



Sikkerhedsledelse:

Sikkerhedsverdenen
Politikker og procedurer
Beredskabsplaner
Risikovurderinger
Awareness
Fysisk sikkerhed

Carsten Jørgensen
Department of Computer Science



IT sikkerhed – mange ting

Hele kæden:

Predict - Prevent – Detect - Respond

Tænk sikkerhedskæden som:

Trusselvurdering, system design (system og procedurer), og derefter test



Sikkerhedsledelse – eksempler på CISO opgaver

- Sikkerhedsstrategi
- Skrive og vedligeholde sikkerhedspolitikker
- Ledelsesrapportering
- Risiko vurderinger og sikkerhedschecks
- Sikkerhedsvurderinger af nye løsninger
- Svare på spørgsmål om sikkerhed fra organisationen
- Koordinering af sikkerhedsaktiviteter
- Håndtering af intern og ekstern revision
- Awareness træning
- Holde øje med ændringer i risikobilledet
- ...



Behovet for it-sikkerhed, også når det går galt

IT-sikkerhed



Offensiv it-sikkerhed

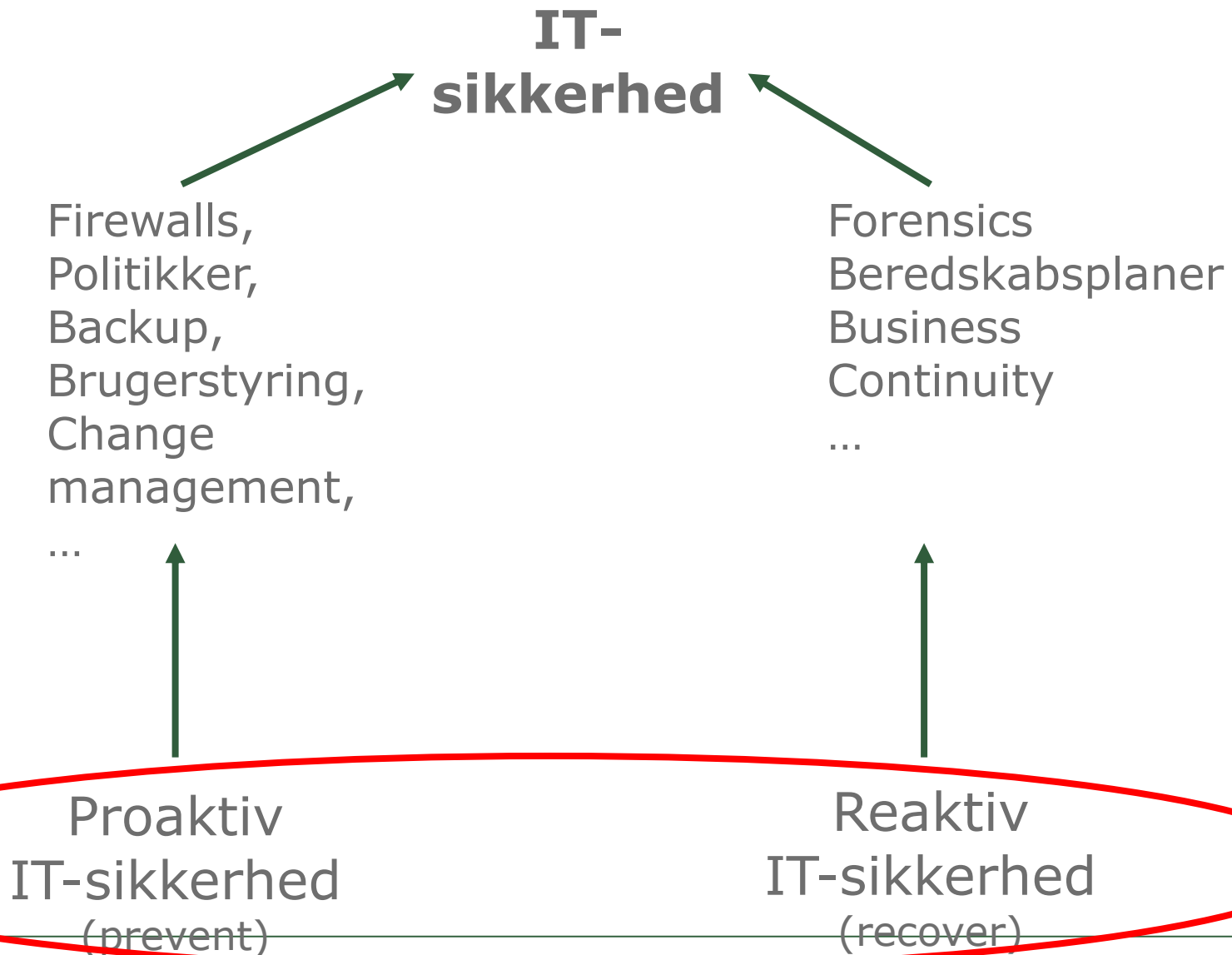
- Penetrationstest
- Code reviews
- ...

Defensiv it-sikkerhed

- Sikkerhedsledelse
- Sikkerhedsarkitektur
- Brugerstyring
- ...



Behovet for it-sikkerhed, også når det går galt





Lovgivning omkring sikkerhed

Aktivitet på alle fronter

GDPR

ENISA

EU arbejder i en række
arbejdsgrupper

NIS

NATO

Internationalt

Ransomware og andre store
sikkerhedshændelser til
bestyrelserne

Antal sikkerhedsfolk 1->2 ->
5 -> 20 -> 150 -> ... ->
6.000

THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS



Produced and supported by
BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL

BIMCO

CLIA



International
Chamber of Shipping
Shaping the Future of Shipping



INTERCARGO
International Association of Dry Cargo Shipowners


InterManager


INTERTANKO


IUMI
International
Union of
Marine Insurance


OCIMF


WORLD SHIPPING COUNCIL
PARTNERS IN TRADE

Kritisk infrastruktur – foranstaltninger til håndtering af sikkerheden

NIS – Network and Information Systems

CIP – Critical Infrastructure Protection

OES – Operator of Essential Services

Sektorer, som leverer kritiske ydelser til samfundet
betydning for opretholdelsen af samfundskritiske funktioner
og tjenester

- Energisektoren
- IT- og Teleområdet
- Transportsektoren
- Fødevarerektoren
- Sundhedssektoren

Nedbrud kan medføre
dramatiske konsekvenser



Kritisk infrastruktur – foranstaltninger til håndtering af sikkerheden

EU NIS Directive (NIS-D): The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU

National capabilities:

EU Member States must have certain national cybersecurity capabilities, eg they must have a national CSIRT, perform cyber exercises etc.

Cross-border collaboration:

Cross-border collaboration between EU countries, eg the EU CSIRT network

National supervision of critical sectors:

EU states must supervise the cybersecurity of critical market operators



Kritisk infrastruktur – foranstaltninger til håndtering af sikkerheden

Sektoransvarsprincip: Den enkelte sektor har ansvaret for at sikre et beredskab, så samfundets kritiske funktioner kan opretholdes

Tyskland: Straf på 100.000EUR per sikkerhedshændelse

Næste år forventes stafferammen at komme op på niveau med GDPR: "Op til 20.000.000 EUR eller op til 4% af virksomhedens globale årlige omsætning"

"As a rule reference should be made to the state of the art generally recognised for the field of application in question in the form appropriate for the fulfilment of the given protection aim."

ISO 27001 certificering

Install technical precautions in form of systems, capable of detecting attacks on the IT infrastructure





Faculty of Science



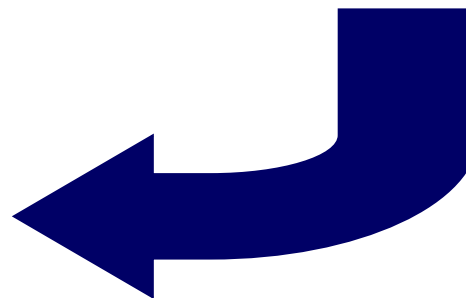
Sikkerhedsledelse

Behovet for it-sikkerhed

**IT-sikkerhed -
hvad er det
rigtige niveau ??** →

- Det kan være svært at afgøre, hvad det rette niveau skal være.
- "Høj" sikkerhed er ikke altid nødvendigt
- "Lav" sikkerhed kan være katastrofalt !
- "Best practice" ?

