IT Infrastructure

ITIS-323

Chapter-6

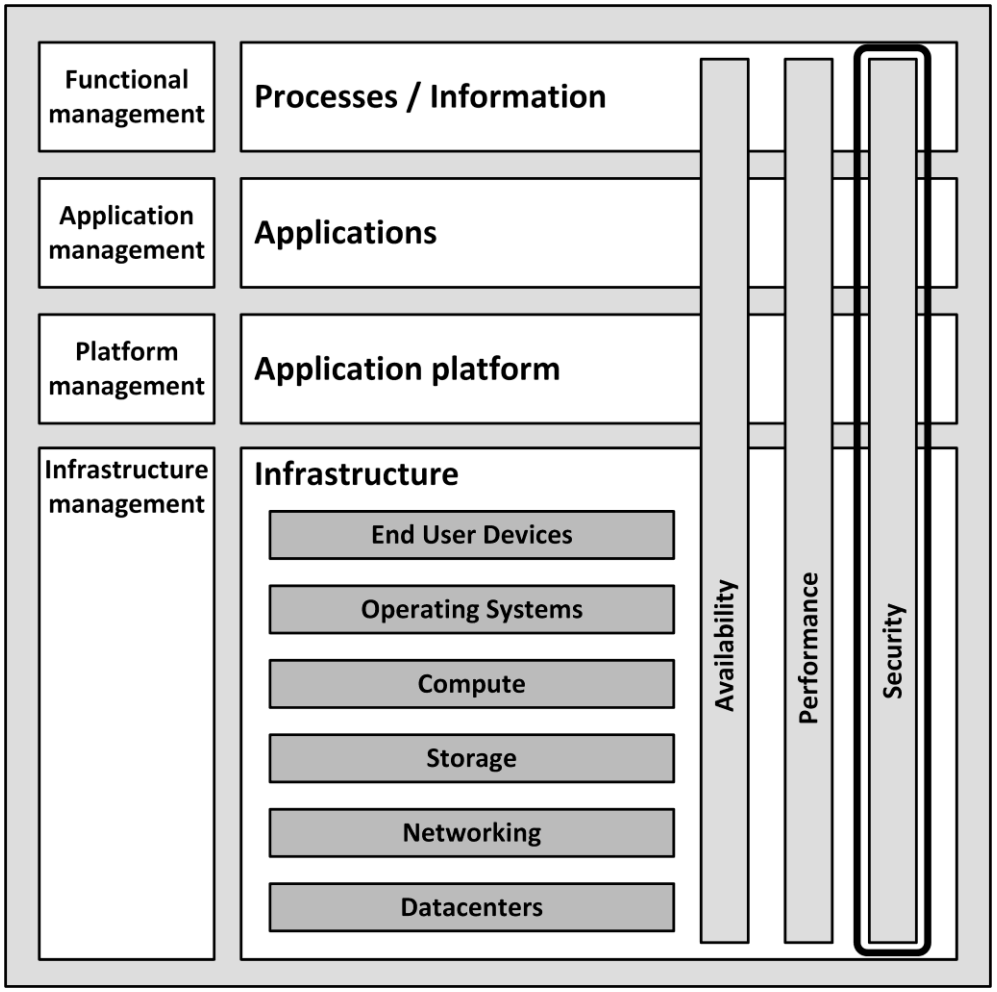
Dr Mohamed Abdeldaim Abdelhadi

2024

Lecture Overview

- ❑ Introduction
- ❑ Computer crimes
- ❑ Computer crimes
- ❖ Risk list
- ❖ Risk response
- ❑ Exploits
- ❖ CIA
- ❑ Security controls
- ❖ Attack vectors

Introduction



الأمن هو مزيج من:

- التوفر
- السرية
- النزاهة

يركز على التعرف على الهجمات ومقاومتها

بالنسبة للبنية التحتية لتكنولوجيا المعلومات
فإن التوافر هو سمة غير وظيفية في حد ذاته

Computer crimes

اسباب ارتكاب الجرائم ضد البنية التحتية لتكنولوجيا المعلومات:

- التعرض الشخصي والهيبة
- إحداث الضرر
- الكسب المالي
- الإرهاب

. الحرب

Risk management

Risk management

تتمحور إدارة الأمن حول إدارة المخاطر.

يجب أن يرتبط الجهد الذي نبذله في تأمين البنية التحتية ارتباطًا مباشرًا بالمخاطر المطروحة.

