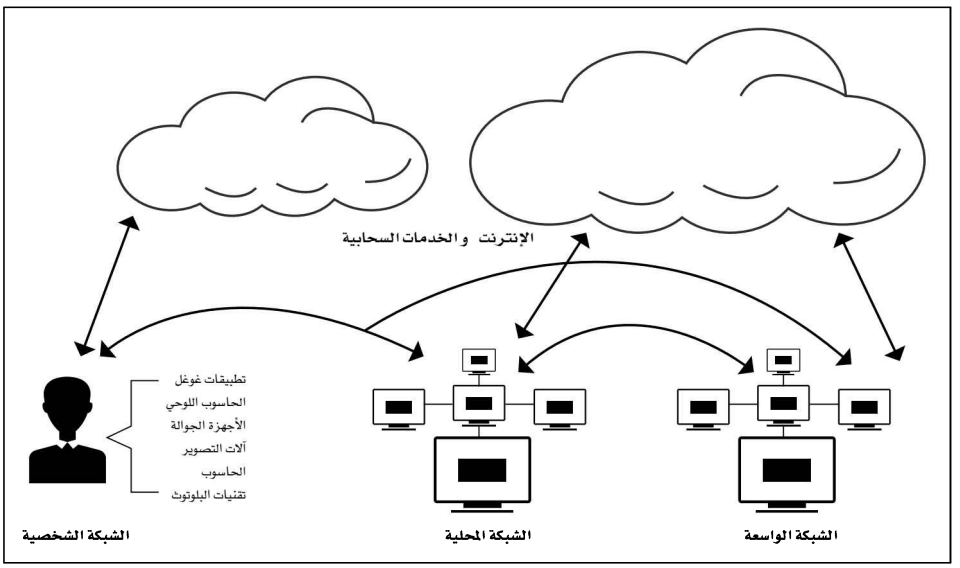
مع تطور الخدمات الإلكترونية، تطورت الأخطار والجرائم السايبرية (أو السيبرانية)، وظهرت طرق جديدة لارتكاب الجرائم في الفضاء السايبري أو السيبراني، وعلى المجتمع بأفراده ومؤسساته الاحتياط من وجود الجرائم السايبرية واتخاذ التدابير اللازمة لمواجهتها، فهي لن تتوقف، لا، بل ستتطور، وسيقع على عاتقنا اتخاذ الاحتياطات اللازمة في هذا المجال. لقد أصبح الفضاء السايبري واقعًا منذ منتصف

(1) اعتمدت الفقرات الأربع الأولى من هذا الفصل على تقرير اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا): الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية، توصيات سياساتية، 2015م.

التسعينيات، وأوجد بيئة جديدة تنتشر فيها الجرائم السايبرية، وقد عجزت القوانين الجزائية حتى الآن عن متابعة هذا التطور.

وظهرت تقنيات جديدة، مثل الصوت عبر الإنترنت (VoIP) Voice–over–IP، والحوسبة السحابية (انظر الشكل،Cloud Computing) التي يصعب معها تطبيق القانون التقليدي وإجراء التحقيقات القضائية؛ نظرًا لتشابكها وتعقيداتها، وأسهمت تقنيات الغفلية (تقنيات إخفاء الهوية الحقيقية للمستخدم) وتنامي تسويق البرامج المعلوماتية التي يستخدمها المخترقون في تطور الجرائم السايبرية، ولم يعد المخترقون يحتاجون إلى خبرات كبيرة؛ لأن برامج الاختراق أصبحت متوافرة وجاهزة، وقد أظهرت إحدى الدراسات أن (22%) فقط من الهجمات السايبرية معقدة، وتحتاج إلى محترفين.

نظام الأنظمة القادم في المعلومات والاتصالات (المعلوماتية)



Source: The Future of National and International Security on the Internet, Chapter 9, Maurice Dawson et al. 2014.

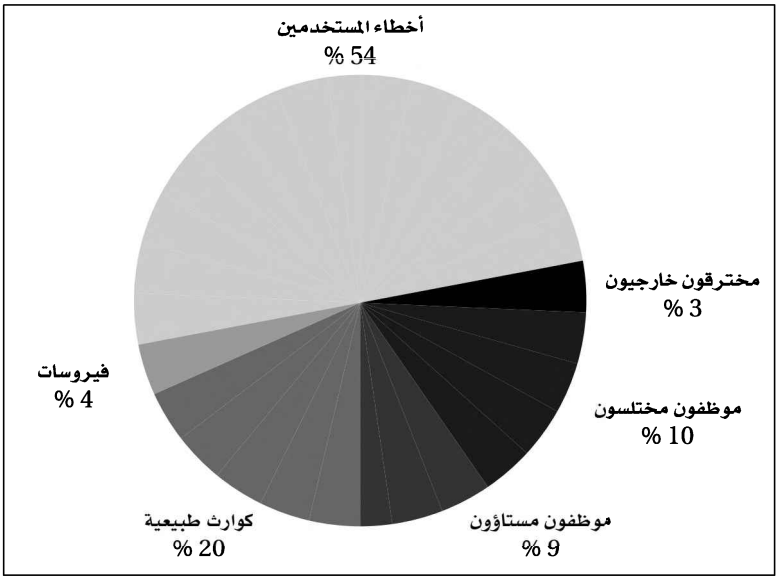
لقد بدأت الحكومات والشركات تعي تدريجيًّا أخطار الجرائم السايبرية وأهمية الأمن السايبري على الأمن الاقتصادي والسياسي للبلد وعلى مصالح العامة، وتبدو

الإنترنت جنة لمخترقي الشبكات بسبب ظهورهم عليها ظهورًا افتراضيًّا مُغْفَلًا دون اسم، وقد بات هؤلاء يعون ارتفاع عوائد الجرائم السايبرية، وتدني أخطار ونسب اكتشافها، وصعوبة إثباتها في بعض الدول، وبالفعل يتأتى عن الجرائم السايبرية خسائر مالية قد تكون مباشرة أو غير مباشرة، وهي خسائر فادحة تلحق بالأفراد والاقتصاد على حد سواء، فعلى سبيل المثال جرى عام 2012م تقدير قيمة الأضرار الناشئة عن الجرائم السايبرية في أستراليا، وكانت قرابة (2) مليار دولار.

وتظهر الدراسات أن نسبة مستخدمي الإنترنت الذين يقعون ضحايا الجرائم السايبرية تتراوح ما بين (1. 17%)، وهذه النسبة تزداد في الدول الأقل نموًّا، ووفق دراسة للأمم المتحدة، أكد مسؤولو تطبيق القانون في دول آسيا، في مسح صدر أوائل عام 2014م، أن الجرائم السايبرية في ازدياد، وبدرجات تتفاوت، وأن أخطار الجرائم السايبرية في مؤسساتهم قد ازدادت في الأشهر الأربعة والعشرين الماضية، ويبدي (44%) من المستخدمين في دول منطقة الشرق الأوسط وشمال إفريقيا مخاوف كبيرة من تعرض حسابات بريدهم الإلكتروني أو غيره من الحسابات على الإنترنت للاختراق، وهذه النسبة أعلى قليلًا مما هي عليه في العالم عمومًا، وهي (41%).