**Det er
forretningen og
lovgivningen der
stiller krav til
sikkerhedsniveau**



Behovet for it-sikkerhed

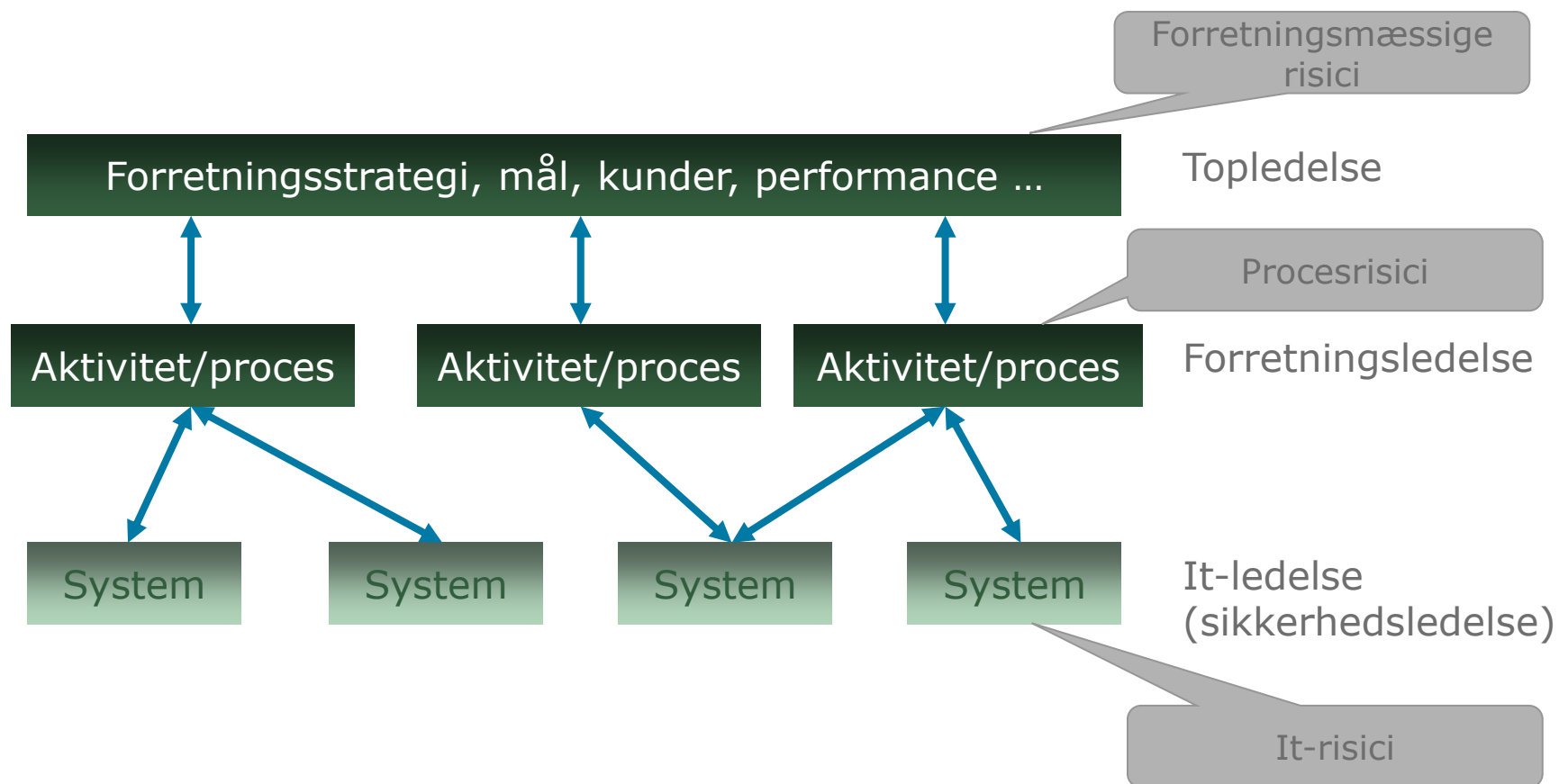
Sikkerhedsledelse

Compliance

Risikovurdering og risikohåndtering



I forretningsmæssig kontekst





Politikker, procedurer, guidelines

Sikkerhedspolitikker og procedurer

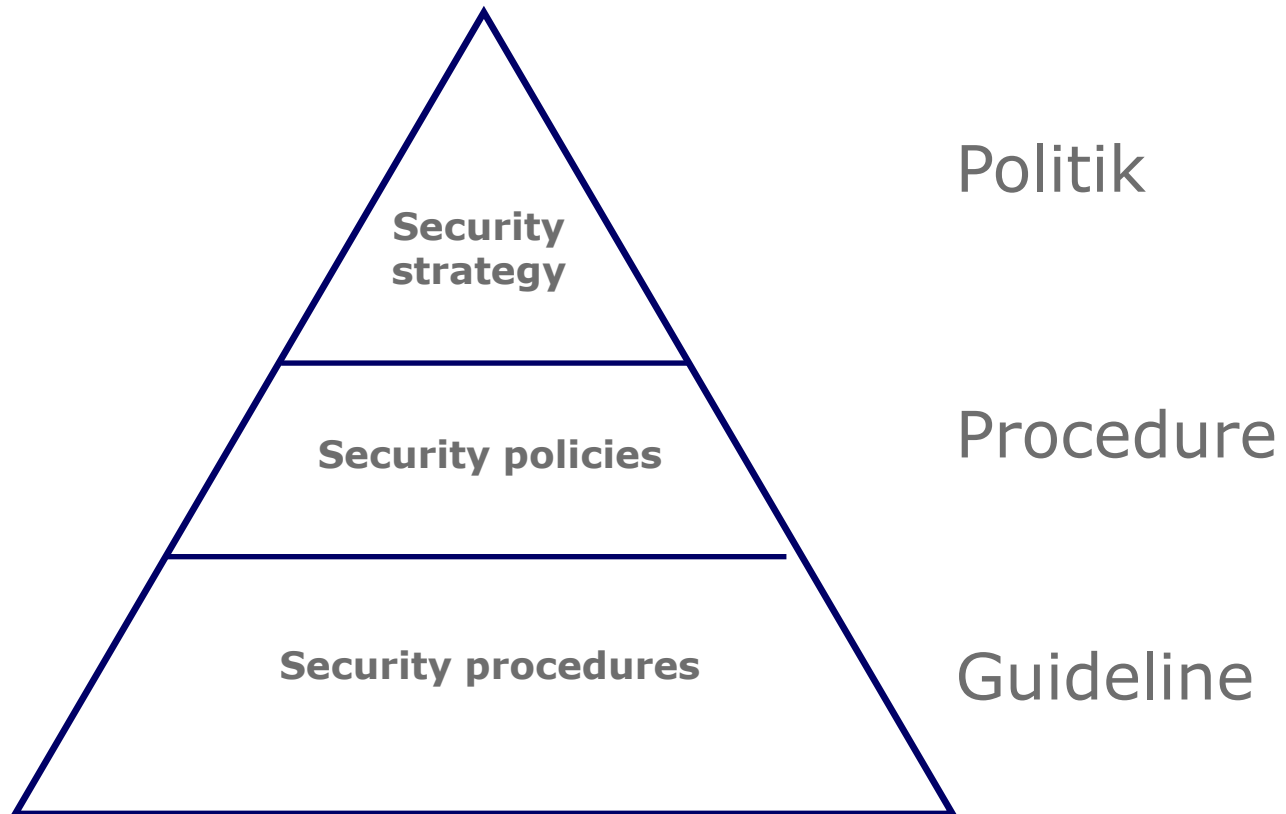
- Må jeg åbne port 81 fra Any til Any?
- Må Alice få admin-rettigheder til økonomisystemet?
- Må Bo rette direkte i databasen?
- Må jeg sende dokumenterne i en mail til kunden?
- Må udviklerne teste med produktionsdata?
- Må jeg udlevere information over telefonen?

Hvem tager beslutningen?

Hvad er beslutningen baseret på?



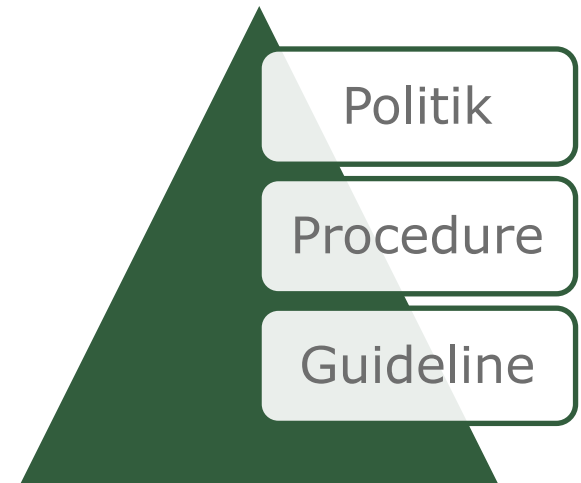
Sikkerhedsmål



Sikkerhedsmål

Sikkerhedspolitik :

Definerer mål, det er strategien.
Hvorfor, ikke hvordan.

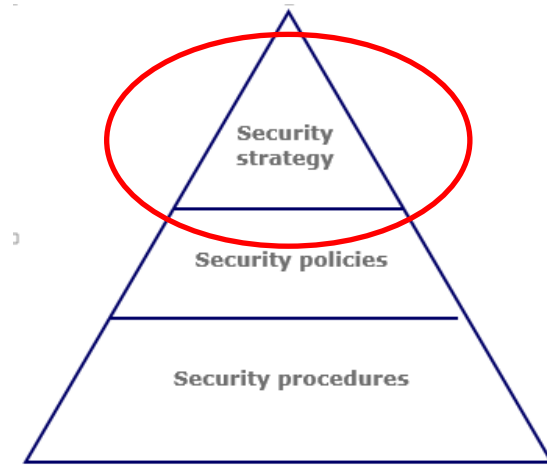


Sikkerhedsguidelines:

Detaljeret specifikation, definerer hvordan en sikkerhedspolitik skal implementeres i et specifikt produkt eller specifik situation.

Bruges som målepunkt for at vurderer om de udførende har gjort deres arbejde.

Strategy - eksempel



1 Purpose

The Falck Group organization depends on IT systems to a great extent to achieve its daily operations and business goals.

This IT Security Strategy defines the directions for the IT Security Policies and Procedures necessary to maintain stable and trustworthy IT services to all business entities within the Falck Group.

The purpose of the IT Security Strategy is to:

- Ensure contractual obligations can be met, including ensuring that Falck Group can provide assistance in situations of emergency
- Minimize the risks of financial losses
- Maintain business system availability
- Ensure regulatory compliance
- Maintain customer and partner confidence
- Protect intellectual property and safeguard the Falck Group brand

Sikkerhedspolitikker



8.9 Secure disposal or re-use of electronic equipment and other media

Overwriting

Before equipment can be disposed or reused outside Falck Group all data must be securely overwritten using specialized software. Alternatively the storage media must be physically destroyed.

The standard “*delete*” and “*format*” functions do not remove data from electronic equipment. Therefore specialized disk or device “sanitation” software, such as the free DBAN software must be used to erase the data by completely overwriting the disk.

Eksempler på dokumentation

Procedure for system dokumentation
 Procedure for Identifikation og Klassifikation af Informationsaktiver
 Procedure for Patch- Change- & Configuration Management
 Procedure for backup / sikkerhedskopiering
 Procedure for Informationsudveksling
 Procedure for fejlhåndtering & support
 Procedure for håndtering af følsomme oplysninger
 Procedure for data destruktion / data wipe
 Procedure for logning / kontrolspor
 Procedure for vedligehold og forbedringer
 Procedure for risiko og sårbarhedsanalyser
 Procedure for trussels vurderinger
 Procedure for Change Management / ændringsprojekter
 Procedure for funktionsadskillelse
 Procedure for Håndtering af eksterne Leverandører
 Procedure for Håndtering af eksterne samarbejdspartnere
 Procedure for Netværks- og system sikkerhed
 Procedure for Adgangs- og brugerstyring (IAM)
 Procedure for Sikkerhedshændelser / Incident Management
 Procedure for Fysisk sikkerhed
 Procedure for nød- og beredskabsplaner
 Procedure for Informations- og it-sikkerheds awareness / træning
 Procedure for databærende medier & mobilt udstyr
 Procedure for kryptering
 Procedure for beskyttelse mod vira, malware og ondsindet/uønsket programmel
 Procedure for brug af trådløse netværk
 Procedure for anskaffelse og udvikling samt vedligehold af it-systemer



Formatet på dokumentationen er vigtig



Eksempel på dokumentation

Dokument / Tekst samling	Indhold	Målgruppe	Anvendelse / Formål
IT-sikkerhedshåndbog	IT-sikkerhedspolitik og strategi. Retningslinier, forholdsregler og generel information	Ledelsen, alle medarbejdere, samt eksterne ressourcer	Beskriver overordnet niveauet på XXX's IT-sikkerhed, hvordan IT-sikkerheden opretholdes, og herunder hvilke retningslinier som skal følges.
IT-driftshåndbog	Instrukser og beskrivelse af arbejdsgange for drift af IT-systemerne. Teknisk dokumentation af systemerne	IT-afdelingen samt delvis system- / dataejere i øvrige afdelinger	Skal fungere som drejebog og dokumentation for drift af XXX's IT-system og derigennem sikre ensartethed, og person- uafhængighed.
IT-sikkerhedsdokumentation	Underskrevne / godkendte blanketter, f.eks. ved brugeroprettelse. Tro og love erklæringer. Kontrollerede og godkendte sikkerheds- rapporter / logs.	IT-afdelingen, ledelsen, berørte system- / dataejere i øvrige afdelinger	Sikre at denne type papirbaseret dokumentation med underskrifter opbevares sikkert og overskueligt.
CM / PM	Registrering af problem og forandringer med sikkerhedsmæssig eller driftsmæssig betydning.	IT-afdelingen	Kombineret dokumentation og videndatabase. Udførte forandringer / fejlrettelser bliver dokumenteret elektronisk et sted.
IT-brugsvejledning	Brugerrettede instrukser, vejledninger og gode råd i sikkerhedsmæssigt korrekt brug af systemerne.	Alle brugere	Sikre, at brugerne har adgang til tilstrækkelig information for, at kunne overholde XXX's IT-sikkerheds politik, strategi og retningslinier, ved brug af systemerne.
System- og dataklassificeringer	Identificering, placering af ansvar, beskrivelse og sikkerhedsmæssig klassificering for hvert system og hver datagrube.	IT-afdelingen samt berørte system- / dataejere i øvrige afdelinger	Udgør overordnet, samt sikkerhedsmæssig, beskrivelse / dokumentation af systemer og datagrupper. Fungerer også som en aftale mellem systemejere / dataejere og IT-afdelingen i lighed med SLA'er
SLA (er)	Beskrivelse af aftalt serviceniveau i forskellige situationer, og for forskellige delsystemer	IT-afdelingen samt berørte system- / dataejere i øvrige afdelinger	Sikrer, gennem underskrevne aftaler, at systemejere og dataansvarlige er enige med IT-afdelingen om indsatser og responstider for opretholdelse af tilgængelighed og sikkerhed for hvert system og hver datagrube, som beskrevet i respektive klassificering
Risikovurderinger	Beskrivelse af hver gennemført risikovurdering i kronologisk orden	Ledelse og IT-afdelingen, samt delvis system- / dataejere i øvrige afdelinger	Risikovurderinger skal dels forebygge at sikkerhedsmæssige aspekter ikke overses ved forandring af IT-systemerne, og dels udgøre en del af beslutningsgrundlaget for gennemførelse af en forandring. Samling af risikovurderinger i kronologisk orden letter revision



Compliance

Compliance:

Is driven by business needs

Is practiced to satisfy external third party requirements and facilitate business operations

Is “done” when the third party is satisfied

Security:

Is driven by the need to protect against constant threats to an organization's assets

Is not practiced to satisfy a third party's needs, but will usually address many 3rd party needs

Sikkerhedsmål - Compliance



Compliance er en baseline

Security Compliance

- Audit process to review security processes
- Goal is to verify compliance with security plan
- Use internal or external personnel
- Usually based on use of checklists which verify:
 - Suitable policies and plans were created
 - Suitable selection of controls were chosen
 - That they are maintained and used correctly
- Often as part of wider general audit



ISO 27001/27002 – mange områder man ofte glemmer

1. Overordnede retningslinier

Sikkerhedspolitik, m.m

2. Organisering af informationssikkerhed

Ansvarsforhold, m.m

3. Styring af informationsrelaterede aktiver

*Ejerskab, **klassifikation**, m.m*

4. Medarbejdersikkerhed

*Ansættelse, uddannelse, **jobophør** m.m*

5. Fysisk sikkerhed

Sikring af bygning og udstyr, el m.m

6. Styring af netværk og drift

*Drift, **ændringer**, **funktionsadskillelse**, **ekstern drift**, netværkssikkerhed, online systemer, **overvågning** m.m*

7. Adgangsstyring

Brugeradm., adgangskoder, adgang til netværk, segmentering m.m

8. Indkøb, udvikling og vedligeholdelse af informationsbehandlingssystemer

*Kravspec., **kontroller**, kryptografi, ændringsstyring, mobilt udstyr m.m*

9. Styring af sikkerhedsbrud

Rapportering, håndtering, beviser m.m

10. Beredskabsstyring

***Beredskabsplaner** m.m*

11. Overensstemmelse med lovbestemte og kontraktlige krav

Lovgivning, systemrevision, m.m



ISO 27001/27002 – et redskab

version



IT-NYHEDER

BLOGS

IT-JOB

IT-JOB

IT-FIRMAER

WHITEPAPER

Sektioner: Datacenter Karriere Kultur Ledelse Mobil og tele Offentlig it Sikkerhed

nsen

18

ISO27001 (DS484) vs. IT sikkerhed

Hvis man tror at ISO27001 (DS484) er en væsentlig del af en IT sikkerheds strategi.

Så skal man have sine skolepenge tilbage.

Det er en række overfladiske anbefalinger på niveau med "husk nu at låse døren til serverrummet og før regnskab med hvem der officielt har en nøgle udleveret."

Tilsammen udgør de måske 1% af det der skal til for at man kan påstå at have nogenlunde styr på sin IT sikkerhed.



11



0

anmeld

log ind

eller

opret en konto

for at skrive kommentarer

27001-
r under

g viden
r ud fra et

fælles koncept.

