Sikkerhedsledelse:

- Sikkerhedsverdenen
- Politikker og procedurer
- Beredskabsplaner
- Risikovurderinger
- Awareness
- Fysisk sikkerhed

Carsten Jørgensen
Department of Computer Science

Sikkerhed er mange ting

Organisatorisk
Dokumentation, fx politikker, regler, processer, procedurer, vejledninger, logs, referater, rapporter, testresultater, målinger, evalueringer mv.

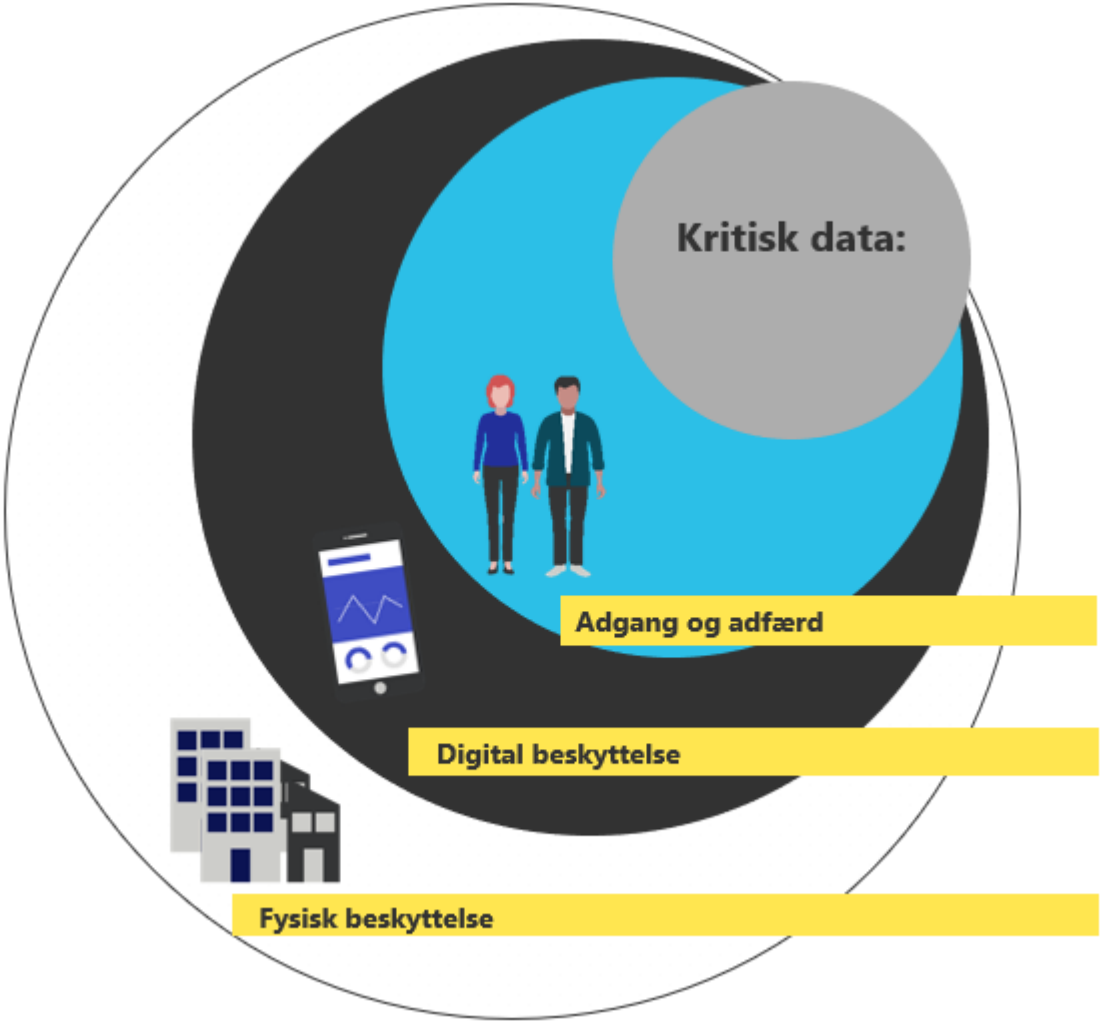
Adfærd
Personale skal leve op til informationssikkerhedspolitik ved hjælp af vejledninger, uddannelse og awareness. Alle skal vide hvornår en hændelse skal rapporteres

Fysiske rammer
De fysiske rammer skal beskyttes. De skal leve op til de krav, der sættes for at kunne beskytte systemer og information

Teknologisk sikring
Består i styring af adgange, logning, back-up, kryptering osv, osv.