ويبدو أن الغالبية العظمى من الجرائم السايبرية في دول المنطقة العربية هي تلك التي تكون المعلوماتية فيها وسيلة ارتكاب الجريمة، وليس محلها، فوفق إحدى الدراسات عام 2011م، احتلت دولة الإمارات العربية المتحدة المرتبة (19) عالميًّا، في حين جاء لبنان في المرتبة (25) عالميًّا من حيث ترتيب الدول التي تتعرض لهجمات سيبرانية، وفي لبنان تحديدًا، لا تتجاوز جرائم التعدي على الأنظمة والبيانات (5%) من المجموع، في حين أن (95%) منها هي جرائم تقليدية بوسيلة معلوماتية، مثل الاحتيال والقدح، وكذلك في السودان، حيث لا تتجاوز نسبة جرائم التعدي على الأنظمة والبيانات (8%)، في حين تزيد نسبة جرائم شبكات التواصل الاجتماعي على (70%).

مثال حول تهديدات نظم المعلومات في بعض الأوساط:



المصدر: وزارة التربية والتعليم، عُمان.

في منطقة الشرق الأوسط، ومن خلال استطلاع قامت به شركة (PWC) عام 2014م، يعتقد (48%)، أن أخطار الجرائم السايبرية في مؤسساتهم قد ازدادت خلال العامين السابقين.

2.2 ارتفاع معدلات الجرائم السايبرية في دول منطقة الشرق الأوسط

ارتفعت نسبة الجرائم السايبرية في دول منطقة الشرق الأوسط، فعلى سبيل المثال، قد ارتفع معدل الجريمة الإلكترونية في دولة الإمارات العربية المتحدة بنسبة (25%) عام 2013م مقارنة بعام 2012م، وقد ارتفع معدل الجريمة السايبرية في كثير من الدول العربية بين عامي 2012 و2013 مثلًا، وتصدرت قضايا الاحتيال والابتزاز بهدف الحصول على المال ولأهداف غير الأخلاقية قائمة الجرائم المرتكبة، وذلك بحسب إحصاءات صادرة عن شرطة دبي، وقد ورد عن الإدارة العامة للتحريات والبحث الجنائي

أن «البلاغات ترد من كلا الجنسين ومن أعمار مختلفة، وتتركز بالنسبة إلى النساء على مواقع الزواج الإلكترونية، حيث يستغل الجاني إقبال الإناث من مختلف الأعمار على هذه المواقع لأغراض متعددة»، وارتفعت الجرائم السايبرية في دولة الكويت عام 2012م من (563) قضية إلى (997) قضية عام 2013م، وازداد عدد الجرائم السايبرية المبلغ عنها في سلطنة عُمان لدى سلطة التحقيق من أقل من (200) في نهاية عام 2011م إلى أكثر من (800) قضية في نهاية عام 2013م.

ومن صفات الجرائم السايبرية السرعة التي تتم بها، إذ قد تحدث الأضرار حتى قبل أن تعي الضحية باستهدافها، وهو ما قد لا يتيح للضحية الدفاع عن نفسها، ويقدر عدد ضحايا الجرائم السايبرية بنحو (559) مليون ضحية في العام، أو أكثر من (1,5) مليون ضحية في اليوم، وتشير بعض الإحصاءات إلى أن (72%) من مستخدمي الإنترنت من الرجال يقعون ضحية هذه الجرائم مقابل (65%) من مستخدمي الإنترنت من النساء، وتدل هذه الإحصاءات على أن الرجال هم عرضة لجرائم الإنترنت أكثر من النساء، وخاصة الفئة العمرية ما بين (18 إلى 31) سنة، ويرجع ذلك إلى استخدامهم للإنترنت مددًا زمنية أطول، ولجرأتهم بالدخول إلى مواقع مختلفة، وانخراطهم في سلوك محفوف بالأخطار عبر الإنترنت ما يعرضهم أكثر للاحتيال والسرقات والبرمجيات الخبيثة.

ويلاحظ ارتفاع الجرائم السايبرية ضد المرأة، وخاصة تلك التي تتعلق بالعنف ضدها، حيث إن (95%) من السلوك العدواني على الإنترنت كالتحرش، والمطاردة، واللغة المسيئة، والصور المهينة هي موجهة ضد النساء، وعادة ما تصدر من الشريك أو من شريك سابق، وفي دراسة حديثة أجراها الاتحاد الأوروبي عام 2014م، يظهر أن (4%) من النساء ما بين سن (18 و29) عامًا قد عانين خلال السنة السابقة ملاحقة عبر الفضاء السايبري (Cyberstalking) في حين أن (11%) من النساء اللواتي تمت مقابلتهن لغرض الدراسة، وهن في عمر (15) سنة فما فوق، قد تلقين نوعًا من الرسائل غير المرغوب فيها، كالرسائل الجنسية الهجومية عبر البريد الإلكتروني أو الرسائل

النصية (SMS)، أو التحرش غير اللائق عبر شبكات التواصل الاجتماعي، وتبقى الولايات المتحدة الأمريكية البلد الأول المنتج للبريد الواغل (أو غير المرغوب فيه)، ويقدر أن البريد الواغل قد استهلك عام 2012م قرابة (70%) من مجمل حركة البيانات على الإنترنت.

ويُعدّ مكتب التحقيقات الفيدرالي في الولايات المتحدة الأمريكية جرائم تكنولوجيا المعلومات من أهم الجرائم التي تواجهها الولايات المتحدة، ويعتقد نحو (60%) من أصحاب الأعمال في الولايات المتحدة أن الضرر اللاحق بهم من جراء الجرائم السايبرية يفوق الضرر الناجم عن الجرائم العادية، وأكد تقرير صادر عن الأوروبول عام 2011م حول تقييم أخطار الجريمة المنظمة أن تكنولوجيا الإنترنت أصبحت عاملًا أساسيًّا لتسهيل معظم أنشطة الجريمة المنظمة.

وهكذا لا بد من التساؤل عما إذا كانت هذه الوسيلة الجديدة للتواصل؛ أي الإنترنت، تعطي نتائج إيجابية أم أن عيوبها تفوق إمكاناتها، والجواب عن هذا السؤال رهن بنجاعة التدابير المتخذة في كل دولة لضمان الأمن والأمان السايبري.

3.2 التمييز بين تنظيم السلوك، والجرائم، والأمن في الفضاء السايبري

قد لا تكون جميع الاعتداءات في الفضاء السايبري مُجَرَّمَةً في القانون الجزائي في بعض الدول، وذلك على الرغم من الأضرار التي قد تنشأ عنها، وفي هذه الحالة، تُعدّ المضايقات والهجمات الإلكترونية سلوكًا غير ملائم يتطلب قواعد وخططًا لتنظيم السلوك في الفضاء السايبري، وعندها يجري التركيز على الأخطار العريضة الشخصية والاجتماعية الناتجة عن استعمال الحاسوب.