- إدارة المخاطر هي عملية من:

- تحديد مستوى مقبول من المخاطر
- تقييم المستوى الحالي للمخاطر
- اتخاذ خطوات لتقليل المخاطر إلى المستوى المقبول
- الحفاظ على هذا المستوى

Risk list

يمكن استخدام قائمة المخاطر لتحديد المخاطر الكمية
يتم حساب المخاطر بناءً على :

- اسم الأصل - المكون الذي يحتاج إلى الحماية
- الثغرة - نقطة الضعف - نقطة ضعف أو عملية أو تعرض مادي يجعل الأصل عرضة للاستغلال
- الاستغلال - طريقة لاستخدام واحدة أو أكثر من نقاط الضعف لمهاجمة أحد الأصول
- الاحتمالية - تقدير لاحتمالية حدوث الاستغلال
- التأثير - شدة الضرر عند استغلال الثغرة الأمنية

Risk list

- P=Probability
- I=Impact
- R=Risk

Asset	Vulnerability	Exploit	P	I	R
Laptop	Laptop gets stolen	Sensitive data on hard disk is exposed	5	3	15
Printer	Printer hard disk contains sensitive data	Repair man could swap hard disk and the hard disk could get on the market with sensitive data	1	3	3
Work-stations	Virus attack unknown to virus scanner	Unavailability or disclosure of data	2	3	6
SAN storage system	Data protection via LUN masking contains error	Data could get exposed to wrong server	1	2	2

Risk response

هناك أربع استجابات للمخاطر:

- قبول الخطر
- تجنب المخاطرة - عدم القيام بأعمال تنطوي على المخاطرة
- نقل المخاطر - على سبيل المثال نقل المخاطر إلى شركة تأمين
- التخفيف من المخاطر وقبول المخاطر المتبقية

Exploits

يمكن سرقة المعلومات بطرق عديدة ,أمثلة على ذلك:

- يمكن لمسجلي المفاتيح إرسال معلومات حساسة مثل كلمات المرور إلى أطراف ثالثة
- يمكن لأدوات شم الشبكة إظهار حزم الشبكة التي تحتوي على
- معلومات حساسة أو إعادة تشغيل تسلسل تسجيل الدخول
- يمكن أن تصل البيانات الموجودة على الأشرطة الاحتياطية خارج المبنى إلى الأيدي الخطأ
- يمكن أن تصل أجهزة الكمبيوتر أو الأقراص التي تم التخلص منها إلى الأيدي الخطأ
- يمكن للموظفين الفاسدين أو غير الراضين نسخ المعلومات
- توجيه المستخدمين النهائيين إلى موقع ويب خبيث يسرق المعلومات (التصيد الاحتيالي)

CIA

ثلاثة أهداف أساسية للأمن (CIA):

- السرية - تمنع الإفصاح المتعمد أو غير المتعمد غير المصرح به للبيانات
- النزاهة - تضمن أن:

- لا يتم إجراء أي تعديلات على البيانات من قبل موظفين أو موظفين غير مصرح لهم
- العمليات
- لا يتم إجراء تعديلات غير مصرح بها على البيانات من قبل موظفين أو عمليات مصرح بها.
- اتساق البيانات

- التوفر - يضمن الوصول الموثوق به وفي الوقت المناسب إلى البيانات أو موارد تكنولوجيا المعلومات من قبل الموظفين المناسبين

CIA

- Example of confidentiality levels

Confidentiality Level	Description
1	Public information
2	Information for internal use only
3	Information for internal use by restricted group
4	Secret: reputational damage if information is made public
5	Top secret: damage to organization or society if information is made public

CIA

- Example of integrity levels

Integrity Level	Description
1	Integrity of information is of no importance
2	Errors in information are allowed
3	Only incidental errors in information are allowed
4	No errors are allowed, leads to reputational damage
5	No errors are allowed, leads to damage to organization or society

CIA

- Example of availability levels

Availability Level	Description
1	No requirements on availability
2	Some unavailability is allowed during office hours
3	Some unavailability is allowed only outside of office hours
4	No unavailability is allowed, 24/7/365 availability, risk for reputational damage
5	No unavailability is allowed risk for damage to organization or society

Security controls

ضوابط تخفيف المخاطر
يجب أن تعالج الضوابط الأمنية واحدًا على الأقل منCIA
يمكن تصنيف المعلومات بناءً على مستوياتCIA
يمكن تصميم الضوابط وتنفيذها استنادًا إلى مستوى المخاطر
المحددة ل CIA

