المنظمة العربية للتنمية الصناعية والتعدين
المؤتمر العربي الدولي السادس لتكنلوجيا المعلومات
تكنلوجيا المعلومات :وسيلة لمواكبة التطور والابداع
المملكة المغربية
29-31 اكتوبر 2013

حماية نظم المعلومات ودورها في سلامة المعاملات الالكترونية في المنظمات الصناعية

د. سناء عبدالكريم الخناق

UTM- Razak School of Engineering and Advanced Technology
Universiti Teknologi Malaysia
Jalan Semarak, 54100 Kuala Lumpur MALAYSIA

مشكلة البحث

ما هي التهديدات والخروقات الامنية الداخلية والخارجية التي تواجه المنظمات االصناعية والتي تقف كحاجز امام استخدامها لنظم تكنلوجيا المعلومات الصناعية ؟ وكيف يمكن حماية هذه الانظمة؟

- ما هي انواع المخاطر والتهديدات التي تواجه التعاملات في منظومة تكنلوجيا المعلومات الصناعية؟
- ما هي الاستراتيجيات التي يمكن للمنظمة الصناعية صياغتها للتصدي للمخاطر والتهديديات لحماية منظومة تكنلوجيا المعلومات فيها؟
- ماهي الاجراءات التي يمكن اتخاذها لضمان حماية التعاملات الالكترونية في المنظمات الصناعية؟

لغرض الاجابة على تساؤلات البحث تم تحديد الاهداف التالية

- التعرف على ماهية وانواع نظم تكنلوجيا المعلومات المستخدمة في المعاملات الالكترونية للعمليات الصناعية.
- تسليط الضوء على اهم انواع المخاطر والتهديدات الامنية التي تواجه المعاملات الالكترونية لمنظومة المعلومات الصناعية.
- التعرف على اهم الاستراتيجيات الحماية الوقائية التي يمكن اتخاذها كخطوة استباقية لمنع حدوث الاختراقات الالكترونية.
- التعرف على الاستراتيجيات العلاجية المبنية على احتمالية حدوث التهديديات التي تواجه أمنية تكنلوجية المعلومات المستخدمة في المنظمات الصناعية.
- تحديدالاستراتيجيات القانونية لحماية أمنية نظم المعلومات الصناعية.
- التوصية بالآلية التي لابد للمنظمات الصناعية في الوطن العربي اعتمادها في حالة اعتماد تكنلوجيا المعلومات في انظمتها التصنيعية مع ضمان امنيتها وسلامتها وبما يضمن الاستفادة القصوى من التحكم الكفوء بعملية الانتاج.

بعض التجارب لاختراق الابعاد الامنية لنظم المعلومات الصناعية

- في كانون الثاني عام 1998 قام بعض المهاجمين المجهولين الخارجيين باختراق مركز التحكم المركزي لنظام خطوط الانابيب لشركة Gazprom لفترة من الزمن والتحكم في التدفق في خط الانابيب

- في اذار عام 2000 تمكن احد المقاولين الساخطين من الوصول الى نظام السيطرة لمحطة معالجة مياه مجاري في مدينة Maroochy Shire in Queensland، وقام باغراق المنطقة المحيطة بملايين اللترات من مياه الصرف الصحي غير المعالجة

- في كانون الاول 2000 قام المهاجمون باختراق شبكة الحاسوب في احدى محطات توليد الطاقة عبر بروتوكول تبادل البيانات غير المضمونة (الامينة)، حيث تم استخدام الحواسيب المضيفة في لعب بعض الالعاب الحاسوبية عبر الشبكة المتصلة بالحاسوب. ان استخدام موارد الحاسوب وتردات الشبكة قد عمل على اعاقت العمل في المحطة

- في كانون الثاني 2003 اصيب نظام الرصد الامني للمحطة النووية Davis-Besse بنوع من الهجوم Slammer worm التي تجاوزت الجدران النارية Firewall لنظام الحاسوب المحمول للشركة المقاولة الذي كان متصل – عبر المودم – بشبكة المحطة الشركة المؤسسة

- في تموز 2003 في احدى شركات السكك الحديدية الامريكية CSX اصبت ب(Worm) لشبكة الاتصلات المستخدمة في الشركة، وقد استخدم ذلك في اعطاء اشارة الى جميع القطارات بالتوقف لنصف يوم

أهداف استخدام نظم تكنلوجيا المعلومات في المنظمات الصناعية

انواع تكنلوجيا المعلومات المستخدمة في العمليات الصناعية

الروبوتات	أجهزة الكمبيوتر	التصميم بمساعدة الحاسوب
نظم التصنيع المرنة	التصنيع بمساعدة الحاسوب	المحاكات بالحاسوب