أما عندما تكون هذه الأفعال مُجَرَّمَةً جزائيًّا، فتُعدّ هذه الهجمات والمضايقات السايبرية جرائم سيبرانية، وتتطلب خطة وطنية ضمن إستراتيجية للأمن السايبري،

حيث يجري إعداد خطة لفضاء سيبراني آمن وموثوق وتنفيذها، بحيث تكون الدولة قادرة على مجابهة الهجمات على البيانات والأنظمة، ولا سيما الهجمات التي تطول البنية الأساسية الحساسة والأنظمة المعلوماتية للأمن القومي.

ويمكن القول: إن العمل على توفير الأمن والأمان وتنظيم السلوك في الفضاء السايبري يسهم حكمًا في مجابهة الجرائم السايبرية، ويؤكد الاتحاد الدولي للاتصالات في دراسة صادرة عنه أن وضع إستراتيجية لمكافحة الجرائم السايبرية هو عنصر لا يتجزأ من إستراتيجية الأمن السايبري.

4.2 الطابع الدولي للجرائم السايبرية

يُعدّ الطابع الدولي للجرائم السايبرية من أبرز الصفات التي تميزها، وهي بذلك تتحدى النظام القانوني المحلي والدولي، إذ يطغى في كثير من الأحيان الطابع الدولي على الجريمة السايبرية، فهي جريمة عابرة للحدود، وقد تتضمن أكثر من عنصر أجنبي، فالفعل الجرمي قد يحصل في بلد معين، وتتحقق النتيجة الجرمية في بلد آخر، مثل: حالة اختراق نظام معلوماتي عن بعد، وقد تتحقق النتيجة الجرمية في جميع البلدان، مثل: حالة نشر قدح وذم بحق شخص معين على موقع إلكتروني يمكن الوصول إليه من معظم دول العالم.

ولا تطول الجرائم السايبرية اليوم الأفراد فقط، بل أصبحت جرائم شاملة قد تأخذ شكل هجمات ضخمة منسقة تطول البنية الأساسية الحساسة للمعلومات في أكثر من دولة، أو شكل أنشطة إرهابية على الإنترنت، وعام 1998م، عمدت مجموعة الدول الصناعية الثماني التي هي أكثر تطورًا في العالم (G8) إلى إطلاق خطة عمل لمحاربة الجرائم السايبرية وإنشاء شبكة خبراء متاحة (7) أيام في الأسبوع على مدار (24) ساعة في اليوم؛ للمساعدة على التحقيقات المتعلقة بجرائم المعلوماتية، وكذلك تدريب أجهزة الأمن لدى تلك الدول وتجهيزهم.

5.2 مقتطفات من أخبار عالمية حول تعاظم أهمية أمن المعلومات وأمانها

19,7 مليار هجمة إلكترونية في العالم يوميًّا.

أعلن المركز الوطني للأمن الإلكتروني (الرياض) عن رصد محاولات هجوم إلكتروني تعرضت لها جهات حكومية ومحلية عدة عن طريق رسائل بريد إلكترونية لسرقة المعلومات، وكشفت شركة (سيسكو) العالمية عن تصديها لنحو 19,7 مليار هجمة إلكترونية يوميًّا في العالم، إضافة إلى افتقار العالم لأكثر من مليون مختص أمني في مجال الحماية الإلكترونية.

الاقتصادية، الثلاثاء 17 شعبان 1437هـ/ الموافق 24 مايو 2016م.

الهجمات الإلكترونية الخبيثة تتكاثر وتكبد الشركات 400 مليار دولار سنويًّا.

جيليان تيت من واشنطن.

بشكل عام، الهجمات الإلكترونية تتزايد بشكل كبير، وتكلف الشركات 400 مليار دولار سنويًّا، بحسب بيانات من (مايكروسوفت).

وقال توم بيرت، نائب المستشار العام في شركة (مايكروسوفت)، في مؤتمر نظمته (فاينانشيال تايمز) في واشنطن الأسبوع الماضي (مشيرًا إلى مشكلة تخلف التشريعات ضد الجرائم المعلوماتية): «لنفكر في حالة وجود شبكة برامج خبيثة في سنغافورة يديرها قراصنة في بلغاريا تسببوا في ضرر لشخص في أمريكا. من يملك السلطة القضائية؟ وما القوانين المستخدمة؟». «لا أحد يعرف، في الفضاء الإلكتروني، كما هي الحال في النظام المالي العالمي قبل عقد من الزمن، مجموعة كبيرة من النشاط الإجرامي في خطر أن يتم تجاهلها؛ لأن القواعد الوطنية غير مناسبة لعالم رقمي سريع النمو».

الاقتصادية، الأربعاء 13 رجب 1437هـ/ الموافق 20 إبريل 2016م.

مكتب أمن المعلومات الألماني ينصح بعدم دفع الفدى لقراصنة الكمبيوتر.

برلين – د ب أ.

هناك زيادة ملحوظة في نمط جديد من عمليات القرصنة والاحتيال عبر الإنترنت، حيث ينجح هؤلاء المحتالون في تهريب برامج إلى أجهزة الكمبيوتر الشخصي لضحاياهم تؤدي إلى تشفير الملفات الشخصية لهؤلاء الضحايا، ثم يطلبون منهم إرسال مال عبر خدمات تحويل أموال مجهولة مقابل استعادة الدخول على هذه الملفات.

ولكن مكتب أمن المعلومات الألماني ينصح الضحايا بعدم دفع أي أموال للمحتالين؛ لأنه حتى في حالة دفع الفدية لا يوجد ما يضمن للضحية استعادة الدخول على ملفاتهم.

والأفضل من وجهة نظر المكتب الاحتفاظ بنسخة احتياطية من هذه الملفات الشخصية المهمة على قرص صلب خارجي أو شريحة ذاكرة منفصلة بعيدًا عن جهاز الكمبيوتر، بحيث يمكن استرداد هذه الملفات في حالة تعرضها للسطو.

يُذكر أن برامج مكافحة الفيروسات تستطيع غالبًا التعرف إلى برامج التجسس التي تستهدف الحصول على فدية، لكنها لا تستطيع منع تشفير الملفات الشخصية. في الوقت نفسه، فإن الشخص الذي يقوم بعمل نسخة احتياطية من ملفاته المهمة بشكل منتظم يستطيع استعادة الحالة الأصلية للكمبيوتر الشخصي بسرعة معقولة بعد التعرض لعملية قرصنة.

صحيفة الرياض، الإثنين 24 ربيع الأول 1437هـ/ 4 يناير 2016م.

باحثون يخترقون شفرات نظام كمبيوتر كوريا الشمالية المضاد للتجسس.

ووفقًا لموقع independent البريطاني، تمكن مجموعة من الباحثين الدخول على هذا النظام والتعرف إلى تفاصيله الخفية، واكتشف مجموعة من الباحثين النظام السري الذي تعمل به أجهزة الكمبيوتر الخاصة بكوريا الشمالية، الذي تم تطويره من أجل الحفاظ على المعلومات المهمة بشكل سري ووقف تسريبها، وإبقاء الاتصالات مشفرة، وكانت منذ مدة قصيرة مجهولة للغاية، وهذا النظام يحمل اسم Red Star OS ويعتمد على برنامج

Linux وهو يبدو مشابهًا لنظام تشغيل Mac OS، ولكنه يحتوي على كل أنواع التكنولوجيا المتطورة التي تسمح لكوريا الشمالية بالسيطرة على طريقة استخدامه.

