العنوان:	الحماية الأمنية من الأخطار المحتملة على شبكات الحاسب الآلي
المصدر:	المجلة العربية للدراسات الأمنية
الناشر:	جامعة نايف العربية للعلوم الأمنية
المؤلف الرئيسي:	أحمد، السماني عبدالمطلب
مؤلفين آخرين:	عمار، زكريا أحمد(م. مشارك)
المجلد/العدد:	مج 28, ع 56
محكمة:	نعم
التاريخ الميلادي:	2012
الشهر:	نوفمبر - محرم
الصفحات:	243 - 271
رقم MD:	391890
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	EcoLink
مواضيع:	الحاسبات الالكترونية، الأمن الالكتروني، الانترنت، برامج الحماية، المخاطر الأمنية
رابط:	http://search.mandumah.com/Record/391890

الحماية الأمنية من الأخطار المحتملة على شبكات الحاسب الآلي (دراسة مسحية تحليلية في مدينة الرياض)

أ.د. السماني عبد المطلب أحمد(*)

م. زكريا أحمد عمار(**)

الملخص

هدفت هذه الدراسة إلى تحقيق أفضل حماية ممكنة لشبكات الحاسب الآلي بظروف وصول مرنة، عن طريق حصر المخاطر التي تؤثر سلباً على أمن شبكات المعلومات، وحصر التدابير الاحتياطية المطبقة لتجنب تلك المخاطر، وذلك بتطبيق الاستبانة كأداة لجمع البيانات على عينة الدراسة التي تتكون من مهندسين وفنيين ومدراء يعملون في إدارات تقنية المعلومات في المؤسسات التعليمية في الرياض، حيث بلغ عدد الاستبانات القابلة للتحليل ١٠٥ استبانة، وتوصلت الدراسة إلى وجود فروق ذات دلالة إحصائية بين المخاطر وبين التدابير المتخذة لتجنب تلك المخاطر، وذلك لصالح المخاطر وفي ذلك دلالة على عدم اكتمال تنفيذ التدابير الوقائية من قبل الكادر الفني في مؤسسات عينة الدراسة، وبناء على النتائج المستخلصة من التحليل أوصى الباحثان بضرورة زيادة الاهتمام بالكادر البشري العامل في حماية الشبكات المحلية، من حيث الكفاءة وكفاية العدد والتدريب والتحفيز لتمكين ذلك الكادر من القيام بتدابير الحماية الفيزيائية، وإعداد وتشغيل وتحديث أجهزة وبرامج الحماية، وكذلك تنفيذ الاختبارات الدورية لكشف الثغرات الأمنية، بالإضافة لضرورة توفير السياسات الأمنية والإجراءات اللازمة لتنفيذ أعمال الحماية.

(*) عميد كلية الحاسوب بجامعة التيلين، الخرطوم، السودان.

(**) مركز المعلومات، جامعة نايف العربية للعلوم الأمنية، الرياض.

المدخل إلى الدراسة

في عصرنا هذا اعتمدت المؤسسات في تسيير أعمالها على تقنية المعلومات وشكلت شبكات الاتصال وسطاً تنساب فيه البيانات وتسكن فيه خزائن المعلومات وبذلك تحتاج هذه الشبكات إلى حماية تصون سلامة محتوياتها وتضمن استمرارية عملها، ونظراً لكثرة الأخطار التي تهدد سلامة البيانات التي تنساب في الشبكات أو البيانات المحتضنة في خزائنها وتعدد الأخطار التي تهدد استقرار تلك الشبكات وأمنها كالإصابة بالفيروسات والبرامج الضارة ومحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل والعبث، تأتي أهمية الحماية على مدار الساعة لمكونات شبكات المعلومات المادية والبرمجية بتثبيت أجهزة وبرامج الحماية في بوابات الشبكات المحلية وداخل تلك الشبكات، وإدارة تلك الأجهزة والبرمجيات من الزاوية الأمنية وسد الثغرات أولا بأول لتضييق فرص قراصنة المعلومات والمنافسين والأعداء من التمكن من اختراق أو سرقة أي بيانات من شبكات المعلومات. ومن هنا أتت فكرة هذه الدراسة.

مشكلة الدراسة

إن المشكلات الأمنية التي أوجدتها شبكات الحاسب وبخاصة شبكة الانترنت والتي تتلخص بتعطيل وتدمير المواقع الحكومية والتجارية، والتسلل إلى الشبكات وسرقة أسرار الشركات والحكومات والمؤسسات الأمنية والدفاعية، وترويج برامج التخريب والتجسس والقرصنة، وسرقة المواقع وانتهاك حقوق الملكية الفكرية، بالإضافة إلى أن شبكة الانترنت صارت وسيلة اتصال فعالة للعصابات والمجرمين والمخالفين للقانون والأعراف الاجتماعية والأخلاقية السائدة، وتوفر بيئة خصبة لترويج التجارة المحرمة وغسل الأموال والجرائم المنظمة، وتشكل ميداناً حديثاً من ميادين الحرب الإلكترونية. كما أنها تؤمن تربة مناسبة لنمو شبكات التجسس العالمية التي تمارس نشاطات جمع المعلومات وانتهاك الخصوصية على مدار الساعة. (الشهري، 2001: 186، 184).

وفي هذه الدراسة يتناول الباحثان المخاطر التي تتعرض لها شبكات الحاسب الآلي ومخازن المعلومات المتصلة بها وتتعرض أيضاً للتدابير الاحتياطية التي تلزم لتجنب تلك المخاطر. وبناء على ما تقدم فإن مشكلة الدراسة تتمحور حول تحديد المخاطر التي يمكن أن تضر بشبكات الحاسب الآلي وتحديد التدابير الاحتياطية التي يتم من خلالها تفادي المخاطر التي يمكن أن تؤذي موارد شبكات الحاسب الآلي

وتؤثر سلبا على إجراءات حمايتها ومصادر المعلومات الموجودة فيها أو المنقولة من خلالها، وذلك من خلال الإجابة على التساؤل الرئيس التالي: ما المخاطر المحتملة على شبكات الحاسب الآلي وما تدابير الوقاية منها، ويتفرع منه سؤالان هما:

1- ما المخاطر التي يمكن أن تؤثر سلباً على أمنية شبكات الحاسب الآلي؟

2- ما التدابير الاحتياطية اللازمة لتجنب المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات؟

أهمية الدراسة

تؤمن هذه الدراسة مصدراً مهما للعاملين بمجال التحقيق في الجرائم المستحدثة حيث يستفاد منها بالتعرف على عناصر بناء نظم حماية الشبكات وتفاصيل تثبيتها ومخرجات أجهزتها من تسجيلات لحركة البيانات اليومية التي تساعد في جمع الأدلة الجنائية في حالات التحقيق والتحري في مجال الجرائم الالكترونية. (البشري، ٢٠٠٤: ٢٣). وتقدم للعاملين في الأجهزة الأمنية مرجعاً أمنياً مهماً للوقاية من الجرائم الالكترونية. وتقدم هذه الدراسة أيضاً معلومات مفيدة جداً للراغبين في تصميم الشبكات ومراكز المعلومات أخذين بالاعتبار الاحتياطات الأمنية اللازمة لحماية شبكاتهم مختصرين الجهد والمال والوقت.