Det skal implementeres under vejledning af Digitaliseringsstyrelsen, og der bliver oprettet et videnscenter i samarbejde med Statens It, som kan rådgive om implementeringen af ISO27001, eventuelt i forenklet form.

Sikkerhedsmål

Hvordan vurderer man hvad der skal beskyttes,
hvordan det skal beskyttes –
og hvor mange ressourcer skal indsættes ?



Sikkerhedsledelse

- Sikkerhed er ikke (kun) teknik, sikkerhed er ikke (kun) it-afdelingens ansvar
- Sikkerhed er relevant uanset hvor stor en virksomhed er

IT-sikkerhed er en forretningsrisiko, derfor er det ledelsens ansvar

Ledelsen kan ikke uddelegere ansvaret
(men man kan uddelegere udførsel)





Beredskabsplaner

Business Continuity

Accidents happens



19 April 2014 Last updated at 21:46 GMT



Family's car catches fire in Longleat lion enclosure



Driver Helen Clements talks about the moment her car caught fire: "Luckily we couldn't see the lions"



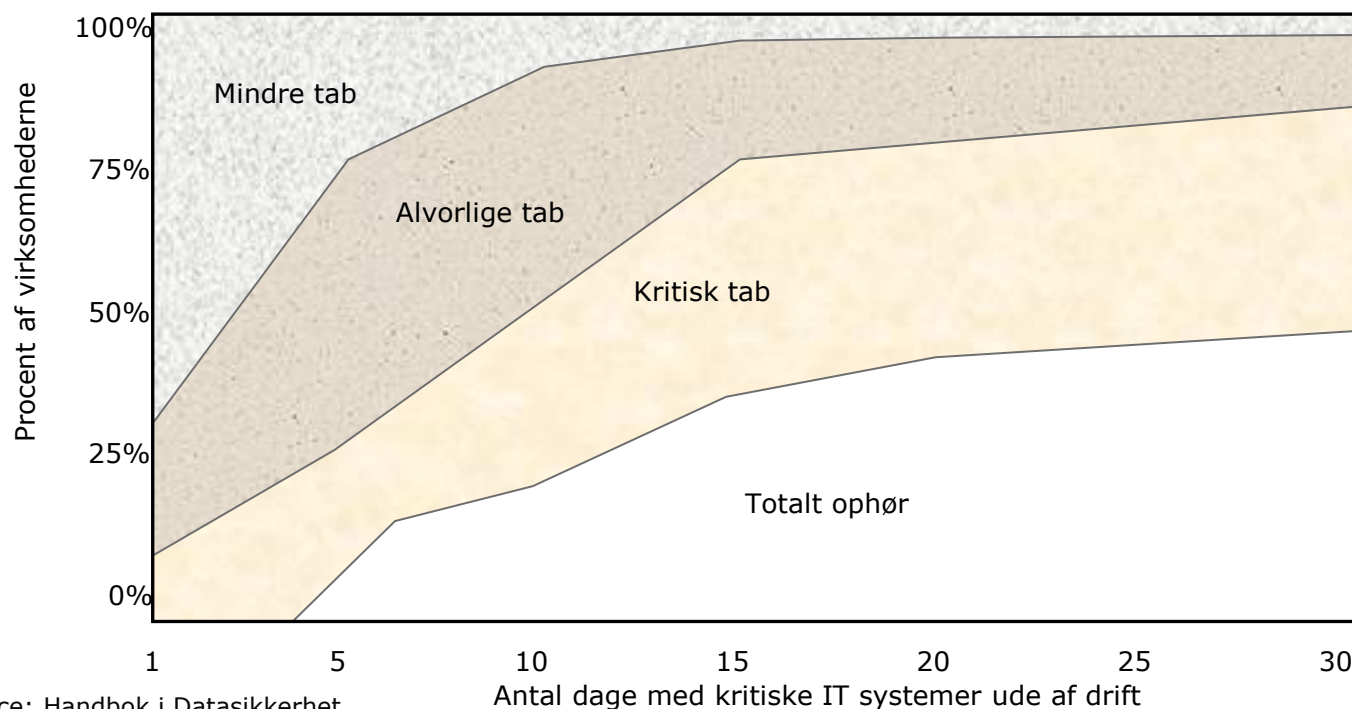
FUCK

you be any more unfortunate

HVORFOR er beredskab vigtigt?

Nedbrud af IT-services vil have en stor betydning for de fleste virksomheders overlevelsessevne.

Kan derfor true virksomhedens overlevelsessevne.



Source: Handbok i Datasikkerhet



Brand i Apotekerforeningen



It-chef efter brand i København: Godt vi fik remote backup

En voldsom ildebrand i Apotekerforeningens bygning har raseret flere etager. Men udover nogle nedbrændte desktop-computere kan it-chefen tage situationen roligt på grund af fuld backup-løsning, fortæller han.

AF JESPER KILDEBOGAARD, TIRSDAG 04. MAJ 2010 KL. 13:16
EMNER: BACKUP DISASTER RECOVERY IT-DRIFT

Ilden har ødelagt alt på de øverste etager i Dehns Palæ i København, hvor Dansk Apotekerforening holder til. Et potentielt mareridt for en it-ansvarlig, men ikke noget voldsomt problem for Niels Braae, Apotekerforeningens it-chef.

»Vi har fuld backup at det hele på en ekstern lokation, så vi mister ikke et eneste vigtigt bogstav. Og serverrummet står ikke i den del af bygningen, der brænder, så der er ikke noget centralt, der er ramt,« fortæller han via mobiltelefon tirsdag middag, mens brandvæsenet stadig kæmper for at få kontrol over ilden.



ISS-ansatte er ved at redde værdier ud af Dansk Apotekerforenings hovedkvarter i Dehns Palæ i Bredgade i København. (Foto: Kenneth Meyer)

Når kunderne ikke kan betjenes som de plejer

- Hvor længe kan et helt eller delvis udfald af IT i forretningen accepteres?
- Hvordan og hvilke forretningsprocesser skal kunne afvikles ved en beredskabssituation?
- Er det overhovedet muligt at klare opgaverne uden IT?
- Hvor omfattende en situation skal beredskabet indrettes efter?
- Hvilke forebyggende foranstaltninger bør igangsættes for lettere at kunne håndtere en beredskabssituation?



Case



FAIL

EVACUATION PLAN

Run and run
as fast as you
can



FAIL

Beredskab

Adobe Reader

62 / 76 177% Tools Sign Comment

12 Business IT Service Continuity and Major Incident/Disaster Recovery

12.1 Falck Group IT Service Continuity and Recovery

Ad hoc teams as well as recovery plans and procedures must be established to minimize the effects of major incidents and disasters associated with IT services in Falck Group, such as loss of service or equipment, virus infections, attacks originating on the internet, fire, fire in neighboring property or natural disasters.

Falck Group Entities must create IT Continuity and Major Incident/Disaster Recovery Plans and Procedures for all IT services classified as Business Critical or Critical to ensure the continued operation of the company following a major incident/disaster.

The procedures should ensure that:

- Effects of the event are contained
- The damage to the IT-services is minimized
- Normal operation can be restored as quickly as possible
- Temporary alternate operations and the return to normal operation take place



