الوحدة 5: المبادئ الأساسية للأمن المعلوماتي

الهدف:

الجانب النظري	الجانب التطبيقي
فهم أساسيات الأمن المعلوماتي، والوعي بأهم التهديدات التي قد يتعرض لها الأفراد والمؤسسات، واكتساب المعارف الضرورية لحماية البيانات والمعلومات الرقمية .	تطبيق مبادئ الأمن المعلوماتي في سياقات حياته اليومية، واكتساب مهارات في: التعرف على مفاهيم الهجوم والدفاع في الأمن السيبيراني، محاكاة سيناريوهات واقعية (تصيد، كلمات مرور، إعدادات الخصوصية)، تنفيذ خطوات أساسية للحماية من المخاطر الرقمية.

المحتوى:

- مقدمة
- تعريف الأمن المعلوماتي
- المبادئ الأساسية للأمن المعلوماتي:
  - السرية
  - السلامة
  - التوافر
- أنواع التهديدات
- ممارسات الوقاية
- حالة الوقوع تحت تهديد
- أمثلة واقعية

مقدمة:

لا يختلف اثنان عاقلان في كون هذا العصر هو عصر المعلومات، حيث أصبحت البيانات هي البنية التحتية الأساسية للحياة الحديثة، والمحرك الرئيس للاقتصاديات العالمية، ووقود الابتكار في شتى المجالات.

ومع هذا الاعتماد المتزايد على الأنظمة الرقمية وتقنيات الاتصال الحديثة، برزت الحاجة الملحّة إلى حماية المعلومات من كل تهديد قد يمسّ سريتها أو سلامتها أو توفرها. فالأمن المعلوماتي لم يعد خيارًا ثانويًا، بل تحول إلى ركيزة أساسية لضمان استمرارية المؤسسات وحماية خصوصية الأفراد وصون سيادة الدول.

يهدف هذا الدرس إلى التعريف بالركائز الأساسية لضمان سلامة المعلومات في البيئة الرقمية، بدءاً من فهم التهديدات وصولاً إلى تطبيق أفضل ممارسات الحماية والوقاية التي من شأنها أن تحول دون الوقوع ضحية لمثل هذه التهديدات، وفي حالة الوقوع كيف يكون التصرف السليم.

1. مفهوم الأمن المعلوماتي:

الأمن المعلوماتي (***Information Security - InfoSec***) هو مجموعة من السياسات والإجراءات والأدوات التي تهدف إلى حماية المعلومات الحساسة للمؤسسات والأفراد من الوصول غير المصرح به، أو الكشف، أو الاستخدام، أو التعديل، أو التعطيل، أو الإتلاف. فهو يهدف إلى الحفاظ على الخصائص الأساسية للمعلومات، والتي تُعرف باسم "**المبادئ الأساسية لأمن المعلومات**" أو ما يعرف بـ (***CIA Triad***).

الفرق بين الأمن المعلوماتي والأمن السيبراني:

يُستخدم هذان المصطلحان في كثير من الأحيان بالتبادل، ولكن هناك فرق في النطاق:

الأمن المعلوماتي (*InfoSec*) : هو مصطلح أوسع وأشمل؛ حيث يركز على حماية المعلومات بجميع أشكالها (رقمية، ورقية، مادية، أو صوتية)، بغض النظر عن طريقة تخزينها أو وسيلة نقلها. يشمل الأمن المعلوماتي الأمن المادي (مثل حماية مراكز البيانات) بالإضافة إلى الأمن الرقمي.

الأمن السيبراني (*Cybersecurity*) : هو جزء من الأمن المعلوماتي، يركز بشكل خاص على حماية البيانات الرقمية والأنظمة والتكنولوجيا التي تعالجها وتخزنها وتنقلها من التهديدات والهجمات الإلكترونية في الفضاء السيبراني (الإنترنت).

بشكل أساسي، الأمن السيبراني هو شكل من أشكال الأمن المعلوماتي، لكن نطاق الأمن المعلوماتي أوسع ليشمل جميع أنواع المعلومات ووسائط التخزين.

