العنوان:	ندوة حول : سياسة امن المعلومات
المصدر:	مجلة المصرفي
الناشر:	بنك السودان المركزي
المؤلف الرئيسي:	خير، بشرى خير الحاج
المجلد/العدد:	ع 54
محكمة:	لا
التاريخ الميلادي:	2009
الشهر:	ديسمبر
الصفحات:	46 - 47
رقم MD:	80655
نوع المحتوى:	بحوث ومقالات
قواعد المعلومات:	EcoLink
مواضيع:	الحاسبات الإلكترونية، أمن المعلومات، تكنولوجيا المعلومات، العمليات المصرفية الإلكترونية، التنمية الادارية، تكنولوجيا الاتصالات، الانترنت، البرمجيات، المخاطر، الندوات
رابط:	http://search.mandumah.com/Record/80655

ندوة حول: سياسة أمن المعلومات

رصد ومتابعة: بشري خير الحاج خير
الإدارة العامة للسياسات والبحوث والإحصاء

في إطار خطتها الرامية لتطوير وحماية وأمن المعلومات، نظمت الإدارة العامة لتقنية المعلومات ندوة بعنوان السياسة التأمينية للمعلومات استهدفت بها الإدارة العامة للسياسات والبحوث والإحصاء. حيث حضرها موظفي الإدارة العامة للسياسات والبحوث والإحصاء. افتتح الندوة السيد جمال عبد الرحيم مدير إدارة التقنية المصرفية مستعرضاً أهم النظم التقنية المستخدمة في البنك وموضحا أن البنكً يمتلك بنية تحتية من شبكات وبرامج ونظم تضاهيً تلك التي توجد في الدول المتقدمة كنظام" symbol" والمقاصة الالكترونية ونظام التسويات الآنية الإجمالية " RTGS" بالإضافة إلى عدد آخر من النظيمات الصغيرة والتي تصل إلى عشرة أو اكثر كنظام الحضور والانصراف...الخ .مشيراً إلى أن امتلاك هذا العدد من النظم والبرمجيات في شبكة كًبيرة تبلغ سعتها ما يزيد على 1200 شخصاً متصلة داخلياً وخارجياً، الأمر الذي يحتم على الإدارة بذل مجًهود كبير لتأمينًها من االمخاطر حاثاً الجميع على التعاون لتحمل المسؤولية التى قد تتجاوز ادارة التقًنية لتشمل كل ادارات البنك، ومنوهاً لأهمية زيادة الوعي بأمن المعلومات بضرورة الحرص على المعرفةً والتواصل مع إدارة التقنية في حالة المشاكل التى تواجههم أثناء العمل. ومشيراً إلى أن الهدف من السياسة التأمينية يتلخص في تعريف المستًخدمين والإداريين بالتزاماتهم وواجباتهم المطلوبة لحماية نظم الكمبيوتر والشبكات، وكذلك حماية المعلومات بكافة أشكالها في مراحل إدخالها ومعالجتها وتخزينها ونقلها وإعادة إسترجاعها. بالإضافة إلى تحديد الأجهزة الإلكترونية التي يتم من خلالها تحقيق وتنفيذ الواجبات لكل من له علاقة بالمعلومات ونظمها وتحديد المسؤوليات عند حدوث الخطر. وبيان الإجراءات المتبعة لتجاوز التهديدات والمخاطر والتعامل معها والجهات المناط بها القيام بذلك.

قام بتقديم الندوة المهندس عمار أيوب احمد، حيث تركز حديثه في ثلاثة محاور رئيسية تمثلت في التعريف بأمن وسياسة أمن المعلومات والتعريف بالمخاطر والتهديدات ونقاط الضعف وأنواع الهجمات والاعتداءات وأساليبها التقنية وطرق الحماية عند حدوث الاعتداءات والأساليب الاحترازية لمنع الاعتداءات. واختتم حديثه بأهم الحقائق التى يجب على الجميع الاهتداء والعمل بها في كل الأحوال.

وقد استخدم مقدم الندوة في توضيح فكرته العروض التقديمية بالإضافة إلى الاستعانة بفيلم وثائقي يوضح ويوثق لكيفية حدوث التحايل واختراق المؤسسات والنظم، الأمر الذي أدى إلى حسن المتابعة والإصغاء والتفاعل من الحضور. يمكن تلخيص أهم ما جاء في العرض التقديمي في المحاور التالية:

أولا: التعريف بأمن وسياسة المعلومات:

1. عًلم أمن المعلومات:

يعرف من الزاوية الأكاديمية بأنه العلم الذي يبحث في توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. أما من الناحية التقنية فهو عبارة عن مجموعة الوسائل والأدوات والإجراءات اللازم توافرها لضمان حماية المعلومات من المخاطر الداخلية والخارجية. أما من الزاوية القانونية فهو العلم الذي يهتم بوضع التشريعات لحماية المعلومات من الأنشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها "كجرائم الكمبيوتر والإنترنت."

2. سياسة أمن المعلومات وكيفية بناءها:

هي عبارة عن مجموعة القواعد التي يطبقها الأشخاص لدى التعامل مع التقنية ومع المعلومات داخل المنشأة وتتصل بشؤون الدخول إلى المعلومات والعمل على نظمها وإدارتها. والتي لابد أن يساهم في إعدادها وتفهمها وتقبلها وتنفيذها كل من: مسؤولي أمن الموقع، مديري الشبكات، وموظفي الكمبيوتر، فريق الإستجابة للحوادث والاعطاب، وممثلي مجموعات المستخدمين، ومستويات الإدارة العليا.

3. متى توصف سياسة أمن المعلومات بأنها ناجحة؟

يرتبط نجاح السياسة إذا كانت تحتوي على درجة عالية من التعميم، القبول، الواقعية، توفر الأدلة والتوجيهات والإرشادات والوضوح.