Security controls

- Example

Control	C 1	C 2	C 3	C 4	C 5		I 1	I 2	I 3	I 4	I 5		A 1	A 2	A 3	A 4	A 5
Standard security policy	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X
Central archiving of documents		X	X	X	X												
User based password protection		X	X	X	X			X	X	X	X			X	X	X	X
Anti-virus measures		X	X	X	X			X	X	X	X			X	X	X	X
Screensaver lock when leaving workplace			X	X	X				X	X	X						
Webmail not allowed			X	X	X												
Logging of authentication and authorization requests			X	X	X				X	X	X				X	X	X
Secured datacenter and systems management room				X	X					X	X					X	X
Encrypted laptops				X	X												
Security key management				X	X												
Penetration hack-tests				X	X					X	X					X	X
IDS systems				X	X					X	X					X	X
Internet access limited to specific sites				X	X					X	X					X	X
Encrypted e-mail				X	X												
Printing only allowed in specific closed rooms				X	X												

Attack vectors

- التعليمات البرمجية الخبيثة

التطبيقات التي، عند تنشيطها، يمكن أن تتسبب في زيادة التحميل على الشبكة والخادم، أو سرقة البيانات وكلمات المرور، أو مسح البيانات

- الديدان

البرامج ذاتية التكرار التي تنتشر من كمبيوتر إلى آخر، تاركةً عدوى أثناء انتقالها

- الفيروسات

جزء من برنامج ذاتي التكرار يرفق نفسه ببرنامج أو ملف يمكّنه من الانتشار من كمبيوتر إلى آخر، تاركاً عدوى أثناء انتقاله

- حصان طروادة

يبدو أنه برنامج مفيد ولكنه في الواقع يسبب ضرراً بمجرد تثبيته أو تشغيله على جهاز الكمبيوتر الخاص بك

Attack vectors

هجوم الحرمان من الخدمة

- محاولة لزيادة التحميل على البنية التحتية للتسبب في تعطيل الخدمة
- يمكن أن يؤدي إلى تعطل النظام، مما يعطل المؤسسة عن أداء أعمالها
- في هجوم الحرمان من الخدمة الموزع (DDoS) يستخدم المهاجم العديد من أجهزة الكمبيوتر لزيادة التحميل على الخادم
- تقوم مجموعات من أجهزة الكمبيوتر المصابة بشفرة خبيثة، تُسمى شبكات الروبوتات، بتنفيذ الهجوم

Attack vectors

- تدابير DDoS الوقائية:
  - تقسيم الأعمال والموارد العامة
  - نقل جميع الموارد التي تواجه الجمهور إلى موفر سحابة خارجي
  - إعداد قابلية التوسع التلقائي (التحجيم التلقائي والنشر التلقائي) باستخدام المحاكاة الافتراضية وتقنية السحابة
  - الحد من عرض النطاق الترددي لحركة مرور معينة
  - قم بتقليل وقت البقاء (TTL) لسجلات DNS لتتمكن من إعادة توجيه حركة المرور إلى خوادم أخرى عند حدوث هجوم
  - مراقبة الإعداد للكشف المبكر

Attack vectors

التدابير المضادة DDoS:

- أبلغ مزود الإنترنت الخاص بك على الفور واطلب المساعدة
- قم بتشغيل برنامج نصي لإنهاء جميع الاتصالات الواردة من نفس عنوان IP المصدر إذا كان عدد الاتصالات أكبر من عشرة
- التغيير إلى خادم بديل (بعنوان IP آخر)
- توسيع نطاق البيئة التي تواجه الجمهور ويتعرض للهجوم
- إعادة توجيه أو إسقاط حركة المرور المشتبه بها

Attack vectors

- الهندسة الاجتماعية
- تستخدم المهارات الاجتماعية للتلاعب بالأشخاص للحصول على المعلومات التي يمكن استخدامها في الهجوم
  - مثل كلمات المرور أو غيرها من المعلومات الحساسة
- بطبيعتها ، يريد الناس مساعدة الآخرين

Attack vectors

التصيد الاحتيالي

- تقنية للحصول على معلومات حساسة
- يرسل المخادع بريدا إلكترونيا يبدو أنه يأتي من مصدر شرعي ، مثل بنك أو شركة بطاقات ائتمان ، يطلب "التحقق" من المعلومات
- يحتوي البريد الإلكتروني عادة على رابط إلى صفحة ويب احتيالية

Attack vectors

الاصطياد

- يستخدم الاصطياد وسائط فعلية ، مثل محرك أقراص فلاش USB ، يترك ليتم العثور عليه
- يعتمد على فضول الناس لمعرفة ما هو عليه
- يأمل المهاجم أن يلتقط بعض الموظفين الجهاز ويحضره داخل المؤسسة
- عند وضع الجهاز في جهاز كمبيوتر مملوك للمؤسسة، يتم تثبيت البرامج الضارة تلقائيا

Any Questions…….?