أمن الحاسبات والمعلومات
الفصل السادس: التهديدات

إعداد الدكتور / أسامة حسام الدين

كلية علوم وهندسة الحاسبات بينبع
جامعة طيبة

محتوى الفصل السادس

- نقدم في هذا الفصل التهديدات على نظم المعلومات وبنية المعلومات للشركات والأفراد وتقسم إلى 12 بند

1. الخطأ البشري
2. سرقة حقوق الملكية الفكرية
3. التسلل (تخطي الحواجز الأمنية)
4. الابتزاز والفدية
5. التخريب المتعمد
6. السرقة
7. البرمجيات الخبيثة
8. قوى الطبيعة
9. تدني كفاءة مزودي الخدمة
10. مشكلة في العتاد
11. مشكلة في البرامج
12. النظم العتيقة

تعريف التهديد

التهديد: الخطر الذي يحوم حول الممتلكات المعلوماتية. مثل انقطاع الكهرباء والسرقة

- **الثغرات:** هي ضعف في النظام يمكن أن يتم استغلاله من قبل التهديد. يقوم التهديد ببناء مستغل (بكسر الغين) لاستغلال الثغرة. كل الثغرات المتعلقة بممتلك ما تسمى **سطح الهجوم**. على سبيل المثال سطح الهجوم المتعلق بنظام التشغيل ويندوز عند عدم تحديثه.
- **المستغل:** الميكانيكية المستخدمة في استغلال الثغرة للوصول إلى الممتلك
- **المخاطرة:** تقيس احتمالية وجود **الهجوم** وهو احتمالية أن يقوم التهديد باستغلال الثغرة للوصول للممتلك والحصول على ما يريد.

تعريف التهديد

التهديد: هو الوحدات البرمجية أو الأشخاص أو الكيانات والتي تشكل خطرا دائما على الممتلكات المعلوماتية

- يجب أن تحدد الإدارة كل التهديدات المحتملة التي تواجه الشركات والأفراد.
- بعد تحديد كل التهديدات الممكنة يمكن للإدارة أن تقوم بحماية المعلومات من خلال انشاء سياسات في الشركة أو التدريب أو استخدام تقنيات وأدوات الحماية.

كمثال: تعرف الشركة ان نظام التشغيل ويندوز اكس بي به ثغرات كثيرة. تقوم الإدارة بتحديد التهديدات المحتملة على الشركة والتي ستستغل تلك الثغرات. كمن يريد الاستيلاء على حقوق الملكية الفكرية أو سرقة بيانات الشركة.

1 الخطأ البشري

- يقوم الشخص بالخطأ عن غير قصد. على سبيل المثال بإزالة بيانات حساسة أو تسريب معلومات. يتم ذلك بسبب:
  - قلة الخبرة
  - سوء التدريب
  - الفرضيات الغير صحيحة
- الأخطاء تشمل:
  - تسريب معلومات حساسة
  - إدخال معلومات خاطئة
  - حفظ ملفات في أماكن غير آمنة.
- بنظرك من هو الأكثر خطورة, الموظفة، الهاكر، السارق؟


هاكر

2 سرقة حقوق الملكية الفكرية

- بيانات الملكية تحتوي على الابتكارات والأفكار الجديدة لتطوير الشركة مثل **براءات الاختراع**، وأفكار لابتكار المنتجات الجديدة. يجب تسجيل براءات الاختراع في قنوات التسجيل الخاصة بذلك لحمايتها.
- شركات انتاج البرمجيات أيضا تحتاج إلى حماية برامجها ضد سرقة الملكية الفكرية. من أفكار الحماية ان يتم تشغيل نسخ البرامج فقط مع وجود **تصريح** (License). يتم الحصول على التصريح مطبوع من الشركة أو عن طريق الإنترنت.

- يمكن حماية البرمجيات أيضا بتركيب **الفوب** (بالصورة) وهو جهاز يتم تركيبه في جهاز الحاسب عند تشغيل البرنامج. لا يعمل البرنامج إلا بتركيب الفوب إذ يتأكد البرنامج من أنه مركب قبل التشغيل.