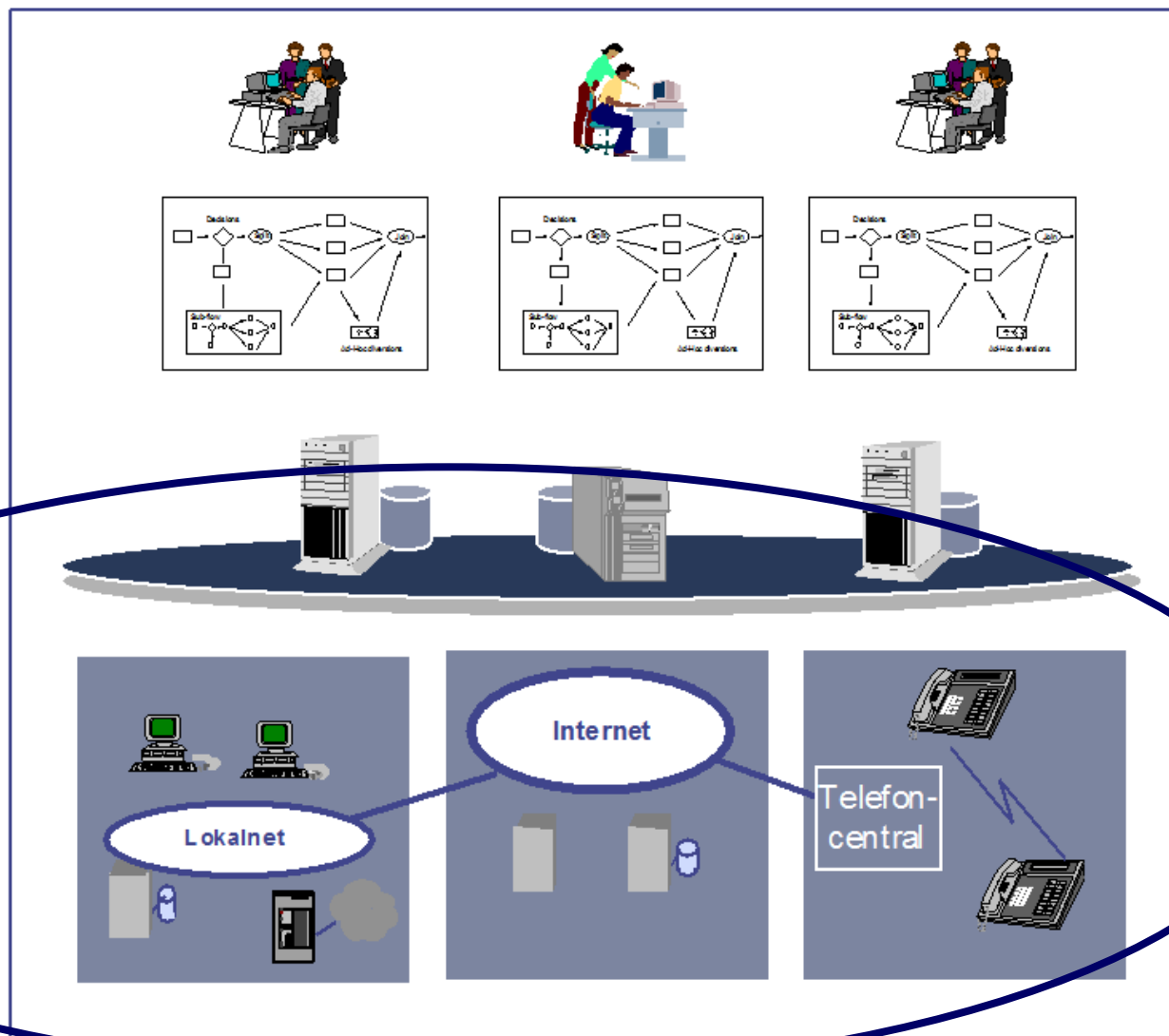
Forretningsprocesser og beredskab

Personer

Forretnings-
processer

IT Systemer
&
Data

IT Infrastruktur



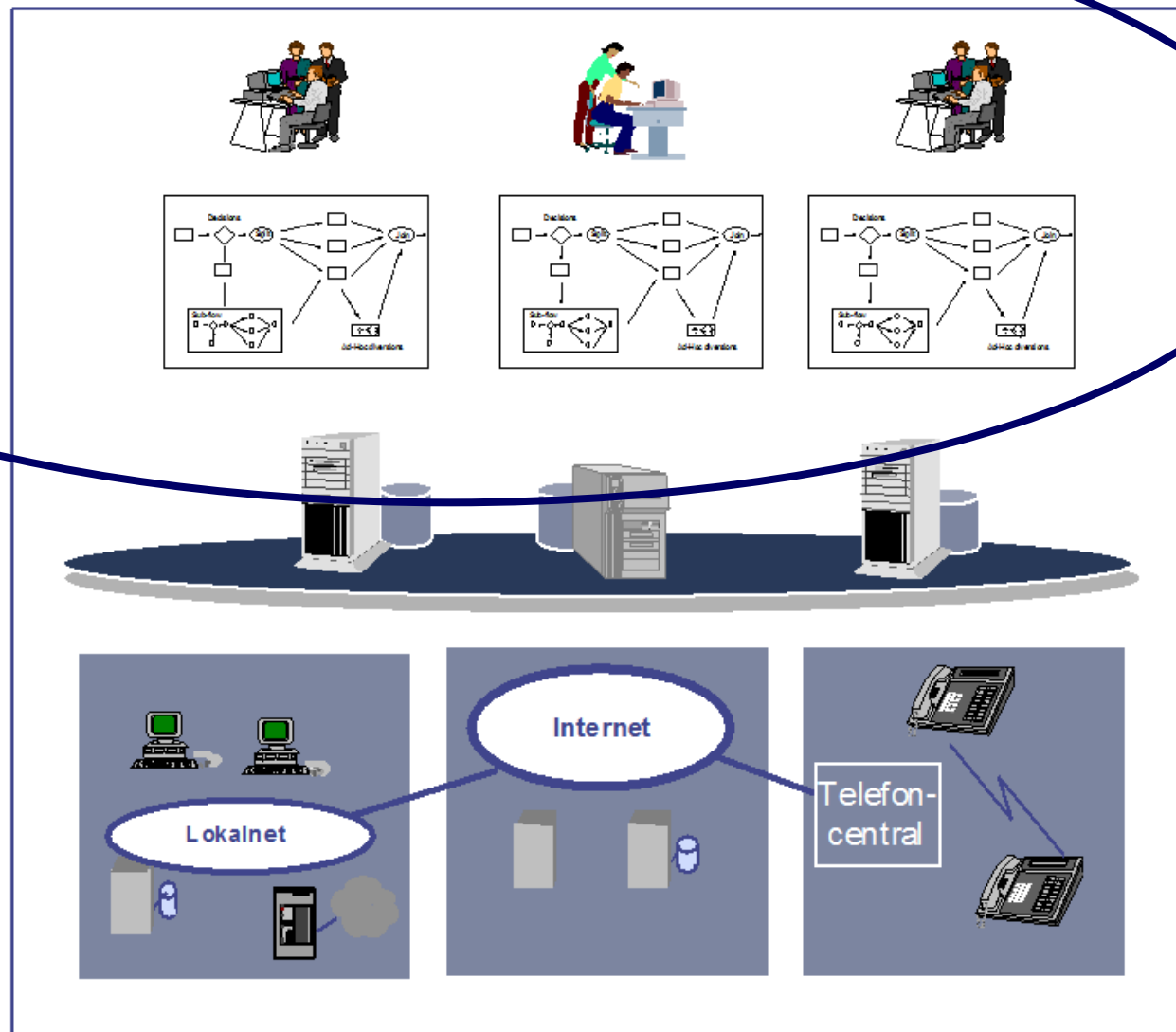
Disaster recovery

Forretningsprocesser og beredskab

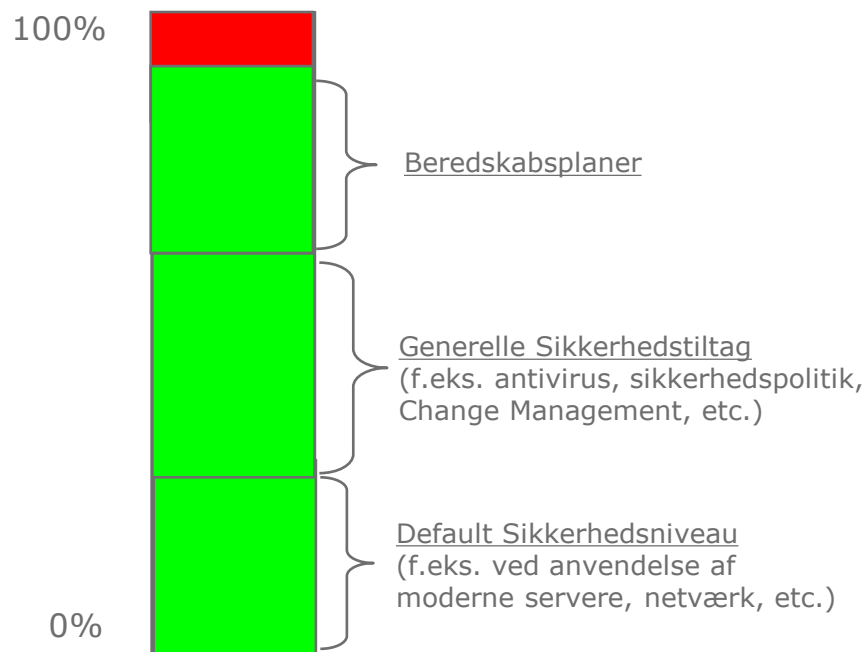
Personer

Forretnings-
processerIT Systemer
&
Data

IT Infrastruktur



HVORFOR er beredskab vigtigt?



Man kan aldrig sikre sig 100% mod nedbrud af længere varighed, men et beredskab vil øge paratheden til at håndtere situationer, som falder udenfor de almindelige driftsprocedurer.

Pause

A screenshot of the Words of Heart app landing page. The background is a dark, moody image of a person's silhouette looking out over a body of water at dusk or dawn. The text is centered and white, with a few elements in orange. The main headline is 'FIND AND DATE PEOPLE WHO HAVE THE SAME PASSWORD'. Below it is a subtext: 'We believe that something as intimate as your password best describes your inner self.' There are two buttons: a white 'LOGIN' button and an orange 'REGISTER' button. At the bottom, there is a contact email address.

FIND AND DATE PEOPLE WHO HAVE THE SAME PASSWORD

We believe that something as intimate as your password best describes your inner self.

LOGIN

REGISTER

contact: contact@wordsofheart.com

Words of Heart: Dating app matching people through their passwords



Faculty of Science



Risikovurdering

Risikovurderingen



Risiko

Hvis en psykolog mister sin laptop (glemmer eller stjålet)

Hvor alvorligt er det, hvad er sandsynligheden?

Hvis netværk compromiteres med efterfølgende uautoriseret adgang til data på server

Sandsynligt? Hvor slemt ville det være?

Afdeling i Århus har besluttet at bruge Dropbox til at udveksle data med firma i Tyskland

Konsekvens?

Projektleder forslår: pga ny deadline udgår de planlagte code reviews og penetrations tests

Risiko?



For ledelsen

Det er svært for ledelsen at svare på:

”Hvad er den faktiske risiko, og hvad er de faktiske omkostninger eller andre konsekvenser ved et sikkerhedsbrud i min virksomhed?”



Risikovurdering

- Risikovurdering er en proces der **identificere de risici** som kan påvirke IT ressourcerne eller organisationen som helhed.
- Risikovurderingen danner grundlaget for at kunne **prioritere** sikkerhedsindsatsen og besvarer spørgsmålene:
 - Bruger vi for få eller for mange ressourcer på sikkerhed?
 - Bruger vi de tilgængelige ressourcer bedst muligt?
- Risikovurderinger gennemføres **periodisk** (typisk årligt) samt ved **anskaffelse** af nye it-systemer eller større **ændringer** i organisationen, it-miljøet eller trusselsbilledet.

Undgår ting som "Er internettet sikkert?"



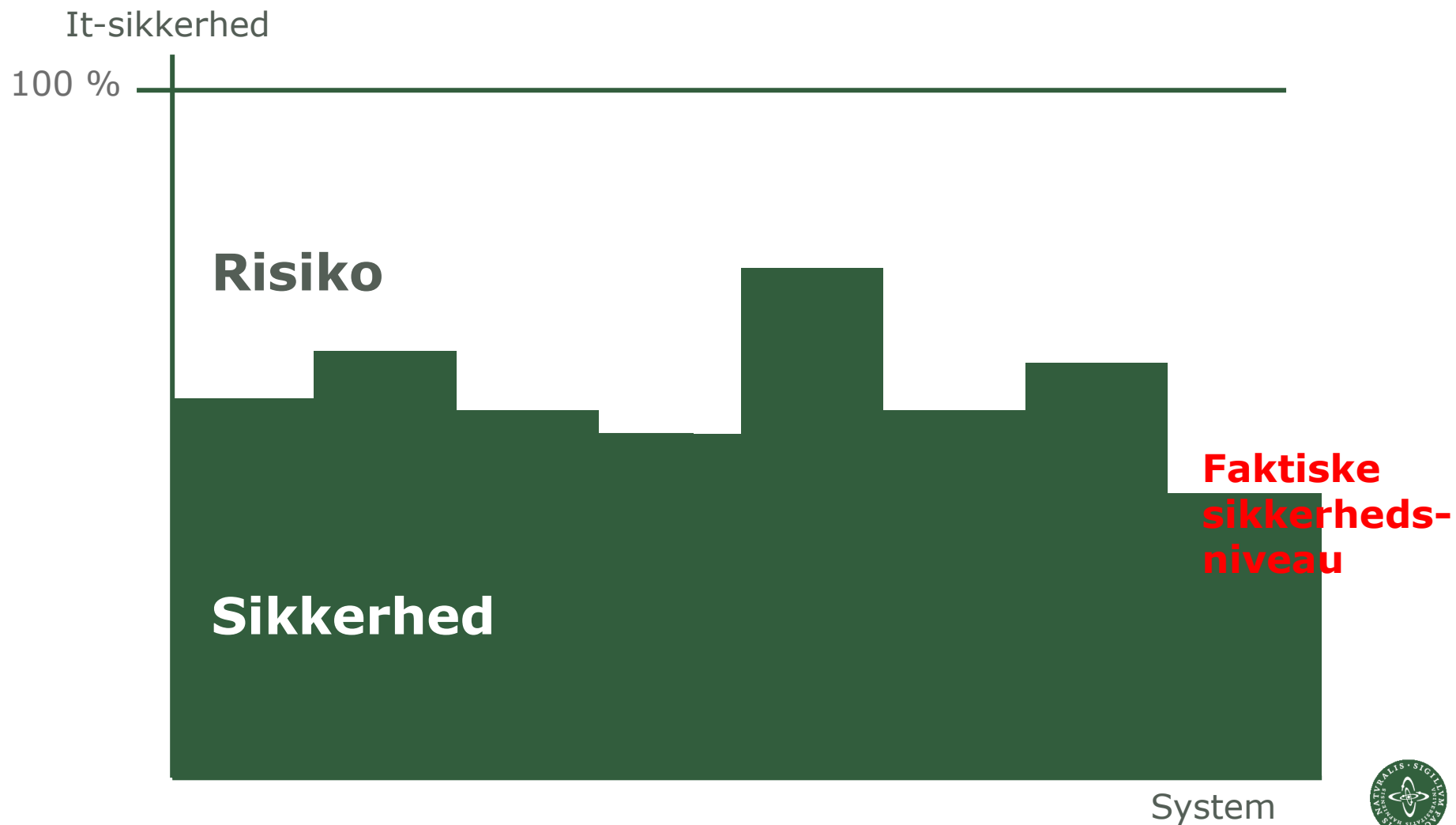
Risikovurdering – aldrig 100% sikkerhed

“The only system which is truly secure is one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, and is surrounded by nerve gas and very highly paid armed guards. Even then, I wouldn't stake my life on it.”

Gene Spafford



Ønskede sikkerhedsniveau ?



Different approaches to risk assessment

How do you identify relevant risks and threats?

Threat assessment
Risk modeling

> <

Risk assessment



Threats and risks

Threat assessments asks
"what could happen to this box/system/data?"

Risk assessments asks
"how much should I care?"

Playground in a kindergarden
or
Gate to a bank



Threat modeling – the 5 questions

1. What do you want to protect?

Assets

2. Who do you want to protect it from?

Adversaries and threats

3. How likely is it that you will need to protect it?

Probability

4. How bad are the consequences if you fail?

Risk

5. How much trouble are you willing to go through in order to try to prevent those?

Value

What assets
need to be
protected

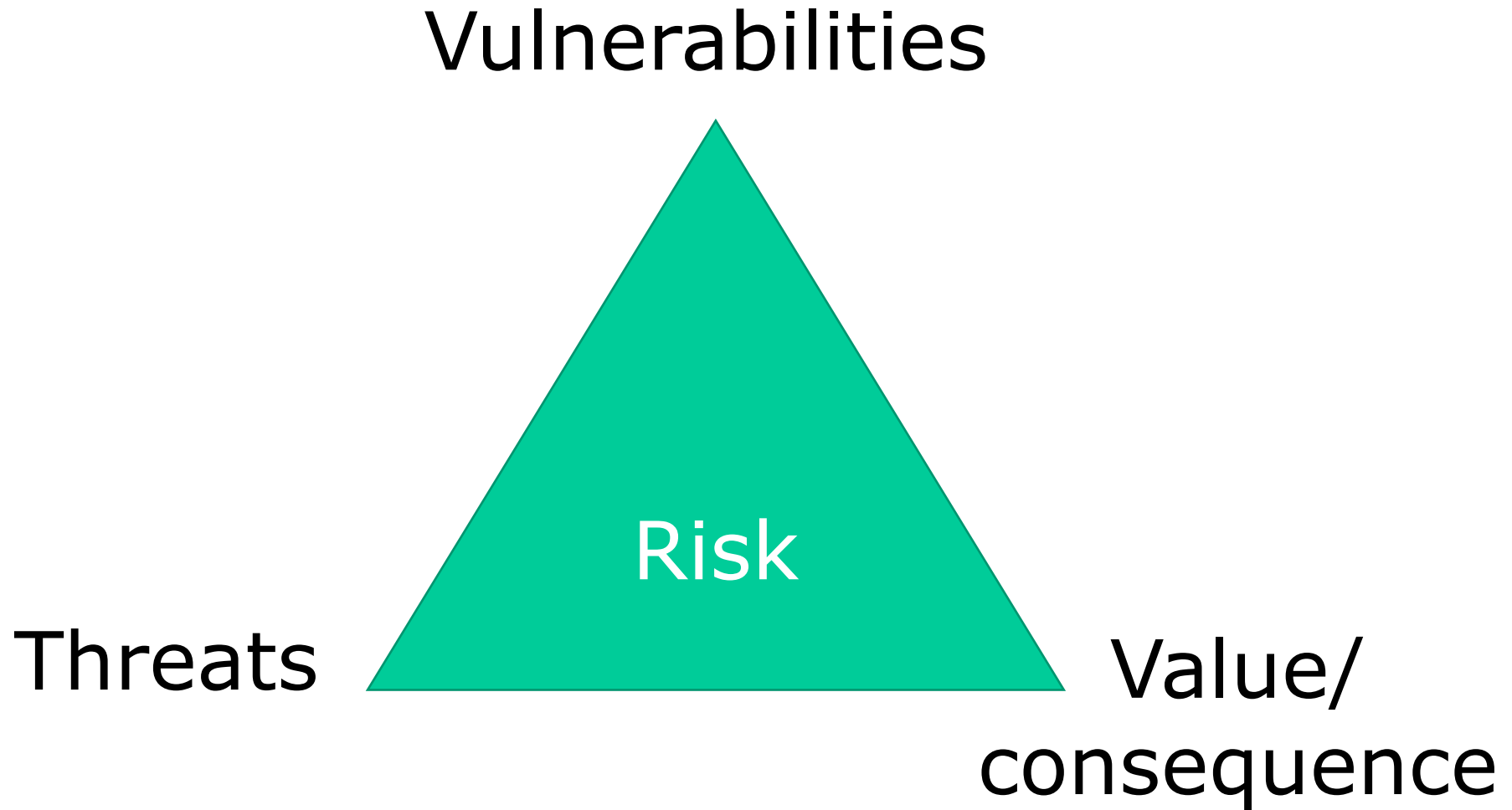


How are those
assets
threatened



What can be
done to counter
those threats

Risk assessment



Risikovurdering – oversvømmelse af serverrum

Trussel: Oversvømmelse

Sårbarhed: Serverrummet er i kælderen

Sandsynlighed: Erfaringen er, at vi får en oversvømmelse hver 20. år. Med de nuværende klimaforandringer forventer vi, at der vil komme oversvømmelser fra havnen hver 5. år

Konsekvens: Kælder oversvømmes og vand ødelægger derved servere

Sikkerhedstiltag: Flytning af serverrum til 3.sal kan fjerne sårbarhed, alternativt outsource/cloudsource



Risikovurdering – hvordan kommer relevante med?