الاقتصادية، الأربعاء 19 ربيع الأول 1437هـ/ الموافق 30 ديسمبر 2015م.

الجريمة الإلكترونية... الإنترنت المنبر الأخطر للمتطرفين.

ابتزاز إلكتروني.

كشفت ختام بنت عاهد الشريدة ـ اختصاصية علوم الحاسب وأمن المعلومات بجامعة الأميرة نورة بنت عبدالرحمن ـ مشكلات الجرائم الإلكترونية قائلةً: أولًا: الاحتيال والجرائم المالية (Fraud and financial crimes): وتشمل مجموعة متنوعة من الاحتيال على الإنترنت، وذلك ما يسمى التَّصَيُّد (Phishing)، وكذلك الهندسة الاجتماعية (Social Engineering) التي تستهدف المستخدمين والشركات بشكل مباشر، ويشمل هذا النوع من الاحتيال ما يقوم به الموظفون الفاسدون في المؤسسات المالية من خلال إدخال بيانات خاطئة أو تعليمات غير مصرح بها، أو استخدام عمليات غير قانونية بهدف السرقة، وكذلك تعديل البيانات المخزنة أو حذفها، أو إساءة استخدام أدوات النظام الموجودة أو حزم البرامج أو كتابة شفرات برمجية لأغراض الاحتيال، مضيفةً أنه يأتي ثانيًا: الابتزاز الإلكتروني (Cyber extortion): ويكون ذلك بقطع الخدمة (DDOS) عن المواقع الإلكترونية وخوادم البريد الإلكتروني، أو نظم التشغيل للحاسبات، أو غيرها من هجمات القراصنة الخبيثة، ويكون هدفها الابتزاز المالي، وكذلك الإرهاب الإلكتروني (Cyber terrorism) وهي الاختراقات التي تشكل جهدًا منظمًا لإرهابيين إلكترونيين، أو وكالات مخابرات أجنبية، أو أي جماعات تسعى لاستغلال ثغرات أمنية محتملة في الأنظمة الحيوية، مبينةً أنه يأتي ثالثًا: الإرهابيون الإلكترونيون (Cyber terrorists): وهم الأشخاص الذين يدفعون حكومات أو منظمات لتلبية أهدافهم السياسية أو الاجتماعية من خلال إطلاق هجوم إلكتروني على أجهزة حواسيب وشبكات والمعلومات المخزنة عليها.

وأضافت: الحرب الإلكترونية (Cyber warfare) هي قائمة بالفعل بين كثير من الدول من خلال أجهزة الحاسوب وشبكات الإنترنت، ويعتقد محللون أن مثل هذا النوع من الهجمات قد يصبح القاعدة في الحروب المستقبلية بين الدول، حيث بدأت بعض الجيوش بتشكيل وحدات خاصة بالحروب، هدفها اختراق الدول الأخرى وتدمير بنيتها التحتية الإلكترونية، وربما يتم تكليف القادة العسكريين لقيادة مثل هذه الحروب مستقبلًا.

صحيفة الرياض، الأحد16 ربيع الأول 1437هـ/ 27 ديسمبر 2015م.

سرقة بيانات أربعة ملايين شخص بعد اختراق موقع (تولك تولك) البريطاني.

أعلنت شركة للاتصالات البريطانية (تولك تولك) أن بيانات عملائها في خطر بعد عملية القرصنة التي تعرض لها موقعها الإلكتروني الأربعاء الماضي.

الاقتصادية، الأحد 12 محرم 1437هـ/ الموافق 25 أكتوبر 2015م.

إجراءات عقابية لتعزيز أمن المعلومات في القطاع الخاص.

مراد أحمد وسام جونز ودنكن روبنسون من لندن وهانا كوتشلر وجينا كوهين من سان فرانسيسكو.

تعرضت الولايات المتحدة لهجمات قراصنة الكمبيوتر على نطاق أوسع بكثير، بدءًا من مجموعة متاجر التجزئة (تارجت) عام 2013م، التي فقدت سجلات 70 مليونًا من عملائها، إلى الهجوم المدمر على شركة أفلام سوني في العام الماضي.

تشهد تكلفة الهجمات الإلكترونية على الشركات تصاعدًا سريعًا، ووفقًا لمعهد بونيمون، وهو مجموعة أمريكية مختصة في بحوث الأمن الإلكتروني، ارتفعت التكلفة في المملكة المتحدة بنسبة 14 في المئة العام الماضي،

وتشير التقديرات إلى أن التكلفة على شركات الخدمات المالية ستصل إلى 8,5 مليون جنيه إسترليني لكل شركة هذا العام، أكثر من ضعف التكلفة البالغة ثلاثة ملايين جنيه

عام 2012م، ويتوقع أن تعاني شركات الطاقة والخدمات ارتفاعًا حادًّا، مع ارتفاع التكاليف لتصل إلى 6,5 مليون جنيه لكل مجموعة عام 2015م، مقارنة بـ 5,2 مليون جنيه العام الماضي.

غير أن الأثر المالي لشن هجمات على الشركات في المملكة المتحدة يختلف عن الأثر في الولايات المتحدة. وفقًا لمعهد بونيمون يكلف الاختراق العادي الشركة في المملكة المتحدة 6,3 مليون دولار؛ أي أقل من نصف المبلغ في الولايات المتحدة، البالغ 15 مليون دولار.

وبحسب تقرير صادر عن شركة برايس ووترهاوس كوبرز للخدمات المهنية، تعكف الشركات في جميع أنحاء العالم على تعزيز ميزانيات الأمن، مشيرًا إلى أنها زادت استثماراتها في هذا الجانب بنسبة 24 في المئة العام الماضي، وتحاول المصارف العمل معًا للتصدي لهذه المشكلة، وأنشأت لهذا الغرض (مركز تحليل وتبادل معلومات الخدمات المالية) الذي يتبادل البيانات المتعلقة بالتهديدات الأمنية، ولدى هذه الهيئة المختصة بالصناعة 5500 عضو، بما فيها بنك جيه بي مورجان تشيس، وسيتي جروب، وبنك ويلز فارجو، وإتش إس بي سي.

الاقتصادية، الإثنين 20 محرم 1437هـ/ الموافق 02 نوفمبر 2015م.

الفضاء الإلكتروني يعطي مفهومًا جديدًا للحرب.

عام 2014م، متوسط ما يسمى هجوم التهديد المتواصل استمر 205 أيام قبل أن يتم كشفه، وذلك وفقًا لشركة فايرآي للأمن الرقمي، وأكثر البلدان التي تعرضت للهجوم عام 2015م كانت الولايات المتحدة، وكوريا الجنوبية، واليابان، وكندا، والمملكة المتحدة وألمانيا، وقليل من الأشخاص في أوساط الدفاع الإلكتروني الغربي ترددوا في تحديد المجرمين الرئيسين: روسيا، والصين، مع إيران التي تلحق بسرعة.

