العنوان:	سياسة أمن المعلومات في الجامعات : حالة دراسية
المصدر:	Cybrarians Journal
الناشر:	البوابة العربية للمكتبات والمعلومات
المؤلف الرئيسي:	الصاحب، محمود حسن
المجلد/العدد:	ع 33
محكمة:	نعم
التاريخ الميلادي:	2013
الشهر:	ديسمبر
الصفحات:	41 - 54
رقم MD:	510926
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	HumanIndex
مواضيع:	المؤسسات التعليمية، سياسة المعلومات، أمن المعلومات، تكنولوجيا المعلومات، الاستهاد المرجعي، المكتبات الجامعية، فلسطين، جامعة بوليتكنك
رابط:	http://search.mandumah.com/Record/510926

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة ومتخصصة في مجال المكتبات والمعلومات

العدد 33، **ديسمبر** 2013

سياسة أمن المعلومات في الجامعات: حالة دراسية

د. محمود حسن الصاحب
عميد كلية تكنولوجيا المعلومات وهندسة الحاسوب
جامعة بوليتكنك، فلسطين
alsaheb@ppu.edu

المستلخص

يقدم هذا البحث عرضا لاهمية أمن المعلومات في الجامعات ويعرض أهم التهديدات التي تواجهها أنظمة المعلومات في الجامعات، والاسباب التي تجعل الجامعات اكثر عرضة للتهديدات. ويَخلُص البحث الى ضرورة وجود وثيقة لسياسة أمن المعلومات في الجامعات، متبوعة بمجموعة من الإجراءات والتعليمات، والتي بدونها يصبح الالتزام بعدم إرتكاب الجرائم الحاسوبية أخلاقيات قد لا يلتزم الكثيرون بها او يُختلف حولها باختلاف التربية والثقافة. كما يعرض هذا البحث وثيقة أمن المعلومات لاحدى الجامعات ومجموعة من التوصيات.

الاستشهاد المرجعي

صاحب، محمود حسن. سياسة أمن المعلومات في الجامعات: حالة دراسية .- Cybrarians Journal .- ع 33، ديسمبر 2013 .- تاريخ الاطلاع <أكتب هنا تاريخ الاطلاع على المقال> .- متاح في: <أنسخ هنا رابط الصفحة الحالية>

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة ومتخصصة في مجال المكتبات والمعلومات

العدد 33، ديسمبر 2013

University Information Security Policy
Case study

Mahmoud Hasan Saheb

Dean of Information Technology and Computer Engineering College

Palestine Polytechnic University

alsaheb@ppu.edu

Abstract

This paper discusses the information security importance in the universities, and highlights the security threats that they are facing, and the reasons that makes the universities facing these threats. The paper discusses the importance of the existence of an Information Security Document, followed by set of regulations and procedures. Without these regulations, not committing any security criminal act becomes a matter of ethics which many people may have different views according to their culture. This paper presents an Information Security Document for one of the universities as a case study, followed by a set of recommendations.

Keywords: Information Security, Information Security Document, Information Security Management, ISO27000

مقدمة

يعرف أمن المعلومات بأنه حماية نظام المعلومات من التهديدات المقصودة وغير المقصودة. وللقيام بهذه المهمة يجب تحديد مكونات النظام، والتهديدات واتخاذ الإجراءات المناسبة لمنع هذه التهديدات، أو التقليل من ضررها على المؤسسة. يتكون النظام من المكون المادي والبرمجي والبيانات وأنظمة

قواعد البيانات والتطبيقات والشبكة والمستخدمين. وكل مكون قد يتعرض لمجموعة مختلفة من التهديدات.[9]

ويعرف التهديد بأنه اية حالة او حدث سواء أكان مقصوداً او غير مقصود يؤثر بصورة سلبية في النظام وبالتالي في المؤسسة. لا يمكن حصر التهديدات بصورة كاملة، لذلك يجب تحديد التهديدات الأكثر خطورة وإتخاذ الإجراءات المناسبة من حيث الكلفة لمنعها، أو التقليل من تأثيرها.

وعادة ما تظهر تأثيرات التهديدات على شكل:

- سرقة البيانات.
- انتهاك السرية.
- انتهاك الخصوصية.
- فقد تكامل البيانات.
- تعطل النظام.