أهداف الدراسة

تهدف هذه الدراسة إلى حصر المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات المعلومات، وحصر التدابير الاحتياطية اللازمة لتجنب تلك المخاطر، وتقديم حلول لحماية شبكات الحاسب الآلي من الأخطار المحتملة.

مصطلحات الدراسة

تستخدم الدراسة مفاهيم ومصطلحات علمية فيما يلي تحديد موجز لها:

1- المخاطر: مصطلح المخاطر "Risks " في أمن المعلومات يعني الثغرات التي توجد في أصول تقنية المعلومات كالحاسبات والخوادم وقواعد البيانات، والتي يمكن أن تستغل في تهديد أمن تلك الأصول بالاختراق أو إيقاف الخدمات. ومنها على سبيل المثال استخدام البرمجيات الخبيثة عن طريق إدخالها كمرفق البريد الإلكتروني. (http://en.wikipedia.org)

2- الحاسب الآلي: هو الجهاز الذي يقبل أو يعالج أو يخزن أو يسترجع البيانات من خلال برامج الحاسب الآلي. (شمدين، ٢٠٠٣: 121) وله تسميات أخرى كالحاسب المكتبي (Desktop) ومحطة العمل (Workstation) والحاسب المحمول (Laptop) ويمكن عد الحاسب الكفي حاسبا آليا.

3- الشبكة: لغة هي شركة الصياد وجمعها شبك وشباك. وشبكة الأمور واشتبكت وتشابكت: اختلطت والتبست، وطريق شابك: متداخل ملتبس، وأسد شابك: متشابك الأنياب. (آبادي، 1987: 1219) والشبكة اصطلاحاً: هي مجموعة من الحاسبات تعطى عناوين شبكية عمومية، ويمكن ربط هذه الحاسبات في مجموعات حسب توضعها في المناطق الجغرافية (Brenton, Hunt, 2003: 42). فالشبكة المحلية (LAN) تنتشر على مساحة جغرافية محدودة. والشبكة الواسعة تنتشر على مساحة جغرافية واسعة.

4- الحماية: الحماية لغة: حمى الشيء يحميه حمياً وحماية، منعه، وحمى المريض ما يضرره: منعه إياه، فالحماية لغة المنع (آبادي، 1987: 1647). والحماية الأمنية لشبكة الحاسب الآلي: هي العمليات التي يتم فيها حماية الأصول المعلوماتية الرقمية بغرض حماية الخصوصية وصيانة التكامل وضمان الاستمرارية.

الإطار النظري للدراسة

تحاول هذه الدراسة التعرف على المخاطر التي يمكن أن تتعرض لها شبكات الحاسب الآلي والتي تؤثر بشكل سلبي على وسائل حماية الشبكات المستخدمة في المؤسسات التي تستخدم تقنية المعلومات، ثم تحليلها وبناء على النتائج المستخلصة من التحليل يضع الباحثان توصيات تفيد تلك المؤسسات في تحسين جودة الحماية لشبكاتها وتفادي الوقوع في الانقطاعات التي تسبب خسائر مادية ومعنوية كبيرة. وفيما يلي بعض المفاهيم الضرورية التي تتمحور حولها الدراسة.

أولاً: أهداف الحماية الأمنية لشبكات الحاسب الآلي

إن الازدياد في اعتماد المؤسسات التجارية والمنشآت الوطنية والمنظمات الأولية على تطبيقات شبكات الحاسب والإنترنت، زاد من أهمية بقاء أنظمة المعلومات قيد التشغيل بصورة مستمرة حيث إن

توقفها يؤدي إلى خسائر كبيرة معنوية ومادية، ومهما اختلفت أسباب التوقف عن العمل فهي في النهاية نتيجة لضعف الحماية. ويوجد ثلاثة أهداف رئيسة لحماية الشبكات هي الخصوصية، والتكاملية، والاستمرارية (Cisco SPstems, 2001: 32)..

1- الخصوصية (Confidentiality): وتهتم بحماية البيانات من الكشف غير المرخص وكذلك بحماية خصوصية وسرية البيانات في المنشأة وبخاصة عندما تكون تلك البيانات خاصة بمستفيدين من خارج المنشأة، وعلى جميع العاملين بالمنظمة واجب الحفاظ على سرية بيانات منظمتهم ويعد هذا الواجب من المتطلبات القانونية.

2- السلامة (Integrity): تشير إلى ضمان كمال وسلامة البيانات بالمحافظة عليها من التعديل أو التخريب أو التدمير والتلف بطريقة غير مرخصة، على سبيل المثال: تكون السلامة مؤمنة عندما تكون الرسالة المستلمة مطابقة للرسالة المرسلة، ولا بد من إجراء القياسات اللازمة للتأكد من سلامة كل البيانات بغض النظر عن خصوصيتها أو درجة سريتها.

3- التوفر (Availability): "تعرف على أنها التشغيل المتواصل لأنظمة الحاسب الآلي، تحتاج التطبيقات مستويات مختلفة للتوفر، تبعاً لتأثر العمل (Business) سلباً بفترة التوقف، وحتى يستمر تطبيق ما بالتوفر فيجب أن تكون جميع مكونات النظام متوفرة أيضاً بحيث تتضمن التطبيق وقاعدة البيانات والخادم وأجهزة التخزين وسلامة الشبكة من البداية إلى النهاية".(Cisco Systems, 2001: 32). وعادة يمثل التوفر بكسر عشري مثل 0,9998.

ثانياً: العناصر الرئيسة لحماية الشبكة أمنياً

الاستخدام الناجح لتقنيات الشبكات يتطلب حماية البيانات ومصادر الشبكات من التلف ومن الانتهاك والاختراق، وتتضمن حلول حماية الشبكات خمسة حلول هي التعريف بالهوية، وحماية الحدود، وسرية البيانات، وإدارة الحماية، وإدارة السياسات. (Cisco SPstems, 2001: 32).

1- التعريف بالهوية (Identity): يشير مفهوم التعريف بالهوية إلى التعريف الإيجابي الدقيق لمستخدمي الشبكة ومضيفاتها وتطبيقاتها وخدماتها ومصادرها.

2- حماية حدود الشبكة (Security Perimeter): تقدم حماية الحدود الوسائل اللازمة لضبط الوصول إلى التطبيقات الحرجة في الشبكة والبيانات والخدمات بالسماح فقط للمستفيدين الشرعيين بتمرير المعلومات عبر مكونات الشبكة، فيتم إعداد الموجهات والموزعات للقيام بتصفية الحزم (Packet Filtering) وتثبيت جدران الحماية المتخصصة متعددة الوظائف، بالإضافة لبرامج الحماية من البرامج الضارة والفيروسات والبريد الدعائي، وتثبيت برامج إدارة الشبكة ومراقبتها.