يقول أحد كبار ضباط القيادة الإلكترونية العسكرية في الولايات المتحدة: إن واحدة من تكتيكات موسكو المفضلة هي تسليح عصابات الجريمة بأدوات قرصنة وبرمجيات خبيثة،

والتعاقد معها لتنفيذ عمليات ضد الخصوم، أو لحشد ما يسمى هجمات (العلم المزيف) لإرباك عمليات الإسناد.

ستيوارت بول روب، مسؤول الاستخبارات العسكرية السابق والرئيس التنفيذي حاليًّا لمجموعة استخبارات الأعمال KCS يقول: «إن التعقيد المتزايد لأدوات البرمجيات الخبيثة، والموارد المالية الكبيرة للدول التي تستخدمها، وانتشار العصابات الإجرامية المنظمة في هذا القطاع، يجعل من الصعب على نحو متزايد فهم مدى خطورة هذه القضايا تمامًا».

ويقول أحد كبار المسؤولين البريطانيين الذي هو على معرفة وثيقة بالقدرات الهجومية في المملكة المتحدة: «إن بإمكاننا إيقاف كل شيء في أي مكان نريده، لكننا لسنا في سبيلنا لفعل ذلك. جزء من المشكلة هو في معرفة الآثار التي تترتب على ذلك، وكيف سيستجيب الخصم، فلا أحد يريد حربًا فعلية».

الاقتصادية، الأربعاء 20 شوال 1436هـ/ الموافق 05 أغسطس 2015م.

قراصنة صينيون يستحوذون على معلومات حساسة عن موظفي «الاستخبارات الأمريكية».

كشفت مصادر أمريكية عن حصول قراصنة المعلوماتية على معلومات حساسة بينها تصاريح أمنية خاصة بالموظفين والمتعاقدين، إثر اختراق بيانات موظفين في الإدارة الأمريكية، بخلاف معلومات في غاية الخطورة عن موظفي وكالة الاستخبارات المركزية، وأشارت المصادر إلى أن المحققين يبحثون في هجومين إلكترونيين منفصلين، يعتقد بشكل كبير أن مصدرهما هو الصين، اخترقا سجلات الموظفين الحكوميين في قاعدة بيانات مكتب إدارة شؤون الموظفين.

وقال مسؤول أمريكي: إن قاعدة البيانات (حساسة جدًّا، وهي موصولة بجهات سيادية عدة»، في حين ذكر تقرير الصحيفة أن القاعدة ربما تحتوي على ملفات لبعض موظفي وكالة الاستخبارات المركزية، وكانت الإدارة الأمريكية قد أعلنت، الأسبوع الماضي، أنها

رصدت عمليات قرصنة معلوماتية طالت المعطيات الشخصية لأربعة ملايين موظف فيدرالي على الأقل، في هجوم إلكتروني ضخم يُشتبه بأن مصدره الصين.

الاقتصادية، الأحد 1436/8/27هـ/ الموافق 14 يونيو 2015م.

هجوم إلكتروني يستهدف مصلحة الضرائب الأمريكية.

واشنطن: أ. ف. ب.

اعترفت مصلحة الضرائب الأمريكية بأنها تعرضت لهجوم إلكتروني أسفر عن سرقة معطيات ضريبية تتعلق بنحو مئة ألف شخص، وقال مكتب الدخل الداخلي في بيان: إن القراصنة قاموا أولًا بجمع معلومات شخصية عن مكلفي الضرائب من طرف ثالث بينها تاريخ الميلاد والعنوان ورقم الضمان الاجتماعي، ثم استخدموا هذه المعطيات لدخول الخدمة الإلكترونية لمصلحة الضرائب، وأضاف البيان أنهم «حصلوا من مصدر خارجي على معلومات كافية لعبور عملية التعريف التي تتألف من مراحل عدة، بما في ذلك أسئلة التحقق من الهوية التي لا يمكن إلا لمكلف الضرائب الإجابة عنها»، وأوضح أن هذا الهجوم وقع بين شباط/ فبراير ومنتصف أيار/ مايو، مشيرًا إلى مئتي ألف اختراق سمح نصفها بسرقة معطيات.

ويأتي هذا الحادث في أوج تصاعد هجمات إلكترونية واسعة على شركات أمريكية كبرى بينها مصارف مهمة، يثير قلق البيت الأبيض.

الاقتصادية، الأربعاء 09 شعبان 1436هـ/ الموافق 27 مايو 2015م.

مخاوف من «حرب إلكترونية» تسير على خطى الحروب النووية.

في الشهر الماضي استضافت هولندا المؤتمر العالمي للفضاء السيبراني (الإلكتروني) لعام 2015م، الذي جمع ما يقرب من 2000 من المسؤولين الحكوميين والأكاديميين وممثلي الصناعات، وغيرهم. حيث تولى الباحث والكاتب الأمريكي جوزيف س. ناي الأستاذ في جامعة هارفارد، ومؤلف كتاب (هل انتهى القرن الأمريكي؟) رئاسة لجنة من المختصين لمناقشة الفضاء الإلكتروني والأمن، وقد ضمت اللجنة نائب رئيس شركة مايكروسوفت واثنين من الوزراء الأجانب.

وكان هذا المؤتمر الذي ضم أطرافًا متعددة من أصحاب المصلحة هو الأحدث في سلسلة من الجهود الرامية إلى إرساء قواعد الطريق من أجل تجنب الصراع السيبراني.

ويشير ناي في مقال له بعنوان (معايير دولية في الفضاء الإلكتروني) إلى أن القدرة على استخدام الإنترنت لإلحاق الضرر أصبحت الآن راسخة ثابتة.

ويضيف ناي: ثم ظهرت في أوائل التسعينيات الشبكة العنكبوتية العالمية، وتنامت من بضعة ملايين من المستخدمين آنذاك إلى أكثر من مليار مستخدم اليوم، وفي غضون ما يزيد على الجيل قليلًا، أصبحت شبكة الإنترنت الركيزة الأساسية للاقتصاد العالمي والحوكمة في مختلف أنحاء العالم.

وستضاف مليارات عدة أخرى من المستخدمين في العقود المقبلة، فضلًا على عشرات المليارات من الأجهزة (المتصلة بالإنترنت) التي تتراوح بين منظمات الحرارة إلى أنظمة التحكم الصناعية، وكل هذا الترابط المتعاظم يعني ضمنًا نشوء نقاط الضعف التي تستطيع الحكومات أو الجهات الفاعلة غير الحكومية استغلالها، وفي الوقت نفسه، بدأنا توًّا نتصالح مع العواقب المترتبة على ذلك فيما يتصل بالأمن الوطني، والواقع أن الدراسات الإستراتيجية للمجال السيبراني (الإلكتروني) تشبه الإستراتيجية النووية في الخمسينيات: فالتحليلات لا تزال غير واضحة حول معنى الهجوم، والدفاع، والردع، والتصعيد، والمعايير، والحد من التسلح.

ويُستَخدَم مصطلح (الحرب الإلكترونية) على نحو غير محكم على الإطلاق لوصف مجموعة واسعة من السلوكيات بدءًا من الاستطلاعات البسيطة وتشويه المواقع والحرمان من الخدمة إلى التجسس والتدمير، وهو في هذا يعكس تعريفات القواميس لكلمة (حرب) التي تشمل أي جهد منظم «لوقف أو إلحاق الهزيمة بشيء يُنظر إليه بوصفه خطرًا أو سيئًا» (على سبيل المثال الحرب على المخدرات).