4. ما هي منطلقات أساس سياسة أمن المعلومات:

تتركز في الحرص على الإجابة على الأسئلة آلاتية. ماذا أريد أن أحمي؟ من ماذا أحمي المعلومات؟ كيف أحمي المعلومات؟ وهنا يجب التمييز بين معلومات لا تتطلب الحماية وقد يصلها من يشاء ومعلومات يصل إليها أشخاص معينين ومعلومات سرية للغاية يصلها شخص معين.

5. مناطق ومستويات أمن المعلومات:

تشمل أمن الاتصالات وأمن الكمبيوتر بكل مستوياته والمتمثلة في الحماية المادية، الحماية الشخصية، الحماية الإدارية، الحماية الإعلامية – المعرفية.

6. عناصر أمن المعلومات:

- السرية أو الموثوقية Confidentiality"": التأكد من أن المعلومات لا تكشف ولا يطلع عليها من قبل أشخاص غير مخولين بذلك.
- التكاملية وسلامة المحتوى "Integrity": التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو العبث به في أية مرحلة من مراحل المعالجة.

- استمرارية تدفق المعلومات أو الخدمة "Availability": التأكد من استمرار عمل النظام المعلوماتي وتفاعله معه، وأن مستخدم المعلومة لن يتعرض إلى منع استخدامه لها أو دخوله إليها.
- عدم إنكار التصرف المرتبط بالمعلومات ممن قام به"Non-Repudiation": ويقصد به ضمان عدم إنكار الشخص الذي قام بتصرف ما متصل بالمعلومات أو مواقعها.

7. سياسة أمن الإنترنت:

تنصب أساسيات أمن المعلومات في حقل تحقيق أمن الإنترنت على مواضع ثلاث تشمل: أمن الشبكة، أمن التطبيقات، وأمن النظم.

ثانيا: المخاطر ونقاط الضعف وأنواع الهجمات وأساليبها التقنية:

1. المخاطر:

تتجه المخاطر والاعتداءات إلى الأجهزة والمعدات والأدوات المادية التي تتكون منها النظم، كالخدمات" Servers" والطابعات "Printers" ومكوناتها الداخلية ووسائط التخزين المادية والبرامج وكافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها بالإضافة إلى الإتصالات والتي تشمل شبكات الإتصال التي تربط أجهزة الحاسوب بعضها ببعض محلياً وإقليمياً ودولياً، وتنتج هذه المخاطر عادة من الآتي:

- انقطاع المصدر كهربائي عن الكمبيوتر.
- سوء استخدام كلمة المرور.
- اختراق الأنظمة.
- الاعتداء على حق التخويل.
- زراعة نقاط الضعف.
- مراقبة الاتصالات
- اعتراض الإتصالات.
- إنكار الخدمة.
- عدم الإقرار بالقيام بالتصرف.

2. نقاط الضعف "Vulnerabilities":

وتعني عنصر أو نقطة أو موقع في النظام يحتمل ان ينفذ من خلاله المعتدي أو يتحقق بسببه الاختراق. أوهي الأسباب المحركة لتحقيق التهديدات أو المخاطر كالأشخاص الذين يستخدمون النظام ولم يكن لهم تدريب كاف. الاتصال بالإنترنت إذا لم يكن مشفراً. الموقع المكاني للنظام إذا لم يكن غير مجهز بوسائل الحماية. لذا يجب ان تكون هناك الوقاية Countermeasures"" هي الوسيلة الأنجع للتغلب على نقاط الضعف.

3. الهجمات"Attacks":

اصطلاح لوصف الاعتداءات بنتائجها أو بموضع الإستهداف، ويستخدم كإصطلاح مرادف للهجمات، وإصطلاح الإختراقات أو الإخلالات" Breaches" من أمثلة الهجمات: هجمات إنكار الخدمة، هجمات إرهابية، هجمات البرمجيات، هجمات الموظفين المستائين، الهجمات المزاحية والهجمات الحاقدة.

ثالثا: وسائل الأمن التقنية:

1. توَفر خطط احترازية
2. توفر الإجراءات ومراحل تنفيذها.
3. استخدام كلمة السر" Password".
4. وضع سياسات وضوابط للدخول للشبكة.
5. الجدران النارية" Firewalls".
6. التشفير"Cryptography" .
7. نظام تحري الاختراق "Intrusion IDS-Detection System".
8. نظام منع الاختراق "Intrusion Prevention System" .
9. برمجيات مقاومة الفيروسات" Antiviruses".

وخلاصة القول انه لا بد من توفر نظام متكامل للتعامل مع المخاطر والحوادث والاعتداءات، ويعد ذلك مطلباً رئيسياً بالنسبة لمؤسسات الأعمال كما في حالة البنوك والمؤسَّسات المالية، وان يعلم الجميع الحقائق الآتية:

الحقيقة الأولى:

- علينا أن ندرك إبتداءاً أن الكمبيوتر الآمن على نحو مطلق هو فقط الكمبيوتر الذي لَم يوصل بعد بمصدر الكهرباء.

الحقيقة الثانية:

- إن تحديد المخاطر والثغرات والإعتداءات عملية مستمرة، يوماً بعد يوم، وهي هنا ما يميز خطط الأمن بعضها عن بعض.

الحقيقة الثالثة:

- أنه لا يوجد مؤلف أو باحث أو مرجع يقدم قائمة شاملة للمخاطر والاعتداءات وثغرات الحماية لان الهجمات تمتد عبر طريق يضم أكثر الأشخاص إحترافاً للجريمة مع أكثرهم بساطة، ويضم هواة وخبراء، ويضم حَاقدين وحسني النية، ويضم جواسيس يلفظهم المجتمع.