التدابير الوقائية لتجنب الثغرات الأمنية في شبكات الحاسوب المحلية
دراسة مسحية تحليلية

زكريا أحمد عمار [١] ياسر عامر الكبيسي [٢]

ملخـــص

هدفت هذه الدراسة إلى إيجاد حلول لتجنب الثغرات الأمنية الخطرة في شبكات الحاسوب المحلية وتحديد التدابير اللازمة لتجنب حصول الثغرات وإزالة الموجود منها، للوصول إلى أفضل حماية ممكنة بظروف وصول مرنة، وذلك بتطبيق الاستبانة كأداة لجمع البيانات على عينة الدراسة المتكونة من خبراء في تقنية المعلومات من أساتذة جامعات ومهندسين وفنيين ومدراء يعملون في إدارات تقنية المعلومات في المؤسسات التعليمية في الرياض، حيث بلغ عدد الاستبانات القابلة للتحليل ١٠٥ استبانات، وقد أظهرت نتائج التحليل الإحصائي عن وجود فروق ذات دلالة إحصائية بين درجة خطورة الثغرات الأمنية وبين التدابير الوقائية المتخذة لتجنبها، وذلك لصالح درجة خطورة الثغرات الأمنية، الأمر الذي يدل على عدم اكتمال التدابير الوقائية التي تتخذها المؤسسات التعليمية لتلافي الثغرات الأمنية. وأوصت الدراسة بضرورة زيادة الاهتمام بالكادر البشري العامل في حماية الشبكات المحلية، من حيث الكفاءة وكفاية العدد والتدريب والتحفيز. لتمكينها من القيام بتدابير الحماية الفيزيائية وإعداد وتشغيل وتحديث أجهزة وبرامج الحماية، وكذلك تنفيذ الاختبارات دورية لكشف الثغرات الأمنية، بالإضافة لضرورة توفير السياسات الأمنية اللازمة لتنفيذ أعمال الحماية.

الكلمات المفتاحية: حماية الشبكات المحلية، أمن المعلومات، شبكات الحاسوب، تحديثات الحاسب الآلي.

تاريخ استلام البحث ٧/ ٨/ ٢٠١١؛ تاريخ قبول البحث ١٢/ ١٠/ ٢٠١١

مقدمـــــة

يشهد عالمنا المعاصر ثورة في تقنية المعلومات، من أهم ظواهرها شبكة الانترنت، التي أثرت في حياة الناس إلى حد الاعتماد عليها، فقد أصبحت جزءاً من حياة الأفراد والحكومات والشركات، وقد ظهرت مواقع الإنترنت بهدف خدمة المستفيدين بمسميات مختلفة تغطي معظم نواحي الحياة العلمية والخدمية. ووصل الأمر إلى أن تعطل وتقف خدمات الإنترنت يعطل ويوقف كثيراً من أعمال الناس، مثل حجوزات السفر وعمليات البنوك والاتصالات الالكترونية. وبما أن فضاء شبكة الانترنت فضاء عالمي سريع التغير ويصعب إحكام السيطرة عليه، فقد كثرت الأخطار التي تهدد أمن شبكات الحاسوب المحلية المتصلة بالإنترنت، وغدت سلامة البيانات المحتضنة في خزائنها عرضة للانتهاك والقرصنة والتعديل والتزوير، والإصابة بالفيروسات والبرامج الضارة والتعرض لمحاولات الاختراق لأغراض سرقة المعلومات أو التخريب أو التعديل والعبث، وحيث أن الثغرات الأمنية في شبكات الحاسوب المحلية تتكون بشكل أساسي من ثغرات تقنية وثغرات في الإعداد وأخرى في السياسات الأمنية، (Cisco systems,2004) ، من هنا جاءت أهمية هذه الدراسة لتحديد خطورة الثغرات الأمنية في شبكات الحاسوب بما تتضمنه من ثغرات تقنية أو ثغرات ناتجة عن الإعداد أو ثغرات ناتجة عن نقص في السياسات الأمنية.

(١، ٢) مركز المعلومات في جامعة نايف العربية للعلوم الأمنية.

