TSIT01 Datasäkerhetsmetoder

Föreläsning 10: Del 2: Backuper, intrusion detection

Ingemar Ragnemalm

Lösenord

Tidigare föreläsningar:

- Starka lösenord
- Biometri, fingeravtrycksläsare mm
- Elektroniska nycklar, RFID, QR-koder...

Fråga för rapporterna: Effektivitet, kostnad?

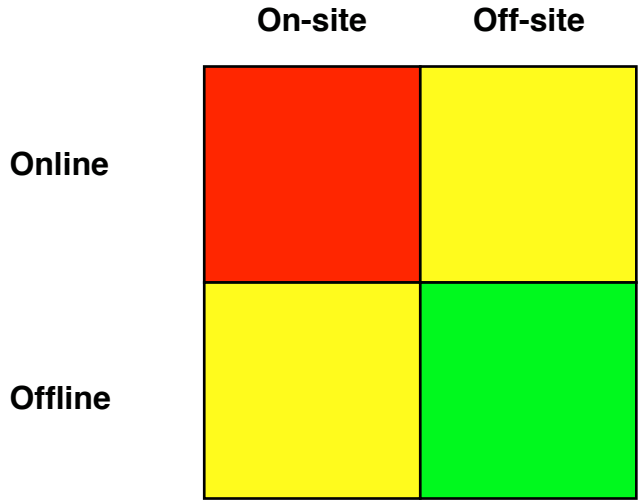
Åter till dessa backuper

3-2-1-metoden, vad betyder den?

- Allt i tre kopior
- Minst 2 media
- En på annan plats

3 och 1 viktiga, 2 tveksam

Backupmatrisen



Fyra fall

Online, on-site: Enkelt, billigt, osäkert

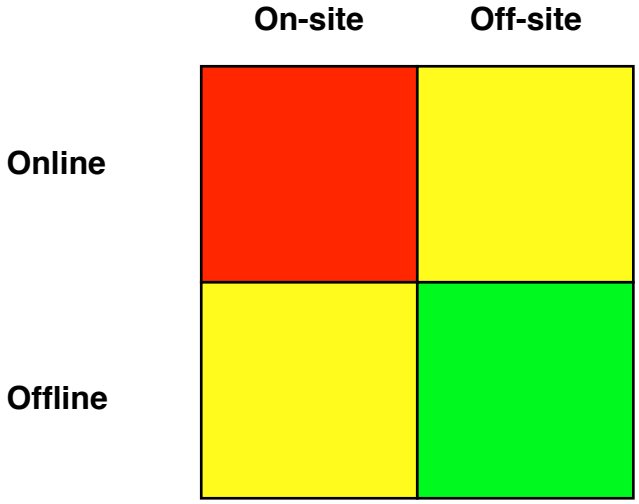
Offline, on-site: Känsligt mot onsite, inbrott, bränder mm

Online, off-site: Känsligt mot onlineattacker

Offline, off-site: Mycket säkert men dyrt

Dessutom: Skrivbarhet, förstörbarhet on-line.

Backupmatrisen vs 3-2-1



Val av backuper

Grafen tidgare? Om en av de tre kopiorna är på grönt eller två på var sin gul är säkerheten hög! Alla behöver (bör) inte vara på grönt!

WORM: Säkert mot onlineattacker men dyrt!

Räcker "röd" backup med tanke på den låga skadan?

Automatisk eller manuell? Automatisk är billigare i tid och säkrare i hur ofta det görs! Manuell är säkrare i kontroll, insyn.

Kostnad, behov, lämplighet?

Online är inte att lita på!

Du kan tappa kontot!

Många fall, inte minst på Facebook.

Microsoft locked my account - I lost 30 years of photo & work and they won't respond

Säkra dina data!

Intrusion detection

Intrusion detection

Hur ser vi att en attack pågår?

Kan vi identifiera angriparen?

Kan vi stoppa angreppet?

Kan vi vilseleda angriparen?

Intrusion Detection Systems (IDS) finns för att hantera detta.

Misstänkt beteende

Angripare beter sig annorlunda.

Problem: Gråzoner. False positives och false negatives måste undvikas.

Hur kan beteenden analyseras?

- Observerbara mätvärden
- Statistiska metoder
- Deep learning/AI

Typer av IDS

Host-baserade (HIDS)

Analyserar händelse inom systemet

Nätverksbaserade (NIDS)

Analyserar händelser på nätverket

Honeypots

"Honungsfällor", falska system för att lura angripare

- Skyddar de äkta systemen
- Samlar information om angriparen
- Får angriparen att hänga kvar så admin kan införa åtgärder

Vanliga användare har ingen anledning att besöka. Fullt synliga för angripare.

Typer av honeypots

"Low interaction", honungsfällan är en ren emulator. Enkel, saknar många funktioner.

"High interaction", ett faktiskt system, en separat dator med avsiktligt lägre säkerhet. Måste installeras med försiktighet.

Placering av honeypots

Utanför brandväggen: Lättåtkomlig för angripare, låg risk för övriga systemet. Kan inte upptäcka interna attacker.

Innanför brandväggen: Svårare att komma åt, detetekterar attacker inom systemet, men kan utnyttjas för att angripa det!

Script-honeypots

En slags honungsfälla är det dåliga attackscriptet!

Script kiddies vill ha färdiga scripts. Så ge dem dessa scripts... som går fel.

Kan både bromsa attacker och leverera information.

Exempel: Team Fortress 2 (ev fake - det är online)

Svårt säkerhetsproblem: Attacker i angriparens egen dator!

Red hat. Anfall på deras egen planhalva.

Antag att de flesta är script kiddies. Publicera "fusk" som fungerar dåligt. Lura script kiddies att använda dem.

Plötsligt flyttas problemet till dem, de måste lura ut vad som är fusk!

BILD SKIPPAD

Är det en honeypot?