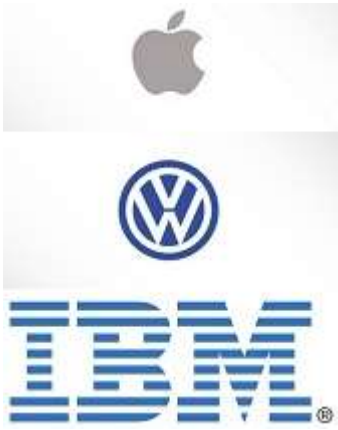
2 سرقة حقوق الملكية الفكرية

يتم حماية الممتلكات الإلكترونية باستخدام العلامات التجارية (Trademark) والعلامات المائية (Watermark)

- **العلامة التجارية** عبارة عن رمز تجاري معروف للشركة. تقوم بإلصاقه على المنتجات الخاصة بها.
- **العلامة المائية** هي عبارة عن رمز أو كتابة معينة يتم إلصاقها بالمنتج أو على الفيديو للتعريف بمالكه او تصنيف المستند


Alert - Individual Salaries Above Industry Range

Employee	Annual Salary	Industry Maximum Salary
Vaughn Marcian	$120,000	$95,000
Beorie Bello	$120,000	$95,000
Gordon Cutting	$70,000	$50,000



3 التسلل (تخطي الحواجز الأمنية)

التسلل هو النشاط البشري أو الإلكتروني لخرق **سرية** الممتلكات، أو محاولة الوصول إلى شيء غير مصرح بالوصول إليه.

- على سبيل المثال على المستوى الدولي (**التجسس**) حيث يتم جمع معلومات عن الجيش أو الأماكن الحيوية للدولة الضحية. ويمكن أيضا جمع معلومات عن الشركة من خلال الوصول الغير مصرح به لبياناتها.
- من أشهر التهديدات هجمة (**قراءة الكتف**) حيث يقف المهاجم خلف الضحية عند ادخال كلمة المرور على الحاسب أو في ماكينة الصراف ATM أو الجهاز اللوحي أو الهاتف الذكي ليحصل عليها. يمكن استخدام الكاميرات لقراءة الكتف.

3 التسلل (تخطي الحواجز الأمنية)

التسلل يتم بتخطي الحواجز الأمنية سواء الحواجز الفيزيائية كالأسوار والبوابات أو تخطي نظم الأمن الإلكترونية كتخطي الجدار الناري أو تخمين كلمة المرور.

يقوم ثلاث أنواع من الأشخاص بهجمة التسلل:

- **الهاكر**: هو الشخص المحترف في تخطي الحواجز الأمنية. يمكن أن يقوم بذلك بشكل عشوائي عندما يكون هاكر مبتدئ (صغار الهاكر).
- **الكراكر**: هو شخص متخصص في كسر حماية البرامج وكسر الحواجز الأمنية في الشركات. عادة ما يقوم الكراكر بعمل برنامج (كراك) يقوم بالمهمة بدلا منه.
- **الفريكر**: الشخص المتخصص في التصنت على المحادثات الهاتفية. أو الحصول على مكالمات مجانية بلا تصريح.

4 الابتزاز

يحدث الابتزاز عندما يقوم شخص بالاستيلاء على بيانات على حاسب الضحية سواء كان هذا الشخص داخليا او خارجيا. الابتزاز يكون بأحد النوعين:

- **التهديد بالإفشاء**: ويحدث عندما لا يرغب الضحية في إفشاء أو تسريب تلك المعلومات. كأن تكون معلومات غير قانونية أو إباحية أو تكون معلومات تجارية كمعلومات الزبائن.
- **التهديد بالحجب:** وفيها تكون المعلومات مهمة جدا لسير المؤسسة وبدونها تتعطل. كبيانات المستخدمين أو أرصدة المستخدمين أو أرقام كروت الائتمان الخاصة بهم. يقوم المهاجم عادة بعمل برمجية خبيثة تسمى **(برمجية الفدية)** وهذا البرنامج يقوم بتشفير تلك البيانات ولا يعطى مفتاح فك التشفير إلا بعد دفع الفدية

يقوم المبتز بالمقايضة على إفشاء أو حجب المعلومة.

