أمن المعلومات على شبكة الإنترنت

د. إياس بن سمير الهاجري

4002 م
أمن المعلومات على شبكة الإنترنت

د. إياس بن سمير الهاجري

(*) مدير عام وحدة خدمات الإنترنت، مدينة الملك عبد العزيز للعلوم والتقنية، الرياض.

135
3. أمن المعلومات على شبكة الإنترنت

1. مقدمة

لم يكن هناك قلق بشأن مخاطر أمنية يمكن أن تتعرض لها شبكة الإنترنت في أول عمرها، إذا أنها كانت محصورة في عدد محدود من الأكاديميين والباحثين في مراكز أبحاث وجامعات محدودة. لذلك عندما تم تصميم البروتوكول الأساسي لنقل المعلومات على شبكة الإنترنت المعروف باسم (TCP/IP) لم يؤخذ في الاعتبار مخاطر أمنية، يمكن أن تتعرض لها الأجهزة المرتبطة بالشبكة. لكن مع مرور الوقت ودخول القطاع التجاري للشبكة وتوسع استخداماتها وتنوعها، وما تتجّع عنه من ازدياد سريع في أعداد المستخدمين على الشبكة، فقد شملت جميع فئات المجتمع المختلفة بتنوع خلفياتهم العلمية والعملية بمختلف الأعمار، بدأت تظهر مشاكل أمنية على شبكة الإنترنت.


سجلت أول حالة اعتداء أمني على شبكة الإنترنت في عام 1988 م أي بعد مضي ما يقرب من عشرين عاماً على إنشائها، حيث قام روبرت موريس الطالب في جامعة كورنيل بتطوير فيروس (عرف لاحقاً باسم 137
فيروس موريس) استغل هذا الفيروس ثغرة في نظام البريد الإلكتروني المستخدم آنذاك مكته من استنهاص نفسه ولنل نسخه إلى عدد كبير من أجهزة الحاسوب الآلي المرتبطة بالشبكة. أحدث هذا الفيروس شللًا مؤقتًا في جميع الأجهزة التي أصابها، وكانت ما يقرب من 10٪ من مجموع الأجهزة المرتبطة بالشبكة آنذاك.

أوضح هذا الحادثة عمليًا كيف أن مشكلة أمنية قد تبدو صغيرة يمكن أن تحدث أضرارًا جسيمة على الشبكة. لذا حرصت وزارة الدفاع الأمريكية ممثلة في وكالة الأبحاث المتقدمة إلى تأسيس فريق لمتابعة الطوارئ التي تحدث على الشبكة. تطور هذا الفريق ليصبح مركزًا متكاملًا يعرف باسم أفضل إدارة إحدى الجامعات (Coordination Center) (CERT) (Carnegie Mellon University) (Carnegie Mellon University) وبدعم أساسي من وزارة الدفاع الأمريكية. تبع هذا المركز إنشاء مراكز أخرى كبيرة في قطاعات حكومية وأكاديمية وتجارية لعل من أبرزها مركز متابعة الطوارئ التابع لوزارة الطاقة.

ومع التوسع السريع في استخدمات الشبكة ازدادت المخاطر الأمنية تبعًا لذلك، فقد قامت معاهد متخصصة بتدريب الفنيين المعينين بإدارة وتشغيل الحاسبات والشبكات على أحدث طرق ووسائل الحماية من المخاطر الأمنية المختلفة. لقد تبنت السلطات الأمنية الأمريكية إلى مخاطر الجرائم المعلوماتية وللأسف على شبكة الإنترنت، لهذا فقد أنشأ مكتب التحقيقات الفيدرالية الأمريكي (FBI) (FBI) مركزًا متخصصًا لحماية المشاكل الأولية من تلك المخاطر حيث يعمل على تحليل ودراسة المخاطر المحتملة، وإصدار تحذيرات في حال اكتشاف ثغرة أمنية جديدة في أحد الأنظمة
الحاسبية، كما يعمل كذلك على البحث والتحرير في حالة حدوث هجمات على تلك المشايخ.