أهمية الدراسة

في بيئة شبكات المعلومات السريعة التغير تظهر في كل يوم فيروسات وبرامج ضارة جديدة، وفي كل يوم تطفو برمجيات وتغيب أخرى نتيجة عدم قدرة منتجيها على الاستمرار في التسابق والمنافسة، تبرز أهمية الحاجة لترقية التجهيزات وتحديث البرمجيات، وفي بحر التغيرات في تقنية المعلومات تجد قراصنة المعلومات الذين يستغلون ما يُكتشف من مواطن الضعف في التصميمات وتوزيع التجهيزات والتأخر في تثبيت التحديثات. وحيث أن وجود الثغرات الأمنية في شبكات الحاسوب واحد من العناصر الضرورية لشن الهجمات الالكترونية إلى جانب وجود الدافع وتوفر طرق تنفيذ الهجوم، (الغثبر، ٢٠٠٩)، فإن حصر الثغرات الأمنية الخطرة هدف مهم جداً وخصوصاً إذا علمنا أن القراصنة المبتدئون يجدون في شبكة الانترنت كثيرا من الشبكات التي تكثر فيها الثغرات الناتجة عن عدم التحديث وعدم اتخاذ التدابير اللازمة للحماية. ويمكن بيان أهمية الدراسة كما يلي:

١ ـ تقدم للعاملين في حماية شبكات الحاسب الآلي مرجعاً أمنياً مهماً للوقاية من الجرائم الإلكترونية.

٢ ـ تقدم هذه الدراسة معلومات مفيدة جداً للراغبين في تصميم الشبكات ومراكز المعلومات آخذين بالاعتبار الاحتياطات الأمنية اللازمة لحماية شبكاتهم مختصرين الجهد والمال والوقت.

مشكلة الدراسة

قدر عدد مستخدمي الانترنت في العالم حتى نهاية عام ٢٠٠٨ م (بـ) ١٨٤,٣١٣,٥٧٤,١ مستخدماً، وفق إحصائيات الإنترنت العالمية(Miniwatts Marketing Group,2011) ، بنسبة ٢٣,٥ ٪، من عدد سكان العالم البالغ ٦,٧١٠,٠٢٩,٠٧٠ نسمة بنهاية العام ٢٠٠٨م، وتزيد نسبة البريد الإلكتروني الاقتحامي عن ٤٠٪ من البريد الإلكتروني المقدر يومياً بـ(١٢,٤) بليون رسالة، بمتوسط (٢٢٠٠) رسالة لكل مستخدم سنوياً وفق تقديرات موقع Top Ten Review لعام ٢٠٠٤م ، (القاسم،٢٠٠٨). ويشير تقرير أعدّته مجموعة (Radicati) بأن عدد مستخدمي البريد الإلكتروني في عام ٢٠٠٧ قد بلغ ١,٢ بليون مستخدم، وتوقع التقرير ازدياد العدد إلى ١,٦ بليون عام ٢٠١١ بزيادة ٧٪ خلال أربع سنوات (Radicati Group,2011). من خلال هذه الإحصائيات يمكن استنتاج ضخامة التعاملات الإلكترونية في وسط شبكات المعلومات وإدراك ضخامة الأخطار التي تزداد بازدياد مستخدمي الإنترنت.

بعد شيوع استخدام شبكات الحاسوب وبخاصة شبكة الانترنت ظهرت مشكلات أمنية تتلخص بتعطيل وتدمير المواقع الحكومية والتجارية، والتسلل إلى الشبكات المحلية وسرقة أسرار الشركات والحكومات والمؤسسات الأمنية والدفاعية، وترويج برامج التخريب والتجسس والقرصنة، وسرقة المواقع وانتهاك حقوق الملكية الفكرية، كما أنها تؤمن تربة مناسبة لنمو شبكات التجسس العالمية التي تمارس نشاطات جمع المعلومات وانتهاك الخصوصية على مدار الساعة (الشهري،٢٠٠١). وأساس هذه المشكلات الأمنية هو وجود الثغرات الأمنية الخطرة في التصاميم والإعداد وتنفيذ التحديثات.

في هذه الدراسة يتناول الباحث الثغرات الأمنية الخطرة في شبكات الحاسوب المحلية ومخازن المعلومات المتصلة بها وتدابير إزالتها.

هدف الدراسة

هدفت الدراسة إلى تحديد الثغرات الأمنية في شبكات الحاسوب المحلية، وكذلك تحديد التدابير اللازمة لإزالة نقاط ضعف تلك الشبكات، للوصول إلى أفضل حماية ممكنة بظروف وصول مرنة.