وهناك أربع فئات رئيسة للتهديدات الإلكترونية للأمن الوطني، وكل منها تحتل مدة زمنية مختلفة، وتتطلب (من حيث المبدأ) حلولًا مختلفة: الحرب الإلكترونية والتجسس الاقتصادي، وهو ما يرتبط إلى حد كبير بالدول، وفئة الجريمة الإلكترونية والإرهاب

الإلكتروني، وهو ما يرتبط في الأغلب بجهات فاعلة غير تابعة لدولة، وتتبع أعلى التكاليف حاليًّا من التجسس والجرائم، ولكن الفئتين الأخريين ربما تصبحان أعظم تهديدًا على مدى العقد المقبل مقارنة بحالهما اليوم. وعلاوة على ذلك، مع تطور التحالفات والتكتيكات، ربما تتداخل الفئات بشكل متزايد.

ويختم ناي المقال مرجحًا أن يستغرق إبرام الاتفاقيات بشأن القضايا الخلافية مثل الاقتحام الإلكتروني لأغراض مثل التجسس وإعداد ساحة المعركة وقتًا أطول، وعلى الرغم من ذلك، فلا ينبغي لعدم القدرة على تصور اتفاقية شاملة للحد من التسلح الإلكتروني أن تمنع التقدم بشأن بعض القضايا الآن، فإن المعايير الدولية تميل إلى التطور ببطء، فقد استغرق الأمر عقدين من الزمان في حالة التكنولوجيا النووية، وكانت الرسالة الأكثر أهمية التي أبرزها المؤتمر الهولندي الأخير هي أن نقاط الضعف الإلكترونية الهائلة تقترب الآن من هذه النقطة.

الاقتصادية، الأحد 06 شعبان 1436هـ/ الموافق 24 مايو 2015م.

100 مصرف في العالم تتعرض لسرقات إلكترونية بمليار دولار.

تعرض أكثر من 100 مصرف ومؤسسة مالية في نحو 30 دولة إلى عمليات سطو إلكترونية (غير مسبوقة)، وقدرت شركة (كاسبرسكاي لاب) للأمن الإلكتروني حجم المسروقات خلال الهجمات التي بدأت منذ عام 2013م بنحو مليار دولار حتى الآن.

قال مركز تحليل الخدمات المالية وتبادل المعلومات، المسؤول عن تبليغ المصارف بأنشطة القرصنة الإلكترونية من جهته: إنه اطلع على تقرير (كاسبرسكاي لاب) منذ يناير الماضي، مؤكدًا أن المصارف بدأت في اتخاذ الإجراءات اللازمة لتجنب تلك الهجمات وحماية عملائها.

الاقتصادية، الثلاثاء 28 ربيع الثاني 1436هـ/ الموافق 17 فبراير 2015م.

العلوم والتقنية: 445 مليار دولار خسائر الهجمات الإلكترونية في العام الواحد.

إن تكلفة خسائر الهجمات الإلكترونية في العام الواحد قدرت بـ 445 مليار دولار عالميًّا، ومن المتوقع أن تتزايد فاتورة خسائر تلك الهجمات في المستقبل نتيجة التوسع في الخدمات الإلكترونية ودخول مفاهيم تقنية جديدة، وذلك يعزز الحاجة إلى تطوير جهود البحث العلمي في مجال أمن المعلومات لدعم المصالح الوطنية من خلال نقل وتوطين التقنيات وبناء القدرات وابتكار الخوارزميات الوطنية التي يمكن استخدامها بشكل آمن لحماية البيانات.

الاقتصادية، الأربعاء 21 جمادى الثاني 1437هـ/ الموافق 30 مارس 2016م.

فيروسات إلكترونية في محطة نووية ألمانية.

قالت الشركة المشغلة لمحطة الطاقة النووية في ألمانيا أمس الأول: إنه جرى اكتشاف أن المحطة التي تولد الكهرباء مصابة بفيروسات كمبيوتر، لكنها لا تشكل خطرًا على عمليات المنشأة؛ لأنها معزولة عن الإنترنت، وتدير شركة (آر. دبليو. إي) للمرافق محطة جوندريمينجن النووية التي تقع على بعد نحو 120 كيلومترًا شمال غرب ميونيخ، وقالت الشركة بحسب (سكاي نيوز): إن الفيروسات اكتشفت في الوحدة (ب) في المحطة في نظام للكمبيوتر جرى تعديله عام 2008م لإضافة برنامج لإظهار البيانات مرتبط بمعدات لنقل قضبان الوقود النووي.

واكتشفت أيضًا فيروسات في 18 محرك أقراص قابلًا للنزع في أجهزة كمبيوتر مكتبية تجري صيانتها بشكل مستقل عن أنظمة تشغيل المحطة.

الاقتصادية، الخميس 21 رجب 1437هـ/ الموافق 28 إبريل 2016م.

فيروسات تهاجم الهواتف الذكية تحت غطاء متاجر التطبيقات.

كثيرون هم المستخدمون الذين لا يقومون بتحميل التطبيقات على هواتفهم الذكية إلا إذا كان مصدرها متاجر التطبيقات الرسمية، مثل متجر أبل ومتجر جوجل بلاي؛ خوفًا

من أن تصيب هواتفهم إحدى البرمجيات الخبيثة أو برمجيات الفدية، لكن هذا الشيء لم يعد يكفي لحمايتهم، حيث بدأت البرمجيات الخبيثة وهجمات الفدية تلبس ثوب التطبيقات الرسمية في متاجر تطبيقات الهواتف الذكية والأجهزة اللوحية، وكشفت شركة Kaspersky لأمن المعلومات أن عدوى البرمجيات الخبيثة المستهدفة للأجهزة المتنقلة كانت هي الأكثر جدوى بالنسبة إلى مجرمي الإنترنت، حيث كانت تحدث عن طريق إحدى البرمجيات الخبيثة الموجودة في تطبيقات الأجهزة المتنقلة التي يتم تنزيلها من app- stores وكذلك من خلال وجود برمجية خبيثة في حزمة برامج أولية للهاتف، وذلك بسبب الإقبال المتزايد على خدمات الأجهزة المتنقلة في المنطقة، الذي أدى دورًا في جذب انتباه مجرمي الإنترنت الذين يقومون بتطوير أدواتهم بشكل مستمر.

الاقتصادية، الثلاثاء 19 رجب 1437هـ/ الموافق 26 إبريل 2016م.

أضرار الشركات في المملكة المتحدة بسبب الجرائم السايبرية:

أفادت (81%) من الشركات الكبيرة، و(60%) من المؤسسات الصغيرة في المملكة المتحدة بتعرضهم لاختراق معلوماتي عام 2013م، وكانت قيمة الضرر لأقسى حالات الجرائم السايبرية تقع بين (600) ألف ومليون جنيه إسترليني للشركات الكبيرة، وبين (65) ألف و(115) ألف جنيه إسترليني للشركات الصغرى، ويرى مسؤولو بنك إنجلترا أن الهجمات السايبرية أكبر تهديد للاستقرار المالي في المملكة المتحدة.