وفي دول أخرى كذلك مثل أستراليا وبريطانيا توجد مراكز معنية بأمن المعلومات. ففي أستراليا توجد هيئة وطنية من مهامها حماية أنظمة الاتصالات والمعلومات الحساسة، التي يكون لاختراقها أثر سلبي مباشر على الأمن الوطني، كما تقوم كذلك بمساعدة ودعم جميع الدوائر الحكومية فيما يخص أمن المعلومات. تلعب هذه الهيئة كذلك دوراً مهماً بالتعاون مع القطاع الصناعي في تطوير أنظمة لتشهير المعلومات. أما في بريطانيا فتوجد إدارة معنية بأمن المعلومات، تعمل ضمن إحدى الجهات الاستخبارية البريطانية. تعمل هذه الإدارة على وضع السياسات والقيود الخاصة بأمن المعلومات، كما تعمل كذلك على حماية المشايخ المعلوماتية الحساسة من أخطار الاختراقات. وفي الهند توجد إدارة مختصة في مكافحة جرائم الإنترنت تابعة لمكتب التحقيقات المركزي، وهو أكبر هيئة أمنية معنية بمتابعة الجرائم والتحقيق فيها.

3. أبعاد ومصادر أمن المعلومات

يشمل أمن الحاسبات والشبكات جميع الإجراءات الضرورية لحماية أجهزة شبكات الحاسبات، وما يتعلق بها من طرفيات وآلات طابعة وأقراس حفظ، كما يشمل أيضاً إجراءات حماية المبنى الذي يضم تلك الأجهزة. إن جميع تلك الإجراءات ما هي إلا حماية المعلومات المخزنة في أجهزة الحاسبات ولذلك يطلق مصطلح أمن المعلومات في بعض الأحوال للتعبير عن أمن الحاسبات. إن أهمية أمن الحاسبات والشبكات لها ثلاثية أبعاد رئيسية:

١٣٩
1. تأمين سرية المعلومات

وذلك يتمثل في ضمان حفظ المعلومات المخزنة في أجهزة الحاسبات وعدم الإطلاع عليها إلا من قبل الأشخاص المخولين بذلك. كما يشمل ضمان سرية المعلومات خلال انتقالها على الشبكة.

2. تأمين سلامة المعلومات

وэтому يعني أن المعلومات المخزنة في أجهزة الحاسبات أو المنقلة على الشبكات يجب ألا يتم تغييرها إلا من قبل الأشخاص المخولين بذلك.

3. تأمين وجود المعلومات

وذلك يتمثل في ضمان عدم حذف المعلومات من قبل أشخاص غير مخولين بذلك.

تواجه أجهزة الحاسبات وشبكات الحاسبات مخاطر أمنية يمكن تصنيفها إلى ثلاثة أصناف: مخاطر طبيعية ومخاطر داخلية ومخاطر خارجية. فالمخاطر الطبيعية تشمل الكوارث الطبيعية كالحرائق والزلزال، أما المخاطر الداخلية فتتمثل في عمليات التخريب التي تصدر من أشخاص يعملون داخل نفس المؤسسة التي تملك أجهزة الحاسبات والشبكات، وأما المخاطر الخارجية فتصدر من أشخاص من خارج المؤسسة. إن كثيراً من المخاطر الداخلية تكون عفوية نتيجة أخطاء في استخدامات الأجهزة تؤدي إلى فتح ثغرات أمنية في تلك الأجهزة.

أما عن الدوافع وراء عمليات تخريب أجهزة الحاسب فهي كثيرة.

١٤٠
فقد تكون دوافع التخريب سياسية بين دول متحاربة تسعى كل منها للحصول على معلومات استراتيجية من الأخرى، وقد تكون تجارية كأن تقوم مؤسسة تجارية بسرقة أو تخريب معلومات حساسة لمؤسسة منافسة لها. إن غالبية الأعمال التخريبية تكون من قبل مخربين محترفين، إما لأغراض تطفلية أو حب للشهرة وإثبات القدرات أمام أقرانهم.