أسئلة الدراسة

طرح الباحث تساؤلاً رئيساً يتمثل بالسؤال التالي: ما هي الثغرات الأمنية في شبكات الحاسوب المحلية وكيف يمكن التخلص من الثغرات الأمنية تلك، الأمر الذي يقود إلى تساؤلين فرعيين هما:

١ ـ ما الثغرات الأمنية عالية الخطورة التي تُستغل لاختراق شبكات الحاسوب المحلية.

٢ ـ ما التدابير الوقائية المتخذة لمنع استغلال الثغرات الأمنية.

مصطلحات الدراسة

شبكات الحاسوب: هي مجموعة من الحاسبات مربوطة فيما بينها بوسط نقل، تحتوي أجهزة خادم لتخزين ومعالجة البيانات وتحوي على حدودها بوابات للتصفية والحماية، وخصوصاً تلك الحدود التي تتصل بالشبكات العامة كالإنترنت. وتصنف شبكات الحاسوب إلى شبكات محلية وهي التي تنتشر في مساحة جغرافية محدودة، وإلى شبكات واسعة وتنتشر على مساحة جغرافية كبيرة قد تشمل مدناً متعددة أو دولاً وقد تتوزع على أكثر من قارة. (عمار،٢٠١١).

التدابير الوقائية: هي مجموعة الإجراءات والسياسات والتي تتخذ لتجنب حصول الاعتداءات والهجمات على أنظمة الحاسوب وموارد شبكات المعلومات.

الثغرات الأمنية: هي أوجه الضعف في نظام المعلومات أو إجراءات أمن النظام أو عناصر التحكم الداخلية أو التنفيذ التي يستغلها أو يستهدفها مصدر تهديد. وهي ترجمة للكلمة الانجليزية Vulnerability (الغثبر،٢٠٠٩)

الدراسات السابقة

بعد البحث المتعمق وجد الباحث عدداً من الدراسات ذات علاقة وثيقة بهذا الموضوع ومنها:

دراسة شيخ فاروق عمارة (٢٠٠٧) بعنوان « The Control of Firewalls using Active Networks» هدفت إلى وضع برامج صغيرة مسبقة التعريف داخل تلك الأجهزة تمكن من إعادة توجيه حزم البيانات بفتح أو إغلاق المنافذ تبعاً لمحتوى الحزم باستخدام تقنيات الشبكة النشطة، 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 الثغرات الأمنية عالية الخطورة في الشبكات المحلية وتدابير تجنبها وضمنت جدران الحماية كواحد من أهم تدابير الوقاية.

أجرى نور بك باشا إدريس و بحراني دهران شانموجان (٢٠٠٧)، دراسة بعنوان «Hybrid Intelligent Intrusion Detection» هدفت إلى إيجاد حلول لمشكلة عدم كفاية نظام كشف التجسس[1] (IDS) لمنع التجسس على شبكات الحاسوب كونها محدودة الإمكانات، ومن أهم توصيات دراستهما: ضرورة استخدام نظام للكشف الذكي عن التجسس على شبكات الحاسوب، واستخدام جهاز عالي الأداء من حيث المعالجة. وتتوافق دراسة إدريس مع ما ذكره الباحث في دراسته 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 الثغرات الأمنية عالية الخطورة في شبكات الحاسوب المحلية.

أجرى سليمان مهجع العنزي (٢٠٠٣) دراسة حول جرائم نظم المعلومات وتوصلت الدراسة إلى أن حجم استخدام منفذ شبكة الانترنت وبرامج الاختراق الموجودة بها (٢٥ , ٤٪). وتوصلت الدراسة أيضاً إلى أن برامج الحماية تعد وسيلة ضبط وتحقيق هامة بشكل دائم، وتساعد بما نسبته (٢ , ٩٤٪) في تحديد نوع الجريمة، وما نسبته (١ , ٩٥٪) في تحديد توقيت ارتكاب الجريمة. وكشفت الدراسة عن أنه بالإمكان الاعتماد على عنوان (IP) بما نسبته (٢ , ٩٤٪) وعلى برامج الحماية (٤ , ٩١٪) ووسائل تتبع المخترقين (٩ , ٧٤٪). و تُبرز دراسة (العنزي) أهمية وسائل الحماية في ضبط الجريمة الإلكترونية وذلك يتوافق مع هذه الدراسة في موضوع حماية الشبكات من الثغرات الأمنية الخطرة 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 (Logs).