Fysisk sikkerhed – Drop Table

IT sikkerhed – mange ting



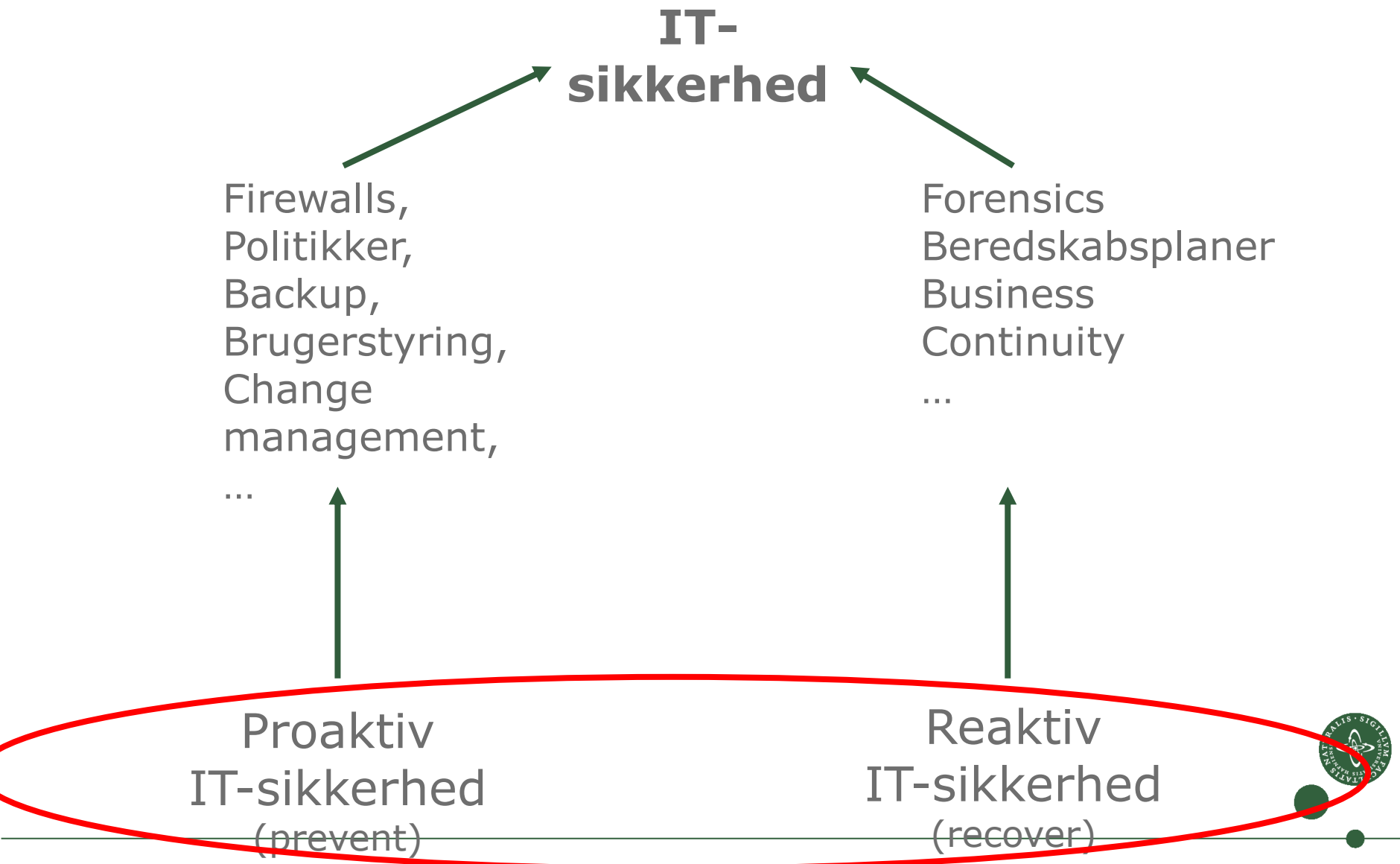
Sikkerhedsledelse – eksempler på CISO opgaver

