امن المعلومات

الجزء الأول: المستخدم

أ. د. أسامة حسام الدين

2021 م

المحتوى العام

- الجزء الأول: المستخدم.
- الجزء الثاني: القراصنة.
- الجزء الثالث: الهجمات.
- الجزء الرابع: طرق الحماية.

المستخدم المنزلي

محاور الأمن المعلومات

- محور المعلومات الشخصية.
- محور المعلومات داخل الشركات.
- محور المعلومات بين الدول (الحرب الإلكترونية).

المعلومات الشخصية

.توجد نوعين من الهويات، الهوية الحقيقة والهوية الإلكترونية.

الهوية الإلكترونية وهي التي تدخل بها إلى العالم الرقمي، اسم المستخدم، بياناتك على فيسبوك و تويتر وغيرها .وهي المعلومات التي تظهر بها للأخرين على شبكة الأنترنت، ويفترض أن تكون قليلة للغاية.

الهوية الحقيقية وهي التي يعرفك بها أصدقائك وأسرتك وزملائك في المحيط الحقيقي الذي تعيش فيه .مثل اسمك، عنوانك الحقيقي،

يجب أن تختار شيئا ما يعبر عن شخصيتك ويجب أن تحاول إخفاء الهوية الحقيقية بقدر الإمكان.

المعلومات الشخصية

نعرض في الشكل المعلومات الشخصية والخاصة.

أين توجد المعلومات – معلومات التصفح

- عندما تتسوق عبر الإنترنت، تقوم الشركات الكبرى مثل جوجل بتتبع رغباتك الشرائية وإرسال عروض وإعلانات مطابقة لرغباتك.
- يمكن أيضا معرفة ما تحب وما تكره واتجاهاتك السياسية والفكرية والدينية من خلال زيارة بسيطة لحساباتك في مواقع التواصل الاجتماعي.
- يتم تسجيل المواقع التي زرتها على المتصفح History
- يتم تسجيل كلمات المرور والروابط التشعبية التي تم فتحها من قبل في cookies أو ملفات الارتباط.
- **عرض بسيط لكيفية مسح البيانات من المتصفح**

أين توجد المعلومات – معلومات التصفح

- بالإضافة لتاريخ التصفح History الموجود في المتصفحات فإن جوجل يحتفظ بكل الأنشطة التي تمارسها على الإنترنت.
- يمكن الوصول لها من خلال الرابط التالي https://myactivity.google.com
- احذر كل الحذر من أن يطلع أحد على أسرارك الخاصة.
- **كيفية عرض الأنشطة التي قمت بها من قبل على النت من جوجل myactivity**

ماذا يريد المهاجمين منك؟

•المال ثم المال ثم المال.

ماذا يريد المهاجمين منك؟

- اسم الشخص وتاريخ ميلاده يعني شيئا بالنسبة للقراصنة عندما يكون احدهما على سبيل المثال هو كلمة المرور
- الصور الخاصة والمعلومات الخاصة، يريد المهاجم الحصول عليها بغرض الابتزار Blackmail
- مراقبة نشاطك من خلال الكاميرا أو المايك الخاص بالهاتف أو الحاسب الآلي وبعدها الابتزاز
- رقم بطاقة الائتمان، الانترنت البنكي وغيره الكثير والكثير

بياناتك التي تدلي بها عن نفسك بنفسك

- الصورة التي التقطتها لنفسك على الهاتف ثم شاركتها مع زملائك على الشبكات الاجتماعية لم تصبح في حوزتك بعد،
- لن تستطيع التحكم في انتشارها أو مشاركتها، وإن أردت يوم من الأيام أن تحذفها من الإنترنت فلن تستطيع.
- عندما تشاركها زملائك فمن الممكن أن يقوم شخص بحفظها على جهازه (هذا إن كانت الصورة مثيرة للاهتمام) أو اخذ لقطة لشاشة الحاسب وبها صورتك
- بعدها يحتمل أن تكون صورتك على أي خادم حول العالم. فكيف تضمن التحكم بها؟