٣. جرائم الإنترنت

إن شبكة الإنترنت شأنها شأن أي شبكة معلوماتية ينطبق عليها موجز أمن المعلومات ذو الأبعاد الثلاثة وهي سرية المعلومات، وسلامتها أي ضمان عدم تغييرها إلا من قبل المصرح لهم بذلك، أما البعد الثالث فهو ضمان وجود المعلومات أي عدم حذفها إلا من قبل المصرح لهم بذلك. إن جرائم الإنترنت ليست محصورة في النموذج الذي سيق ذكره، فالأهداف في جرائم الإنترنت قد تكون المعلومات نفسها وهذه ينطبق عليها ذلك النموذج، وقد يكون الهدف في جريمة الإنترنت الأجهزة نفسها فيسعي المجرم إلى تخريب أو تعطيل تلك الأجهزة. وقد يكون أشخاص أو جهات هي الهدف من الجريمة كتلك المتعلقة بالتهديد أو الابتزاز أو تشويه السمعة.

بقي أن نذكر أن هناك جرائم متعلقة بالإنترنت تتشكل في طبيعتها مع جرائم التخريب أو السرقة التقليدية، كأن يقوم المجرمون بسرقة أجهزة الحاسب المرتبطة بالإنترنت أو تدميرها مباشرة، أو تدمير وسائل الاتصال كالأسلاك والأطباق الفضائية وغيرها. حيث يستخدم المجرمون أسلحة تقليدية إبتداء من المشارط والسكاكين وحتى عبوات متفجرة، وكمثال
لهذا الصنف من الجرائم قام مشغل أجهزة في إحدى الشركات الأمريكية بصنع بندق على أجهزة شركة منافسة وذلك لإحراقها حيث دمر مركز الحاسب الآلي الخاص بتلك الشركة المنافسة برمته. وفيما يلي استعراض لعدد من جرائم الإنترنت:

3.1 صناعة ونشر الفيروسات

وهي أكثر جرائم الإنترنت انتشاراً وتأثيراً. إن الفيروسات كما هو معلوم ليست وليدة الإنترنت فقد أشار إلى مفهوم فيروس الحاسب العالم الرياضي المعروف فون نيومون في منتصف الأربعينات الميلادية. لم تكن الإنترنت الوسيلة الأكثر استخداماً في نشر وتوزيع الفيروسات إلا في السنوات الخمس الأخيرة، حيث أصبحت الإنترنت وسيلة فعالة وسريعة في نشر الفيروسات. إن الهدف المباشر للفيروسات هو المعلومات المخزنة على الأجهزة المقتحمة حيث تقوم بتغييرها أو حذفها أو سرقتها ونقلها إلى أجهزة أخرى.

3.2 الاختيارات

تشتمل في الدخول غير المصرح به إلى أجهزة أو شبكات حاسب آلي. إن جمل عمليات الاختيارات (أو محاولات الاختيارات) تتم من خلال برامج متوفرة على الإنترنت يمكن له خبرات تقنية متواضعة أن يستخدمها لشن هجماته على أجهزة الغير، وهنا تكمن الخطورة.

تختلف الأهداف المباشرة للاختيارات، فقد تكون المعلومات هي الهدف المباشر حيث يسعى المخترق لتغيير أو سرقة أو إزالة معلومات معينة. وقد يكون الجهاز هو الهدف المباشر بغض النظر عن المعلومات المخزنة عليه.
، كأن يقوم المخترق بعمليته بقصد إبراز قدراته «الاختراقية» أو لإثبات وجود
ثغرات في الجهاز المخترق.

من أكثر الأجهزة المستهدفة في هذا النوع من الجرائم هي تلك التي
تستضيف المواقع على الإنترنت، حيث يتم تحريف المعلومات الموجودة
على الموقع أو ما يسمى بتغيير وجه الموقع (Defacing) على الموقع من الأجهزة يعود إلى عدة أسباب من أهمها كثرة وجود هذه الأجهزة
على الشبكة، وسرعة انتشار الخبر حول اختراق ذلك الجهاز خاصة إذا كان
يضم مواقع معروفة. إن من أخطر هذا النوع من الجرائم هو قيام فئة محترفة
من هؤلاء المخترقين لأسابيع إرهابية أو أسباب أخرى باستهداف أجهزة
مركزة وطنية حساسة بها أبعاد إما أمنية أو عسكرية أو مالية، مما قد يحدث
خسائر مالية أو معنوية فادحة.