- 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
- …

IT sikkerhed – mange ting

Hele kæden:
Predict - Prevent – Detect - Respond

Behovet for it-sikkerhed, også når det går galt



Behovet for it-sikkerhed, også når det går galt

Offensiv it-sikkerhed
- Penetrationstest
- Code reviews
- …

Defensiv it-sikkerhed
- Sikkerhedsledelse
- Sikkerhedsarkitektur
- Brugerstyring
- …

Lovgivning omkring sikkerhed

Aktivitet på alle fronter

GDPR
ENISA
EU arbejder i en række arbejdsgrupper
NIS og NIS2

NATO
Internationalt

Ransomware og andre store sikkerhedshændelser til bestyrelserne

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

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
- Fødevaresektoren
- Sundhedssektoren

Nedbrud kan medføre dramatiske konsekvenser

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 stige: ”Op til 10.000.000 EUR eller op til 2% 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

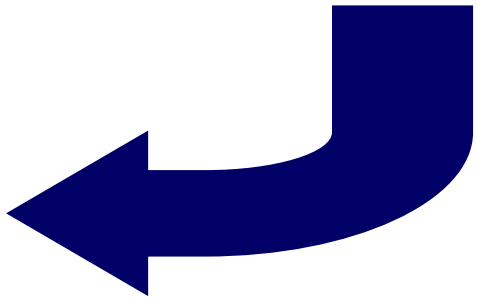
Sikkerhedsledelse

Behovet for it-sikkerhed

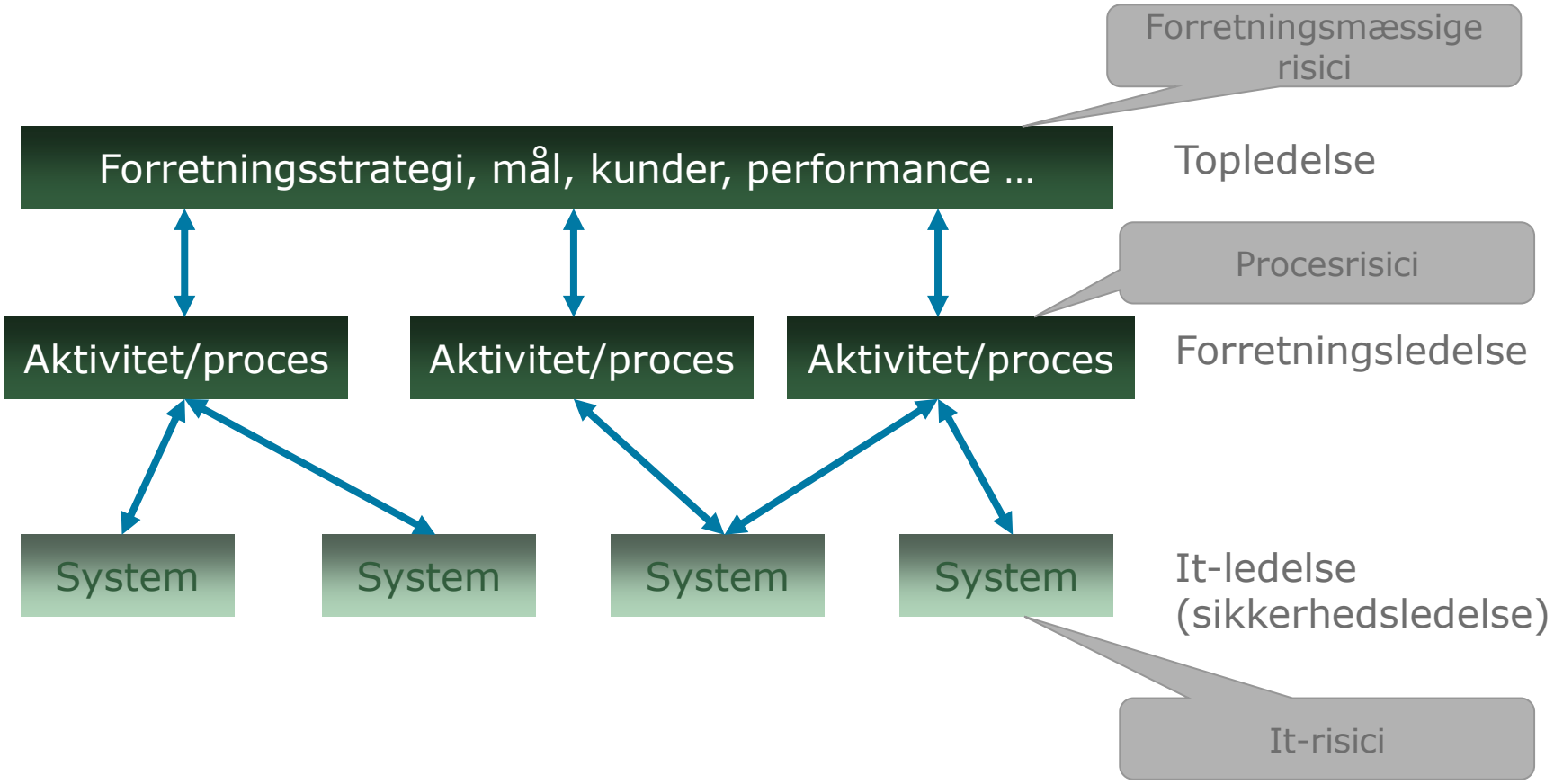
IT-sikkerhed - hvad er det rigtige niveau ??