ماذا افعل؟

.لا تشارك معلومات كثيرة على الإنترنت. لا تدع فرصة للمهاجمين أن يصلوا إلى بياناتك بالخداع الرمحي والابتزاز

.لا تعطي أيميلك لأحد إلا الذي تثق به. كلما شاركت أيميلك كلما زاد البريد المزعج Spam . وأيضا لا تشارك رقم هاتفك للجميع. قم بعمل حساب بريد إلكتروني غير مهم وشاركه للجميع.

.احذر الدخول على المواقع الغير موثوقة ، مثل مواقع الكراك، ولا تقم بتنزيل أو تثبيت برامج إلا بعد التأكد منها. لعل البرنامج الذي تثبته على جهازك يكون برمجية تجسس.

.قم بمسح أثر التصفح سواء في المتصفحات أو في أنشطة جوجل mvactivity (private browsing) .

.عرض بسيط لكيفية عمل تصفح آمن.

المستخدم في شركة

معلومات الشركة

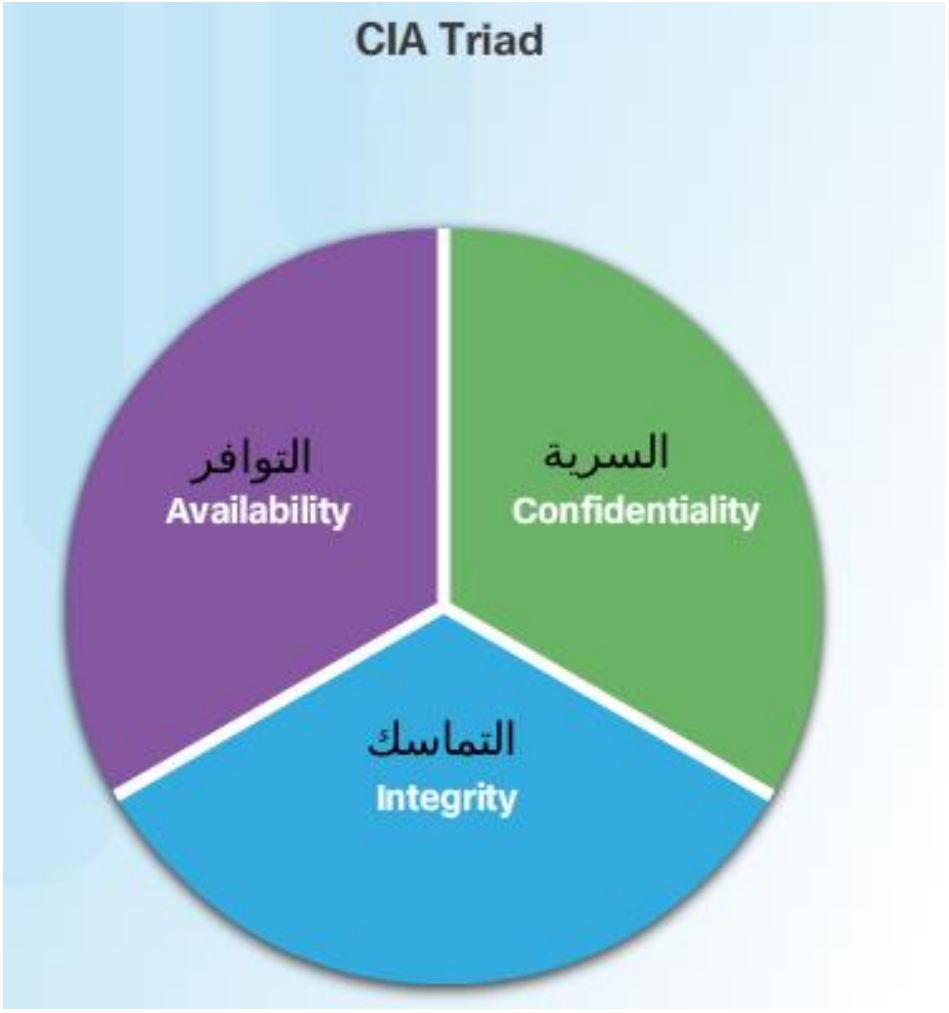
بيانات العاملين والموظفين في الشركة. مثل الرواتب والمعلومات الشخصية

