



Benchmarking and Auditing

Kresten Jacobsen

Intro to System Security

Goals

Prevention

Detection

Recovery

C-I-A

Confidentiality

Integrity

Availability

Threats

Snooping

Modification

Spoofing

Repudiation of Origin

Denial of Receipt

Delay

Security Policies

Requirements

- Common understanding (implicit / explicit)
- Trust (in people and computers)
- Assumption (that policies are enforced)

Policy types

- Confidentiality
- Integrity Policy
- Availability Policy

Building Secure Infrastructures

You need

- Policies
- Procedures

Running systems which require

- Configurations
- Settings
- Supporting infrastructure – e.g. networks
- Supporting infrastructure – logging, dashboards, monitoring



Benchmarking - CIS 20 CSC

1 through 6: *Basic*

7 through 16: *Foundational*

17 through 20: *Organizational*

#1 AUTORISEREDE OG UAUTORISERDE NODER	#2 AUTORISERET OG UAUTORISERET SOFTWARE	#3 KONTINUERLIG SÅRBARHEDSVURDERING	#4 KONTROLLEDER BRUG AF ADMIN. RETTIGHEDER
Når en ny enhed installeres på et netværk, er der en risiko for at netværket udsættes for ukendte sårbarheder og fejl. Angribere kan udnytte nyt hardware, der ikke er konfigureret og patchet med de nyeste sikkerhedsopdateringer. Angribere kan gennem sådanne enheder installere bagdøre som senere kan bruges til kriminel aktivitet.	En organisation, der ikke aktivt vedligeholder et overblik over den software, der findes på dens netværk, er sårbar overfor angreb. Yderlige fører en mangelfuld software-håndtering til, at software installeres unødvendigt på maskiner og dermed medfører en større sårbarhed.	Cyberkriminelle udvikler deres værktøjer og teknikker næsten ligeså hurtigt, som forskere og leverandører lukker sårbarheder. Det er derfor vigtigt at patching f.eks. foregår effektivt, og at der tages bestik af det nuværende, opdaterede trusselsbillede.	Den mest almindelige metode, angribere bruger til at infiltrere en organisation, er gennem en medarbejders misbrug af privilegier. En angriber kan nemt overbevise en bruger om at åbne en ondartet vedhæftelse eller downloade en ondartet fil. Gennem denne infektion kan angriberen tage kontrol over brugeren og eskalere brugeren rettigheder.
#5 SIKRE KONFIGURATIONER AF HARD- OG SOFTWARE	#6 OVERVÅGNING OG ANALYSE AF AUDIT LOGS	#7 E-MAIL- OG BROWSERBESKYTTELSE	#8 MALWARE-FORSVAR
Default-konfigurationer af hard- og software er ofte ekstremt mangelfulde i forhold til it-sikkerhed. Sådanne enheder og systemer kan som regel udnyttes nemmere, og som følge deraf bliver de også oftere angrebet målrettet.	Nogle gange er audit logs det eneste sted, man kan finde beviser på et angreb. Mange organisationer opbevarer audit logs i henhold til compliance men gennemgår dem ikke. Når audit logs ikke regelmæssigt gennemgås, ved organisationen ikke nødvendigvis, om den er blevet kompromitteret. Dette udnyttes af cyberkriminelle.	Webbrowsere og e-mail-klienter er almindelige indgangs- og angrebssteder pga. direkte interaktion med brugere og andre systemer. Indhold kan designes til at lokke brugere til selv at komrommittere organisationens systemer. Sådanne komrommitteringer kan åbne systemet for andre angreb og føre til tab af værdifulde data og ressourcer.	Malware er en hjørnesten i internets trusselslandsby. Med slutbrugere som mål, leveres malware typisk gennem browsere, e-mails og mobile enheder. Den onsdindede kode kan indfange fortrolige data, sprede sig til beslægtede systemer og ødelægge deres indhold. Et effektivt forsvar mod malware er en automatiseret opdatering af anti-virussignaturer.
#9 BEGRÆNSNING OG KONTROL AF NETVÆRK	#10 MULIGHED FOR GENDANNELSE AF DATA	#11 SIKRE KONFIGURATIONER AF NETVÆRKSNODER	#12 PERIMETERBESKYTTELSE