- 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



I forretningsmæssig kontekst



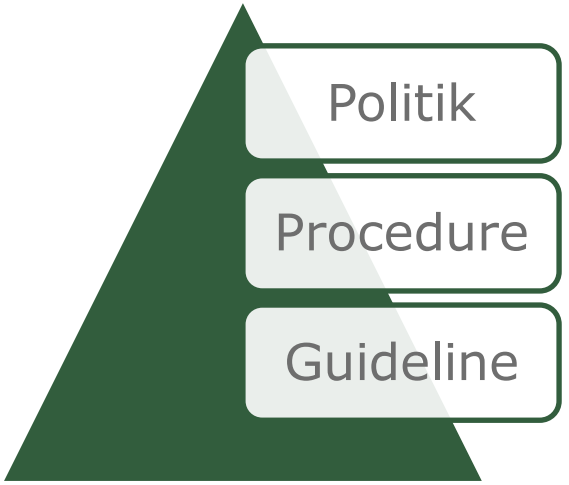
Politikker, procedurer, guidelines

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



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

Sikkerhedsguidlines:
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

Compliance vs. security

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

- 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

Beredskabsplaner

Business Continuity

Accidents happens

BBC News Sport Weather Capital Future

NEWS WILTSHIRE

Home UK Africa Asia Europe Latin America Mid-East US & Canada Business Health Sci/En