3- خصوصية البيانات: عندما تفرض ضرورة العمل حماية البيانات من التسريب يصبح التحقق من هوية المستخدم قضية أساسية ويتوجب على مسؤولي أمن الشبكات أن يفعلوا خصائص التحقق من الهوية المتوفرة في أجهزة الاتصال الشبكية. واستخدم تقنيات التشفير الرقمية.

4- إدارة الحماية الأمنية: (Security Management) من المهم جداً تفقد حالة تدابير الحماية بالمراقبة الدورية للتأكد من بقاء الشبكة محمية بشكل فعال، حيث تستطيع ماسحات مواطن الضعف تحديد النقاط الواجب مراعاة تدابير الوقاية فيها، وتستطيع أنظمة كشف ومنع التلصص القيام بالمراقبة وتنفيذ ردود الأفعال المناسبة للحوادث المخالفة للقواعد المحددة في ملف الإعداد. وبذلك يمكن أن تحصل المنظمة على مشهد له معنى مفيد لكل من سيل البيانات وحالة حماية الشبكة.

ثالثاً: المخاطر التي تتعرض لها شبكات الحاسب الآلي

تتعدد الأخطار التي يمكن أن تتعرض لها شبكات الحاسب الآلي فمنها ما يهدد البيانات خلال مرورها بالشبكات سواء في الكابلات أو الأثير أو أثناء نقل النسخ الاحتياطية ومنها ما يهدد فقدان البيانات أو تخريبها في أجهزة الخادم. (داود، 305: 2000). وتكون نتائج التهديدات مختلفة كفقد البيانات المرسلة، ووصول البيانات إلى جهة أخرى، وحدوث خطأ أو تحريف في البيانات خلال انتقالها ويمكن تصنيف تلك المخاطر تبعاً لمصدرها إلى ما يلي:

1- مخاطر خارجية:

أ- التعدي على الكابلات وتخريبها.

ب- اندلاع الحريق.

ت- حصول إغراق بالمياه بسبب الفيضانات.

ث- اختراق لتعديل البيانات وتغيرها أو إتلافها.

ج- التعرض لهجوم إرهابي.

2- مخاطر داخلية:

أ- اختراق أجهزة الخادم من داخل المؤسسة (عبث، إساءة استخدام...).

ب- استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة.

ت- زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة.

ث- الإصابة بفيروسات مصدرها الانترنت.

ج- الإصابة بفيروسات مصدرها وسائط التخزين و ذواكر (الفلاش).

ح- تنزيل برامج غير مصرح بها.

خ- سرقة الأجهزة ووسائط التخزين.

د- الدخول غير المصرح إلى مركز البيانات وتعطيل عمل أجهزته.

ذ- تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع.

رابعاً: التدابير الوقائية (الاحتياطية) اللازمة لتجنب مخاطر الشبكات:

من أهم التدابير الاحتياطية التي ينبغي توفيرها لتجنب المخاطر التي يمكن أن تتعرض لها شبكات المعلومات ما يلي:

1- توفير حراسة عند بوابات مركز البيانات على مدار الساعة.

2- تجهيز مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار.

3- قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.

4- تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول.

5- توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل.

6- تشغيل نظام للنسخ الاحتياطي والاسترجاع الآلي يومياً.

7- وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.

8- تطبيق التشفير على وسائط النسخ الاحتياطي.

9- إبعاد وسائط النسخ الاحتياطي ووسائط التخزين عن أماكن تسرب المياه.

10- إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.

11- تركيب برامج مخصصة لمراقبة استخدام الشبكة.

12- توفير خطة طوارئ واضحة ومعتمدة واختبارها كل ثلاثة أشهر.

13- إعداد خطة للتراجع (Rollback) تطبق عند فشل خطة الطوارئ.

14- توعية جميع الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.

15- اعتماد ميزانية خاصة بخطة الطوارئ.

16- مطابقة إجراءات العمل لتتوافق مع معايير دولية (أيزو) تتعلق بالحماية.

17- عقد اتفاقيات تعاون مع المتخصصين في الحماية.

18- تنفيذ اختبار دوري لنقاط الضعف انطلاقا من داخل وخارج الشبكة.

19- تفعيل خصائص التشفير لقواعد البيانات.

20- استخدام التشفير على اتصالات الشبكة الافتراضية (VPN).

21- استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة.

22- توفير مركز بيانات (Data center) بديل لاستخدامه عند الطوارئ.

23- تجهيز الوسيط (Proxy) بخدمة توليد التقارير وتحليلها.

24- توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية.

25- توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها، وأخر يقوم بإدارة برامج الحماية وتحديثها.

26- تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.

27- توظيف الأفراد المناسبين من حيث المؤهل والخبرة في أعمال الحماية.

28- توفير برنامج إدارة الحماية من جميع جوانبها.

29- تأمين أجهزة احتياطية لجدار الحماية والموجه والوسيط وأجهزة الخادم.

30- توفير إدارة خاصة بأمن المعلومات، وربطها مباشرة برئيس أو مدير المؤسسة.

31- اشتراط توفر المهارات المناسبة مستخدمي الحاسب الآلي.

32- عقد دورات تدريب للتوعية في أمن المعلومات والحماية.

33- توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة المختصة.

34- توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي.

35- تحديث نظام تشغيل أجهزة الشبكة بشكل دوري.

36- إتاحة استخدام خاصية التحقق من الصحة في جدران الحماية.

37- توفير سياسة خاصة بكلمات المرور وتطبيقها.

38- توفير نظام لمراقبة حركة البيانات والتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة.

39- زيادة الاعتماد على أنظمة التشغيل الأقل تأثرا بالفيروسات، وتقليل الاعتماد على أنظمة التشغيل الأكثر تأثرا بالفيروسات.

الدراسات السابقة

أولاً: الدراسات العربية:

1- أجرى سليمان مهجع العنزي دراسة حول جرائم نظم المعلومات وتوصلت الدراسة إلى أن حجم استخدام منفذ شبكة الانترنت وبرامج الاختراق الموجودة بها (4,25%) من مؤسسات عينة الدراسة. وتوصلت الدراسة أيضاً إلى أن برامج الحماية تعد وسيلة ضبط وتحقيق مهمة بشكل دائم، وتساعد بما نسبته (94,2%) في تحديد نوع الجريمة، وما نسبته (95,1%) في تحديد توقيت ارتكاب الجريمة. وكشفت الدراسة عن أنه بالإمكان الاعتماد على عنوان (IP) بما نسبته (94,2%) وعلى برامج الحماية (91,4%) ووسائل تتبع المخترقين (74,9%). و تبرز دراسة (العنزي) أهمية وسائل الحماية في ضبط الجريمة الإلكترونية وذلك يتوافق مع هذه الدراسة في موضوع حماية الشبكات من المخاطر حيث أكدت على ضرورة تركيب برامج

وأجهزة الحماية وإعدادها الإعداد المناسب والقيام بالتحديث المستمر لتقوم بصد جميع الهجمات وتسجيلها من خلال تفعيل خصائص تسجيل الأحداث وتسجيلها (Logs). (العنزي، ٢٠٠٣).