Find relevante trusler, inspiration

Angreb

- Cyber Crime
- Tyveri af udstyr
- Industrispionage
- Sabotage
- Hacking
- Virus og orme
- Denial of Service Attacks
- Social Engineering
- Bedrageri

Uheld

- Brand
- Oversvømmelse
- Lynnedslag
- Strømafbrydelse
- Fejl på hardware
- Fejl i software
- Menneskelige fejl
- Tab af nøglepersoner
- Tab af netværksforbindelse

CIA

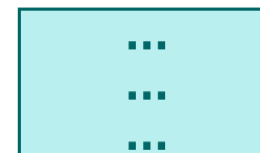


(Confidentiality, Integrity, Availability)

Externe



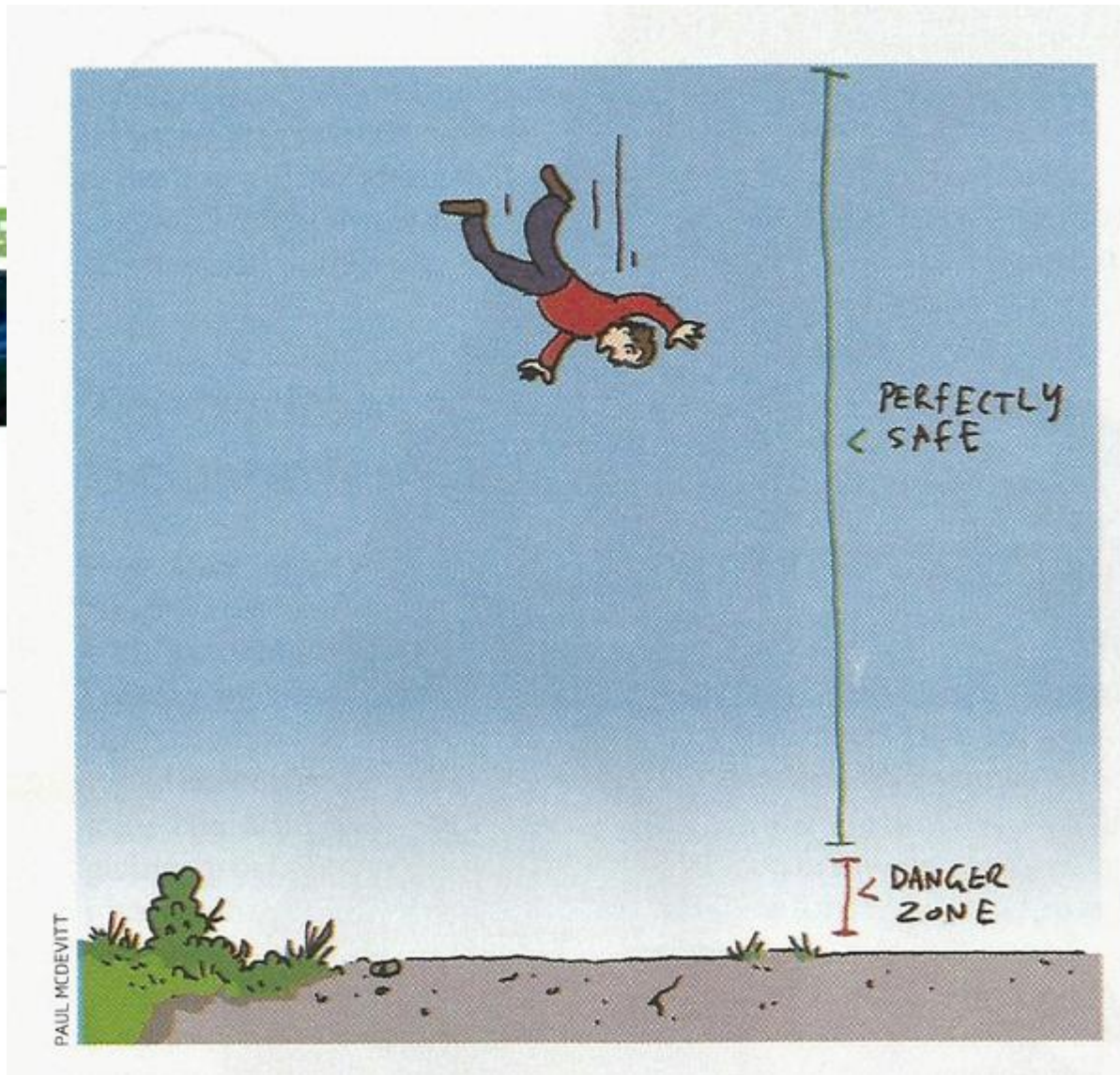
Interne



Mennesker

Teknologi

Skal DanID købe DDoS-beskyttelse?



ough

Hvad skal risikovurderingen bruges til!

Vær klar på **hvorfor** du laver risikovurderingen !
(er det at finde trusler, et ledelsesværktøj, sikre ressourcer...)

Risikovurderinger skal være et værktøj - de skal kunne bruges aktivt

Skal være klart og tydeligt visuelt:

- Prioriterer aktiviteter
- Kommunikerer risikobilledet



Ledelsesopmærksomhed og synlighed

Hvordan sikre man, at der bliver afsat ressourcer til sikkerhed?

Hvorfor skal "Projekt B" bruge 10% af budgettet på it-sikkerhed?



Threat modeling – the 5 questions

1. What do you want to protect?

Assets

2. Who do you want to protect it from?

Adversaries and threats

3. How likely is it that you will need to protect it?

Probability

4. How bad are the consequences if you fail?

Risk

5. How much trouble are you willing to go through in order to try to prevent those?

Value

WHAT IS A “RISK ASSESSMENT”?

Risk assessment

ISO 27005 / ISO 31000

NIST 800-30/CSF

OCTAVE

PCI-DSS

ISACA

COBIT

ISF

ENISA

EBIOS

OWASP

CIS RAM

FAIR

MEHARI (MEthod for Harmonized Analysis of Risk)

Harmonised TRA

...



Risikovurdering – en definition

Risiko : *sandsynligheden* for, at en trussel vil blive udnyttet til et gennemført angreb, og *konsekvensen*, hvis angrebet finder sted

Risiko = "Trussel x Sårbarhed x Værdi af Aktiv"

Sikkerhedstiltag kan enten nedbringe sandsynligheden, konsekvensen eller begge



Hvad skal risikovurderingen bruges til!

Trusselsvurderingen finder trusler

– samles i et risiko register

Nr.	Beskrivelse
1	Persondata i Dropbox
2	Server hacket
3	Malware fører til datatab



Hvad skal risikovurderingen bruges til!

Trusselsvurderingen finder trusler

– samles i et risiko register

Nr.	Beskrivelse	Sandsynlighed	Konsekvens
1	Persondata i Dropbox	Høj	Høj
2	Server hacket	Mellem	Lav
3	Malware fører til datatab	Mellem	Mellem



Risikovurdering

Trusler skal vurderes efter identifikation

- Teknisk risikovurdering
- Forretningsmæssig risikovurdering

Hvad er forskellen ?



Forretningsmæssig risikoanalyse

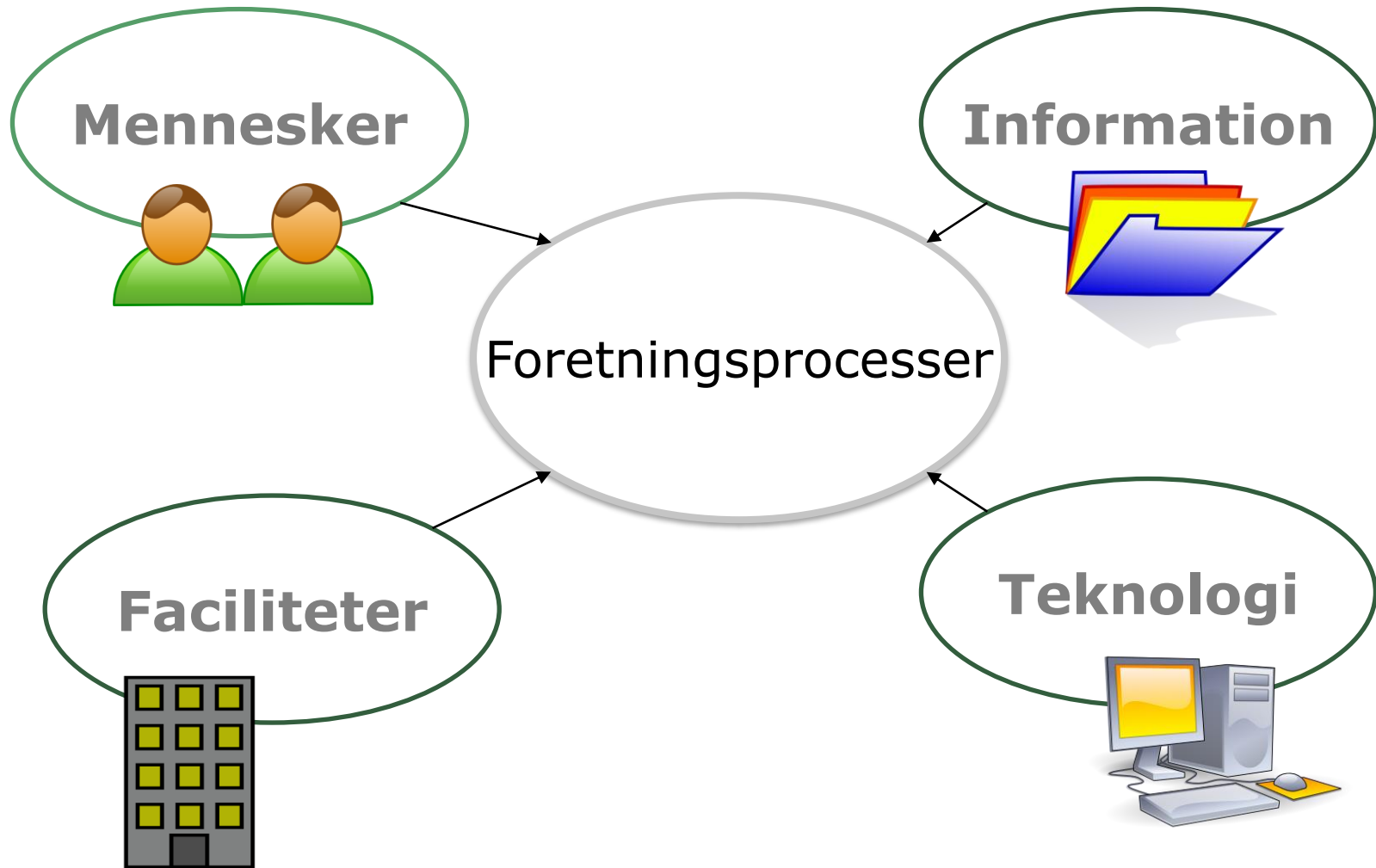
Interview med ledere og
forretningsansvarlige

Afdækning af konsekvenser:

Tab af indtægt, image tab, negativ omtale
i pressen, mister mulighed for at opfylde
kontrakter osv.



Typer af aktiver



Accepterer risiko

- En risiko kan accepteres, hvis det vurderes, at risikoen er lav, eller at udgifterne til at implementere sikringsforanstaltninger ikke står mål med truslen.
- Man skal ikke bruge flere penge på beskyttelse end værdien af de aktiver man skal beskytte.
- Eksempel
 - Meteornedslag er katastrofale men sjældne
 - Giver det mening at installere et meteorskjold?



Remember your risk assessment basics

Eliminate/Mitigate
Minimize (compensate)
Transfer
Accept

Prevent – Detect – Respond



Risikovurdering - simpel

No.	Threat	Risk
1.	Unencrypted data is stored on device. If device is stolen or otherwise lost data is readable and usable.	Low
	<i>Comments:</i> Encryption should be enabled by default on the devices. Confidential data is not stored on the device and cannot be accessed from the device.	
2.	Users will choose not to use access PINs or use weak PINs ("1234"). If device is lost or stolen, the device, apps and all data can be accessed.	Medium
	<i>Comments:</i> Authentication requirements should be applied through policies and device management solutions, or through user awareness (less effective). However the data that can be accessed on the device is not Confidential.	