مجتمع وعينة الدراسة

استفاد الباحث من المنهج الوصفي بإجراء المسح الميداني لمجتمع الدراسة الذي تكون من المؤسسات التعليمية الخاصة والحكومية والمشتركة في مدينة الرياض، حيث بلغ عدد المؤسسات التعليمية التي خضعت للبحث (٧٥) مؤسسة تعليمية أخذت كعينة عشوائية من أصل (٤٢٩) مؤسسة تعليمية في مدينة الرياض. وقد تم اختيار المؤسسات التي

(1) IDS: Intrusion Detection System.
(2) UTM: Unified Threat Management.

تعتمد على تقنيات الحاسب الآلي في تسيير أعمالها الأكاديمية والمالية، وتم الاكتفاء بهذه العينة نظراً لكبر مجتمع الدراسة، وصعوبة الوصول إلى جميع المؤسسات التعليمية المنتشرة على منطقة جغرافية واسعة. وبلغ عدد أفراد العينة (١٠٥) أفراد، مكونين من مهندسين وإداريين وفنيين يعملون في إدارة وتشغيل أجهزة وبرمجيات حماية شبكات الحاسوب المحلية في مراكز تقنية المعلومات الموجودة في المؤسسات التي خضعت للدراسة.

أداة الدراسة

اختار الباحث الاستبانة كأداة لقياس متغيرات الدراسة وذلك لمناسبتها لطبيعة الدراسة، بغرض تحقيق أهداف الدراسة والإجابة عن تساؤلاتها، وقد صيغت الاستبانة بصورة تتناسب مع تساؤلات الدراسة وتضمنت البيانات الشخصية والوظيفية لأفراد عينة الدراسة. كما تضمنت أسئلة شملت عدداً من العبارات حول الثغرات الأمنية في شبكات الحاسوب، وكذلك التدابير الاحتياطية اللازمة لتجنب الثغرات الأمنية الخطرة، وقد عرضت على عشرة محكمين يعملون في مجال تقنية المعلومات والحاسب الآلي، وقد أبدوا آراءهم في مناسبة عبارات الاستبانة لمواضيع أسئلة الدراسة، وتم حساب معامل ثبات أداة الدراسة للعينة (١٠٥) بمقياس كرونباخ ألفا وذلك باستخدام برنامج (SPSS) لمعالجة البيانات في الحاسب الآلي. وقد أسفرت النتائج أن معامل ثبات عبارات الأداة هي (٠,٩٥٥٨)، دالة إحصائياً عند مستوى ٠,١، وهي قيمة مرتفعة تدل على قوة الارتباط بين العبارات ومواضيع الأسئلة العائدة لها.

محددات الدراسة

اقتصرت الدراسة على موضوع محدد هو الثغرات الأمنية الخطرة في شبكات الحاسوب المحلية واستخلاص التدابير لتجنب تلك الثغرات. واقتصرت الحدود البشرية للدراسة على العاملين في شبكات الحاسوب وحمايتها من حيث الإعداد والتحديث والتطوير في مراكز وأقسام تقنية المعلومات في المؤسسات التعليمية. وأطّرت الحدود الزمنية بفترة تطبيق الدراسة المسحية في الأشهر الستة الأخيرة من عام ٢٠٠٩م. وأما الحدود المكانية فاقتصرت على عينة عشوائية من المؤسسات التعليمية الموجودة في مدينة الرياض بالمملكة العربية السعودية.

المعالجة الإحصائية

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

أ ـ التوزيعات التكرارية والنسب المئوية لوصف البيانات

ب ـ المتوسط الحسابي الموزون.

ج ـ 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.

د ـ معامل ارتباط بيرسون لتوضيح العلاقات بين متغيرات عناصر البحث.

هـ ـ اختبار (ت) T-test للفرق بين متوسطين، واختبار LSD البُعدي للتعرف على مصادر الفروق الدالة إحصائياً وذلك بين المتغيرات التابعة والمتغيرات المستقلة.

نتائج الدراسة

قام الباحث بحساب المتوسطات والانحراف المعياري في استجابات عينة الدراسة وكذلك حساب الفروق في المتوسطات بين خطورة الثغرات الأمنية وبين التدابير الوقائية المتخذة لتلافي تلك الثغرات، وبسبب طول جداول المتوسطات اكتفى الباحث بإيراد جدول الفروق في المتوسطات، وفق الجدول رقم (١).