3. 3.1 تعطيل الأجهزة

كثر مؤخراً ارتكاب مثل هذه العمليات، حيث يقوم مرتكرها
بتعطيل أجهزة أو شبكات عن أداء عملها بدون أن تتم عملية اختراق فعلية
لتلك الأجهزة. تتم عملية التعطيل بإرسال عدد هائل من الرسائل بطرق
فنية معينة إلى الأجهزة أو الشبكات المراد تعطيلها الأمر الذي يعيقها عن
تآدية عملها.

من أشهر الأمثلة على هذا النوع من الجرائم تلك التي تقوم بتعطيل
الأجهزة المستضيفة للمواقع على الشبكة. إن الأسباب وراء استهداف هذا
النوع من الأجهزة تتمثل أسباب استهدافها في جرائم الاختراقات والتي
سبق ذكرها في "ثانيا".
3.3.2 انتقال الشخصية

هي جريمة الإرهاب الجديدة كما سماها بعض المختصين في أمن المعلومات، وذلك نظرًا لسرعة انتشار ارتكابها خاصة في الأوساط التجارية. تتمثل هذه الجريمة في استخدام هوية شخصية أخرى بطريقة غير شرعية، وتهدف إما لغرض الاستفادة من مكانة تلك الهوية (أي هوية الضحية) أو لإخفاء هوية شخصية المجرم لتسهيل ارتكابه جرائم أخرى. إن ارتكاب هذه الجريمة على شبكة الإنترنت أمر سهل وهذه من أكبر سلبيات الإنترنت الأمنية. وللتغلب على هذه المشكلة، فقد بدأت كثير من المعاملات الحساسة على شبكة الإنترنت كتجارية في الاعتماد على وسائل مثيرة لتوزيع الهوية النموذجي الرقمي والتي تجعل من الصعب ارتكاب هذه الجريمة.

3.3.5 المضايقة والملاحقة

تتم جرائم الملاحقة على شبكة الإنترنت غالباً باستخدام البريد الإلكتروني أو وسائل الحوارات الآنية المختلفة على الشبكة. تشمل الملاحقة رسائل تهديد وتخويف ومضايقة. تنفق جرائم الملاحقة على شبكة الإنترنت مع مثيلاتها خارج الشبكة في الأهداف والتي تتمثل في الرغبة في التحكم في الضحية. تميز جرائم المضايقة والملاحقة على الإنترنت بسهولة إمكانية المجرم في إخفاء هويته علاوة على تعدد وسهولة وسائل الاتصال عبر الشبكة، الأمر الذي ساعد في تفشي هذه الجريمة. من المهم الإشارة إلى أن كون طبيعة جريمة الملاحقة على شبكة الإنترنت لا تتطلب اتصالاً ماديًا بين المجرم والضحية لا يعني بأي حال من الأحوال قلة
خطرته، فقدرة المجرم على إخفاء هويته تساعده على التمادي في جريمه، والتي قد تضفي به إلى تصرفات عنف مادية علاوة على الآثار السلبية النفسية على الضحية.

3.3 التغيير والاستدراج
غالب ضحايا هذا النوع من الجرائم هم صغار السن من مستخدمي الشبكة. حيث يوهم المجرمون ضحاياهم برغبتهما في تكوين علاقة صداقة على الإنترنت والتي قد تتطور إلى التقاء مادي بين الطرفين. إن مجرمي التغيير والاستدراج على شبكة الإنترنت يمكن لهم أن يتجاوزوا الحدود السياسية فقد يكون المجرم في بلد والضحية في بلد آخر. وكون معظم الضحايا هم من صغار السن، فإن كثيرًا من الحوادث لا يتم الإبلاغ عنها، حيث لا يدرك كثيرًا من الضحايا أنهم قد تعرّف بهم.

3.7 التشيهير وتشويه السمعة
يقوم المجرم بنشر معلومات قد تكون سرية أو مضللة أو مغلوطة عن ضحيته، والذي قد يكون فردًا أو مجتمعاً أوديناً أو مؤسسة تجارية أو سياسية. تتعدد الوسائل المستخدمة في هذا النوع من الجرائم، لكن في مقدمة قائمة هذه الوسائل إنشاء موقع على الشبكة يحوي المعلومات المطلوبة نشرها أو إرسال هذه المعلومات عبر القوائم البريدية إلى أعداد كبيرة من المستخدمين.