2- أجرى عبد الله بن محمد ناصر السحيباني دراسة بعنوان "كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات"، وقد تناول تصميم برامج شبكة الاتصال والبرامج التطبيقية في المصارف. وأوصى (السحيباني) بضرورة قيام المصارف التجارية بزيادة التركيز على استخدام الرقم السري لدخول المباني وغرف الحاسب الآلي، وإشعار العاملين بوجود مراقبة مستمرة عليهم، وصيانة أجهزة الحاسب الآلي داخل المصرف، وإجراء تجارب لاختبار طرق الاستجابة عند حدوث طارئ أو كارثة، وضرورة إصدار سياسات لأمن المعلومات، وضرورة توظيف متخصصين في أمن المعلومات. وتضيف هذه الدراسة على دراسة السحيباني تفصيل الإعدادات التشغيلية لأجهزة الحماية وتتفق معها في جميع ما ورد فيها مع اختلاف عينة الدراسة. (السحيباني، ١٩٩٦).

ثانياً: الدراسات الأجنبية:

1- أجرى شيخ فاروق عمارة دراسة بعنوان "The Control of Firewalls Using Active Networks" حول ضبط جدران الحماية باستخدام الشبكات النشطة تتمحور حول مشكلة تغيير إعدادات جدران الحماية المبنية على تصفية حزم البيانات بوضع برامج صغيرة مسبقة التعريف داخل تلك الأجهزة التي تمكن من تعديل أو إعادة توجيه حزم البيانات بفتح أو إغلاق المنافذ تبعاً لمحتوى الحزم باستخدام تقنيات الشبكة النشطة (Active network). ومن توصياته التوجه نحو نموذج عام لبرمجة الشبكة يتمتع بخصائص ذكية أهمها: خاصية التنقل، وخاصية الحماية، وخاصية الفعالية. وتختلف هذه الدراسة عن دراسة (عمارة) بتناولها الأخطار المحتملة على الشبكات وتدابير تجنبها وضمنت جدران الحماية كواحد من أهم تدابير الوقاية. (Emarah, 2007).

2- أجرى نوربك باشا إدريس وبحراني دهران شانموجان، دراسة بعنوان "Intelligent Intrusion

Detection" حول نظام هجين للكشف الذكي عن التجسس على شبكات الحاسب، وقد طرح الباحثان مشكلة عدم كفاية نظام كشف التجسس[1] (IDS) لمنع التجسس على شبكات الحاسب الآلي كونها محدودة الإمكانات وتتركز قدرتها على المراقبة وتحتاج للتحديث اليومي لظهور برمجات تجسس يومياً، ومن أهم توصيات دراستها: ضرورة استخدام النظام الهجين واستخدام جهاز عالي الأداء من حيث المعالجة. وتتوافق دراسة إدريس مع ما ذكره الباحثان في دراستهما هذه في أهمية جدران الحماية الذكية المعروفة بالاختصار (UTM)[2] وضرورة استخدامها على بوابات شبكات الحاسب الآلي، واختلفت دراسة إدريس عن هذه الدراسة في اقتصارها على جدران الحماية وعدم تطرقها إلى نواحي الحرية الأخرى التي غطتها هذه الدراسة من منظور الحماية من المخاطر المحتملة. (idris and Shanmugam: 2007).

الإطار المنهجي للدراسة

أولاً: منهج الدراسة

اعتمد الباحثان في دراستهما هذه على المنهج الوصفي الذي يناسب دراسة الظاهرة كما توجد في الواقع حيث وضع الباحثان تساؤلا رئيسا تفرع منه محوران وكل محور منهما يحاكي مخاطر الحماية في المؤسسات التعليمية وتدابير الوقاية من تلك المخاطر. ويتميز المنهج الوصفي بوصف الظاهرة وصفاً دقيقاً ويعبر عنها تعبيراً كمياً أو كيفياً بالإضافة إلى تصنيف المعلومات بطريقة تساهم في ربط العلاقات بين المتغيرات المراد قياسها من خلال الدراسة.

(1) IDS :Intrusion Detection System.

(2) UTM :Unified Threat Management.

ثانياً: حدود الدراسة

أطرت الدراسة بالحدود التالية:

1- الحدود الموضوعية: تقتصر الدراسة على موضوع الحماية الأمنية من الأخطار المحتملة على شبكات الحاسب الآلي وتدابير الوقاية منها.

2- الحدود البشرية: تقتصر الدراسة على العاملين في شبكات الحاسب الآلي وحمايتها من فنيين وإداريين.

3- الحدود الزمنية: هي الأشهر الستة الأخيرة من عام 2009م فترة تطبيق الدراسة المسحية.

4- الحدود المكانية: اقتصرت الدراسة على عينة عشوائية من المؤسسات التعليمية في مدينة الرياض بالمملكة العربية السعودية.

ثالثاً: مجتمع وعينة الدراسة

استفاد الباحثان من المنهج الوصفي بإجراء المسح الميداني لمجتمع الدراسة الذي تكون من مجموعة من المؤسسات التعليمية الخاصة والحكومية والمشتركة في مدينة الرياض عام 2009م وقد بلغ عدد المؤسسات التعليمية التي خضعت للدراسة (٧٥) مؤسسة تعليمية أخذت كعينة عشوائية من أصل (429) مؤسسة تعليمية. وقد تم اختيار المؤسسات التي تعتمد على تقنيات الحاسب الآلي في تسيير أعمالها الأكاديمية والمالية معتمدة على برامج وأدوات تقنية المعلومات، وقد تم الاكتفاء بهذه العينة نظراً لكبر مجتمع الدراسة، وصعوبة الوصول إلى جميع المؤسسات التعليمية.

رابعاً: أداة الدراسة

اختار الباحثان الاستبانة كأداة لقياس متغيرات الدراسة وذلك لمناسبتها لطبيعة الدراسة والمنهج الوصفي المستخدم فيها، بغرض تحقيق أهداف الدراسة والإجابة على تساؤلاتها، وقد صيغت الاستبانة بصورة تتناسب مع تساؤلات الدراسة وتضمنت البيانات الشخصية والوظيفية لأفراد عينة الدراسة. كما تضمنت أسئلة شملت عدداً من العبارات حول المخاطر التي يمكن أن تؤثر سلباً على أمنية شبكات الحاسب الآلي وكذلك التدابير الاحتياطية اللازمة لتجنب تلك المخاطر، وبيان درجة أولوية تلك التدابير. وتم حساب معامل ثبات أداة الدراسة للعينة (105) بمقياس كرونباخ ألفا، وذلك باستخدام برنامج

(SPSS) لمعالجة البيانات في الحاسب الآلي. وقد أسفرت النتائج أن معامل ثبات عبارات المحور الأول: المخاطر الخارجية= 0,8260، المخاطر الداخلية= 0,8349 وللمحور الثاني: تدابير الحماية من المخاطر الداخلية والخارجية= 0,9558 وبالرجوع إلى قيم معاملات الارتباط وجد الباحثان أنها دالة إحصائياً عند مستوى 0,1، وهي قيم مرتفعة تدل على قوة الارتباط بين العبارات ومواضيع الأسئلة العائدة لها.