الضوابط

الضوابط (Controls) هي الإجراءات المضادة للمخاطر. وهناك عدة أنواع من الضوابط:

1. ضوابط التوجيه والتي عادة ما تكون ادارية، مثل وضع سياسات، والمطالبة بالعمل بمقتضى هذه السياسات.
2. الضوابط الوقائية التي تحمي نقاط الضعف وتجعل الهجوم فاشلاً أو تَحدُ من آثاره، وتحتاج الى الرقابة المستمرة لعناصر النظام.
3. ضوابط الكشف، التي تؤدي لاكتشاف الهجمات.
4. الضوابط التصحيحية، والتي تقلل من تأثير هجوم أوتمنعه.
5. ضوابط الإنعاش، والتي غالبا ما ترتبط مع استمرارية الأعمال والتعافي من الكوارث.

وتكون الإجراءات المضادة معتمدة على الحاسوب أوغير معتمدة عليه، أما المعتمدة على الحاسوب فمنها:

- استخدام الصلاحيات و كلمات السر.
- النسخ الاحتياطي.
- تكامل البيانات.
- التشفير.
- استخدام أنظمة RAID.
- مضادات الفيروسات والرسائل المشبوهة.
- الجدران النارية.
- أنظمة المراقبة.

أما الإجراءات غير المعتمدة على الحاسوب فتشمل:

- الحماية المادية ومنع الوصول للنظام.
- استخدام أجهزة الإطفاء وإنذار الحريق.
- وضع الأجهزة في المكان المناسب.
- التدريب.
- الإجراءات الإدارية.

التهديدات في المؤسسات التعليمية

إضافة للتهديدات العامة التي وردت في المقدمة، تعَدُّ الجامعات والمراكز التعليمية بيئة خصبة لمهاجمة أنظمة المعلومات فيها. داخليا تحوي الجامعة عدداً كبيراً من الطلاب بمستويات مختلفة: بعض الطلبة بمستوى ضعيف يمكن ان يقوم بتخريب الأنظمة او الملفات او المعدات بدون قصد، والبعض الاخر بمستوى عالٍ، وتزداد معرفته مع تقدمهِ في الجامعة؛ فيبدأ بالبحث عن ثغرات في الأنظمة والشبكة المحلية التي بين يديه. وقد تكون المعلومات الموجودة في الجامعة محفزاً للطلبة الأذكياء لاثبات تفوقهم

بالوصول إليها للتباهي بقدرتهم بين زملائهم. وتعَدُّ سرقة الاجهزة مصدراً اخر للتهديد لا يمكن تجاهله، كما يلعب عدم وعي متخذي القرار بأهمية أمن المعلومات دورا سلبيا في توفير الموارد اللازمة.

تَستخدم معظم الجامعات برامج تقدم خدمة للطلبة بواسطة الشبكة العنكبوتية مثل: برامج التسجيل والتَعَلُّم الالكتروني وبالتالي فهي عرضة لقراصنة الشبكة العنكبوتية، حيث يمكنهم الاستفادة من السعة التخزينية العالية التى توفرها أجهزة الجامعة والسعة العالية لنقل البيانات. لا يتم إستثمار موارد كافية لحماية المعلومات في المؤسسات التعليمية، في منطقتنا، لاسباب متعلقة بالتكلفة بشكل رئيسي، أو لعدم الوعي الكامل بأهمية الموضوع في الإدارات العليا.

تَضم الجامعات العديد من الشبكات المحلية المرتبطة بكثيرٍ من الشبكات البحثية والمكتبات، وتُشَغل هذه الشبكات أنظمة تشغيل مختلفة وأنظمة معلومات بعضها مفتوح المصدر. هذا التنوع يشكل عقبة كبيرة للعاملين في ادارة الشبكات ويشكل منفذاً كبيراً للراغبين في العبث بهذه الشبكات والأنظمة العاملة فيها. لهذه الاسباب؛ فإن الجامعات تفقد الملايين من الملفات [4]، إضافة لتعرضها للعديد من التهديدات الاخرى.

نظراً لأهمية أنظمة المعلومات في تسيير العمليات اليومية للجامعة، وتأثير ذلك على جودة الخدمات المقدمة فإن على الجامعة ايلاء أهمية كبيرةٍ لحماية المعلومات لديها. إن وجود سياسات وإجراءات وضوابط متعلقة بأمن المعلومات يُساهم في تأمين تكامل وسرية وخصوصية وتوافر البيانات، وتساهم في تقديم الخدمات الجامعية بجودة عالية.