3.8 صناعة ونشر الإباحية
لقد وفرت شبكة الإنترنت أكثر الوسائل فعالية وحاجية لصناعة ونشر
الإباحية. إن الإنترنت جعلت الإباحية بشتي ومصادر عرضها من صور وفيديوهات وحوارات في متناول الجميع، ولعل هذا يعد أكبر الجوانب السلبية للإنترنت خاصة في مجتمع محارس على دينه وتعاليه كمجتمعنا العربي.

إن صناعة ونشر الإباحية تعد جريمة في كثير من دول العالم خاصة تلك التي تستهدف أو تستخدم الأطفال. لقد تمت إدانة مجرمين في أكثر من مائتي جريمة في الولايات المتحدة الأمريكية خلال فترة أربع سنوات والتي انتهت في ديسمبر 1998 م، تتعلق هذه الجرائم بتعريض الأطفال في أعمال إباحية أو نشر مواقع تعرض مشاهد إباحية لأطفال.

3.2. النصب والاحتيال

أصبحت الإنترنت مجالاً رهباً لم له سلع أو خدمات تجارية يريد أن يقدمها، ووسائل غير مسبوقة كاستخدام البريد الإلكتروني أو عرضها على موقع على الشبكة أو عن طريق سحبات الحوار. ومن الطبيعي أن يُساء استخدام هذه الوسائل في عمليات نصب واحتيال. ولعل القارئ الكريم الذي يستخدم البريد الإلكتروني بشكل مستمر تحصله رسائل بريدية من هذا النوع. إن كثيراً من صور النصب والاستناد التي يتعرض لها الناس في حياتهم اليومية لها مثيل على شبكة الإنترنت مثل بيع سلع أو خدمات وهمية، أو المساهمة في مشاريع استثمارية وهمية أو سريحة معلومات البطاقات الائتمانية واستخدامها. وتتغصّد المزادات العامة على البضائع عمليات النصب والاحتيال على الإنترنت. إن ما يميز عمليات النصب والاحتيال على الإنترنت عن مثيلاتها في الحياة اليومية هي سرعتها قدرة مرتقبها على الاختفاء والتلاشي.
3. أمن المعلومات الوطني

لم تعد شبكة الإنترنت بشكل خاص ونظم المعلومات الحديثة بشكل عام في قائمة الكماليات، لقد أصبحت تلك النظم أدوات ضرورية في جميع الدول المتقدمة في إدارة شؤون الحياة المختلفة كالعسكرية والأمنية والتجارية والمالية والتعليمية والصحية. في نفس الوقت انتشرت أدوات التدبير المعلوماتي انتشاراً كبيراً وسهل استخدامها حتى أصبحت في متناول الكثير. إن آثار المخاطر الأمنية التي قد تتعرض لها أنظمة المعلومات ليست محصورة على أفراد أو مؤسسات صغيرة كانت أو كبيرة بل قد تؤثر على البلد بشكل عام. إن الاعتماد على نظم المعلومات في جميع قطاعات الدولة الحساسة كالعسكرية والعسكرية والمالية أصبح أمرًا ملمحاً. إن أمن المعلومات أصبح جزءاً حيوياً وأساسياً من الأمن الوطني.

لذلك كله فإن من المهم تظافر جهود عدد من الجهات الأمنية والفنية والقضائية لأي دولة في حماية أمن معلوماتها الوطني، أو أن يتم ذلك عن طريق إنشاء مركز متخصص بجميع شؤون أمن الإنترنت التنظيمية والفنية، على أن يكون المركز المقترح مرتبطاً إدارياً بجهة لها سلطة أمنية تنفيذية تخوله القيام بهمهما مثل التحري والتحقيق في الجرائم الأمنية وإلزام الجهات المختلفة بتطبيق الأنظمة الكفيلة بالحد من المخاطر الأمنية وتطبيق عقوبات في حق من يخالف تلك الأنظمة وذلك بالتنسيق مع الأجهزة القضائية. إن المهارات الرئيسية المقترحة لذلك المركز يمكن تلخيصها فيما يلي:

1. وضع قواعد شاملة للسياسات الأمنية التي يلزم جميع الجهات الحساسة سواء حكوميةً أو خاصة تطبيقها على أنظمتها المعلوماتية.
2. إيجاد آلية لتابعة تلك الجهات الحساسة في تطبيقها للقواعد المقررة ومخالفتها غير الملتزمين.