2. المبادئ الأساسية للأمن المعلوماتي:

تقوم الحماية الأمنية على ثلاثة مبادئ رئيسية تُعرف باسم "**المثلث (الثلاثي)** (***CIA Triad***)":

المبادئ الأساسية لأمن المعلومات

أ. مبدأ السرية (*Confidentiality*):

يشير مبدأ السرية إلى حماية المعلومات من الوصول غير القانوني (غير المصرح به) (***Unautohorized Access***) إليها من طرف الأفراد غير المخول لهم بذلك (***Unautohorized Person***)، ويشمل مصطلح الوصول في هذه الجملة كلا من: القراءة، المشاهدة، الاستماع، التنفيذ، النسخ، .. ولتحقيق ذلك يمكن استعمال عدة آليات:

- **التشفير (*Encryption*)** : تحويل البيانات إلى تنسيق غير قابل للقراءة دون مفتاح فك التشفير.
- **التحكم في الوصول (*Access Control*)** : استخدام أسماء المستخدمين، كلمات المرور، المصادقة الثنائية وبطاقات الدخول لتقييد من يمكنه الوصول إلى الموارد.
- اعتماد نظام **التصاريح (*Permissions*)**: تطبيق قاعدة "**أقل امتياز**" (***Least Privilege***) لضمان حصول المستخدمين على الحد الأدنى من الأذونات اللازمة لأداء وظائفهم.
- الاعتماد على **بروتوكولات الشبكات الآمنة**: مثل ***HTTPS, VPN***.

ب. مبدأ السلامة (الصحة) (*Integrity*) :

يشير إلى مبدأ ضمان دقة واكتمال وموثوقية البيانات والأنظمة على مدار دورة حياتها وعدم تعديلها بطريقة غير مشروعة، فهو يهدف إلى منع التعديل غير المصرح به أو الحذف. ولتحقيق ذلك يمكن استعمال عدة آليات:

- **التوقيعات الرقمية (*Digital Signatures*)** : استخدام خوارزميات التجزئة (***Hashing***) مثل (***SHA-256***) لإنشاء بصمة فريدة للبيانات، مما يسمح بالكشف عن أي تغيير.
- **بروتوكولات التحكم بالإصدارات (*Version Control*)**: تتبع وإدارة التغييرات على الملفات والأنظمة.
- **النسخ الاحتياطي (*Backups*)**: وجود نسخ احتياطية موثوقة لاستعادة البيانات في حالة التلف أو الاختراق.

ت. مبدأ التو افر (*Availability*):

يشير هذ المبدأ إلى ضمان أن المعلومات والأنظمة والخدمات متاحة للمستخدمين المصرح لهم عند حاجتهم إليها. فهو يهدف إلى منع انقطاع الخدمة الذي قد ينتج عن الهجمات حجب الخدمة (***DoS***) أو أعطال في الأجهزة أو كوارث طبيعية، ولتحقيق ذلك يمكن استعمال عدة آليات:

- **مخططات استمرارية العمل (*Business Continuity Plans*)** : وهي وثائق وخطط منظمة تهدف إلى ضمان قدرة المؤسسة على الاستمرار في أداء وظائفها الأساسية خلال الأزمات وبعدها.
- **أنظمة النسخ الاحتياطي والاسترداد (*Backup Systems*)** : القدرة على استعادة الأنظمة بسرعة بعد وقوع كارثة.
- **أنظمة التحميل المتوازن (*Load Balancing*)** : استخدام مكونات احتياطية (مثل الخوادم، مزودات الطاقة، أو خطوط الاتصال) لضمان استمرار الخدمة في حالة فشل مكون رئيسي.
- **الحماية من هجمات حجب الخدمة (*DDoS Mitigation*)** : الدفاع ضد الهجمات التي تهدف إلى إغراق النظام ومنعه من الاستجابة للمستخدمين الشرعيين.
- **الصيانة الدورية** (***Regular Maintenance***) : تحديث الأنظمة وتصحيح الثغرات (***Patching***) لمنع الانقطاعات الناتجة عن نقاط ضعف معروفة.

3. مبادئ إضافية مكملة:

بالإضافة إلى الثلاثي السابق، هناك ثلاثة مبادئ أخرى تعتبر حاسمة في بناء إطار عمل أمني قوي:

أ. المصادقة/التوثيق (*Authentication*) :

هي عملية التحقق من هوية شخص أو نظام يحاول الوصول إلى مورد. يتم هذا عادةً من خلال شيء يعرفه المستخدم (مثل كلمة المرور)، أو شيء يمتلكه، مثل الرمز المميز (***Token***)، أو شيء هو جزء منه (مثل البصمة).

ب. عدم الإنكار(*Non-Repudiation*) :

ضمان عدم قدرة الطرف الذي قام بإرسال رسالة أو إجراء معاملة رقمية على إنكار قيامه بذلك لاحقًا (جد مهمة في المعاملات البنكية والتجارة الالكترونية). غالبًا ما يتم تحقيق ذلك باستخدام التوقيعات الرقمية، التي تربط المعاملة بشكل لا رجعة فيه بهوية الفرد.