5 التخريب المتعمد

التخريب يعني تدمير نظم الحاسب أو البيانات او الأعمال بهدف تعطيل العمل أو الرغبة في التشهير بالشركات والكيانات المنافسة. يوجد نوعين هامين من التخريب:

- **تخريب حسي:** كأن يقوم شخص بتدمير بيانات خاصة بالشركة أو بشخص ما بهدف تعطل العمل أو التأثير على سمعة الشركة.
- **تخريب معنوي:** ويهدف إلى تدمير سمعة الشركة بالإشاعات والأخبار المزيفة والغير حقيقية. وعادة ما يحدث ذلك بغرض الانتقام مثل الموظف المفصول أو الشركات المنافسة. تقوم بعض مجموعات القراصنة بالدخول على الموقع الضحية بهدف تخريب سمعته.

حدث مؤخرا أن قامت مجموعة اطلقوا على انفسهم مجموعة " الدب المنفوش" بكتابة رسالة على الموقع الرسمي لمعهد سانس (SANS) وهو معهد يعطي دورات وشهادات متخصصة في أمن المعلومات. كانت الرسالة تقول " **هل تثقون فعلا في هذه الأشخاص لتعليمكم أمن المعلومات؟**" كانت بالفعل فضيحة للمعهد اثرت على سمعته وموارده.

5 التخريب المتعمد

يقسم التخريب المعنوي حسب ميول الشخص العدوانية إلى:

- **مثير الفضائح**: وهو الشخص الذي يرغب في التقليل من أهمية شركة وفضيحتها بإفشاء اسرارها أو إثارة الإشاعات. يخترق المواقع الإلكترونية ويبث الإشاعات على المنتديات وشبكات التواصل الاجتماعي.
- **ناشط سياسي إلكتروني Hacktivist**: يقوم الناشط السياسي بدعم فكرة ما، سواء إيجابية أو سلبية في المجتمع الإلكتروني. كأن يقوم بحملة الكترونية انتخابية لشخص ما. أو دعم مذهب ديني أو فكرة متطرفة. يمتلك الناشط السياسي الأدوات كالبرمجيات الخبيثة التي تساعده.
- **إرهابي إلكتروني Cyberterrorist**: وهدفه الأول هو التخريب سواء بسبب الفكر المتطرف أو الانتقام. من الأمثلة على ذلك ان يقوم بتعطيل موقع إلكتروني لمؤسسة حكومية أو تخريب خوادم الإنترنت أو تعطيل خدمتها.

6 السرقة

تهديد السرقة عبارة عن أن يقوم شخص بالاستيلاء على ممتلكات شخص آخر والتي من الممكن ان تكون ممتلكات حسية أو الكترونية أو فكرية. كسرقة الهوية أو سرقة حاسبات أو معدات الشبكة في الشركة أو سرقة البيانات.

- **السرقة الحسية** يمكن حمايتها بسهولة من خلال استخدام:
(الأقفال، العمالة الأمنية المدربة، كاميرات المراقبة، أو أجهزة الإنذار)

- **السرقة الإلكترونية** اكثر تعقيدا في نظم الحماية الخاصة بها مقارنة بالسرقة الحسية. حيث أن الأشياء الحسبة الهامة إذا سرقت ستعرقل العمل ومن ثم يتم اكتشاف سرقتها مباشرة. أما السرقة الإلكترونية (كسرقة نسخة من بيانات هامة) فصعب اكتشافها. فإذا كان المهاجم ماهرا في محو أثار السرقة سيكون من الصعب اكتشاف وجود السرقة، وإذا تم اكتشافها سيكون متأخرا جدا وبعد فوات الأوان.