المصدر: تقرير اللجنة الاقتصادية والاجتماعية لغربي آسيا، الإسكوا.

أستراليا تخصص 230 مليون دولار لتطوير الأمن الإلكتروني.

كانبيرا – واس.

أعلنت الحكومة الأسترالية صباح اليوم الخميس عن تخصيص حزمة بقيمة 230 مليون دولار أسترالي لتعزيز إستراتيجية الأمن الإلكتروني وتطويرها؛ وذلك لحماية المصالح الأسترالية من أي اعتداءات أو هجمات إلكترونية.

ورأى مالكولم تيرنبول رئيس الوزراء الأسترالي في بيان أن عملية بناء بيئة موثوق بها وآمنة على شبكة الإنترنت يُعدّ أمرًا أساسيًّا للتطور ولمواجهة التحديات المستقبلية، ويُعدّ أمرًا أساسيًّا أيضًا في المجالات الاجتماعية والاقتصادية والإستراتيجية.

الخميس 14 رجب 1437هـ/ 21 إبريل 2016م.

الجريمة الإلكترونية.. مليارا دولار خسائر 12 ألف شركة حول العالم.

خلال المدة من تشرين الأول (أكتوبر) 2013 وشباط (فبراير) 2016م تم استهداف أكثر من 12 ألف شركة تجارية في جميع أنحاء العالم بعمليات الاحتيال هذه، التي تعرف أيضًا بمخططات رسائل البريد الإلكتروني الموجهة من الرئيس التنفيذي، وعادت هذه العلميات على المجرمين بمبلغ صافٍ يقدر بملياري دولار، وفقًا لمركز شكاوى جرائم الإنترنت، وهو فريق تحقيق واستخبارات داخل مكتب التحقيقات الفيدرالي يتعقب جرائم الكمبيوتر، وتعرضت لذلك شركات كبيرة وصغيرة في 108 بلدان، والخطر آخذ في التزايد، بحسب ما يقول مسؤولو إنفاذ القانون، ويقول مايكل تومبسون، رئيس فرقة عمل جرائم الإنترنت المالية في مكتب التحقيقات الفيدرالي في نيويورك: «لقد أصبح الأمر خارجًا عن السيطرة»، مضيفًا أن المجرمين «يصبحون أكثر جرأة»، من خلال إدخال أطراف ثالثة، مثل الشركات القانونية والمختصين الاستشاريين، لتنفيذ عمليات الاحتيال، وأصبحوا أكثر تطورًا في كيفية توريط الضحايا المحتملين.

الأحد 19 جمادى الأول 1437هـ/ الموافق 28 فبراير 2016م.

6.2 مقتطفات لمثال المملكة العربية السعودية

هجمات إلكترونية تسعى لاختراق أجهزة عددٍ من الجهات الحكومية.

أوضح المركز الوطني للأمن الإلكتروني أنه تم رصد محاولات هجوم إلكتروني تعرضت له جهات حكومية ومحلية عدة عن طريق رسائل بريد إلكترونية اصطيادي (Phishing email) تهدف إلى اختراق الأجهزة الإلكترونية وسرقة المعلومات عن طريق فتح المرفقات بالإيميل، ثم إرسالها إلى حسابات بريد إلكتروني أخرى،

وأكد المركز الوطني للأمن الإلكتروني على الجميع بضرورة الالتزام بمعايير السلامة الإلكترونية بعدم فتح مرفقات رسائل البريد الإلكترونية المشبوهة تلافيًا لأي أضرار قد تحدث من برمجيات خبيثة تحويها تلك المرفقات.

صحيفة الرياض، الأحد 08 شعبان 1437هـ/ 15 مايو 2016م.

مركز المعلومات الوطني يحذر من ثغرات إلكترونية في مواقع حكومية وصناعية.

حذر مسؤولون في المركز الوطني لأمن المعلومات من وجود ثغرات إلكترونية في مواقع حكومية وصناعية حساسة، مؤكدين أن بعض الشبكات الحكومية تعاني ضعفًا في قدرتها على مواجهة الاختراقات والتهديدات الإلكترونية، التي يسعى المركز الوطني لأمن المعلومات إلى معالجتها.

وأكد وجود تحديات تواجه الأمن الإلكتروني في المملكة على الرغم من إصدار مراسيم ملكية وسياسات تهدف إلى تنظيم أنشطة الأمن الإلكتروني والاستجابة للحوادث الإلكترونية، مشيرًا إلى أنه لا يوجد برنامج واضح لتنظيم السياسات الوطنية وتطويرها لحث الجهات على الالتزام بها.

الاقتصادية، الخميس 23 جمادى الأول 1437هـ/ الموافق 03 مارس 2016م.

كلمة الرياض

وقد واجهت المملكة هجمتين بارزتين: الأولى استهدفت الأنظمة الشبكية لشركة أرامكو، والثانية تم الهجوم فيها على قواعد البيانات في وزارة الخارجية.

الرياض، الأحد 10 صفر 1437هـ/ 22 نوفمبر 2015م.

مؤتمر مكافحة الجرائم المعلوماتية يوصي بـ:

القيام بحملات مستمرة لتوعية جميع فئات المجتمع بأنماط الجريمة المعلوماتية والتعريف بالجهات المعنية للإبلاغ عن تلك الجرائم، وبفتح باب الشراكة والتعاون داخليًّا

وخارجيًّا في مجال مكافحة الجرائم المعلوماتية، وبالتأكيد على قيام المربي بدوره تجاه الصغير وتفعيل الإجراءات النظامية لمحاسبته في حال تقصيره، وبإعداد أدلة إجرائية للضبط والتحقيق في الجرائم المعلوماتية، وإعداد برامج تربوية وإعلامية وتقنية لحماية الصغار من خطر الجرائم المعلوماتية، وحث الجهات الحكومية والأهلية على ضرورة تأمين التعاملات الإلكترونية وسلامتها وفق معايير وطنية محددة، وتحديد جهة مسؤولة عن حماية البنى التحتية المعلوماتية بالتنسيق مع الجهات الحكومية والأهلية، وبدعم المؤسسات التعليمية لتدريب الطلاب والمختصين في أمن المعلومات على أساليب مكافحة الجرائم المعلوماتية وطرقها.

الرياض، السبت 2 صفر 1437/ 14 نوفمبر 2015م.

هاكر سعودي يخترق 23 موقعًا حكوميًّا خلال ساعتين.

تمكن هاكر سعودي، فجر أمس السبت، من اختراق نحو 23 موقعًا إلكترونيًّا حكوميًّا خلال ساعتين، ما بين مواقع تعليمية، وأخرى صحية، ورياضية، وبلدية، ومرورية، وغيرها، مبررًا في رسالته أن سبب تلك الاختراقات هو تجاهل تلك المواقع الحكومية لرسائله عن هجوم محتمل.

عكاظ، الأحد 1436/11/01هـ/ 116 أغسطس 2015م.