ت. المساءلة/المحاسبة(*Accountability*) :

يشير إلى القدرة على تتبع الإجراءات التي يتخذها المستخدمون لتحديد من فعل ماذا ومتى. هذا يتطلب تسجيل جميع الأنشطة في سجلات التدقيق(***Audit Logs***) ، وهو أمر حيوي للكشف عن الانتهاكات الداخلية والخارجية والتحقيق فيها.

4. أنواع التهديدات:

أ. البرمجيات الخبيثة (*Malware*) :

البرمجيات الخبيثة، أو ***Malware*** (وهو اختصار لـ***Malicious Software***) هي برامج صمّمت خصيصًا لاختراق الأنظمة أو إلحاق الضرر بها أو استغلالها دون علم المستخدم أو موافقته. وهي عادة ما تستخدم للتجسس، لسرقة البيانات أو إتلافها أو تشفيرها من أجل طلب الفدية، تعطيل الأجهزة وإيقافها عن العمل، التحكم في الأجهزة عن بعد واستعمالها مطية لقيادة هجومات على الآخرين. وأهم هذه الأنواع نذكر:

- **الفيروسات** (***Viruses***) : برنامج طفيلي، يلتصق ببرنامج آخر ولا ينطلق تلقائيا إلا بعد أن يقوم المستعمل بتنفيذ ذلك البرنامج، ينتشر ببطء وعادة ما يكون هدفه إتلاف البيانات.
- **الديدان** (***Worms***) : هو برنامج مستقل (لا يلتصق بأي برنامج آخر) يتميز بقدرته على الانتشار تلقائيا وبسرعة، عادة هدفه هو استنزاف الموارد (بسبب التكاثر الهائل) كما قد يكون له وظائف تدميرية أخرى.
- **أحصنة طروادة** (***Trojan Horses***): تبدو في ظاهرها كأنها برامج عادية أو مفيدة، ولكنها في الواقع تخفي برمجيات ضارة تُستخدم لفتح باب خلفي (***Backdoor***) من أجل سرقة البيانات أو التحكم بالجهاز.
- **برامج الفدية** (***Ransomware***): تقوم بتشفير الملفات أو قفل نظام الكمبيوتر بالكامل، ومن ثم إظهار رسالة تطلب مبلغ مالي (فدية) من أجل استعادة البيانات أو النظام.
- **برامج التجسس** (***Spyware***): تهدف إلى جمع معلومات سرية حول أنشطة المستخدم (مثل عادات التصفح، ضغطات لوحة المفاتيح، كلمات المرور) وإرسالها إلى طرف ثالث دون موافقة المستخدم. ومن أهمها راصدات لوحة المفاتيح (***Keylogger***)، برامج مراقبة النظام/التجسس البسيط (***System Monitors/Simple Spyware***)، سارقو المعلومات (***Info-Stealers***)، برامج التلصص على الشبكات (***Network sniffer***)، ...
- **البرامج الإعلانات الدعائية** (***Adware***): لعرض أو تنزيل إعلانات غير مرغوب فيها، غالبًا على شكل نوافذ منبثقة، غالبا ما تقوم بتثبيت برامج إضافية أو تغيير إعدادات المتصفح من أجل توجيهه لعرض صفحات محددة تلقائيا.

- **الجذور الخفية (*Rootkits*):** مجموعة من الأدوات المصممة لإخفاء البرامج الضارة الأخرى (كالفيروسات وأحصنة طروادة) عن أنظمة التشغيل وبرامج الحماية، كما تمنح للمخترق وصولًا خفيًا ومستمرًا وذو صلاحيات عالية.

- **البوت والبوتنت (*Bots ; Botnets*):** وهي اختصار للكلمة الإنجليزية (*Robot*) وهي أدوات تحول الجهاز إلى أداة لمهاجمة الأجهزة الأخرى، وعادة ما تستعمل في هجومات حجب الخدمة (*DoS ; DDoS*)، أو من أجل تعقيد مهمة البحث عن المهاجم الرئيسي، وتسمى مجموعة الأجهزة المتحكم فيها بشبكة البوتنت (أو شبكة الزامبي).