Angribere søger ofte efter sårbare netværk og tjenester, der kan tilgås via fjernforbindelser. Mange software-pakker installerer sådanne tjenester som en del af den primære installation uden at informere om det.	Når angribere komrommitterer maskiner, foretager de ofte signifikante ændringer i konfigurationer og software. Nogle gange laver de også diskrete ændringer i data lagret på de komrommitterede maskiner og forringere organisationens operationalitet med forurenede data. Der bør en gang i kvartalet foretages en test af et restore af et tilfældigt systems data.	Angribere trænger gennem forsvar ved at finde huller i enheder som firewalls, routere og switches. Når disse netværksnoder først er komrommitteret, har angriberen adgang til sine målsatte netværk. Herfra kan angriberen om dirigere trafikken gennem sit eget onsdindedse system, som kan opsnappe og ændre informationer, mens de overføres.	Ved at angribe internett forbundne systemer kan angribere inficere et endpoint og herfra udfolde flere angreb på systemer og netværk. Hvis et netværks trafik-flow skal kontrolleres, og angreb skal opdagdes hurtigt, skal netværkets perimeterbeskyttelse opdeles i flere lag.
#13 DATABESKYTTELSE	#14 ADGANG BASERET PÅ NØDVENDIGHED	#15 KONTROLLERET ADGANG TIL WiFi	#16 OVERVÅGNING OG KONTROL AF BRUGERKONTI
Tab af beskyttede og følsomme data er en alvorlig trussel mod organisationens drift og medarbejdernes/borgernes privativ og sikkerhed. Selvom nogle data går tabt som et resultat af tyveri går majoriteten af data tabt som følge af dårligt integrerede retningslinjer.	Mange organisationer separerer ikke omhyggeligt følsom og mindre følsom information. Denne manglende kategorisering medfører som regel, at brugere har adgang til informationer på netværket, de egentlig ikke har adgang til. Hvis sådanne systemer komrommitteres, betyder det, at angriberen har adgang til en ubegrænset mængde data.	Angribere, der kan opnå wireless adgang til en organisation fra et nærliggende område, kan stjæle alvorlige mængder data og kan bibeholde adgangen i lange perioder, hvis de ikke opdagges. For at undgå sådanne angreb bør organisationer benytte scanningsværktøjer tilstæntt wireless intrusion og detection.	Angribere giver sig ofte ud for at være legitime brugere ved hjælp af inaktive brugerkonti. Denne metode gør det svært for netværksansvarlige at identificere angribernes adfærd. Selvom de fleste operativsystemer indeholder funktioner til logging af information om kontobrugen, er disse funktioner nogle gange deaktivert by default.
#17 AWARENESS-TRÆNING	#18 SIKKERHED PÅ APPLIKATIONSSOFTWARE	#19 CYBERBEREDSKAB	#20 PENETRATIONSTESTS
En organisation er afhængig af sine medarbejdere, hvis den ønsker at bekæmpe angreb effektivt. Et passende awareness-program, der vurderer medarbejdernes sikkerhedskvalifikationer, kan give beslutningstagere handlingsrettede informationer om, hvordan sikkerhedsvidstanden skal forbedres.	Kriminelle organisationer angriber som regel sårbarheder i både web-baserede og lokale applikationer. For at kunne stå imod angribernes udnyttelse af sårbarheder bør tredjeparters applikationer være grundigt testet for at finde eventuelle sikkerhedsbrister.	Uden en incident response plan opdager en organisation måske ikke et angreb i første omgang, og selvom angrebet opdagtes, følger organisationen måske ikke de rigtige procedurer for at begrænse skaden, fjerne angrebets tilstede værelse og genskabe sikkerheden og de tabte data.	I penetrationstests efterlyges angribernes adfærd i et forsøg på at penetrere organisationen. Testene afdekket sårbarheder og huller i organisationens systemer. Når sårbarhederne er afdekket, kan de efterfølgende mitigeres.