وعي الطلبة بأمن المعلومات وأخلاقياتها

يلعبُ وعي الطلبة بأمن المعلومات وأخلاقياتها دوراً مهماً في حماية الأنظمة العاملة [3,2]، حيث يُمثل الطلبة أكبر مجموعة من المتعاملين مع أنظمة الجامعات المحوسبة. وقد بينت إحدى الدراسات أن طلبة كليات العلوم الانسانية والعلوم الطبيعية اقل وعيا باخلاقيات أمن المعلومات من طلبة كليات

التكنولوجيا [1]، حيث يدرس طلبة كليات التكنولوجيا العديد من المساقات المتعلقة بتكنولوجيا المعلومات وأخلاقيات التعامل بالمعلومات.

سياسة أمن المعلومات في جامعة بوليتكنك فلسطين

تحدد هده الوثيقة تعريفا لسياسة أمن المعلومات في جامعة بوليتكنك فلسطين، كما تشمل مجموعة من الإجراءات المرتبطة بتنفيذ هذه السياسة وبخاصة المرتبطة بأمن البريد الالكتروني، وأمن الشبكة، وأمن التطبيقات وقواعد البيانات، وأمن كلمات السر، وأمن النسخ الاحتياطي. وقد تم تطوير الإجراءات باستخدام ISO27000 مع مراعاة خصوصية المؤسسة.

توصي وثيقة أمن المعلومات بضرورة إنشاء وحدة تُعنى بالبيانات في الجامعة تشمل وحدة مختصة بأمن المعلومات الالكترونية. وتوصي بان تكون وثيقة سياسة أمن المعلومات هي المرجعية في بناء القوانين والتعليمات الخاصة بأمن المعلومات وان لاتكون التعليمات ناتجة عن رد فعل لحدث او إختراق معين.

سياسة أمن المعلومات في جامعة بوليتكنك فلسطين

تلتزم جامعة بوليتكنك فلسطين، والتي تقع في مدينة الخليل، بالحفاظ على السرية والنزاهة وتوافر جميع الأصول المادية والمعلومات الالكترونية في جميع أنحاء المؤسسة من أجل المحافظة على قدرتها التنافسية والامتثال للاجراءات القانونية. ستستمرمتطلبات المعلومات وأمن المعلومات في التماشي مع اهداف الجامعة, حيث يمثل نظام المعلومات داعما أساسيا وآلية ملائمة لتبادل المعلومات في العمليات الالكترونية مع الحد من المخاطر الى مستويات مقبولة من خلال تحديد وادارة هذه المخاطر. ويتعين على جميع العاملين في المؤسسة الامتثال لهذه السياسة والتدابير الداعمة التي تطبق هذه السياسة. سيتم مراجعة هذه السياسة عند الضرورة و(على الأقل) مرة واحدة سنويا.

حدود سياسة أمن المعلومات في جامعة بوليتكنك فلسطين

حدود هذه السياسة مرتبطة بأنظمة المعلومات الالكترونية والمخاطر المحددة في بند تحليل المخاطر، وهي لا تتحدث عن الضوابط المتعلقة بالبيانات والوثائق الورقية. لا تشمل هذه الوثيقة إجراءات تفصيلية أو قوائم مراجعة (check lists)؛ لذلك على المعنيين متابعة هذه القوائم باستمرار؛ لأن هذة القوائم يطرأ عليها تعديلات كثيرة بشكل مستمر، ويمكن الوصول إلى هذه القوائم من الملاحق المرفقة مع سياسة أمن المعلومات.

تحليل المخاطر

تقدم الجامعة مجموعة من الخدمات الالكترونية للطلبة والعاملين، وتشمل خدمات القبول والتسجيل الالكتروني والتعلم الالكتروني وخدمات المكتبة. وتشمل العديد من الأنظمة مثل الموارد البشرية والمحاسبة والمخازن والعهد والمنح والقروض. كما يوجد العديد من مختبرات الحاسوب المستخدمة من قبل الطلبة والمرتبطة بشبكة محلية وشبكة الانترنت. وتستضيف خوادم الجامعة العديد من صفحات المراكز والدوائر اضافة لصفحة الجامعة الرئيسية.

بعد دراسة أنظمة المعلومات العاملة في الجامعة واجراء المقابلات، وأخذ التكلفة المالية بعين الاعتبار، تبين أن أهم المخاطر واكثرها تأثيرا مرتبطة بالمجالات التالية:

1- تطبيقات الانترنت وقواعد البيانات.
2- البريد الالكتروني.
3- الشبكة.
4- المواقع والأجهزة.
5- كلمات السر.
6- النسخ الاحتياطي.