Farver bruges til at gøre potentiel risiko tydelig



Indhold af del-analyser

System og data klassifikation

F.eks. Kritisk
 Mindre kritisk
 Ikke kritisk
 Ikke relevant



Simpel risikoanalyse

$$\text{Risiko} = \text{Sandsynlighed} \times \text{Konsekvens}$$

Sandsynlighed kan kategoriseres som:

Meget Sandsynlig	(4)
Sandsynlig	(3)
Mindre Sandsynlig	(2)
Ikke sandsynlig	(1)

Konsekvens kan kategoriseres som:

Katastrofal	(4)
Kritisk	(3)
Skadelig	(2)
Uskadelig	(1)

Risiko Matrix

Meget sandsynlig	4	8	12	16
Sandsynlig	3	6	9	12
Mindre sandsynlig	2	4	6	8
Ikke sandsynlig	1	2	3	4

	No/low consequence	Medium consequence	High consequence
No/low probability	$1 \times 1 = 1$	$1 \times 2 = 2$	$1 \times 3 = 3$
Medium Probability	$2 \times 1 = 2$	$2 \times 2 = 4$	$2 \times 3 = 6$
High probability	$3 \times 1 = 3$	$3 \times 2 = 6$	$3 \times 3 = 9$

Low/no risk	
Medium risk	
High risk	



Risikovurdering - applikation

No.	Threat	Likelihood	Consequence	Risk
1.	Unencrypted data is stored on device. If device is stolen or otherwise lost data is readable and usable.	No	High	Low
	<i>Comments:</i>	Encryption should be enabled by default on the devices. Confidential data is not stored on the device and cannot be accessed from the device.		
2.	Users will choose not to use access PINs or use weak PINs ("1234"). If device is lost or stolen, the device, apps and all data can be accessed.	High	Low	Medium
	<i>Comments:</i>	Authentication requirements should be applied through policies and device management solutions, or through user awareness (less effective). However the data that can be		

Risikovurdering – eksempel

Microsoft Excel - F-Dept.xls

File Edit View Insert Format Tools Data Window Help

Type a question for help

85%

A1

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33

1. Forretningsmæssig risikovurdering for telefoni og omstilling [\[retur til oversigt\]](#)

Fortrolighed

I hvilken grad medfører manglende fortrolighed	Vurdering	Kommentarer
a. Tab af konkurrence mæssige fordele ?	Uskadelig	ej aktuelt
b. Risiko for økonomiske tab ?	Kritisk	Store afledte omkostninger til spinhåndtering
c. At det offentlige omdømme påvirkes ?	Skadelig	Medarbejdere forventer at kunne drøfte interne og fortrolige anliggender telefonisk uden risiko for fortrolighedsbrud
d. Yderligere omkostninger ?	Uskadelig	
e. At lovmæssige krav ikke kan opfyldes ?	Uskadelig	

Integritet

I hvilken grad medfører manglende integritet (pålidelighed af data):	Vurdering:	Kommentarer
a. At beslutninger ikke kan træffes tilfredsstillende ?	Skadelig	Informationsindhentning og koordination kan blive vanskeliggjort
b. Risiko for svig ?	Uskadelig	Næppe
c. At de daglige opgaver ikke kan gennemføres ?	Kritisk	E.g. hvis nummer-databasen korrumpes vil man ikke kunne ringe og videregive korrekt internt
d. At det offentlige omdømme påvirkes ?	Skadelig	Negativ medieomtale mv.
e. Medføre yderligere omkostninger ?	Skadelig	Oprydning og omkonfigurering, samt evt. problemer ifht. håndtering af frister
f. At lovmæssige krav ikke kan opfyldes ?	Skadelig	Igangværende opgaver kan påvirkes

Tilgængelighed

Efter hvor lang tid medfører manglende tilgængelighed:	Ved nedbrud under 1 time	Ved nedbrud mellem 1 time og 8 timer	Ved nedbrud mellem 8 timer og 1 døgn	Ved nedbrud mellem 1 døgn og 2 døgn	Ved nedbrud over 2 døgn	Er der tidspunkter hvor nedbrud er særligt kritisk ?
a. At nødvendige beslutninger ikke kan træffes tilfredsstillende?	Skadelig	Kritisk	Kritisk	Katastrofalt	Katastrofalt	
b. Øgede omkostninger?	Uskadelig	Skadelig	Skadelig	Kritisk	Katastrofalt	
c. Mistet indtægt ?	Uskadelig	Uskadelig	Uskadelig	Uskadelig	Uskadelig	
d. At forpligtigelser ikke kan opfyldes?	Skadelig	Kritisk	Kritisk	Katastrofalt	Katastrofalt	
e. At det offentlige omdømme påvirkes?	Skadelig	Kritisk	Kritisk	Kritisk	Katastrofalt	
f. At lovmæssige krav ikke kan opfyldes?	Skadelig	Kritisk	Kritisk	Katastrofalt	Katastrofalt	

Vejledning til overordnet risikovurdering:

I vurderingsfeltet angives et niveau:

1 - Katastrofalt
2 - Kritisk
3 - Skadelig
4 - Uskadelig

Hvis vurderingen udfyldes elektronisk er der "pull-down" kasser til dette formål i vurderingscellerne.

Når man udfylder tilgængelighedsværdierne foregår dette på samme måde.

Katastrofalt
Kritisk
Skadelig
Uskadelig

1 2 3 4 5 6 7 8 9 10 11

Ready NUM

Teknisk risikovurdering – eksempel

Microsoft Excel - T-Serverdrift-risikovurdering.XLS

File Edit View Insert Format Tools Data Window Help

Type a question for help

E3

Skema til it-risikovurdering, Serverdrift & klientmiljø

Indsættelse for det markerede

Se titel

		Vil den nye anvendelsesimplementering eller ændring kunne medføre	Sandsynlighed (S) for at truslen indtræffer	Konsekvenser	Konsekvens (T)	Kalkuleret vægtsat risiko	Kan vi acceptere nuværende situation	Noter	Forslag til tekniske eller administrative tiltag til at imødegå risikoen
6	Brugere	At der sker misbrug af anden brugers systemadgang, f.eks. ved gæt af kodeord, misbrug af udstyr der er loggeret på.	Sandsynlig	Fortrolighed, tilgængelighed og pålidelighed af data kompromitteres	Skadelig	Middel	Nej	Slæseri med password og gule sedler. Skærmlås.	Der bør være skærmlås med 10-15 min. låsetid - særligt på it-personale der har administrative adgange fra desktop og remote-stationer. Indskærp forhold ifht. brug af password på gule sedler.
7		At en ansat laver uautoriserede ændringer af data	Mindre sandsynlig	Tilgængelighed og pålidelighed kompromitteres	Skadelig	Lav	Ja		
8		At en ansat klassificerer data forkert	Meget sandsynlig	At data ikke behandles i overensstemmelse med deres væsentlighed - brud på fortrolighed, tilgængelighed og pålidelighed.	Skadelig	Middel	Ja		
9		En ansat udfører sabotage, f.eks. sletter vitale data	Mindre sandsynlig	Brud på fortrolighed, tilgængelighed og pålidelighed.	Kritisk	Middel	Ja	Navision superbrugere kan slette.	I) Etabler sikkerhedsmæssig checkliste for ansættelser der indebærer admin-privilegier. II) Etabler checkliste og risikouurderingsskabelon for fratrædelse af nøglemedarbejdere.
10		At en ansat får uretmæssig adgang til data	Sandsynlig	Brud på fortrolighed, tilgængelighed og pålidelighed.	Skadelig	Middel	Ja	Der kan være eksterne kontakter i en distributionsliste på mailsystemet som man tror er intern.	
11		At en ansat omgår sikkerheden	Meget sandsynlig	Brud på fortrolighed, tilgængelighed og pålidelighed.	Skadelig	Middel	Nej	I relation til brug af andres password til f.eks. Navision ved f.eks. fravær	Opret yderligere brugeradgange hvis behovet er til stede. Sporbarheden skal være på plads og alternativt må opgaven vente på at nøglepersonen er tilgængelig.
12		At der sker tyveri af interne data / software	Mindre sandsynlig	Brud på fortrolighed, tilgængelighed og pålidelighed.	Skadelig	Lav	Ja		
13		At der ikke er den nødvendige funktionsadskillelse til at imødegå svig og misbrug	Sandsynlig	Brud på pålidelighed.	Skadelig	Middel	Ja	Formalia er på plads, men implementering ifht. JyskeBank halter. Derudover har flere adgang til andres navision password jvf. gule sedler.	
		At tredjeparts personale (samarbejdspartner, konsulent, leverandør) misbruger systemer eller data	Sandsynlig	Brud på fortrolighed, tilgængelighed og pålidelighed.	Skadelig	Middel	Nej	Eksterne er i visse tilfælde oprettet i miljøet og på distributionslister i	Underskrift og tiltrædelse af it-sikkerhedspolitik inden adgange tildeles!

Vejledning til it-risik

NB: Gå til fanen "Vejledn procedure/vejledning.

I) Bekræft at releva yderligere trusler or

II) Vurder sandsynlig indtræffer

III) Beskriv konsek

IV) Vurder konsek

V) Skitser evt. i not eksisterer i organis lave linieskift inden

Vejledning Risikovurdering

Ready

NUM

Vurdering og prioritering

- Anbefal handlinger (f.eks. mitigation/compensation)
- Vurder hvordan det hjælper, giver det værdi, hvordan hjælper anbefalingen egentlig
- Hvis handling ikke hjælper – find noget andet der gør

Risk Mitigation Action Plan for [INSERT NAME OF APPLICATION]							
Issue number and Risk description	Mitigating Action	Priority	Raised (date)	Approved by SO (Date)	Expected go live date	Responsible	Next step and comments



Vurdering og prioritering

High risk:

"Must do", mandatory, must be implemented immediately

"Should do", important but can be implemented in 4-12 months

Medium risk:

"Could do", important but will depend on an assessment of risk/cost

Low risk:

"Need not do", nice to have

Potentiel mitigeringsplan for de næste tre måneder:

Action	Vedr. risk nr:
Informer alle afdelinger om persondata lovgivningen og udfør audit i Århus	1,4
Verificer konfiguration på alle servere	2, 9, 16, 21



Eksempel på konsekvensoversigt

Konsekvens	Kunder	Image	Aktiekurs ¹	Personale Ressource-belastning	Personale Tiltrække nye medarbejdere	Interessenter Offentlige og kontrollerende	Interessenter Samarbejds-partnere	Økonomisk
Uskadelig	Mister under 10 privatkunder	Ingen offentlig omtale	Aktiekursen falder ikke	Under en uges ekstraarbejde	Ingen påvirkning	Ingen påvirkning	Ingen påvirkning	Direkte økonomisk tab under 100 t. kr.
Skadelig	Mister under 500 privatkunder / 5 store virksomheder	Historie i dagblad eller i TV nyheder. Forsiden Børsen	Aktiekursen falder 0-2 %	Under 2 mandeår i ekstra arbejde	Ingen væsentlig påvirkning	Væsentlig påtale eller advarsel fra myndigheder	Samarbejdspartnere ønsker sikkerhed for fortsatte leverancer.	Tab mellem 100 tkr og 10 mio. kr. , svarer til forøgelse af udgifter på under 1%
Kritisk	Mister under 1.000 privatkunder eller 10 store virksomheder	Forsiden af dagblade og hovedhistorie i TV	Aktiekursen falder 2-10 %	Under 10 mandeår i ekstraarbejde	Medarbejdere søger væk / Der modtages færre ansøgninger til stillinger.	Sat under administration af myndigheder	Partnere fornyer ikke samarbejdsaftaler. Ikke muligt at tiltrække nye samarbejdspartnere.	Tab mellem 10 og 50 mio. kr. , svarer til forøgelse af udgifter på under 4%
Katastrofalt	Mister mere end 1.000 privatkunder eller mere end 10 store virksomheder	Forsiden af landsdækkende avis eller hovedhistorie i landsdækkende TV i en længere periode	Aktiekursen falder med 10+ point	Mere end 10 mandeår i ekstraarbejde	Organisationen tiltrækker ikke nye medarbejdere / nøgleressourcer søger bort.	Frataget ret til at drive forretning	Samarbejdspartnere opsiger samarbejdsaftaler.	Tab over 50 mio. kr. , svarer til forøgelse af udgifter på over 4%

Case

Virksomhed A er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har en kendt RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at tage fuld control over serveren. En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring 80% af virksomhedens omsætning, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder persondata om virksomhedens 800.000 kunder.

Threat Assessment:



Case

Virksomhed A er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har en kendt RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at tage fuld control over serveren. En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring 80% af virksomhedens omsætning, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder persondata om virksomhedens 800.000 kunder.

Risk Assessment:

Description	Likelihood	Consequence	Risk	Notes
RCE i CMS	High	High	High	Sikkerhedspatch 2018-A6763G bør installeres



Ledelseskommunikation

Virksomhed A er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har en kendt RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at tage fuld control over serveren. En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring 80% af virksomhedens omsætning, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder persondata om virksomhedens 800.000 kunder.

Ledelseskommunikation: Hvad siger du?