England Northern Ireland Scotland Wales UK Politics Education

19 April 2014 Last updated at 21:46 GMT

Share

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

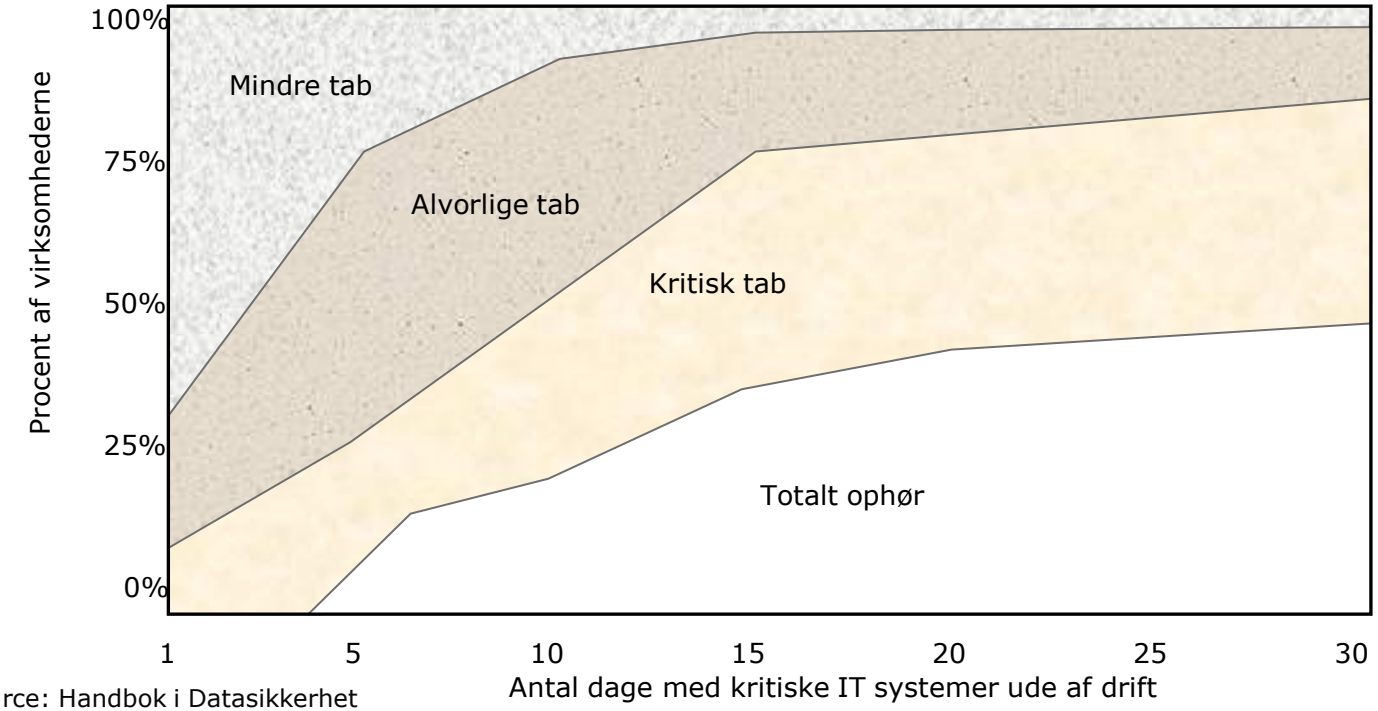
you be any more unfortunate

VERY DEMOTIVATIONAL .com

HVORFOR er beredskab vigtigt?

Nedbrud af IT-services vil have en stor betydning for mange virksomheders overlevelsesevne

Kan i nogen tilfælde true virksomhedens overlevelse



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

Krisestyringsgruppen

- Oversigt over aktiviteter
- Identificer jeres indledende aktiviteter (hvad gør i først?)
- Prioriter aktiviteter

- Marker aktiviteter i forhold til prioriteringen, f.eks. RØD for høj og GRØN for lav prioritering, eller 1-5