السياسات والإجراءات

فيما يلي السياسات والإجراءات المرتبطة بالتهديدات التي تم تبيانها في تحليل المخاطر، وقد تم الاعتماد على (ISO 27000) في بناء هذه السياسات والإجراءات [8,7] ، وسيتم عرض سياسة أمن البريد الالكتروني كمثال:

Cybrarians Journal
ISSN 1687-2215
دورية إلكترونية فصلية محكمة ومتخصصة في مجال المكتبات والمعلومات
العدد 33، ديسمبر 2013

إسم السياسة	**أمن البريد الالكتروني**
ألمرجع	ISO-27000 (A10.8.1 & A.10.8.4)
الهدف	المحافظة على أمن المعلومات المتبادلة داخل الجامعة ومع أية جهة خارجية.
المراجعات	1- نسخة اولية، بتاريخ --\--\----، اسم المُراجع.
تاريخ الإقرار	--\--\----
التعريفات	ضوابط: إجراءات مضادة للمخاطر.
الضوابط	1- عمل سياسات رسمية واجراءات وضوابط لحماية تبادل المعلومات خلال استخدام البريد الالكتروني. 2- المعلومات المنقولة في الرسائل الإلكترونية محمية بشكل مناسب.
الإجراءات	1- فتح حسابات خاصة بالطلبة والعاملين، وحسابات اخرى خاصة بالإداريين. 2- وضع خطة سنوية لتطوير الأنظمة والعاملين في البريد الالكتروني. 3- متابعة وملاحقة أي استخدام خاطئ للبريد الالكتروني. 4- إلزام المستخدمين بالتوقيع على الالتزام بالتعليمات الخاصة باستخدام البريد الالكتروني. 5- وضع آليات للتعامل مع البريد المزعج(Spam). 6- تدريب الموظفين والطلبة.
المسؤوليات	
1- عام	1- يمنع منعا باتا إرسال رسائل البريد الإلكتروني أو اعادة توجيه رسالة تحتوي على تشهير أو قذف أو هجوم أو عنصرية بذيئة التصريحات. إذا تلقيت رسالة بالبريد الالكتروني من هذا النوع،

	يجب على الفور إخطار المشرف. 2- لا تُعد توجيه رسالة دون الحصول على إذن من المرسل الأول. 3- لا ترسل رسائل البريد الالكتروني غير المرغوب فيها. 4- لا تقم بتزوير رسالة او تحاول اعادة صياغتها. 5- لا ترسل رسائل البريد الإلكتروني باستخدام حساب شخص آخر عبرالبريد الالكتروني. 6- لا تقم بنسخ رسالة أو مرفق إلى مستخدم آخر دون الحصول على إذن من المُنشِئ. 7- لا تقم بتمويه أو محاولة إخفاء هويتك عند إرسال البريد. 8- لا تكشف كلمة السر الخاصة بك لأي شخص. 9- لا تسمح لأي شخص باستخدام بريدك الالكتروني. 10- لا تقم بإرسال رسالة مع مرفق كبير لمجموعة كبيرة من المستقبلين. 11- التأكد من الخروج من الحساب بعد إنهاء العمل. 12- لا تفتح رسالة تحوي عنواناً غريباً. 13- قم بحذف الرسائل التي لا يوجد داعٍ للاحتفاظ بنسخة منها. 14- لا ترد على الرسائل التي تطلب منك تعبئة اسم المستخدم وكلمة السر الخاصة بك. 15- يجب الرد على الرسائل خلال 24 ساعة. 16- يمكنك استخدام بريد الجامعة في المراسلات الخاصة بشرط الالتزام بالسياسات العامة، مع ضرورة وضع الرسائل الخاصة في ملف منفصل. 17- عدم استخدام البريد لعمليات الشراء بإسم الجامعة بدون إذن مسبق.

	18- عدم استخدام البريد الالكتروني في عمليات الشراء الخاصة.
10- مركز الحاسوب	1- استخدام الإجراءات الخاصة بالنسخ الاحتياطي حسب ما هو منصوص عليه في هذا المجال. 2- متابعة التنقلات الإدارية لنقل أو إلغاء الحسابات، بالتنسيق مع الموارد البشرية. 3- تركيب التحديثات المتعلقة بمستعرض الرسائل. 4- متابعة البريد المزعج. 4- حماية البريد المرسل والمستقبل من الفيروسات. 6- عقد دورات تدريبية للتعامل مع البريد الالكتروني.
11- مشرفو المختبرات	1- التأكد من الخروج من الحسابات بعد خروج المستخدم من المختبر.
12- الموظفون	1- إذا كانت المعلومات المرسلة سرية فيجب حماية الملف المرسل بكلمة سر. ويجب إبلاغ الجهة المتلقية بان محتوى الرسالة سري، وانه اذا تلقاها بشكل خاطيء فعليه حذفها فورا. 2- عليك استخدام حسابك الخاص للمراسلات المتعلقة بك كشخص، واستخدام البريد الخاص بالمركز الإداري للمراسلات المتعلقة بهذا المركز.
13- الطلاب	1- الالتزام بالتعليمات الخاصة بالبريد الالكتروني.