(Business 101, 2013)

المخاطر الامنية التي تواجه المعاملات الالكترونية في المنظمات الصناعية

مفهوم أمنية نظم المعلومات الصناعية

وهي مجموعة السياسات والاجراءات والتدابير التقنية المستخدمة لمنع الوصول غير المصرح به والتعديلات والسرقة، او الاضرار المادية لنظم المعلومات (Loudoun & Loudoun,2007)، (O'brien, 2011)

- وتحتاج عملية الحفاظ على أمن المعلومات الى الرصد المستمر (ISCM) وهي عملية الحفاظ على التوعية المستمرة على أمن المعلومات، وتحديد نقاط الضعف والتهديدات لدعم القرارات التنظيمية لإدارةالخطر (National Institute of Standards and Technology (2011

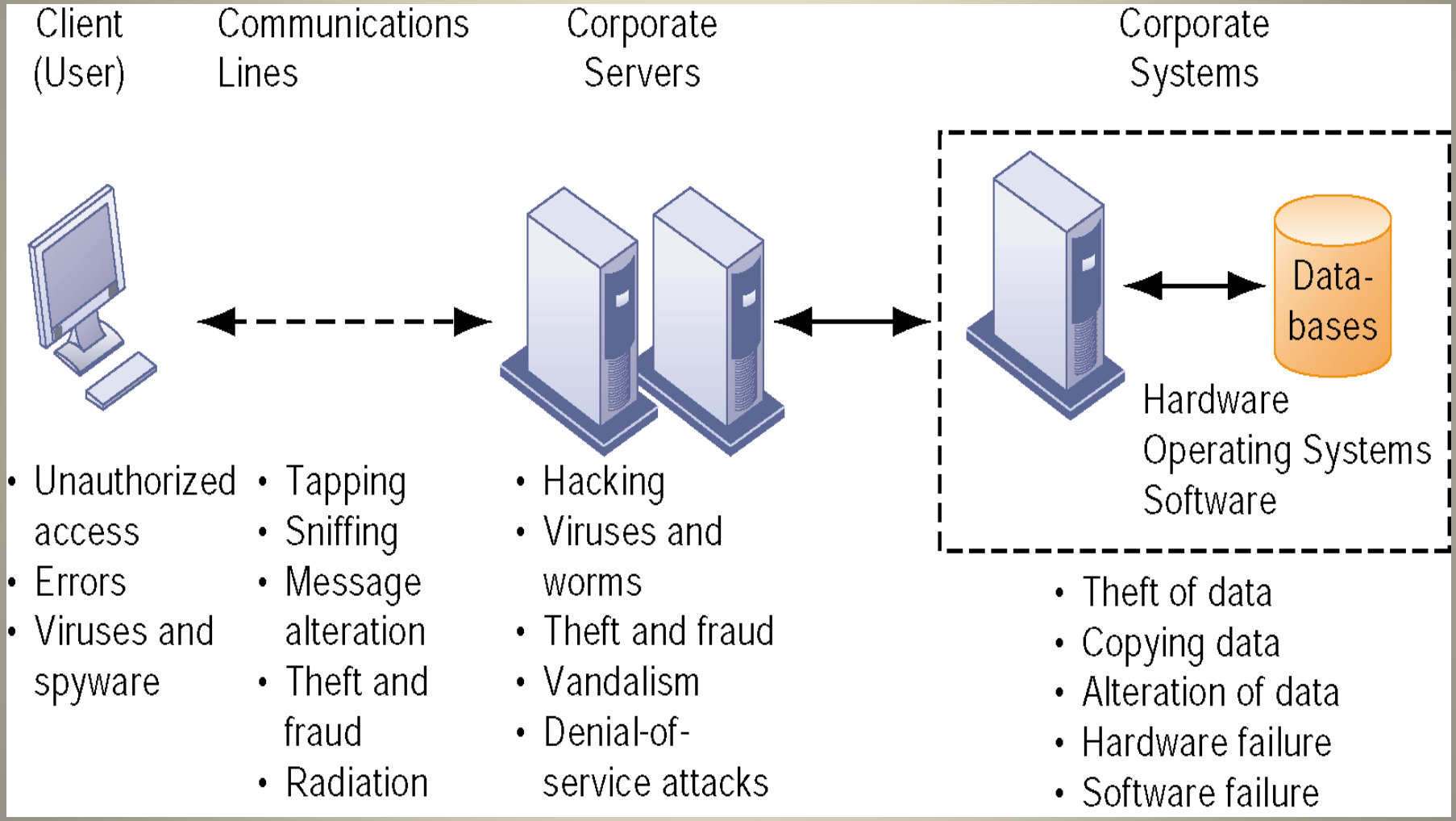
امنية نظم تكنلوجيا المعلومات للمنظومات الصناعية