“Vi har en RCE i CMS, jeg skal bruge 1 mio til at teste og installere et sikkerhedspatch”

Description	Likelihood	Consequence	Risk	Notes
RCE i CMS	High	High	High	Sikkerhedspatch 2018-A6763G bør installeres



Ledelseskommunikation

Hvad tænker lederen?

Jeg har 1 mio i budgettet, skal jeg bruge den på

- a) Forretningsudvikling - businesscase forventer 3% øget salg
- b) Energibesparelser, nedbrug strømforbrug, forventet besparelse 0,1%
- c) "Sikkerhedspatch til RCE i CMS" - et eller andet med hjemmesiden



Ledelseskommunikation

Virksomhed A er en medievirksomhed med en årlig omsætning på 100 mio DKR. Virksomhedens webserver har en kendt RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnyttes til at tage fuld control over serveren. En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden venter til leverandøren har en samlet sevicepack opdatering klar.

Virksomhedens webshop, der står for omkring **80% af virksomhedens omsætning**, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder **persondata om virksomhedens 800.000 kunder**.

Risk Assessment:

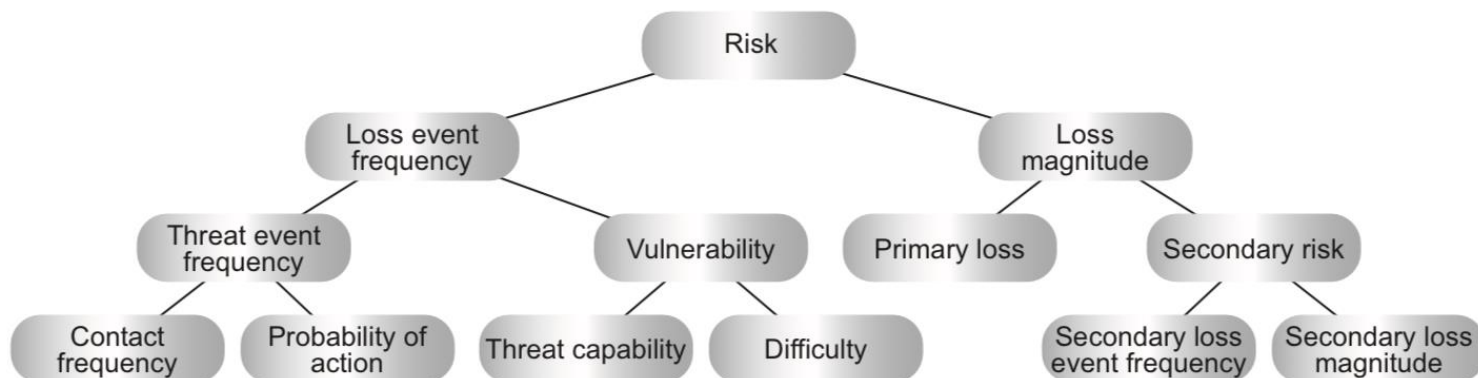
Description	Likelihood	Consequence	Risk	Notes
RCE i CMS	High	High	High	Sikkerhedspatch 2018-A6763G bør installeres

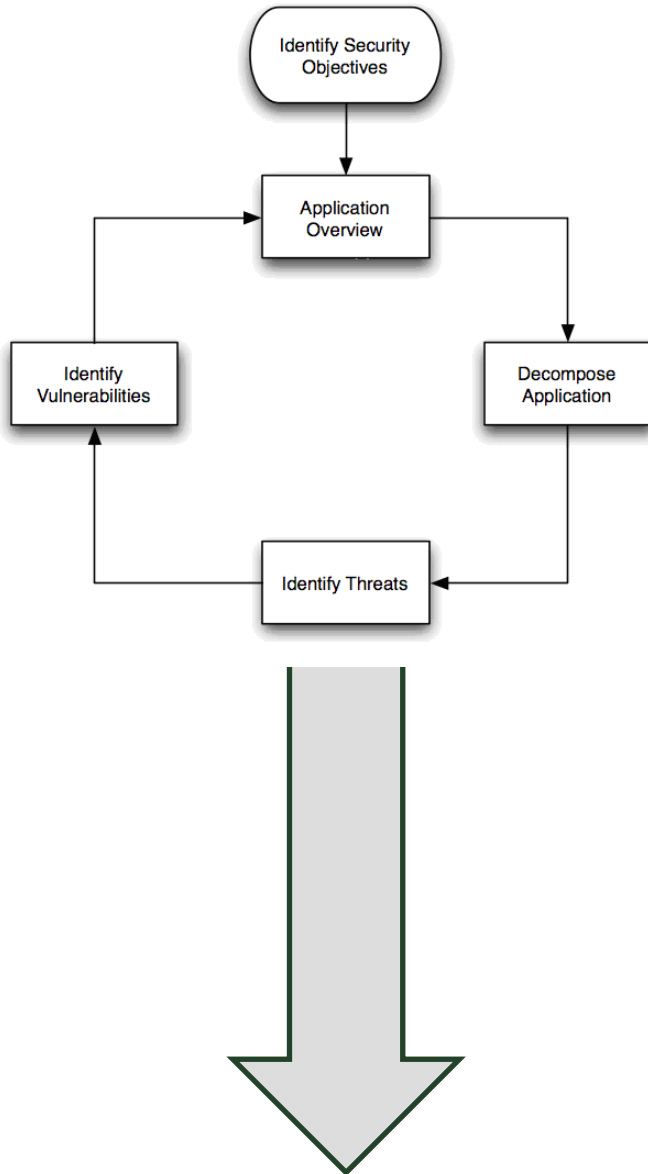


SANDSYNLIGHED OG SIKKERHED (“FAIR”)

“Hvad er sandsynligheden for vi bliver hacket” er ikke et spørgsmål man kan besvare statistisk

“Risikoen for et ransomware angreb på en specifik virksomhed” er også epimistisk, men hvis vi opdeler i relevante komponenter kan man – væsentligt bedre end med de traditionelle vurderinger - lave en vurdering og f.eks. vise ændringer i riskobillede





Løsningen

Overvej
trusler

Find
Sårbarheder

Vurder
sandsynlighed

Vurder
Konsekvens

Hardware, software,
interfaces, people, mission,
system- and data
classification

Tidligere angreb, vurdering
af potentielle trusler

Krav, sikkerhedstests,
potentielle sårbarheder

Angriber motivation,
sikkerhedsmekanismer,
typer af sårbarheder

Hvad er den samlede risiko?

Implementation Plan

Risk (Asset/Threat)	Hacker attack on Internet router
Level of Risk	High
Recommended Controls	<ul style="list-style-type: none"> •Disable external telnet access •Use detailed auditing of privileged command use •Set policy for strong admin passwords •Set backup strategy for router configuration file •Set change control policy for the router configuration
Priority	High
Selected Controls	<ul style="list-style-type: none"> •Implement all recommended controls •Update related procedures with training for affected staff
Required Resources	<ul style="list-style-type: none"> •3 days IT net admin time to change & verify router configuration, write policies; •1 day of training for network administration staff
Responsible Persons	John Doe, Lead Network System Administrator, Corporate IT Support Team
Start – End Date	February 6, 2017 to February 9, 2017
Other Comments	•Need periodic test and review of configuration and policy use

Opsummering

IT-sikkerhedsledelse, incl. risikovurderinger, er en kritisk del af it-sikkerheden

Hele kæden er vigtig:

Predict - Prevent – Detect - Respond





Awareness – sikkerhedskultur og adfærdsdesign

Adfærdsdesign i awareness-arbejdet



Den enkelte medarbejders adfærd er afgørende for hele organisationens informationssikkerhed.

Derfor er det vigtigt at styrke medarbejdernes forståelse af deres ansvar i organisationens informationssikkerhed

Men viden er ikke nok. Der skal adfærdsforandring til, før der kan opstå en stærk sikkerhedskultur.



Grundlaget er viden om sikkerhed

Awareness-arbejdet starter med, at **budskaber og målgrupper defineres**. Man kan ikke forvente sikkerhed uden at have informeret medarbejderne



Håndtering af attachments



USB-nøgler



Stærke kodeord



Udviklingsafdelingen



HR-medarbejdere og jurister

Forarbejdet skal baseres på viden om, hvordan medarbejderne arbejder i dag:
Brug risikovurderinger, globale trusler som ransomware eller phishing, triggers i dagligdagen
(i hvilke situationer kan der opstå brud på sikkerheden) osv.

Materialet skal være **relevant for modtageren**. Hvis det er for generisk eller irrelevant for medarbejderne, mister man deres opmærksomhed.



Sikkerhedspakken – der er mange forskellige metoder

Folder

Plakater

Film

Musemåtter

Intranettet

Tekster i medarbejder/firma blade

Møder

Undervisning

Billeder

Emails

Skærmskånere

Phishing angreb

Social engineering

USB-nøgler efterladt

sikkerdigital.dk



Sikkerhedspakken – der er mange forskellige metoder

Idéer til aktivering af sikkerhedspakken

I kan vælge at have en årlig sikkerhedsmåned med fx følgende indsatser, eller I kan aktivere indsatserne løbende i løbet af året.



Informationssikkerhed på personalemøde

- Hvorfor er informations-sikkerhed vigtigt?
- Alle skal tage e-læringsforløb
- Evt. igangsættes en sikkerhedsmåned bestående af sikkerhedspakkens indhold



Tekst på intranettet

- Tekst på intranettet om informationssikkerhed
- Links til e-læringsforløb og sikkerhedsportalen



Film

- Alle medarbejdere ser den korte film om informations-sikkerhed



Quiz

- Personaleleder beder ansatte om at tage quiz
- Medarbejdernes resultater kan evt. drøftes til et personalemøde



Pjece

- Pjecen med gode råd placeres rundt om i organisationen



E-læring

- Nyansatte medarbejdere gennemgår e-læringsforløb om informations-sikkerhed

- Topledelsen runder mails/nyhedsbrev til medarbejdere om sikkerhedsmåned
- Alternativt mail om vigtigheden af informationssikkerhed generelt

Mail til medarbejdere



- Ledelsen bruger kalenderinvitation til at huske medarbejdere på at skifte password

Kalenderinvitation



- Alle mellemledere gennemfører 'e-læring til ledere' og er ambassadører for medarbejdere

E-læring til mellemledere



- Plakater med gode råd sættes op

Plakat



- Evaluering af sikkerhedsindsatsen
- Afrapportering til ledelsen

Evalueringsrapport udarbejdes lokalt



- Nyansatte medarbejdere får udleveret pjecen med gode råd om informations-sikkerhed

Pjece



For nyansatte

Sikkerdigital.dk

Sikkerhedspakken samlet



Mange awareness-kampagner standser forarbejdet her og går direkte til produktion.

Men efter budskaber og målgrupper er defineret, og det første overblik over forskellige teknikker fra plakater til udsendelse af e-mails er etableret, er det kritisk, at **budskaberne leveres effektivt.**

Kommunikationsstrategi og plan

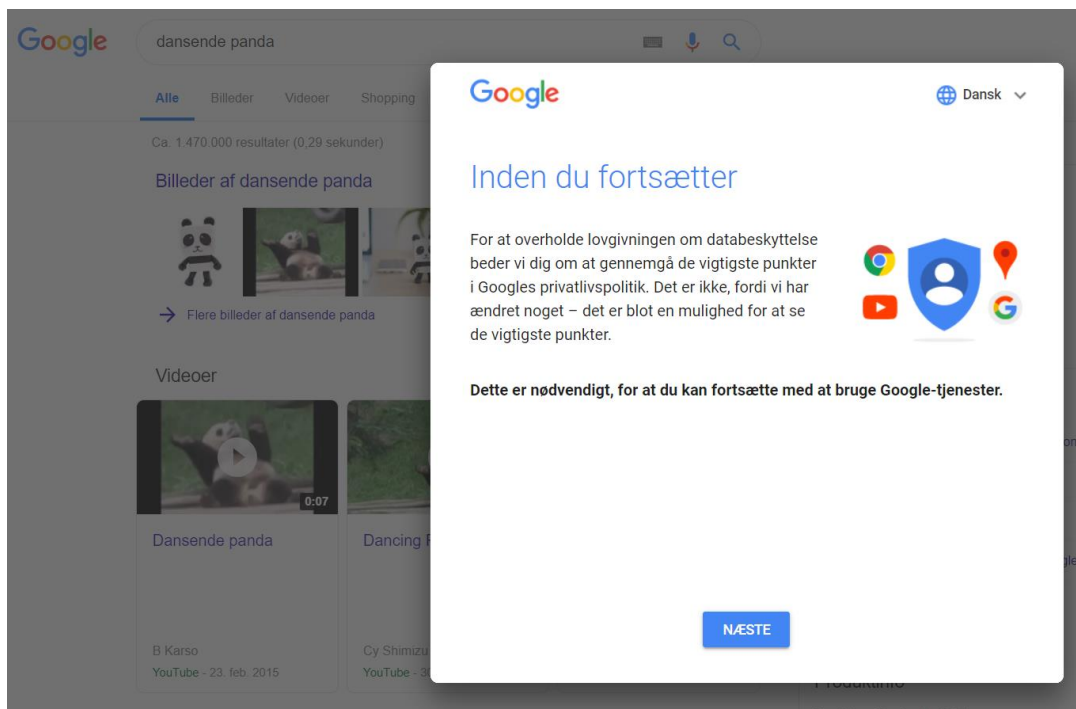
Målgrupper

Folder

E-læring

Opfølgning

Brugerens mentale model



Overførslen af viden er kun effektiv, når modtagerne er **fokuseret** på det, der sker

Det vil sige, at budskaberne skal leveres i en situation, hvor medarbejderne er opmærksomme på sikkerhedsbudskaberne

Mentalt må indlærings-situationen ikke være noget, der *skal overstås*, inden de kan komme videre til deres primære formål

Sikkerhedsformlen

Adfærd = (Evne x Motivation x Trigger)

"Hvad skal man gøre og hvorfor".
"Kodeord skal være svære at gætte, fordi mange angreb starter med ..."