خامساً: أساليب المعالجة الإحصائية

بعد حساب معامل ارتباط بيرسون لقياس الصدق البنائي وكذلك تحديد معامل ثبات الدراسة باستخدام معامل كرونباخ ألفا، تم استخدام المقاييس الإحصائية التالية:

1- التوزيعات التكرارية والنسب المئوية لوصف البيانات.

2- المتوسط الحسابي الموزون.

3- الانحراف المعياري لتحديد مقدار التشتت في إجابات المبحوثين لكل عبارة عن المتوسط والذي يوضح مدى تشتت إجابات المبحوثين كما يفيد في ترتيب المتوسطات عند تساوي بعضها.

4- معامل ارتباط بيرسون لتوضيح العلاقات بين متغيرات عناصر البحث.

5- اختبارات (ت) T- test للفرق بين متوسطين. واختبار LSD البعدي للتعرف على مصادر الفروق الدالة إحصائياً وذلك بين المتغيرات التابعة والمتغيرات المستقلة.

عرض نتائج الدراسة وتحليلها

أولاً: البيانات الديموغرافية لعينة الدراسة

اتصفت عينة الدراسة بعدد من السمات التي حددتها الخصائص الشخصية لأفرادها وتشمل: الجنس، الوظيفة، عدد سنوات الخبرة. وتكمن أهمية هذه المتغيرات في تأثيرها على استجابات أفراد عينة الدراسة، وذلك من خلال الجداول وعرض النتائج المتعلقة بها والتي تتمثل في إجابات أفراد عينة الدراسة على الجزء الخاص بالبيانات الشخصية من الاستبانة على النحو التالي:

1- توزيع عينة الدراسة وفقًا للجنس:

الجدول رقم (1)

توزيع عينة الدراسة وفقاً للجنس

الجنس	العدد	النسبة المئوية
ذكر	90	%85,71
أنثي	15	%14,29
المجموع	105	%100

يوضح الجدول رقم (1) توزيع عينة الدراسة وفقا لجنسهم حيث بلغت نسبة الذكور في عينة الدراسة 85,71% وبلغت نسبة الإناث 14,29% ويعود ذلك إلى أن غالبية المؤسسات التعليمية في الرياض تحوي أقساماً مخصصة للذكور وأخرى مخصصة للإناث وتستفيد جميع تلك الأقسام من شبكة حاسب آلي واحدة تكون فيها مهام الحماية الرئيسة ملقاة على أقسام الذكور.

2- توزيع أفراد عينة الدراسة وفقًا للوظيفة:

الجدول رقم (2)

توزيع أفراد عينة الدراسة وفقاً وظيفة

الوظيفة	العدد	النسبة المئوية
إدارية	10	%9,52
فنية	49	%46,67
إدارية وفنية	44	%41,90
لم يستجيب	2	%1,90
المجموع	105	%100

يتضح من الجدول رقم (2) أن المستجيبين الذين يعملون بوظائف فنية وصلت نسبتهم إلى 46,67%، وأن المستجيبين الذين يعملون بوظائف إدارية وفنية تصل نسبتهم إلى 41,90% وأن الذين يعملون بوظائف إدارية تصل نسبتهم إلى 9,52% ما يشير إلى أن الوظائف الفنية في حقل حماية شبكات الحاسب الآلي وأمن المعلومات هي الأكثر احتياجاً (46,67%) تليها الوظائف الإدارية المشغولة من قبل

أفراد لديهم مؤهلات فنية (41,90%) وهذا أمر طبيعي جدا حيث إن تقنيات حماية شبكات الحاسب الآلي تتضمن تخصصات فنية متعددة وبذلك تكون وظائف الفنيين أكبر من وظائف الإداريين.

3- توزيع أفراد عينة الدراسة وفقًا لسنوات الخبرة:

الجدول رقم (3)

توزيع أفراد عينة الدراسة وفقاً لسنوات الخبرة

سنوات الخبرة	العدد	النسبة المئوية
أقل من 5 سنوات	43	%40,95
من 5 سنوات إلى أقل من 10 سنوات	39	%37,14
من 10 سنوات فأكثر	23	%21,91
المجموع	105	%100

يتضح من الجدول (٣) أن نسبة فئة ذوي الخبرة من ١ إلى خمس سنوات قد بلغت 40,95% ونسبة فئة الذين لديهم خبرة من خمس سنوات إلى أقل من عشر سنوات بلغت 37,14%، ونسبة فئة الذين لديهم خبرة عشر سنوات فأكثر بلغت 21,92%. وإن هذه الاستجابات هي استجابات معقولة لأن سنوات الخبرة من ١- ٥ سنوات التي اتصفت بالنسبة الأكبر بين فئات الخبرة هي السنوات المتوافقة مع ظهور التقنيات الحديثة في مجال حماية شبكات الحاسب الآلي ودخولها إلى المؤسسات التعليمية في السنوات الخمس الأخيرة.

ثانياً: عرض وتحليل النتائج المتعلقة بأسئلة محاور الدراسة:

حيث أن تساؤل الدراسة الرئيس هو: ما المخاطر المحتملة على شبكات الحاسب الآلي وما تدابير الوقاية منها. فإن الحصول على النتائج المرجوة من استجابات هذا التساؤل اقتضى تقسيمه إلى محورين هما: المخاطر الخارجية والمخاطر الداخلية كمحور أول، وتدابير الحماية من المخاطر الداخلية والخارجية كمحور ثان.

المحور الأول: المخاطر الخارجية والمخاطر الداخلية

للإجابة على هذا التساؤل قام الباحثان من خلال تحليل أداة الدراسة بحساب التكرارات والنسب المئوية، ثم حساب المتوسطات الحسابية والانحرافات المعيارية ووضحا الترتيب لعبارات هذا المحور ويوضح الجدول رقم (٤) العبارات وترتيبها والمتوسطات الحسابية والانحراف المعياري.