- Nummerer aktiviteter så man kan se tidsmæssige afhængigheder/rækkefølge

På forhånd

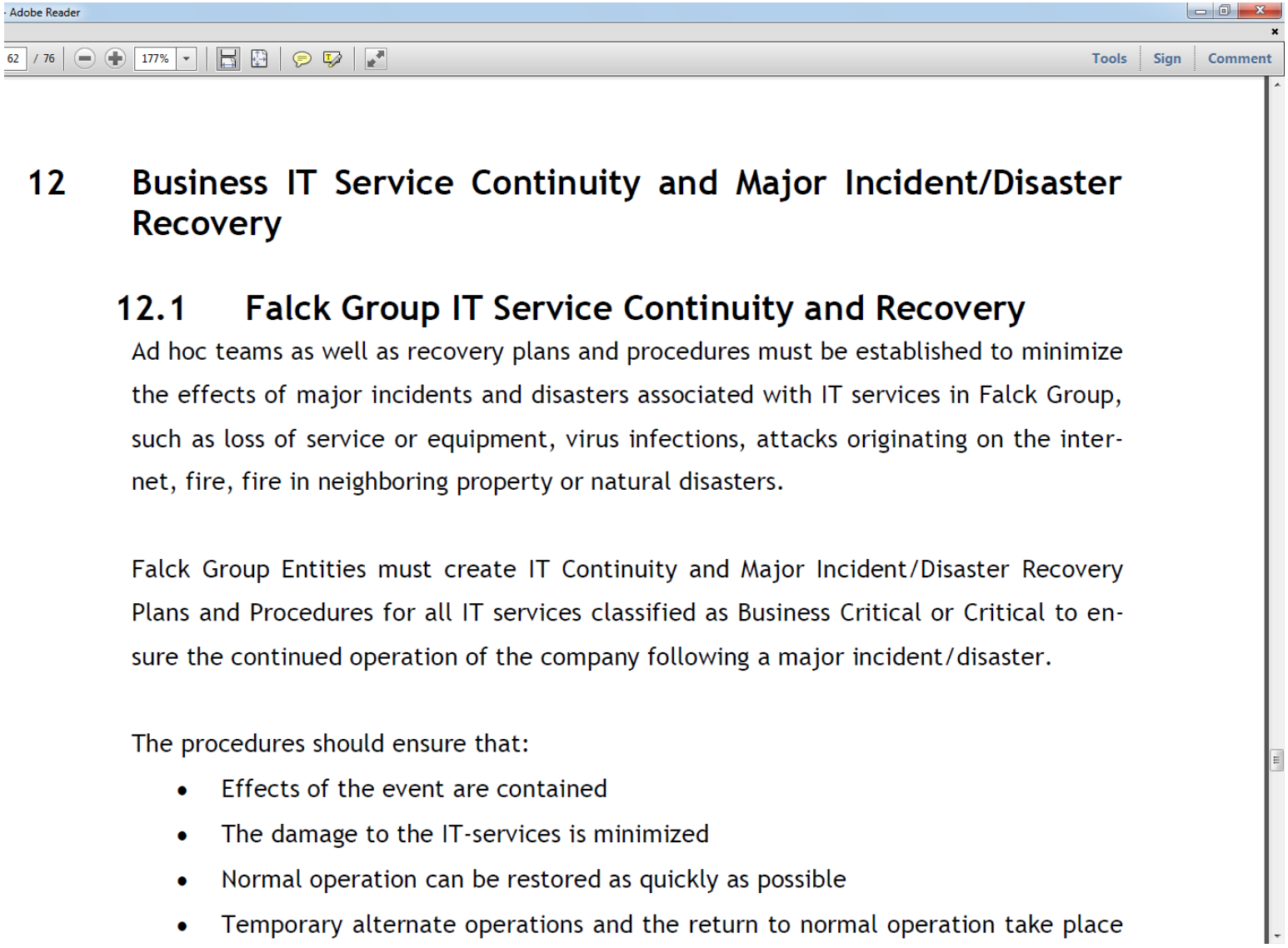
Afbrydelser

Eskalering
Budgetter og regler for godkendelse
Information internt
Kontaktlister (internt og eksternt)
Pressekontakt
Adgang til dokumentation i krisesituation
Oversigt over hardware, incl telefoner
Procedurer for genetablering, incl. tidsestimater


FAIL
EVACUATION PLAN
Run and run as fast as you can
failblog.org


TEES HOSP
Fire Alarm System
Out Of Order
If you discover a FIRE
FIRE FIRE FIRE
DIAL 3333
FAIL
failblog.org