ب. الهندسة الاجتماعية (*Social Engineering*):

هي فن التلاعب النفسي بالبشر وخداعهم لدفعهم إلى الكشف عن معلومات حساسة أو تنفيذ إجراءات تخدم المهاجم، بدلاً من استغلال الثغرات التقنية في الأنظمة، وتعتبر واحدة من أخطر التهديدات في مجال أمن المعلومات لأنها تستغل العنصر البشري والذي يعد أضعف حلقة في سلسلة الأمان.

وهي مبنية على استغلال المشاعر والظروف الإنسانية مثل : الثقة، الخوف، التعاطف، الحب، الفضول، الطمع، الاستعجال، الجهل، البلادة، .. ومن أشهر أنواعها:

- التصيد الاحتيالي (*Phishing*).
- التصيد عبر الهاتف (*Vishing*).
- التصيد عبر الرسائل القصيرة (*Smishing*).
- هجوم الذريعة (*Pretexting*).
- انتحال الشخصية (*Impersonation*).
- الإغراء (*Baiting*).

ت. التصيد الاحتيالي (*Phishing*):

هو أحد أنواع هجمات الهندسة الاجتماعية المجسدة عبر شبكات المعلومات، وهو عبارة عن هجوم إلكتروني يستغل الثغرات البشرية عوض الثغرات التقنية، حيث يقوم المهاجم بانتحال صفة جهة موثوقة (بنك، شركة، مؤسسة، شخص موثوق فيه...) بهدف خداع الضحية وجعله يكشف معلومات حساسة عنه أو عن عمله مثل كلمات المرور، أرقام بطاقات الدفع، بيانات الحسابات، .. أو قد يكون الهدف استدراج الضحية من أجل الحصول على المال.

من بين أشهر الأنواع نذكر:

- **التصيد العشوائي**: يستهدف جمهور واسع من الأشخاص.
- **التصيد الاحتيالي المستهدف (*Spear Phishing*)**: موجه ضد شخص أو مؤسسة محددة.
- **تصيد الحيتان (*Whaling*)**: تصيد الشخصيات المهمة.
- **التصيد بالرسائل النصية(*Smishing*) :** يستهدف مستخدمي الهواتف.
- **التصيد الصوتي(*Vishing*) :** يستخدم المكالمات الهاتفية.

الوسائل المعتمدة لتحقيق ذلك هي غالبا البريد الالكتروني، وسائل التواصل الاجتماعي، وتطبيقات المراسلة .. حيث يتم توجيه الضحية عبر رابط تشعبي إلى موقع مزيف (في غالب الأحيان يكون مشابها للموقع الحقيقي) ومن خلاله يتم سرقة المعلومات الشخصية. ومن أمثلتها:

- رسالة إلكترونية يدعي فيها المهاجم أنه مدير البنك مثلا وأنهم بصدد القيام بأعمال صيانة على الحسابات، وأنه سيتم توقيف الحساب في حالة عدم إرسال البيانات اللازمة.
- رسالة إلكترونية يدعي فيها صاحبها أنه من دولة ما (إفريقيا خاصة) يطلب فيها المساعدة مقابل مبلغ مالي خيالي.
- الإعلانات الزائفة عبر وسائل التواصل الاجتماعي: التوظيف، البيع، ..

ث. الاختراقات الإلكترونية (*Hacking*):

هي عملية استغلال ثغرات في الأنظمة أو الشبكات أو التطبيقات أو في الأفراد أنفسهم من أجل الدخول إلى النظام بطريقة غير شرعية، وبالتالي التحكم فيه أو تعطيله أو سرقة البيانات. مثل الدخول إلى نظام ما عن طريق سرقة هوية شخص له صلاحية الدخول، أو استعمال كلمة مرور مزورة أو خداع حراس الأمن. يمكن تقسيم المهاجمين إلى أربعة أنواع رئيسية:

- **الهاكر الأخلاقي (القبعة البيضاء) (*White Hat hacker*)**: يعمل بشكل قانوني، من أجل اختبار أمن الأنظمة.
- **الهاكر الخبيث (القبعة السوداء) (*Black Hat hacker*)**: يقوم بالاختراق لأغراض إجرامية (التجسس، الربح المالي، التخريب،..).
- **الهاكر الرمادي (القبعة الرمادية) (*Grey Hat Hacker*)**: يعمل بدون إذن، لكن بدون نية ضرر واضحة، عند اكتشاف ثغرة قد يقومون بنشرها للعامة أو يطلبون فدية للمساعدة في إصلاحها. في بعض الأحيان يكون هدفهم هو التحدي وإثبات المهارات، أو الاحتجاج ولفت الانتباه إلى بعض القضايا.
- **المخترقون بدعم حكومي (*State-Sponsored*)**: يعملون بدافع تجسسي أو حربي نيابة عن حكومات بعض الدول لاختراق أنظمة دول أخرى أو منافسين أو جماعات معادية.