مسؤولية قانونية	يُعَدُّ البريد الالكتروني احدى وسائل الاتصال الرسمية، ويُعَدُّ من أملاك الجامعة، والقيام بإساءة إستخدامه تعرضك للمساءلة القانونية في الحالات التالية: 1- انتحال شخصية أخرى. 2- إرسال أو اعادة توجيه بريد يحوي تشهيراً او قذفاً او الفاظاً بذيئة. 3- ارسال رسائل تحوي فيروسات. 4- تزوير محتوى بريد الكتروني. 5- تسريب حسابات وكلمات سر بشكل متعمد.

خاتمة

نظراً لأهمية المعلومات في المؤسسات التعليمية وارتباطها بعدد كبير من الطلبة، ونظراً لأهمية أنظمة المعلومات في إتخاذ القرارات فعلى أصحاب القرار إتخاذ الإجراءات الكفيلة بحماية المعلومات من خلال بناء وحداتٍ إدارية وسياسات واجراءات خاصة. آخذين بعين الاعتبار التوصيات التالية:

1- انشاء وحدة ادارية تُعنى بأمن المعلومات الالكترونية كجزء من وحدةٍ اشمل تُعنى ببيانات المؤسسة. فأمن المعلومات ليس قضية تقنية بحتة، بل هو موضوع اداري ثقافي تقني.
2- اصدار وثيقة لأمن المعلومات، متبوعة بمجموعة من التعليمات والقوانين التي تتوافق مع السياسات. ومراجعة السياسات والتعليمات بصورة دورية، بحيث تكون الإجراءات نتيجة لسياسة واضحة وليست ردة فعلٍ لحدث معين.
3- توعية الطلبة وموظفي الجامعة بأهمية أمن المعلومات ومخاطر وعواقب تجاهل أهميتها، وضرورة لفت نظر متخذي القرار لأهمية الموضوع.
4- توفير المعدات والبرمجيات اللازمة.
5- توفير دورات تقنية دورية في مجال أمن المعلومات في ظل التطور السريع.

6- مراعاة التوازن بين التهديدات والإجراءات المضادة والتكلفة وسهولة الوصول.

شكر:
اود تقديم الشكر الجزيل لكل من ساهم في اعداد سياسة أمن المعلومات في جامعة بوليتكنك فلسطين. واخص بالذكر كلاً من السادة: اياد الهريني، وطارق التميمي، وعلي رمضان، ورضوان طهبوب، وزياد شاور، ومحمد ابو سنينة، ووائل عواد، ومحمد سلهب.

المراجع:

1- Max North et. al. (2010), "A Comparative Study Of Information Security And Ethics Awareness In Diverse University Environments", Journal of Computing Sciences in Colleges, Volume 25 Issue 5, May 2010, Pages 223-230.
2- Foster, A (2004). "Insecure and Unaware. Chronicle of Higher Education", 50(35), A33-A35.
3- North, M., North, S., George, R.(2006), "Computer Security and ethics awareness in university environments: A challenge for management of information systems", ACM SE'06, 434-439, doi 10.1145/1185448.1185544
4- Aanval Wiki, "Network Security Challenges Causing Underestimated Attacks Among Educational Institutions", Viewed 24 may 2012, http://wiki.aanval.com/wiki/Library:Network_Security_Challenges_Causing_Underestimated_Attacks_Among_Educational_Institutions#The_Underestimated_Threats_Among_University_Campuses
5- Zubair Baig (2011), أمن المعلومات في الجامعات السعودية http://conf2.mohe.gov.sa/UIS/Pages/Papers_of_the_workshop.aspx
6- Lauren May and Tim Lane (2006), "A Model for Improving e-Security in Australian Universities", Journal of Theoretical and Applied Electronic

Commerce Research, ISSN 0718–1876 Electronic Version, VOL 1 / ISSUE 2 / AUGUST 2006 / 90 – 96
http://www.jtaer.com/aug2006/may_lane_p8.pdf

7- ISO 27000 Directory, http://www.27000.org

8- Alan Calder & Stew Watkins (2008), Kogan, "IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002, "، 4th Edition, Page 8

9- Thomas Connolly and Carolyn Begg (2006), "Database Systems: A Practical Approach to Design, Implementation and Management", (5th Edition), Addison Wesley