بيانات الملكية. تحتوي على الابتكارات والأفكار الجديدة لتطوير الشركة مثل براءات الاختراع، وهذه المعلومات تزيد من قوة الشركة مقارنة بمنافسيها.

المعلومات المالية. مثل الدخل الشهري والسنوي والميزانيات وسجلات تدفق الأموال من والى الشركة يعطي نظرة عامة عن الصحة المالية للشركة.

" البيانات الضخمة "نظرا لما تنقله حساسات وأشياء إنترنت الأشياء إلى سحب حفظ البيانات على مدار الساعة.

مثلث الحماية الأمنية CIA Triad



مثال :كيفية حماية المال، كيفية حماية الذهب، كيفية حماية شخص مشهور، كيفية حماية ا

السرية Confidentiality

.سرية البيانات تعني حماية البيانات من أن يصل إليها أحد إلا مالك البيانات أو شخص مصرح له بالوصول.

.في الشركة يجب أن تتم حماية البيانات باستخدام نظم التحكم بالوصول Access Control System

.يجب تصنيف البيانات أيضا إلى مستويات في السرية، على سبيل المثال ، سري للغاية وسري وعادي. ثم نعطي الصلاحيات بناء على هذه التقسيمات.

.يمكن حماية سرية البيانات بالتشفير، ولا يصل إلا البيانات إلا من يملك مفتاح فك التشفير.

التماسك Integrity

.يعني الحماية من العبث ببيانات الشركة من التخريب والتعديل المقصود أو غير المقصود من الأشخاص الغير مصرح لهم

.النسخ الاحتياطية هامة جدا لاسترجاع البيانات المخربة

.يمكن استخدام الـ Hashing للتأكد من سلامة البيانات عند عملية النقل وهل وصلت بشكل سليم أم تم التلاعب بها في الطريق؟

تمرين فحص تماسك نسخة snortباستخدام برنامج HashCalc

.من أدوات الهاش المشهورة و

https://www.fileformat.info/tool/md5sum.htm يمكن استخدام برنامج هاش من الويب

512AHS وتستخدم دوال الهاش خوارزميات حسابية

التماسك – خواص دوال الهاش

خاصية الانتشار. :تعني انقطاع العلاقة بين شكل البيانات وشكل الهاش، فتغيير بسيط في البيانات يعطي هاش كود مختلف تماما.

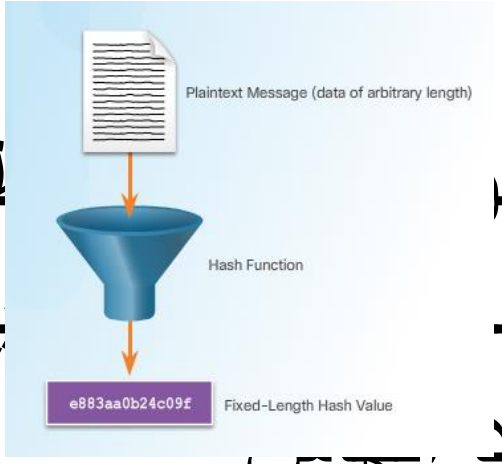
خاصية التشتيت. :تعني انقطاع العلاقة بين طول البيانات وطول الهاش .فكلمة من أربعة أحرف فقط تعطي هاش بطول 32حرف وملف 10جيجا أيضا يعطي هاش بطول 32حرف .