الأمن الإلكتروني.. ومسؤولية العملاء:

استطاعت الجهات الأمنية في وقت وجيز أن تسقط شبكة من العمالة الآسيوية تخصصت في السطو على بيانات العملاء في أجهزة الصرف الآلي، للوصول إلى حسابات العملاء والسحب من أرصدتهم، وهي جريمة ذات خطورة عالية؛ لأنها تتضمن الدخول إلى النظام المصرفي التقني للمصارف، ومن ثم تنفيذ عمليات مالية تبدو في ظاهرها صحيحة، ولكنها نوع من استغلال البيانات والاختلاس المالي، بل الأخطر من ذلك أن هذا النوع من الجرائم جزء من الاحتيالات المالية في ساحات الإنترنت، وجزء من النشاط الإجرامي الذي تحذر منه الجهات المسؤولة عن مكافحة هذا النوع من الجرائم، التي امتدت واتسع نطاقها لتشمل معظم الجرائم المعروفة مع تميز في استخدام التقنية.

ولأهمية التوعية، فإن (الإنتربول) السعودي حذر في أوقات سابقة أكثر من مرة من تزايد ملحوظ في حالات الاحتيال الإلكتروني من خلال عمليات البيع والشراء عبر الإنترنت، حيث أوضح (الإنتربول) السعودي بلوغ قضايا التهديد والابتزاز عن طريق شبكة الإنترنت عالميًّا ما نسبته 18 في المئة من مجمل قضايا الجرائم الإلكترونية، وأن قضايا استغلال الأطفال سجلت ما نسبته 14 في المئة من مجمل الجرائم الإلكترونية، وأن قضايا اختراق البريد الإلكتروني تصدرت مجمل قضايا الإجرام الإلكتروني بما نسبته 27 في المئة، إضافة إلى قضايا السب والتشهير وإساءة السمعة والاختراق والاحتيال الإلكترونيين.

الاقتصادية، السبت 03 رمضان 1436هـ/ الموافق 20 يونيو 2015م.

أمن المعلومات يواجه «خطر الاختراق» من الخارج:

شدد (الدكتور زياد آل الشيخ) على أهمية أمن المعلومات للمواطن، وقال: أجرينا دراسة حديثة على المواقع غير الحكومية على شبكة الإنترنت، وهي نحو (7000) موقع عربي مصنفة على أنّها من أعلى المواقع زيارة عربيًّا، ومن خلال البحث اكتشفنا أنّ (2%) من هذه المواقع فيها فيروسات، وأنّ (5%) منها ممنوع الوصول إليها باستخدام برامج أمن المعلومات، وأن (5,6%) من هذه المواقع تعاني مشكلات استخدامها لأدوات قديمة غير محدثة، ومن ثم يصبح الموقع عرضةً للهجوم، ولهذا لا بد من الاهتمام بأمن معلومات المواطن والعمل على حماية معلوماته الخاصة.

ووضح (الدكتور محمد الشيبي) أنّ عملية الاختراق ـ بناءً على الإحصاءات العالمية ـ هي نحو (80%) من الداخل، و(20%) من الخارج.

الرياض، الثلاثاء 18 رجب 1434هـ/ 28 مايو2013م.

تقرير: السعودية في المرتبة 32 عالميًّا في عدد هجمات الإنترنت:

وضحت شركة (سيمانتك) الشركة العالمية، المتخصصة في مجال الأمن والحماية المعلوماتية، في مؤتمرها الصحافي الذي عقد أخيرًا في الرياض، بحضور كيفن إيزاك، المدير الإقليمي في شركة (سيمانتك) في منطقة الشرق الأوسط وشمال إفريقيا، أن

شركة (سيمانتك) أصدرت تقريرها الـ 13 حول تهديدات أمن الإنترنت ISTR، وبيّنت الإحصاءات التي تضمنت زيادةً متنامية في الهجمات والأنشطة الخبيثة في بلدان منطقة الشرق الأوسط، وأوضح التقرير أن السعودية تجاوزت الإمارات، لتتصدر القائمة في منطقة أوروبا والشرق الأوسط وإفريقيا من حيث عدد الأنشطة الخبيثة لكل مشترك في الإنترنت عبر الحزمة العريضة، خلال النصف الثاني من عام 2007م، وذلك بحصولها على نسبة 33 في المئة، حيث تحتل المملكة حاليًّا المركز 32 عالميًّا، بعد أن كانت في المركز 28 في حزيران (يونيو) من عام 2007م.

وفي السياق نفسه، خلُص تقرير تهديدات أمن الإنترنت ISTR، إلى أن شبكة الويب هي الآن الهدف والوسيلة الأساسية لشن الهجمات بدلًا من الهجمات الشبكية، وأن احتمال تعرض مستخدمي الإنترنت للإصابة بمجرد زيارتهم مواقع ويب المعتادة يزداد يومًا بعد يوم، ويستند التقرير إلى البيانات التي تم جمعها بواسطة ملايين الحسابات على الإنترنت، والبحوث الأساسية، والمراقبة الفاعلة للاتصالات بين المخترقين، وهو يوفر نظرة عامة عن حالة أمن الإنترنت في العالم.

ففي الماضي، كان على المستخدم زيارة المواقع المشبوهة عمدًا أو النقر على مرفقات البريد الإلكتروني الخبيثة ليصبح ضحية تهديد أمني. أما اليوم، فيمكن للمخترقين استغلال المواقع العادية التي تبدو سليمة واستخدامها وسيطًا لشن الهجمات على حواسيب المنازل والشركات، وقد لاحظت (سيمانتك) أن المهاجمين يستهدفون بشكل خاص المواقع التي يُرجَّح أن يثق بها المستخدمون، مثل مواقع الشبكات الاجتماعية.

وعام 2007م، اكتشفت (سيمانتك) 711,912 تهديدًا جديدًا مقارنة بتهديدات بلغت 125,243 في العام 2006م؛ أي بزيادة قدرها 468 في المئة. ويرفع ذلك العدد الإجمالي للتهديدات البرمجية الخبيثة التي اكتشفتها (سيمانتك) إلى1,122,311 حتى نهاية عام 2007م.

قاست (سيمانتك) إطلاق كل من البرمجيات السليمة والخبيثة خلال جزء من زمن التقرير، ووجدت أن 65 في المئة من التطبيقات الفريدة التي أطلقت في تلك المدة، وبلغ

عددها 54,609 تطبيقًا كانت مصنفة على أنها خبيثة، وهذه هي المرة الأولى التي تلحظ فيها (سيمانتك) تجاوز عدد التطبيقات الخبيثة لتلك السليمة.

يقول ستيفن تريلينج، نائب الرئيس لشؤون تقنية الأمن والاستجابة لدى (سيمانتك): «لقد كانت النصيحة بتجنب مواقع الإنترنت المشبوهة أمرًا كافيًا في السنوات السابقة، أما اليوم فإن المجرمين يركزون على استغلال مواقع ويب السليمة لمهاجمة المستخدمين، ما يبرز أهمية الإبقاء على الأوضاع الأمنية قوية بغض النظر عن المكان الذي تذهب إليه والنشاط الذي تمارسه على الإنترنت».

الاقتصادية، السبت 19 جمادى الأولى 1429هـ/ الموافق 24 مايو 2008م.