من أشهر الطرق المستعملة:

- الهندسة الاجتماعية.
- استغلال الثغرات (*Exploiting Vulnerabilities*).
- هجومات القوة الغاشمة (*Brute-Force Attacks*).
- حقن قواعد البيانات (*SQL Injection*).
- هجمات التموضع كرجل في الوسط (*Man-in-the-Middle*).
- هجمات حجب الخدمة (*DoS*).
- الهجومات عن طريق البرامج الضارة.

ج. تسريب البيانات (*Data Breach*):

هو حادثة أمنية يتم فيها الوصول غير المصرح به إلى بيانات سرية أو حساسة أو محمية، واستخراجها من نظام آمن دون علم الإدارة أو موافقتها. وهي عادة ما تحدث نتيجة:

- هجومات إلكترونية خارجية (اختراقات)
- تسريبات من الداخل نتيجة أخطاء بشرية أو نتيجة التواطؤ أو الإهمال واللامبالاة.
- السرقة المادية (سرقة جهاز أو أداة تخزين)

تختلف أثار ومخاطر تسريب البيانات حسب أهمية البيانات المسربة ونوع الضحية:

- بالنسبة للأشخاص: سرقة الهوية (استخدام البيانات الشخصية لأغراض غير قانونية)، انتهاك الخصوصية، الخسائر المادية، التعرض للتصيد المستهدف،
- بالنسبة للمؤسسات: الخسائر المالية، فقدان الأسواق والعملاء، الإضرار بالسمعة، المساءلة القانونية.

أمثلة عالمية شهيرة على تسريب البيانات:

- **شركة ياهو (*Yahoo*) :**تسريب بيانات جميع حسابات مستخدميها (3 مليار حساب) في 2013.
- **شركة فاسبوك (*Facebook*):** تسريب بيانات 87 مليون مستخدم لشركة ***Cambridge Analytica*** في 2018.
- **شركة إيكيفاكس (*Equifax*):** تسريب بيانات 147 مليون شخص (بيانات ائتمانية حساسة) في 2017.

ح. الكوارث الطبيعية أو فقدان الطاقة:

تُعتبر الكوارث الطبيعية ومشاكل فقدان الطاقة من التهديدات غير الإلكترونية التي تؤثر بشكل مباشر على أمن البيانات واستمرارية عمل الأنظمة المعلوماتية، وهو خطر فوري ومهدد بالزوال الدائم للبيانات، ويُعدّ من أكبر التهديدات المادية التي تواجه المؤسسات والأفراد.

مخاطر الكوارث الطبيعية:

- فقدان الوصول إلى البيانات والخدمات (***Loss of Availability***).
- تلف البيانات (***Data Corruption***).
- فقدان البيانات بشكل كلي (***Permanent Data Loss***).
- اختراق سلامة البيانات (***Loss of Integrity***).

ومن أنواعها: الحرائق، الزلازل، الفيضانات، والأعاصير.

مخاطر فقدان الطاقة:

- تعطل أنظمة التشغيل (نظام الملفات)، وقواعد البيانات.
- تلف الملفات المفتوحة وفقدان البيانات غير المحفوظة.
- التلف المادي للأقراص الصلبة وتقصير العمر الافتراضي للمعدات.

5. ممارسات الوقاية:

- التدريب والتوعية للموظفين (***Awareness Training***) : عدم تثبيت البرامج مجهولة المصدر، عدم النقر على روابط غير موثوقة، استعمال كلمات مرور قوية، التثبت من صحة العناوين على الانترنت ووجود علامة التشفير والتأمين، ..
- استعمال وتفعيل الجدران النارية (***Firewalls***) و أنظمة كشف ومنع الاختراقات (***IDS/IPS***) وبرامج مكافحة الفيروسات (***Antivirus***) مع ضرورة تحديثها باستمرار.
- تحديث البرمجيات (***Patch Management***).
- سياسات أمن المعلومات (***Security Policies***).
- تشفير البيانات.
- استخدام نظام صلاحيات الوصول لكل فرد.
- تفعيل المصادقة الثنائية.