الجدول رقم (4)

المخاطر الداخلية والخارجية

م	العبارة	المتوسط	الانحراف المعياري	الترتيب
1	التعدي على الكابلات وتخريبها.	4,61	0,67	3
2	اندلا ع الحريق.	4,63	0,73	2
3	حصول إغراق بالمياه بسبب الفيضانات.	4,47	0,80	5
4	اختراق لتعديل البيانات وتغيرها أو إتلافها.	4,68	0,56	1
5	التعرض لهجوم إرهابي.	4.40	0,89	7
6	اختراق أجهزة الخادم من داخل المؤسسة (عبث، إساءة استخدام...)	4,44	0,86	6
7	استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة.	4,37	0,95	8
8	زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة.	4,05	0,91	12
9	الإصابة بفيروسات مصدرها الانترنت.	4,06	0,85	11
10	الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش.	4,12	0,89	10
11	تنزيل برامج غير مصرح بها.	3,62	1,07	14
12	سرقة الأجهزة ووسائط التخزين.	3,94	1,18	13
13	الدخول غير المصرح إلى مركز البيانات وتعطيل عمل أجهزته.	4,30	1,04	9
14	تعديل إعدادات أجهزته الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع.	4,51	0,86	4
	المتوسط العام للمحور الأول	4,29	0,56	

يوضح الجدول رقم (4) المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب ويتضمن أربع عشرة عبارة توضح المخاطر الداخلية والخارجية وفقاً لاستجابات أفراد عينة الدراسة، ويتضح من هذا

الجدول أن قيمة المتوسط العام لهذا المحور هي (4,29) وانحرافه المعياري (0,56)، وحيث إن المقياس المستخدم خماسي فإن المتوسطات التي تنتمي إلى المجال من (1) إلى (1,80) تشير إلى عديم الخطورة، و المتوسطات التي تنتمي إلى المجال من (1,81) إلى أقل من (2,60) تشير إلى قليل الخطورة والمتوسطات التي تنتمي إلى المجال من (2,61) إلى (3,40) تشير إلى متوسطة الخطورة، والمتوسطات التي تنتمي إلى المجال من (3,41) إلى (4,20) تشير إلى خطر والمتوسطات التي تنتمي إلى المجال من (4,21) إلى (5) تشير إلى خطر جداً. من ذلك يلاحظ أن المتوسط العام لجميع عبارات هذا الجدول ينتمي إلى المجال من (4,29) إلى (5) فهي تعني خطر جداً. ويستنتج من ذلك أن أفراد عينة الدراسة يوافقون على أن المخاطر الداخلية والخارجية التي يمكن أن تتعرض لها شبكات مؤسساتهم خطرة جداً.

المحور الثاني: تدابير الحماية من المخاطر الداخلية والخارجية

الجدول رقم (5)

التدابير الوقائية من المخاطر الداخلية والخارجية

م	العبارة	المتوسط	الانحراف المعياري	الترتيب
1	توفير حراسة عند بوابات مركز البيانات على مدار الساعة.	3,77	1,27	43
2	تجهيز مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار.	4,31	0,98	4
3	قفل مركز البيانات (غرفة أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.	4,56	0,80	1
4	تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول.	4,07	1,00	26
5	توفير مراقبة داخلية باستخدام كاميرات تلفزيونية مع التسجيل.	4,05	1,00	29
6	عمل النسخ الاحتياطي والاسترجاع الآلي يومياً.	4,26	0,84	8
7	وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات	4,23	0,95	9

م	العبارة	المتوسط	الانحراف المعياري	الترتيب
	والحريق.			
8	تطبيق التشفير على وسائط النسخ الاحتياطي.	3,93	1,10	41
9	إبعاد وسائط النسخ لاحتياطي ووسائط التخزين عن أماكن تسرب المياه.	4,29	0,92	7
10	إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.	3,95	1,09	40
11	تركيب برامج مخصصة لمراقبة استخدام المستفيدين.	4,11	0,87	19
12	توفير خطة طوارئ واضحة ومعتمدة.	4,06	1,10	27
13	إعداد خطة للتراجع (Rollback) تطبق في حالة عدم نجاح خطة الطوارئ.	3,93	1,20	42
14	تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.	4,15	0,86	16
15	اختبار خطة الطوارئ.	4,02	0,82	34
16	اعتماد ميزانية خاصة بخطة الطوارئ.	3,97	0,95	37
17	السعي لمطابقة إجراءات العمل لتتوافق مع معايير دولية (آيزو) تتعلق بالحماية.	3,97	1,01	38
18	السعي للتوصل إلى اتفاقيات تعاون مع المتخصصين في الحماية.	4,03	0,94	32
19	تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة.	4,29	0,78	6
20	تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة.	3,96	0,84	39
21	استخدام تشفير لقواعد البيانات.	4,19	0,75	12
22	استخدام خاصية اتصال الشبكة الافتراضية (VPN)	4,21	0,82	11
23	استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة.	4,10	0,73	20

م	العبارة	المتوسط	الانحراف المعياري	الترتيب
24	توفير مركز بيانات (Data Center) بديل لاستخدامه عند الطوارئ	4,08	0,93	24
25	تجهيز الوسيط (Proxy) بخدمة توليد التقارير وتحليلها.	4,08	0,78	23
26	توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية.	4,12	0,84	17
27	توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.	4,08	0,93	22
28	توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.	4,04	0,98	30
29	تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.	4,09	0,98	21
30	توظيف أشخاص مناسبين من حيث المؤهل والخبرة بنسبة 90% على الأقل.	4,01	0,94	35
31	تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها.	4,19	0,85	13
32	تأمين جهاز احتياطي لجدار الحماية والموجه والوسيط وأجهزة الخادم.	4,35	0,88	3
33	توفير إدارة خاصة بأمن المعلومات.	4,00	1,31	36
34	جعل إدارة أمن المعلومات تابعة مباشرة لرئيس أو مدير المؤسسة.	4,05	1,06	28
35	اشتراط توفر المهارات المناسبة لمستخدمي الحاسب الآلي.	4,04	0,97	31
36	عقد دورات تدريب للتوعية في أمن المعلومات والحماية.	4,08	0,95	25
37	توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.	4,11	0,88	18
38	توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي. (Spam)	4,29	0,85	5

م	العبارة	المتوسط	الانحراف المعياري	الترتيب
39	تحديث نظام تشغيل أجهزة الشبكة بشكل دوري.	4,22	1,02	10
40	إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية.	4,15	0,87	15
41	توفير سياسة خاصة بكلمات المرور وتطبيقها.	4,37	0,76	2
42	تدريب المستفيدين من موارد شبكة المعلومات.	4,16	0,95	14
43	توفير برنامج للتحكم بمنافذ الحاسبات ومشغلات الوسائط القابلة للإزالة.	4,03	0,98	33
44	زيادة الاعتماد على أنظمة تشغيل أقل تأثرا بالفيروسات (يونكس، لينوكس..)	3,60	1,11	44
45	تقليل الاعتماد على نظام تشغيل مايكروسوفت كونه الأكثر تأثرا بالفيروسات.	3,50	1,23	45
	المتوسط العام للمحور الثاني	4,09	0,55	

يوضح الجدول (5) المتوسطات الحسابية والانحرافات المعيارية وترتيب العبارات لدرجات أولوية تنفيذ التدابير الوقائية من المخاطر الداخلية والخارجية وفقاً لاستجابات أفراد عينة الدراسة. ويتضح منه المتوسط العام لعبارات هذا المحور الذي بلغ (4,09) بانحراف معياري (0,55) أن أفراد عينة الدراسة يوافقون على أن أولوية اتخاذ التدابير اللازمة لتجنب المخاطر الداخلية والخارجية التي يمكن أن تتعرض لها شبكات مؤسساتهم تحتاج إلى أولوية عالية حيث يتمي إلى المجال من (3,41) إلى (4,20) وفق المقياس الخماسي الذي تم بيانه في المحور السابق.