"Jeg vælger IKKE at klikke, fordi jeg ved, det kan være et problem, og jeg har en anden mulighed."

Problemet er, at mange sikkerhedshændelser starter med en triggerhændelse, som vi reagerer på.

Når mennesker træffer beslutninger



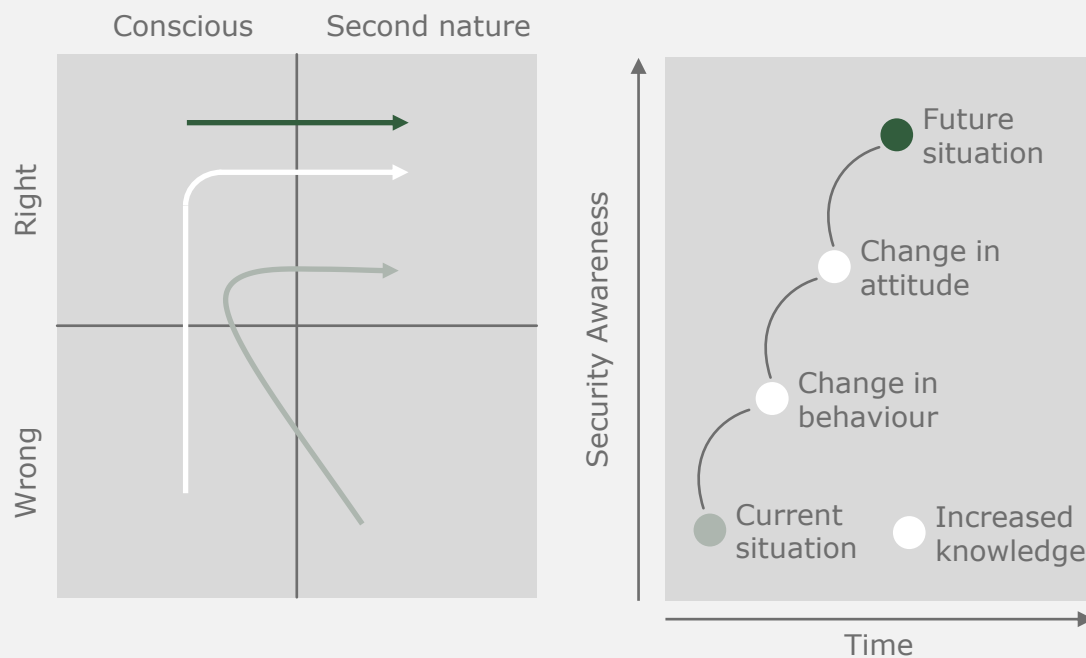
Daniel Kahneman beskriver i "At tænke – hurtigt og langsomt", hvordan, hvorfor og hvornår mennesker træffer beslutninger.

Kahnemans **system 1 og system 2**-model forklarer, hvorfor vi nogle gange handler forkert, selvom vi ved, det er forkert. System 1 handler hurtigt og instinktivt på trigger-hændelsen, inden system 2 når at reagere.

For at forbedre vores beslutninger fra ubevidste og forkerte skal sikkerheden gøres til naturlige handlinger gennem mere træning (beslutninger flyttes fra system 2 til system 1).



Sikkerhed som naturlige handlinger



Sikkerhed kan flyttes fra system 2 til system 1 gennem **opfølgende træning**, der naturligvis stadig skal være relevant for modtageren, og stadig gives i situationer, hvor sikkerhed er det primære fokus.

Ændringer

Awareness er en løbende aktivitet, ikke en engangsopgave

Skift medier og budskab for at undgå blindhed

Ansvar for sikkerhedsaktiviteter skal placeres hos de udførende



Sikkerhed som naturlige handlinger



Konsekvens (positiv, men også negativ) og reinforcement er vigtige redskaber for hurtigt at træne system 1.

Derfor er fx phishingkampagner effektive i denne fase. Det viser medarbejderne konsekvensen af deres handlinger, så system 1 hurtigt lærer at handle rigtigt.

Information præcis på det tidspunkt, man skal til at udføre en potentielt usikker handling, kan fx også være effektiv i denne fase.



Øvelse: Awareness-kampagne for universitetsstuderende

- Hvad er de 3 vigtigste budskaber?
- Hvilken adfærd ønsker I at se?
- Hvad kan være effektive midler til at opnå det (plakater?)

Brug 2 min til at overveje



Physical security

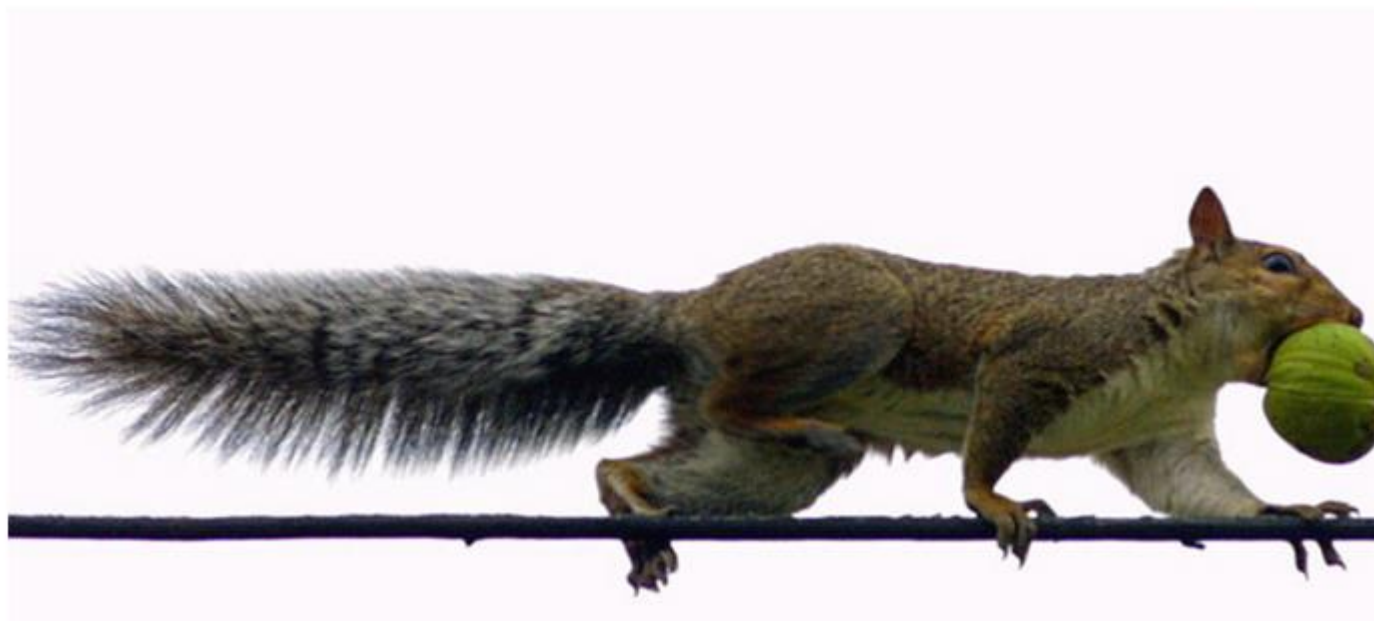
Hvad er den største trussel imod US infrastruktur

Forget hackers: Squirrels are a bigger threat to America's power grid

Who needs fancy military-grade equipment when nimble legs and sharp incisors will do?

By Eugene K. Chow | January 28, 2014

15

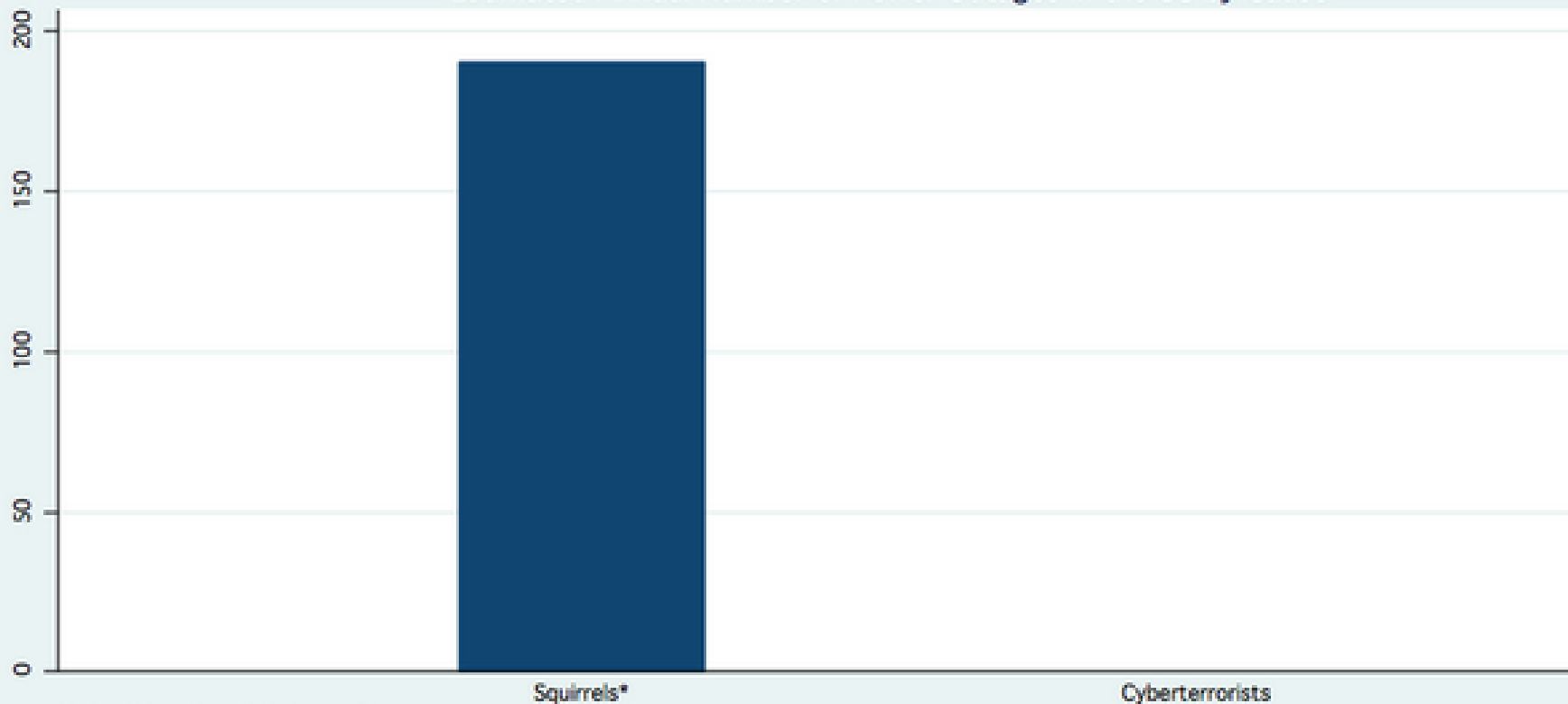


http://www.nytimes.com/2013/09/01/opinion/sunday/squirrel-power.html?pagewanted=all&_r=0



Hvad er den største trussel imod US infrastruktur

Estimated Annual Number of Power Outages in the US by Cause



Produced by Eli Dourado (@elidourado)

* Author's extrapolation of data presented at <http://www.nytimes.com/2013/09/01/opinion/sunday/squirrel-power.html?pagewanted=all>



Fysisk sikkerhed og IT Sikkerhed

Hvad er forbindelsen til IT-sikkerhed?

CIA
Confidentiality
Integrity
Availability



Fortrolighed – Integritet – Tilgængelighed



Availability Policies

Until recently, researchers ignored availability, but it's where the money goes

	Research	Industry
Confidentiality	90%	1%
Integrity/authenticity	9%	9%
Availability	1%	90%



Fysisk sikkerhed – Drop Table





Fysisk sikkerhed – andre overvejelser

Deter – Detect – Alarm – Delay – Respond

Hegn

Døre

Kamera

Video

Vinduer

Strømtavler

Fysisk placering

...

Som alt anden it-sikkerhed: Threat analysis,
design the system (equipment and procedures)
Then test it



Fysisk sikkerhed – andre overvejelser

Narkoman

Vaneforbryder

Specialist

International professionel

”Standardtyv” metoden



Placering af serverrum

Dit firma skal bygge et helt nyt serverrum...
Eksempler på overvejelser?



Fysisk sikkerhed

Lastbil og strømforsyning:

http://www.youtube.com/watch?v=M5CZu_XBf70

Flood:

http://www.youtube.com/watch?v=ANU-oSE5_hU

Tyrkiet:

https://www.youtube.com/watch?v=1M_QTBENR1Q

Halon:

<http://www.youtube.com/watch?v=2fyGGqgVzCY>

Huller i serverrummet:

<http://www.youtube.com/watch?v=sBENKXrxJZI>

Kabling og oprydning:

<http://www.youtube.com/watch?v=r-9VZubB1uI>



Spørgsmål