7 البرمجيات الخبيثة malware

يقوم فرد أو مجموعة بتصميم وإطلاق برامج بهدف الهجوم على نظم المعلومات. يتم تسميتها بالبرمجيات الخبيثة malware. تهدف البرمجيات الخبيثة عادة إلى التخريب أو سرقة البيانات أو تعطيل الخدمة.

البرمجيات الخبيثة تشمل على سبيل المثال لا الحصر:

1. **الفيروسات:** وهي برمجيات خبيثة تنتقل بعائل وسيط وهو الملفات وتنتشر معها
2. **الديدان:** وهي سريعة في الانتشار وتنتقل من حساب إلى حساب بصفة مستقلة.
3. **أحصنة طروادة:** وهي تتسلل إلى الحاسوب دون أن يتم اكتشافها، وتدخل كأنها ملفات عادية.
4. **القنابل المنطقية:** هي عبارة عن برمجيات تنتظر حدث ما حتى تعمل. كتاريخ معين أو حدث معين يقوم به المستخدم.
5. **الباب الخلفي:** وهو عبارة عن برمجية يتم تثبيتها على الجهاز الضحية بغرض التجسس. تظل موجوده على الجهاز لترسل بصفة دائمة معلومات عن الجهاز.

7 البرمجيات الخبيثة malware

6. **هجمة قطع الخدمة:** من أشهر البرمجيات الخبيثة أيضا برمجية "هجمة قطع الخدمة" Denial of Service وتسمى بالاختصار DOS. ولا تقوم تلك البرمجية بالتأثير الفيزيائي المباشر على الخدمة بقطعها ولكن تجعل الخادم (خادم الويب مثلا) مشغول دائما بالرد على طلبات عادية ولكن كمية هذه الطلبات كبيرة تجعله دائما غير متاح للمستخدمين الأبرياء.
7. **الهجمة الموزعة لقطع الخدمة:** وفيها يتم الاستفادة من هجمة قطع الخدمة ولكن بشكل موزع. إذ يقوم المهاجم بزرع برمجيات خبيثة في عدة أجهزة في أماكن متفرقة على الشبكة تسمى هذه الأجهزة **"زومبي"** وعندما تأتي ساعة الصفر تقوم كل الأجهزة بإرسال طلبات عادية للخادم بكميات مهولة مما يعطل خدمته ويمنع الاستفادة منه من قبل المستخدمين الأبرياء.

8 قوى الطبيعة

هي عبارة عن القوى الخارجة عن إرادة البشر وهي من أخطر التهديدات التي تصيب نظم المعلومات لأنها تأتي عادة بلا إنذار مسبق. ليست فقط تصيب البشر ولكن من الممكن أن تعطل تخزين ونقل ومعالجة البيانات. من الأمثلة عليها :

- **النيران:** تستطيع النيران التهام مكونات الحاسوب وتخريب البيانات جزئيا او كليا. ونظم مكافحة النيران مثل رشاشات الماء وطفاية الحرائق تصيب الأجهزة الإلكترونية بالعطب.
- **السيول والفيضانات:** عندما تصل السيول للأجهزة والمعدات وخصوصا إن كانت موصلة بالكهرباء ستعطل مباشرة. لأن الماء موصل جيد للكهرباء وستحدث دوائر قصيرة تحرق المكونات الإلكترونية. كما يمكن للفيضان أن يعطل الوصول للمعدات والأجهزة.

8 قوى الطبيعة

- **الزلازل:** عبارة عن حركة أرضية تؤثر على المباني وأحيانا تسقطها بشكل كامل. تدمر المكونات المعلوماتية في حالة سقوط المبنى. وفي بعض الأحيان يصعب الوصول اليها.
- **الصواعق:** هو تفريغ الشحنات الموجودة في الجو. عادة ما تؤثر الصواعق على الدوائر الكهربية وشبكات توزيع الكهرباء. وينتج عنها في بعض الأحيان النيران والحرائق. والتي من الممكن ان تؤثر على سير العمل الإلكتروني وتعطل الوصول للمعدات المعلوماتية.
- **الزوابع والأعاصير:** تنتج عن الرياح العاتية التي في بعض الأحيان تقطع اسلاك الاتصال المكشوفة وتعطل نظم الاتصالات ونقل المعلومات. وأحيانا يصحبها المطر والسيول التي من الممكن ان تؤثر بشكل مباشر على سير العمل.