١٤٧
3- وضع أنظمة تحدد جزاءات رادعة للجرائم المختلفة على شبكة الإنترنت، وإيجاد آلية لتطبيق هذه الأنظمة.

4- تشكيل فريق فني أمني على مستوى عالي من التأهيل يضم متخصصين في مختلف الأنظمة الحاسوبية المستخدمة ومختصين في مجال التحري والتحقيق، يقوم هذا الفريق بالبحث والتحري في أي اختراق أمني على نظم المعلومات الحساسة. كما يقوم هذا الفريق في التحري والتحقيق في جرائم الإنترنت المختلفة.

5- وضع مقاييس فنية لأدوات ووسائل الحماية التي يجب على جميع الجهات الحساسة تطبيقها في مراكزها المعلوماتية، وإيجاد آلية لتابعة ذلك ومخالفتها غير الملتزمين.

6- وضع مقاييس مهنية تضمن مستوى عالياً من التأهيل للطاقم الفني القائم على إدارة مراكز المعلومات في الجهات الحساسة المختلفة، وإيجاد آلية لتابعة ذلك ومخالفتها غير الملتزمين.

7- تشكيل جهاز في متكامل يضم فنيين متخصصين في جميع الأنظمة الحاسوبية المعروفة يقومون بحجز ممثولة للمشاكل والثغرات الأمنية التي قد تتعرض لها تلك الأنظمة وتوعية المستخدمين بتلك المشاكل والوسائل الكفيلة بحلها. كما يقوم هذا الجهاز الفني على دراسة الأدوات الأمنية المتاحة للتعرف على قدراتها وكفاءتها.

8- إنشاء مركز حاسب آلي مركزي يقوم بحفظ نسخ احتياطية من جميع المعلومات التي لها أهمية أمنية.
خاتمة

لم تكن هناك أهمية كبيرة لأمن الحاسبات والشبكات في بداية العصر الحاسوبي حيث كانت أجهزة الحاسب الآلي مرتفعة الثمن كما كانت مقتصرة على المؤسسات الكبيرة. لقد كانت الإجراءات الأمنية مقتصرة على توفير مبنى مناسب يحمي أجهزة الحاسبات من الحرائق وتوفير نظام أمني يمنع غير المصرح لهم من الدخول إلى المبنى والعبث بالأجهزة.

إن هذه الصورة قد تغيرت كثيرًا مع تطور تقنيات الاتصالات، حيث أصبح بالإمكان توفير شبكات اتصال تربط أجهزة الحاسبات بعضها البعض وتمكن المستخدمين من الوصول إلى تلك الأجهزة عن بعد. إن شبكات الحاسب الآلي لها دور إيجابي في تفعيل استخدامات الحاسب في مجالات عدة ولكن بالمقابل فإن هذه شبكات جعلت الوصول إلى تلك الأجهزة سهلاً إذ لم يعد من الضروري تواجد المستخدم في نفس مكان الأجهزة الأمر الذي وسع نطاق أهمية أمن الحاسبات.

إن ازدهار صناعة تقنية المعلومات وانتشارها في السنوات القليلة الماضية كان سبب في ازدهار وانتشار صناعة أدوات التخريب المعلوماتي. فعن طريق مواقع كثيرة على شبكة الإنترنت، يمكن للشخص قليل الخبرة الحصول على عدة أدوات تخريبية يمكن استخدامها لشن هجوم على أجهزة حاسوبية مرتبطة بالشبكة وإحداث أشكال مختلفة من التخريب.

إن المخاطر المتعلقة بأمن المعلومات تستلزم جهود متضافرة من عدد من الجهات الأمنية والفنية التقنية والقضائية للحد منها بشتى الوسائل الفنية والقضائية.