ثانياً: الفروق والدلالات الإحصائية

1- الفروق والدلالات الإحصائية للمخاطر الداخلية والخارجية وأولويات منع حدوثها

قام الباحثان بحساب الفروق في المتوسطات بين المخاطر الداخلية والمخاطر الخارجية وبين التدابير المتخذة لتجنب تلك المخاطر حسب استجابات عينة الدراسة، وفق الجدول رقم (6) كما يلي:

الجدول رقم (6) الفروق في المتوسطات بين المخاطر الداخلية والمخاطر الخارجية وبين التدابير المتخذة لتجنب تلك الخاطر

المتغير	المتوسط	الانحراف المعياري	n	قيمة (T)	درجة الحرية	قيمة (P)*
المخاطر الداخلية والخارجية	4,29	0,557	105	3,38	104	0,001
تدابير تجنب المخاطر	4,09	0,554				

*دال عندما تكون P أقل من 10.0

يتضح من الجدول (6) أن P = 0,001 هي أقل من 0,01 ويدل ذلك على وجود فروق ذات دلالة إحصائية بين المخاطر الداخلية والخارجية وبين التدابير المتخذة لتجنب تلك المخاطر، حيث بلغ متوسط المخاطر الداخلية مع المخاطر الخارجية 4,29 ومتوسط تدابير تجنب تلك المخاطر، 4,09 وذلك لصالح المخاطر الداخلية والخارجية ويدل ذلك على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتجنب المخاطر الداخلية والمخاطر الخارجية.

2- الفروق والدلالات الإحصائية بين محاور الدراسة وفقاً للمتغيرات الشخصية والوظيفية

أ- الفروق وفق الجنس: للإجابة على هذا السؤال: هل هناك فروق ذات دلالة إحصائية في محاور الدراسة تبعاً لاختلاف الجنس؟ تم تنفيذ اختبار (ت) T- test ويظهر فيه المتغيرات التابعة وهي المخاطر الداخلية والخارجية وتدابير إزالتها. والمتغير المستقل (الجنس) وله حالتان ذكر وأنثى.

الجدول رقم (7)

اختبار (t) للفروق وفق الجنس

المتغير التابع	المتغير المستقل	n	المتوسط	الانحراف المعياري	قيمة (T)*	درجات الحرية	قيمة (P)**
المخاطر الداخلية والخارجية	ذكر	90	4,279	0,594	0,931-	103	0,354
	أنثي	15	4,423	0,193			
تدابير تجنب المخاطر	ذكر	90	4,076	0,593	0,559-	103	0,577
	أنثي	15	4,148	0,256			

** دال عندما تكون قيمة P أقل من **50.0**

ب– تحليل التباين الأحادي (الأنوفا) للمتغيرات الشخصية مع المحاور المختلفة

الجدول رقم (8)

فروق المتوسطات في محاور الدراسة تبعا لاختلاف الخبرة

المحور	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	قيمة P(*)
المخاطر الداخلية والخارجية	بين المجموعات	0,488	2	0,071	0,225	0,799
	داخل المجموعات	32,463	102	0,315		
	المجموع	32,951	104			
تدابير تجنب المخاطر	بين المجموعات	2,514	2	1,257	4,344	*0,015
	داخل المجموعات	29,512	102	0,289		
	المجموع	32,025	104			

(*) دال عندما تكون قيمة P أقل من 50,0

يتضح من الجدول رقم (8) بأنه لا توجد فروق ذات دلالة إحصائية تبعاً للخبرة في محور المخاطر الداخلية والخارجية وتوجد فروق دالة إحصائياً عند مستوى 0,05 في محور تدابير تجنب المخاطر الداخلية والخارجية، وللتعرف على مصادر هذه الفروق تم استخدام اختبار (LSD) البعدي كما يلي:

الجدول رقم (9)

مصادر الفروق في تدابير تجنب المخاطر والتي ترجع إلى اختلاف الخبرة

المحور	الخبرة	N	المتوسط	1	2	3
التدابير	1-أقل من 5 سنوات.	43	4,218	-	-	-
	2-من 5 سنوات إلى أقل من 10 سنوات.	39	3,998	**	-	-
	3-من 10 سنوات فأكثر.	23	4,191	*	-	-

(*) دال عندما تكون قيمة P أقل من 50,0

(*) دال عندما تكون قيمة P أقل من 0,01

يظهر من بيانات الجدول رقم (9) أنه توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ٥ سنوات إلى أقل من ١٠ سنوات دالة عند مستوى أقل من 0,01، وتوجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ١٠ سنوات فأكثر دالة عند مستوى أقل من 0,05.

نتائج الدراسة

توصلت الدراسة إلى مجموعة من النتائج أهمها:

أولاً: نتائج حول الخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب.

1- المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتي تعد خطراً جداً وفقاً لاستجابات عينة الدراسة:

أ- اختراق لتعديل البيانات وتغيرها أو إتلافها.

ب- اندلاع الحريق.

ت- التعدي على الكابلات.

ث- تعديل إعدادات أجهزة الشبكة بطريقة يصعب تعقبها لإطالة فترة الانقطاع.

ج- حصول إغراق بالمياه بسبب الفيضانات.

ح- اختراق أجهزة الخادم من داخل المؤسسة (عبث، إساءة استخدام...).

خ- التعرض لهجوم إرهابي.

د- استخدام برامج بغرض التجسس من قبل المستفيدين من داخل المؤسسة.

ذ- الدخول غير المصرح به إلى مركز البيانات وتعطيل عمل أجهزته.

2- المخاطر التي يمكن أن تؤثر سلباً على أمن شبكات الحاسب والتي تعد خطرة وفقاً لاستجابات عينة الدراسة:

أ- الإصابة بفيروسات مصدرها وسائط التخزين وذواكر الفلاش وشبكة الانترنت.

ب- زيارة مواقع إنترنت غير موثوقة تسمح بتنزيل البرمجيات الضارة.

ت- سرقة الأجهزة ووسائط التخزين.

ث- تنزيل برامج غير مصرح بها.

ثانياً: نتائج حول تدابير الحماية من المخاطر الداخلية والخارجية

1- توجد تدابير حماية من المخاطر الداخلية والخارجية تعد ذات أولوية عالية جداً وفقاً لاستجابات عينة الدراسة وهي:

أ- قفل مراكز البيانات (غرف أجهزة الخادم وأجهزة الشبكة) بحيث لا يدخلها إلا المتخصصون ممن لديهم ترخيص بالدخول.

ب- توفير سياسة خاصة بكلمات المرور وتطبيقها.