- المراقبة المستمرة للأنظمة.
- تفعيل نظام الإنذارات.
- النسخ الاحتياطي (backup): مثل استعمال خطة 3-2-1 والتي تتمثل في 3 نسخ من البيانات على نوعين مختلفين من الوسائط مع نسخة خارج الموقع.
- الحلول السحابية.
- خطط التعافي من الكوارث (***Disaster Recovery Plan***)، وخطط استمرارية العمل.
- استعمال بنية تحتية مناسبة وقوية.
- استعمال مولدات الطاقة الاحتياطية مع أجهزة الحماية من التقلبات المفاجئة في التوتر وأجهزة ***UPS*** للتزويد الفوري للأجهزة بالطاقة حال انقطاعها.

6. حالة الوقوع تحت تهديد أمني:

- قطع الاتصال.
- تغيير كلمات المرور.
- إبلاغ الجهات المعنية.
- فحص الجهاز.
- التحقق من الأضرار.
- استعادة البيانات.
- استخلاص الدروس.

7. أمثلة و اقعية:

- ✓ **هجوم (*WannaCry*) سنة 2017** : عن طريق برنامج فدية، حيث انتشر بسرعة في أكثر من 150 دولة وقام بتشفير ملفات المستشفيات والشركات ومن ثم طلب فدية بعملة "البيتكوين" بقيمة تتراوح ما بين 300 إلى 600 دولار.وقد تسبب في تعطل الكثير من الشركات عبر العالم من بينها عدة مستشفيات في بريطانيا، وعدة جامعات ومؤسسات حكومية.
- ✓ **تسريب بيانات مستخدمي الفايسبوك سنة 2019** : حيث تسربت بيانات أكثر من 500 مليون مستخدم شملت أرقام هواتف وأسماء ومواقع، مما أدى إلى انتهاك واسع للخصوصية وفقدان ثقة المستخدمين.
- ✓ **هجوم (*NotPetya*) سنة 2017** : هو هجوم تخريبي(***Wiper Malware***) في شكل برنامج فدية حيث استهدف عملاق الشحن والنقل البحري الدنماركي شركة (***A.P. Moller-Maersk***) وتسبب في خسائر قدرت ما بين 200 و 300 مليون دولار لتجديد البنية التحتية وأعادت الشركة تثبيت حوالي 4,000 خادم (***servers***)،و 45,000 حاسوب شخصي ، و2,500 تطبيق تأثروا بالهجوم.
- ✓ **هجوم على شركة (*Sony Pictures*) سنة 2014** : يعتبر هذا هجوما مركبا حيث حصل المهاجمون أولا على صلاحية الدخول إلى الخوادم والبريد الالكتروني للشركة ومن ثم عن طريق برامج خبيثة قاموا بمسح الملفات والبيانات، ثم تسريب بعضها مثل رسائل بريد الكتروني خاصة، رواتب الموظفين، ومعلومات أخرى جد حساسة. وقد تسبب هذا الهجوم في خسائر للشركة بملايير الدولارات نتيجة الإصلاحات والتعويضات المادية، وإساءة كبيرة لسمعتها.

- ✓ **ختراق شركة(*Equifax*) سنة 2017** : حيث أدى إلى تسرب بيانات حساسة لأكثر من 147 مليون شخص مما أدى إلى خسائر كبيرة نتيجة الغرامات والدعاوى القضائية.
- ✓ **هجوم فيروس (*Stuxnet*) سنة 2010**: وهو هجوم بفيروس على أنظمة الطرد المركزي بمنشأة "نطنز" لتخصيب اليورانيوم في إيران. وقد تم إدخال الفيروس عن طريق ذاكرة ***usb*** وضعت في كطعم لبعض الأفراد العاملين بالمفاعل. وقد أدى إلى تعطيل حوالي 1000 جهاز طرد مركزي وتسبب في تأخر للبرنامج النووي الإيراني لعدة سنوات.
- ✓ **اختراق ياهو سنة 2013-2014:** تعرض ما يقارب 3 مليارات حساب على ياهو للاختراق (كل الحسابات) مما أدى إلى سرقة بيانات جميع المستخدمين لهذا البريد الالكتروني، وقد اعتبر هذا الاختراق أكبر اختراق في تاريخ الانترنت. وبعد التحقيق تبين أن المهاجمين مدعمين من قبل دولة (***state-sponsored actor***) حيث استعملوا "كوكيز مزوّرة" (***forged cookies***) حتى يتمكّنوا من دخول الحسابات دون كلمة مرور. وقد أدى هذا الاختراق إلى فقدان الثقة في خدمات الشركة وتخفيض كبير في قيمة بيع أصولها وصل إلى حوالي 350 مليون دولار.