الابعاد

- **السرية (الموثوقية) Confidentiality**
- **السلامة (التكامل) Integrity**
- **الاتاحية (التوفر) Availability**
- **الترخيص Authorization**
- **المصادقة Authentication**
- **القابلية للتدقيق Auditability**
- **عدم الإنكار Non-repudiation**
- **حماية الطرف الثالث Third party protection**

(Naedele and Dzung, 2005)

اهم التحديات التي قد تتعرض نظم المعلومات الصناعية



(Loudoun & Loudoun,2007)

انواع الهجمات الامنية حسب تسلسل مراحل نظام المعلومات

- مرحلة دخول المستخدم
- مرحلة الانتقال عبر خطوط شبكة الاتصالات
- مرحلة الشراكة في الحواسيب الخادمة
- الانظمة المتشاركة

التكتيكات الشائعة المستخدمة الهجمات الامنية

اولا: القرصنة

- المتشمم Sniffer:
- الخداع او التحايل Spoofing
- حصان طروادة Trojan
- التطبيقات الخبيثة Malicious Applets
- حرب التلفنة War Dialing
- تجاوز سعة المخزن المؤقت Buffer Overflow
- كلمة الكراكرز Password Crackers
- الهندسة الاجتماعية Social Engineering
- الغوص في حاوية النفايات Dumpster Diving
- ثانيا: الإختلاس عبر الانترنت
- ثالثا: الاستخدام غير المصرح به في العمل
- رابعا: الانتهاكات للإنترنت في مكان العمل
- خامسا: قرصنة البرامجيات
- سادسا: سرقة الملكية الفكرية
- سابعا: الفيروسات والديدان Viruses and worms

استراتيجيات أمنية المعاملات الالكترونية في المنظمات الصناعية

اولا: الاستراتيجية الوقائية

- وهي الاستراتيجيات التي تحدد أفضل الممارسات في مجال التصدي للتهديدات التي تواجه نظم المعلومات الصناعية

- تقييم المخاطر
- وضع سياسات امنية
- التدقيق
- التخطيط لمواجهة الطوارئ والكوارث وضمان استمرارية الأعمال
- الاستعانة بمصادر خارجية لتوفير الامن
- استخدام التقنيات والأدوات الامنية المحدثة
- التحكم بالدخول
- استخدام الجدران النارية وأنظمة كشف الاختراقات، وبرامج ضد الفايروسات
- نظم كشف التسلل

استراتيجيات أمنية المعاملات الالكترونية في المنظمات الصناعية

ثانيا: الاستراتيجيات العلاجية

وهي الاستراتيجيات التي تحدد الاجراءات التي تتخذ في حالة حدوث تمزق أو تهديد بالتمزق في اي جزء من نظام معلومات الشركة، حيث يجب ان تعد الشركة ترتيبات وقائية في حالة تدمير الموارد والتسهيلات المستخدمة وتلفها وجعلها غير صالحة للاستخدام

- **التكرار Redundancy**
- **التنوع Diversity**
- **التحركية Mobility**
- **خطة الطوارئ Emergency Plan**
- **خطة السجلات الحيوية The Vital Records Plan**

(مكليود، 1999)

استراتيجيات أمنية المعاملات الالكترونية في المنظمات الصناعية

ثالثا: الاستراتيجية القانونية

توفير خدمات تضمن امنية المعلومات الصناعية يستدعي معها فهم بيئة المخاطر القانونية، بالاضافة الى ضرورة معرفة المشاريع الصناعية المستقبلية على المدى الطويل وفهم العمليات القانونية التي تنطوي عليها، وكيف يمكن للمنظمة تجنب المزالق القانونية المحتملة عن طريق وضع خطة عمل استباقية للمنظمة في حالة تعرضها الى مثل هذه المشاكل.

ومن اجل تطوير وتنفيذ الاستراتيجيات القانونيةلابد من وضع ثلاثة مستويات من التخطيط وهي

(Malaysia Cyber Security Center, 2006)