ت- تأمين جهاز احتياطي لجدار الحماية والموجه والوسيط وأجهزة الخادم.

ث- مركز البيانات بحساسات الحرارة والحركة ونظام الإطفاء والإنذار.

ج- توفير نظام لحماية البريد الالكتروني من الفيروسات والبريد الدعائي.

ح- تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من داخل الشبكة.

خ- إبعاد وسائط النسخ الاحتياطي ووسائط التخزين عن أماكن تسرب المياه.

د- عمل النسخ الاحتياطي والاسترجاع الآلي يومياً.

ذ- وضع وسائط النسخ الاحتياطي في خزائن مضادة للصدمات والحريق.

ر- تحديث نظام تشغيل أجهزة الشبكة بشكل دوري.

ز- استخدام خاصية اتصال الشبكة الافتراضية (VPN).

2- تدابير الحماية من المخاطر الداخلية والخارجية والتي تعد ذات أولوية عملية وفقاً لاستجابات عينة الدراسة:

أ- تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة.

ب- تصميم أو توفير برنامج إدارة الحماية من جميع جوانبها.

ت- تدريب المستفيدين من موارد شبكة المعلومات.

ث- إتاحة استخدام خاصية التحقق من الصحة في جدار الحماية.

ج- تدريب كل الموظفين على أمن المعلومات كل حسب واجباته الوظيفية.

ح- توفير إجراءات مكتوبة ومعتمدة توضح ما يلزم لتنفيذ أعمال الحماية.

خ– توفير خدمة الاتصال البعيد فقط للأفراد المعتمدين من الإدارة.

د– تركيب برامج مخصصة لمراقبة استخدام المستفيدين.

ذ– استخدام نظام لإدارة الأحداث (Logs) في جميع خوادم وأجهزة الشبكة.

ر– تأمين بديل واحد على الأقل لكل موظف يعمل في مجال الحماية.

ز– توفير موظف واحد على الأقل يقوم بإدارة أجهزة الحماية وتحديثها.

س–توفير مركز بيانات (Data Center) بديل لاستخدامه عند الطوارئ.

ش–تجهيز مركز البيانات بآلية تسجيل للداخلين بالاسم والوقت وسبب الدخول.

ص– توفير خطة طوارئ واضحة ومعتمدة وإعداد خطة للتراجع (Rollback) تطبق في حالة عدم نجاح خطة الطوارئ.

ض– جعل إدارة أمن المعلومات تابعة مباشرة لرئيس أو مدير المؤسسة.

ط– توفير موظف واحد على الأقل يقوم بإدارة برامج الحماية وتحديثها.

ظ– إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.

ع– تطبيق التشفير على وسائط النسخ الاحتياطي.

غ– توفير حراسة عند بوابات مركز البيانات على مدار الساعة.

ثالثاً: نتائج تتعلق بالفروق والدلالات الإحصائية:

1– توجد فروق ذات دلالة إحصائية بين المخاطر الداخلية والخارجية وبين التدابير المتخذة لتجنب تلك المخاطر، وذلك لصالح المخاطر الداخلية والخارجية ويدل ذلك على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات عينة الدراسة لتجنب المخاطر الداخلية والمخاطر الخارجية.

2– توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ٥ سنوات إلى أقل من ١٠ سنوات.

3– توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من 10 سنوات فأكثر.

توصيات الدراسة

في ضوء نتائج الدراسة يقترح الباحثان مجموعة من التوصيات التي يمكن أن تسهم في تدعيم حماية شبكات المعلومات من منظور الأخطار المحتملة وتدابير الوقاية منها، وأهم تلك التوصيات ما يلي:

1- توفير اختصاصيين في أمن المعلومات لإنشاء السياسات الأمنية ومراجعة تنفيذها، والسعي لمطابقة إجراءات أمن الشبكات مع معايير (الآيزو).

2- توفير موظفين ومدراء يحملون مؤهلات علمية تتناسب مع متطلبات أعمال الحماية، وتقدير أعمال الحماية بتقديم المكافآت أو العلاوات أو شهادات التقدير.

3- تخصيص ميزانية كافية لتحسين الحماية، وخطط الطوارئ.

4- توفير لجنة لإدارة التعديلات (شبكات وقواعد بيانات وموقع الانترنت) في المؤسسة.

5- توفير حراسة عند بوابات مراكز البيانات على مدار الساعة، وقفل مراكز البيانات بحيث لا يدخلها إلا المتخصصون المخولون.

6- تنفيذ اختبارات دورية لنقاط الضعف انطلاقا من خارج الشبكة وكذلك من داخلها.

7- إتلاف وسائط التخزين والنسخ الاحتياطي المنتهية الصلاحية.

8- زيادة الاعتماد على أنظمة تشغيل أقل تأثراً بالفيروسات (يونكس، لينوكس..).

مقترحات الدراسة:

تقترح الدراسة على إدارات المؤسسات التي تعتمد في تسيير أعمالها على تقنية المعلومات ما يلي:

1- توفير السياسات الأمنية والإجراءات اللازمة لتنفيذ أعمال الحماية.

2- توظيف الكوادر المؤهلة من ذوي الخبرة في مجال الحماية وتحفيزهم بالمكافآت المالية والمعنوية.

3- العناية بخطط الطوارئ وتدريب المعنيين على تنفيذها وإنشاء مراكز بيانات احتياطية.

المراجع العلمية

المراجع العربية:

آبادى، الفيروز، (١٩٨٧): القاموس المحيط، بيروت: مؤسسة الرسالة، ص١٢١٩

البشري، محمد أمين (٢٠٠٤): التحقيق في الجرائم المستحدثة، الرياض: جامعة نايف العربية للعلوم الأمنية، مركز الدراسات والبحوث.

السحيباني، عبد الله (١٩٩٦): كفاءة الإجراءات الإدارية في المحافظة على أمن المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

شمدين، عفاف (2003): الأبعاد القانونية لاستخدامات تكنولوجيا المعلومات، دمشق.

الشهري،فايز بن عبد الله (٢٠٠١): استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي: دراسة وصفية على عينة من المواقع الأمنية العربية على شبكة الانترنت، مجلة البحوث الأمنية، الرياض: كلية الملك فهد الأمنية، مركز الدراسات.

العنزي، سليمان (2003): وسائل التحقيق في جرائم نظم المعلومات، رسالة ماجستير، الرياض: جامعة نايف العربية للعلوم الأمنية.

المراجع الأجنبية:

Emarah، S :(2007) : The Control of Firewalls Using Active Networks ،In formation Technology and National Security Conference ،Riyadh.

Brenton،C &Hunt ،C (2003) .Mastering - Network security ،SYBEX Inc . US .Cisco System ،Inc.

Cisco Networking Academy Program :First -Year Companion Guide ، Cico Press ، Indianapolice(،USA, 2001).

Idris، N & Shanmugam، B :(2007) Hybrid Intelligent Intrusion Detection System Information Technology and National Security Conference ، Riyadh.

المواقع الالكترونية:

wikipedia.org Cisco.com