Beredskab



12 Business IT Service Continuity and Major Incident/Disaster Recovery

12.1 Falck Group IT Service Continuity and Recovery

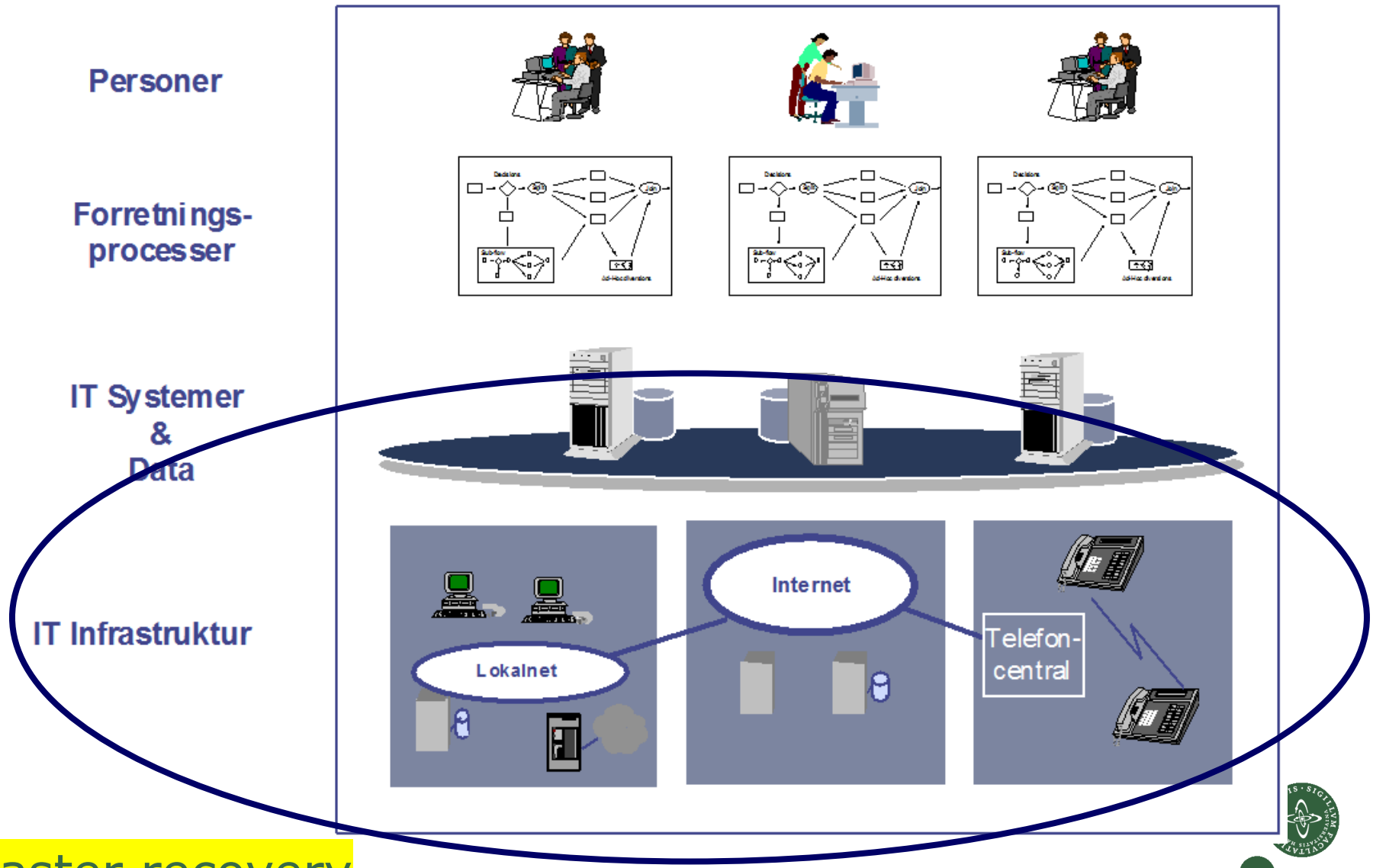
Ad hoc teams as well as recovery plans and procedures must be established to minimize the effects of major incidents and disasters associated with IT services in Falck Group, such as loss of service or equipment, virus infections, attacks originating on the internet, fire, fire in neighboring property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