الجدول رقم (١)

الفروق في المتوسطات بين خطورة الثغرات الأمنية وبين التدابير الوقائية لتلافيها

المتغير	المتوسط	الانحراف المعياري	n	قيمة (T)	درجة الحرية	قيمة (P) *
خطورة الثغرات الأمنية	٤,١٨	٠,٦٦	١٠٥	٢,٤٧٤	١٠٤	٠,٠١٥
التدابير الوقائية	٤,٠٨	٠,٥٥				

* دال عندما تكون قيمة P أقل من ٠,٠٥

يتضح من الجدول (١) أن P=٠,٠١٥ هي أقل من ٠,٠٥ ويدل ذلك على وجود فروق ذات دلالة إحصائية بين درجة خطورة الثغرات الأمنية وبين التدابير الوقائية المتخذة لتجنبها، حيث بلغ متوسط خطورة الثغرات الأمنية ٤,١٨ ومتوسط تدابير تجنبها، ٤,٠٨ وذلك لصالح درجة خطورة الثغرات الأمنية ويدل ذلك على عدم اكتمال التدابير الوقائية المتخذة لتجنب الثغرات الأمنية.

الجدول رقم (٢)

فروق المتوسطات في محاور الدراسة تبعا لاختلاف العمر

المحور	مصدر التباين	مجموع المربعات	درجات الحرية	متوسط المربعات	قيمة ف	قيمة p (*)
خطورة الثغرات الأمنية	بين المجموعات	٣,٨١٠	٢	١,٩٠٥	٤,٦٤٢	٠,٠١٢*
	داخل المجموعات	٤١,٠٣١	١٠٠	٠,٤١٠		
	المجموع	٤٤,٨٤٠	١٠٢			
تدابير تجنب الثغرات الأمنية	بين المجموعات	٣,٨٢٤	٢	١,٩١٢	٧,٠٧٤	٠,٠٠١*
	داخل المجموعات	٢٧,٠٣٠	١٠٠	٠,٢٧٠		
	المجموع	٣٠,٨٤٥	١٠٢			

(*) دال عندما تكون قيمة p أقل من ٠,٠٥

يتضح من الجدول رقم (٢) بأنه توجد فروق ذات دلالة إحصائية بين خطورة الثغرات الأمنية وبين تدابير تجنبها ذات دلالة إحصائية عند مستوى ٠,٠٥، وللتعرف على مصادر الفروق الدالة إحصائياً تم استخدام اختبار (LSD) البُعدي كما يلي:

الجدول رقم (٣)

مصادر الفروق في الثغرات الأمنية و تدابير تجنبها والتي ترجع إلى اختلاف العمر

المحور	الخبرة	n	المتوسط	١	٢	٣
الثغرات الأمنية	١-أقل من ٣٠ سنة	٤٤	٤,٢١٥	-	-	-
	٢- من ٣٠ إلى أقل من ٤٠ سنة	٤٠	٣,٩٦٠	-	-	**
	٣- من ٤٠ سنة فأكثر	١٩	٤,٤٩١	-	**	-
تدابير تجنب الثغرات الأمنية	١-أقل من ٣٠ سنة	٤٤	٤,٢٠٩	-	**	-
	٢- من ٣٠ إلى أقل من ٤٠ سنة	٤٠	٤,٨٢٩	-	-	**
	٣- من ٤٠ سنة فأكثر	١٩	٤,٢٥٥	-	**	-

(**) دال عندما تكون قيمة p أقل من ٠,٠١

يظهر من بيانات الجدول رقم (٣) ما يلي:

١ ـ توجد فروق في الثغرات الأمنية بين استجابات الفئة العمرية من ٣٠ إلى أقل من ٤٠ سنة واستجابات الفئة من ٤٠ سنة فأكثر دالة عند مستوى أقل من ٠,٠١.

٢ ـ توجد فروق في الثغرات الأمنية بين استجابات الفئة العمرية من ٤٠ سنة فأكثر واستجابات الفئة من ٣٠ إلى أقل من ٤٠ سنة دالة عند مستوى أقل من ٠,٠١.

٣ ـ توجد فروق في تدابير تجنب الثغرات الأمنية بين استجابات الفئة العمرية أقل من ٣٠ سنة واستجابات الفئة من ٣٠ إلى أقل من ٤٠ سنة دالة عند مستوى أقل من ٠,٠١.