8 قوى الطبيعة

- **الكهرباء الاستاتيكيه:** هي الكهرباء التي تنتج بحك قطعة من الصوف بقضيب من الحديد. وهي كهرباء بسيطة لكنها أحيانا تكون مخربة. على سبيل المثال إذا لم يتخذ مهندس الصيانة الاحتياطات اللازمة عند صيانته للأجهزة ستنتقل الكهرباء الاستاتيكيه الى الشرائح الالكترونية وتحرقها.
- **التلوث بالأتربة:** تدخل الأتربة في الفتحات الضيقة جدا بين الشرائح الالكترونية وتستطيع مع قليل من الرطوبة في الجو ان توصل الكهرباء وتنتج دوائر قصيرة تحرق الشرائح الالكترونية.

يجب ان يفكر مديرو الامن في الشركة في إقامة خطط لمواجهة تلك الكوارث والحد من تأثيرها. من الخطط العامة لذلك، خطط الحفاظ على استمرارية العمل، خطط مواجهة الأحداث، وخطط التعافي من الكوارث.

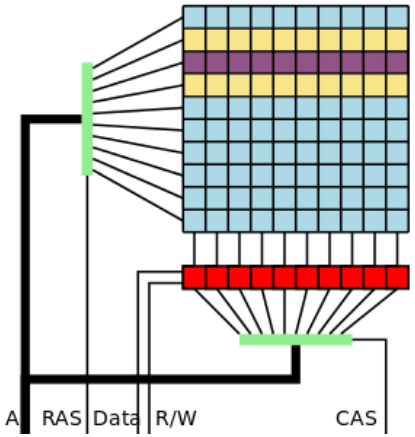
9 تدني كفاءة مزودي الخدمة

تعتمد الشركات في عملها الرقمي على عدة خدمات رئيسية تقدمها شركات أخرى. مثل خدمة الانترنت والكهرباء وقطع الغيار و الورق والأحبار حتى النفايات.

- **مزودي خدمة الإنترنت ISP**: بعض الشركات تعتمد اعتماد كليا على الانترنت في عملها، على سبيل المثال موقع سوق دوت كوم و أمازون. تعطل خدمة الانترنت تعني الخسارة الفادحة للشركة.
- **المرافق العامة** : شبكة الهاتف النقال والكهرباء والماء ونقل النفايات والصرف الصحي وغيرها. تعمل بعض نظم التبريد المركزي اعتمادا على المياه. وإذا تعطلت شبكة الصرف سيتم إخلاء المبنى من الموظفين.
- **الكهرباء**: تعمل الأجهزة الإلكترونية بالكهرباء، وأحيانا يؤثر انقطاع وعودة الكهرباء المفاجئ على الأجهزة.

10 مشكلة في العتاد

عادة ما تحدث الثغرات الأمنية للعتاد بسبب عيب في التصميم.