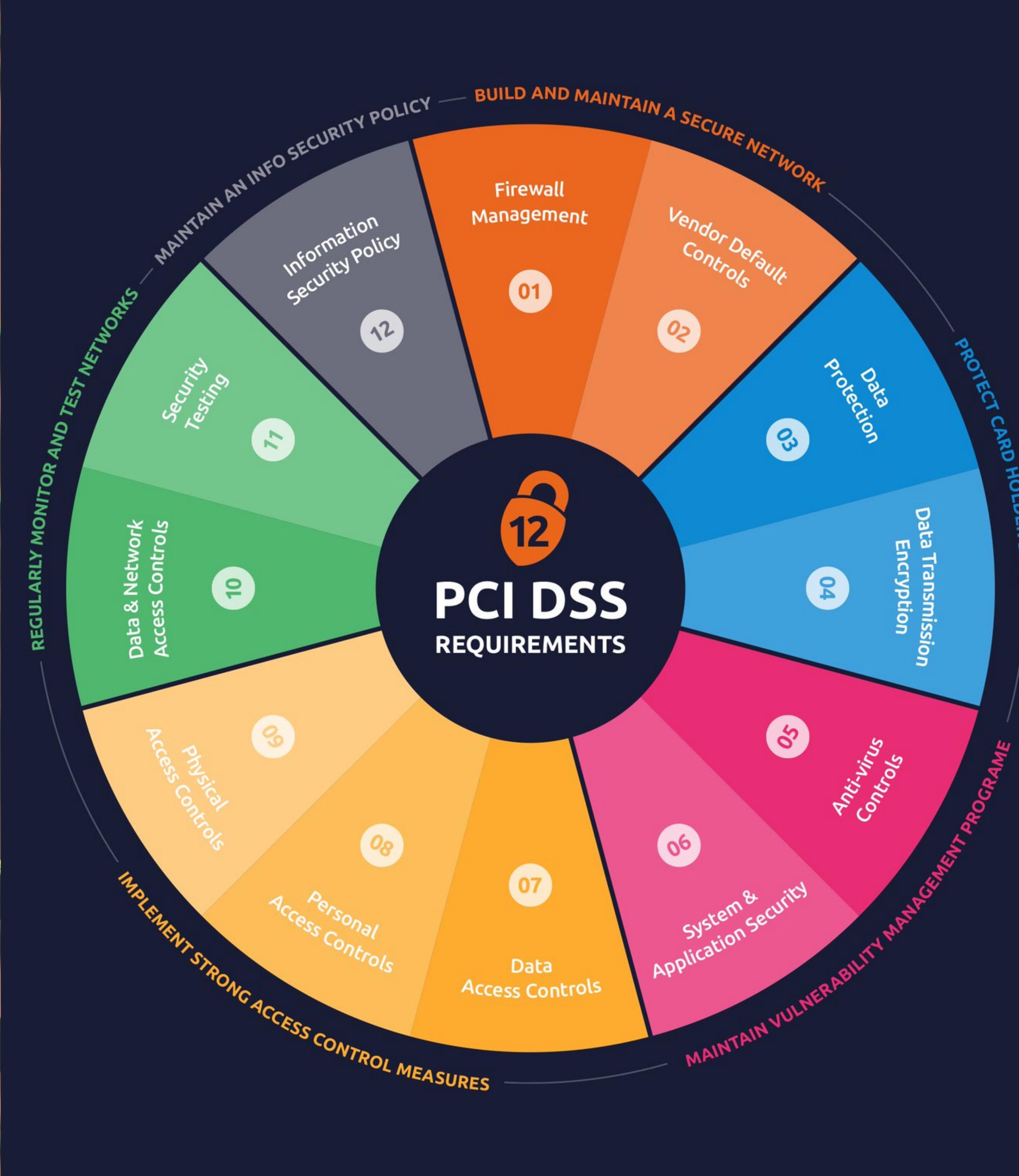
Compliance

Why?

- A formal system
- Requirement
- Accountability
- Transparency

Controversy

- C.Y.A.?
- Checkmark Security?



Auditing - PCI DSS

Build and Maintain a Secure Network

Protect Cardholder Data

Maintain a Vulnerability Management Program

Implement Strong Access Control Measures

Regularly Monitor and Test Networks

Maintain an Information Security Policy