٤ ـ توجد فروق في تدابير تجنب الثغرات الأمنية بين استجابات الفئة العمرية من ٣٠ إلى أقل من ٤٠ سنة واستجابات الفئة من ٤٠ سنة فأكثر دالة عند مستوى أقل من ٠,٠١.

٥ ـ توجد فروق في تدابير تجنب الثغرات الأمنية بين استجابات الفئة العمرية من ٤٠ سنة فأكثر واستجابات الفئة من ٣٠ إلى أقل من ٤٠ سنة دالة عند مستوى أقل من ٠,٠١.

وقد توصلت الدراسة إلى مجموعة من النتائج أهمها مرتبة تبعاً لتسلسل أسئلة الدراسة ما يلي:

النتائج المتعلقة بخطورة الثغرات الأمنية:

حسب استجابات أفراد عينة الدراسة كانت الثغرات الأمنية الخطرة جداً كما يلي:

١ ـ عدم تحديث أنظمة تشغيل جدران الحماية بانتظام.

٢ ـ عدم وجود سياسة للحماية.

٣ ـ عدم تحديث خاصية الحماية من الفيروسات في جدران الحماية بانتظام.

٤ ـ عدم تثبيت تحديثات أنظمة تشغيل أجهزة الخادم والحاسبات المكتبية بانتظام.

٥ ـ قلة الخبرة لدى العاملين بالحماية.

حسب استجابات أفراد عينة الدراسة كانت الثغرات الأمنية الخطرة كما يلي:

١ ـ عدم وجود خاصية كشف ومنع التلصص IPS في جدران الحماية المستخدمة.

٢ ـ أداء بعض الأجهزة ضعيف ولا تستطيع تشغيل مكافح الفيروسات.

٣ ـ وجود كلمات مرور افتراضية في بعض الأجهزة والبرمجيات العاملة بالشبكة.

٤ ـ قلة الكفاءة المهنية عند المستفيدين من موارد الشبكة.

٥ ـ عدم تحديث خاصية الحماية من البريد الدعائي Spam في جدران الحماية.

تدابير تجنب الثغرات الأمنية عالية الخطورة حسب استجابات أفراد عينة الدراسة هي:

١ ـ تنفيذ اختبار دوري لكشف الثغرات الأمنية من داخل الشبكة.

٢ ـ استخدام أدوات قياس أداء أجهزة الشبكة.

٣ ـ تزويد وتفعيل خاصية الحماية من البريد الدعائي (Spam) في جدار الحماية.

٤ ـ تزويد وتفعيل خاصية تصفية المواقع غير المرغوب فيها في جدران الحماية.

٥ ـ استخدام قائمة تتضمن المهام اليومية لأعمال الحماية.

٦ ـ تركيب أدوات كشف ومكافحة الفيروسات على أن تكون مرخصة ويجري تحديث بياناتها يومياً.

النتائج المتعلقة بالفروق والدلالات الإحصائية:

١ ـ توجد فروق ذات دلالة إحصائية بين درجة خطورة الثغرات الأمنية التي يمكن أن تُستغل لاختراق شبكات الحاسوب المحلية وبين التدابير الوقائية المتخذة لتجنب الثغرات الأمنية، وذلك لصالح خطورة الثغرات الأمنية، ويدل ذلك على عدم اكتمال التدابير الوقائية المتخذة لتنب حصول الثغرات الأمنية.

٢ ـ توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ٥ سنوات إلى أقل من ١٠ سنوات.

٣ ـ توجد فروق جوهرية في التدابير لصالح ذوي الخبرة من ١٠ سنوات فأكثر.

توصيات الدراسة

في ضوء النتائج التي توصلت إليها الدراسة يوصي الباحث بما يلي:

١ ـ العناية بالموارد البشرية العاملة في مجال حماية الشبكات، من حيث التخصص والكفاءة وكفاية العدد والتدريب والتحفيز.

٢ ـ توفير السياسات الأمنية والإجراءات اللازمة لتنفيذ أعمال الحماية. والسعي لمطابقة إجراءات حماية الشبكات مع معايير (الآيزو).

٣ ـ ضرورة تركيب جدران حماية فعالة على حدود الشبكات المحلية، و عدم التساهل في تدابير الحماية الفيزيائية.