Ahmed	f1e43d880f09c64ac6378af6de47702
Ahmad	44bc2be4245c022748235a46dedf15
ملف كامل 100ميجا	c248c6b98c56ff0362bc4013eb33c8f

تمرين خاصيتي الانتشار والتشتيت

فحص التماسك Integrity Check

.عند تسجيل المستخدم في النظام لا يتم حفظ كلمة السر الخاصة به ولكن تحفظ الهاش الخاص بكلمة السر. وعند ولوج المستخدم ، يأخذ النظام كلمة السر المدخلة ويقوم بأجراء هاش عليها ثم يقارنها بالهاشات المخزنة ، وان وجد تطابق، يدخل المستخدم للنظام، والا لن يسمح بدخول المستخدم.



.عند إرسال بيانات م لطرف، يتم إرسال كود الهاش الخاص بالبيان يقوم المستقبل بفحص التماسك باستخدام كود هاش.

التوافر Availability

.تعني التوافر أن تقوم بحماية النظام مع توافره للمستخدمين

.فلا يعقل أن تحمي أموال البنك بغلق البنك أو أن تحمي نفسك على سبيل المثال بألا تخرج من المنزل ابدأ !!!

الإجراءات الوقائية للحفاظ على التوافر

.صيانة المعدات

.توفير نسخ احتياطية

.ترقية نظم التشغيل إلى احدث الإصدارات

.إعداد العدة لتجاوز الكوارث المحدثة من الإنسان كالحرق والتخريب المتعمد أو غير المتعمد

عواقب إفشاء أسرار الشركة

- تدمير السمعة :وذلك بالوعود الكاذبة والمضللة للعملاء ونشر شائعات عن الشركة تضعف من موقفها في السوق
- الفضيحة: تسريب للمعلومات الحساسة الخاصة بالشركة.
- السرقة :سرقة المعلومات الحساسة وإعطاءها للمنافسين مما يوحي بالاستيلاء على سلاح الدفاع وإعطاؤه للعدو كسلاح هجوم .وأحيانا الابتزاز.
- تحقيق الخسائر :وذلك بتعطيل الخدمات على الموقع الإلكتروني للشركة أو تعطيل خدمة خوادمها بهجمات مثل "هجمة تعطيل الخدمة."
- سرقة المعلومات الفكرية :وهو محاولة الاستيلاء على الخطط

مثال على اختراق الشركات | Vtech

- شركة الألعاب Vtech عانت من الاختراق الأمني لقواعد البيانات الخاصة بها في نوفمبر 2015.
- نجح المهاجمون في الحصول على المعلومات الشخصية مثل البريد الإلكتروني والأسماء وكلمات السر والصور الشخصية وسجل الدردشة الخاص بالمستخدمين.
- قد كانت المشكلة عند الشركة حيث أنها لم تستخدم نظام اتصالات مشفر ولذلك كانت البيانات سهلة المنال.
- بعد الهجمة توقفت اسهم الشركة في البورصة وخسرت كثيرا من المال.
- قامت بتشفير البيانات ولكنها استخدمت الهاش MD5 المعروف خوارزميته.

مثال على اختراق الشركات | lastpass

- لاحظ المراقبون نشاط غريب على الخوادم في 2015م.
- لحسن حظ الشركة لم يتمكن المهاجمون من الوصول إلى مفتاح فك شفرة البيانات.
- قامت الشركة بزيادة السرية على الموقع بالتأكد من صلاحيات المستخدم لو حاول الولوج من عنوان منطقي مختلف أو من جهاز مختلف توضيح عملي.
- وأيضا استخدام طريقة المفتاحين للدخول للموقع) .مثلا كلمة السر مع رسالة برقم سري إلى الجوال(.
- يجب على المهاجم أن يصل إلى كلمة السر الأساسية master password وهي كلمة السر التي يستخدمها العملاء للدخول إلى موقع الشركة.

سؤال ؟