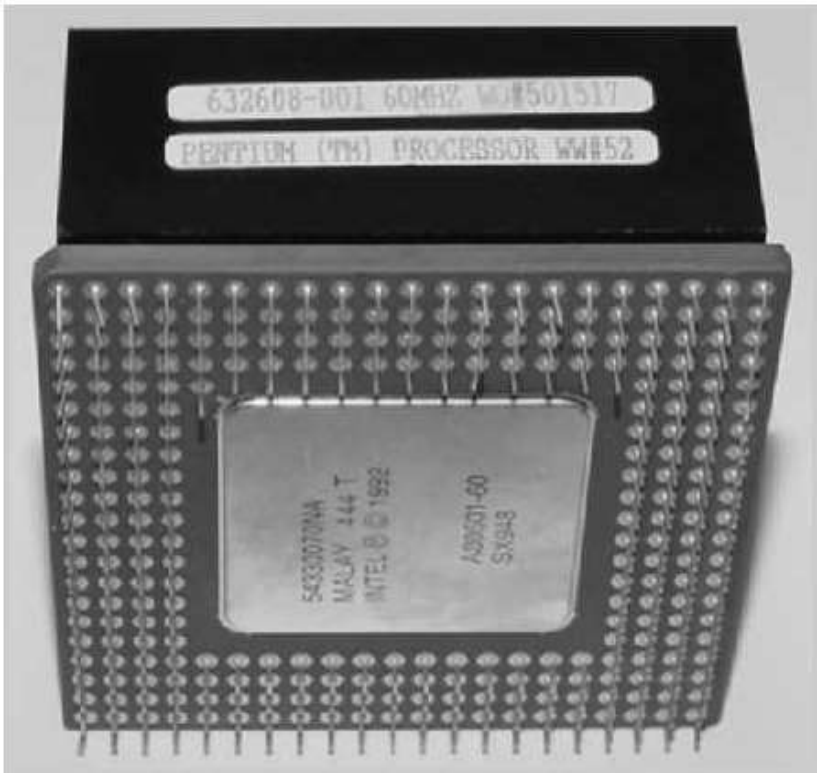


على سبيل المثال الذاكرة العشوائية يتم تصميمها باستخدام مكثفات متجاورة، ونظرا لهذا التجاور فأن التأثير على احدها من الممكن أن يؤثر على المكثف المجاور.

بناء على هذا العيب في التصميم تم استغلال التجاور في الوصول إلي مناطق في الذاكرة غير مصرح بها فيما يسمى بهجمة Rowhammer .

على الرغم من أن هجمات العتاد هي هدف للهجمات الكبرى إلا أن الحماية منها تتم ببرمجيات ونظم حماية فيزيائية بسيطة.

10 مشكلة في العتاد



ومن المشاكل في التصميم أيضا مشكلة في المعالج بنتيوم 2. حيث أعلنت شركة انتل أن هناك مشكلة في القسمة العشرية يمكن معرفة ان كانت موجودة بقسمة 4195835 و3145727 .

تكررت مشاكل العتاد مع شركة انتل اكثر من مرة حتى انها أعلنت أنها لا تضمن إن كان المنتج الجديد به عيوب أو لا.

11 مشكلة في البرمجيات

- الكثير من الأكواد البرمجية كتبت وتم محاولة إزالة كل الأعطاب منها وتم توزيعها ثم بعدها تم اكتشاف اعطاب أخرى.
- تكون الأعطاب بسبب خطأ برمجي بعدم تغطية كل الحالات في البرنامج. وبعد توزيع البرنامج تحدث حالة نادرة تسبب العطب.
- أحيانا تكون الأعطاب بسبب تحميل البرنامج عند العميل على عتاد مختلف عن الذي قام بتصميم البرنامج عليه.
- تكون تلك الحالات الغير مغطاة ثغرة ينتج عنها أن يقوم القراصنة بزرع باب خلفي.
- يتم تسجيل الأعطاب المشهورة للبرامج على مواقع عامة مثل www.securityfocus.com,

SecurityFocus™

12 النظم العتيقة

- مشكلة النظم العتيقة أنها قد تم دراستها من قبل القراصنة وتم معرفة كل الثغرات الموجودة بها.
- على سبيل المثال يسهل جدا إيجاد ثغرات في نظام التشغيل ويندوز اكس بي، على عكس النظم الحديثة مثل نظام التشغيل ويندوز 10.
- يجب على مديري النظم تحديث البرامج بشكل دوري وانزال الرقع والتحديثات الجديدة لسد الثغرات المحتملة.
- حدث أن أوقفت شركة سيمانتك منتج مضاد للفيروسات لها. وأجبرت كل المستخدمين على استخدام منتج اخر وإيقاف العمل بالمنتج القديم.

الأسئلة