٤ ـ ضرورة تركيب مكافحات الفيروسات في جميع الأجهزة المربوطة بشبكة المنشأة والحرص على تحديثها بشكل آني لأجهزة الخادم وبشكل يومي لحاسبات المستفيدين.

٥ ـ تنفيذ اختبارات دورية لكشف الثغرات الأمنية، وسد الثغرات المكتشفة مباشرة.

المراجع

الغثبر، خالد وسراج إمبابي، (٢٠٠٩)، قاموس مفردات أمن المعلومات، مركز التميز لأمن المعلومات، ط١، ص١٦٧.

الغثبر، خالد ومحمد القحطاني، (٢٠٠٩)، أمن المعلومات بلغة ميسرة، مركز التميز لأمن المعلومات، ط١، ص ص٢٤-٢٥.

القاسم، محمد ، وعبدالرحمن الحمدان،(٢٠٠٨) ، أساسيات أمن المعلومات، ط٢، ص١٠٨.

عمار،زكريا،(٢٠١١)، حماية الشبكات الرئيسة من الاختراق والبرامج الضارة، رسالة ماجستير، جامعة النيلين، الخرطوم. ص١١

فايز بن عبد الله الشهري، (٢٠٠١)، استخدامات شبكة الانترنت في مجال الإعلام الأمني العربي، مجلة

البحوث الأمنية، مركز الدراسات بكلية الملك فهد الأمنية، الرياض، المجلد ١٠، العدد ١٩، ص ص١٨٤-١٨٦.

Cisco systems,(2004), Fundamentals of network security, Indiana, Cisco press.p15.

Top Ten Review, (2011) , available at:

http://www.spam-filter-review.toptenreviews.com/spam-statistics.html

Miniwatts Marketing Group, (2011) available at: http://www.internetworldstats.com/blog.htm#20060918

Radicati Group,(2011), available at: http://www.marketwire.com/press-release/The-Radicati-Group-Inc-Releases-Q32007--Market-Numbers-Update-781416.htm

زكريا أحمد عمار بكالوريوس هندسة إلكترونية، جامعة حلب، ماجستير تقانة المعلومات من جمهورية السودان - جامعة النيلين عام ٢٠١١م حاصل على شهادة مدقق داخلي في نظام إدارة الجودة ISO 9000:2008 شاركت في دورة الدليل الرقمي الجنائي في جرائم الإرهاب الالكتروني عام ٢٠٠٩ في الدوحة بتقديم ورقة عمل بعنوان«مسرح جريمة الإرهاب الإلكتروني ووسائط التخزين الرقمية» ، كما شاركت في دورة الدليل الرقمي الجنائي في جرائم الإرهاب الالكتروني عام ٢٠٠٩ في الدوحة بتقديم ورقة عمل بعنوان «أساليب حماية الشبكات الوطنية من جرائم الإرهاب الإلكترونية والحد من استخدامها كوسيلة يمكن إساءة استخدامها في العمليات الإرهابية» وأيضا في الحلقة العلمية الدليل الرقمي عام ٢٠٠٨ بتقديم ورقة عمل بعنوان «مسرح الجريمة الإلكترونية» العمل الحالي يعمل في جامعة نايف العربية للعلوم الأمنية منذ ٢٠٠١م، في مركز المعلومات والحاسب الآلي رئيساً لقسم الشبكة وأمن المعلومات وأدرس في بعض مقررات الجرائم الإلكترونية والأدلة الرقمية بكلية علوم الأدلة الجنائية و كلية الدراسات العليا بالجامعة ، وشاركت بكتابة عدة مقالات حول أمن المعلومات في مجلة عصر الحاسب الصادرة من جمعية الحاسبات السعودية، ومجلة الأمن والحياة الصادرة من جامعة نايف العربية للعلوم الأمنية، وحضرت حضر عشرات الدورات المتخصصة بشبكات الحاسب الآلي وامن المعلومات كما أنني عضو في جمعية الحاسبات السعودية، ونقابة المهندسين السوريين.

م. ياسر عامر الكبيسي مدير البرامج العلمية جامعة نايف علربية للعلوم الامنية ـ بكالوريوس هندسة سيطرة ونظم ـ الجامعة التكنولوجية ـ بغداد حاصل على الشهادة الاحترافية التالية : PMP, ITIL Foundation v3