- المستوى الاستراتيجي،
- المستوى التكتيكي،
- المستوى التشغيلي

الاستنتاجات

من خلال المحاور السابق ذكرها يتبين

- أن أنظمة المعاملات الالكترونية في المنظمات الصناعية شهدت في السنوات الماضية زيادة كبيرة في استخدام الشبكات الحاسوبية وتقنيات الإنترنت ذات الصلة لتبادل المعلومات في المعاملات الالكترونية كالاعمال الإشرافية والادارية داخل المنظمات التصنيعية بشكل عام وفي العمليات التصنيعية والتحكم بها بشكل خاص.
- وبما يسمح لتحقيق وفورات كبيرة في التكاليف وتحسين التواصل مع كافة الجهات المعنية في الصناعة.
- وبالرجوع الى تقييم تجارب بعض الشركات وفي دول مختلفة تظهر بوضوح المخاطر الامنية لاستخدام تكنولوجيا المعلومات وخاصة المعتمدة منها على الإنترنت. الا انه وبذات الوقت فان التخطيط السليم الطويل الاجل يمكن التخفيف من تلك المخاطر.
- والأكثر أهمية من ذلك هو وضع الاستراتيجيات الأمنية سواء منها الوقائية او العلاجية او القانونية، والتصميم الدقيق للبنية التحتية لتكنلوجيا المعلومات الصناعية.

التوصيات

اولا: استحداث او تحديث وحدة ادارية لامنية المعلومات الصناعية

من اجل ان تقوم المنظمات العربية من تحقيق ميزة تنافسية من خلال استخدام تكنلوجيا المعلومات الصناعية – دون ان اعاقة من التهديدات والخروقات الامنية السابقة الذكر– لابد لها ان ان تقوم باستحداث ادارة متخصصة يطلق عليها

ادارة امنية المعلومات الصناعية.

التوصيات

ثانيا: تحديد المهام التي تقوم بها ادارة امنية المعلومات الصناعية

- تتولى هذه الادارة القيام برسم كافة الاستراتيجيات والسياسات الوقائية والرقابية واحيانا حتى القانونية، اللازمة لحماية نظم المعلومات فيها، للقيام بالحفاظ على امن وسرية المعلومات من التهديدات الخارجية والداخلية، بالاضافة الى السياسات والقرارات التي يمكن تنفيذها في حالة حدوث خروقات مقصودة او غير مقصودة في المنظومة المعلوماتية والحاسوبية في المنظمة، مع التقييم المستمر لتحقيق الاهداف الامنية. وتقوم الادارة ايضا بتنفيد، إدارة، مراقبة وتصحيح، وصيانة وتحسين نظام ادارة أمن العلومات فى سياق الأنشطة العامه للمنظمة والمخاطر التى تواجهها.

التوصيات

ثالثا: الارتباط الاداري ادارة امنية المعلومات الصناعية

- ويمكن ان تضاف مهمة ضمان ورعاية امن المعلومات الصناعية كاحدى واجبات المدير التنفيذي للمعلومات في الشركة Chief Information Officer

- بالنسبة للمنظمات التي لا تتواجد فيها هذه الوظيفة فيمكن تعيين مدير قسم متخصص يتمتع بالمهارات التصورية للتهديدات التي تواجه انظمة المعلومات الصناعية، وكذلك يتمتع بالقدرات اللازمة للتعامل مع انشطة ادارة البيانات والمعلومات، ويكون هذا القسم ضمن ادارة العمليات الصناعية

- اما في المنظمات الكبيرة فيتم استحداث وظيفة مدير لتخطيط الطوارئ Manager of Contingency Planningالذي تكون مسؤوليته تخطيط الطوارئ التي توفر مستوى معقول من الامن من مجرمي الحاسوب والكوارث الطبيعية

التوصيات

رابعا: المعايير والمنهجية المتبعة ادارة امنية المعلومات الصناعية

- تقدير الجهد المطلوب لتنفيذ وصيانة وتشغيل آلاليات والعمليات الأمنية الازمة.
- تحديد الأهداف الأمنية للمصنع، وكذلك الوظائف والتدابير والتكامل مع الانظمة التصنيعية التي توفيرها من قبل بائعي هذه النظم.
- مقارنة تغطية التهديدات وتكلفة الحلول الأمنية المقدمة.
- تنفيذ وتشغيل آلية امنية فعالة عبر المحطات والمواقع المتعددة في المؤسسة.
- التاكيد على أن الدفاع ضد التهديدات القائمة على نظم تكنولوجيا المعلومات يتوافق مع افضل الحلول المطروحة لحل المشكلة.
- ان التكامل بين العمليات التصنيعية الالية وادارة الشركة تستدعي توفير انظمة امنية تمكن النظام
  - من توقع المتطلبات الأمنية وتطوير الوظائف ذات الصلة.
  - إنشاء معمارية أمنية يمكن إعادة استخدامها عبر عدة مشاريع. هذا يقلل من التكاليف في كتابة المقترحات، والهندسة، والمشتريات للأجهزة الأمنية وتطبيقاتها

التوصيات

خامسا: الآلية الواجب القيام بها لضمان تحقيق ادارة امنية المعلومات الصناعية لاهدافها

- مرحلة وضع الخطة
- مرحلة الفعل
- مرحلة التحقق
- مرحلة العمل


شكراً جزيلاً