Disaster recovery

Business continuity

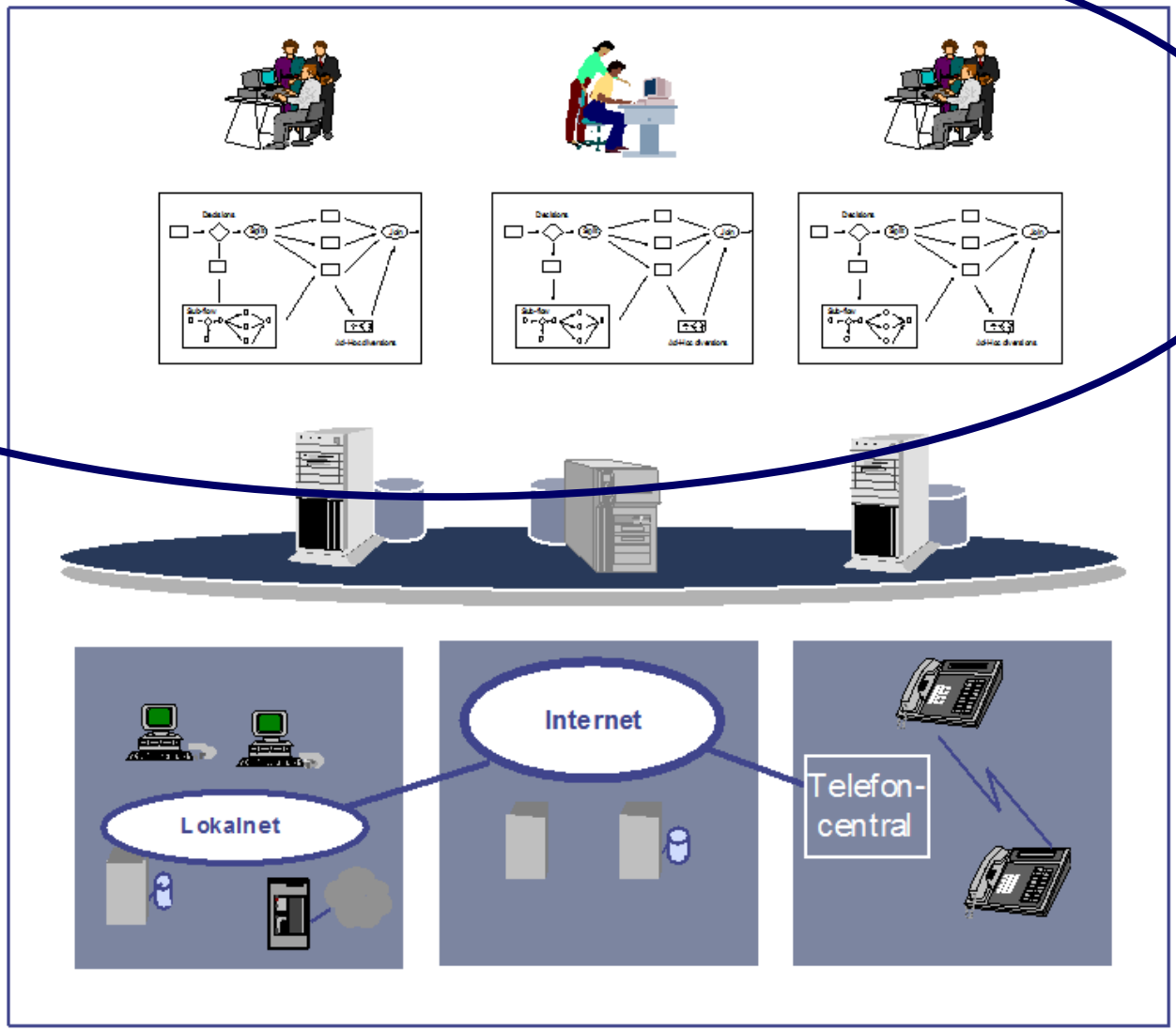
Forretningsprocesser og beredskab

Personer

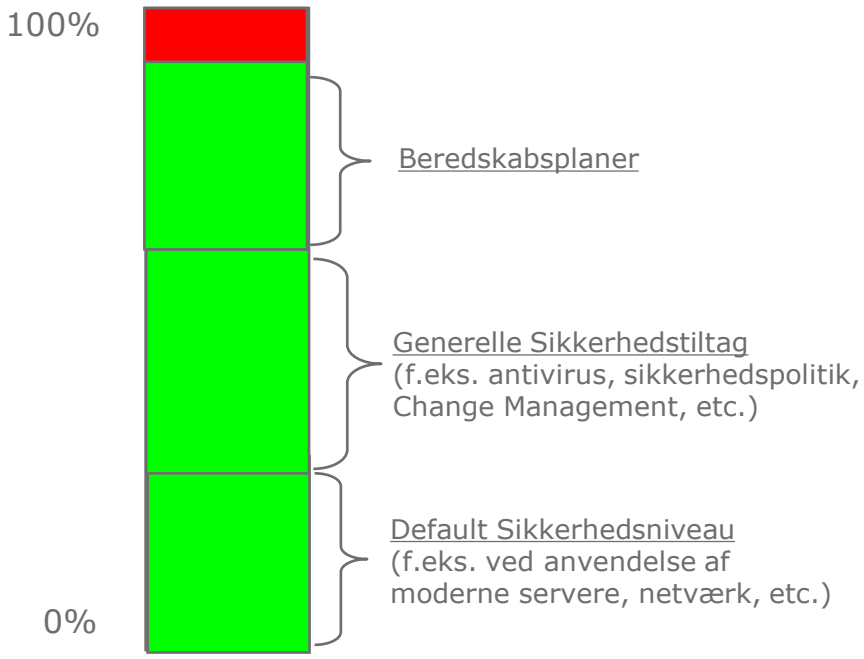
Forretnings-processer

IT Systemer & Data

IT Infrastruktur

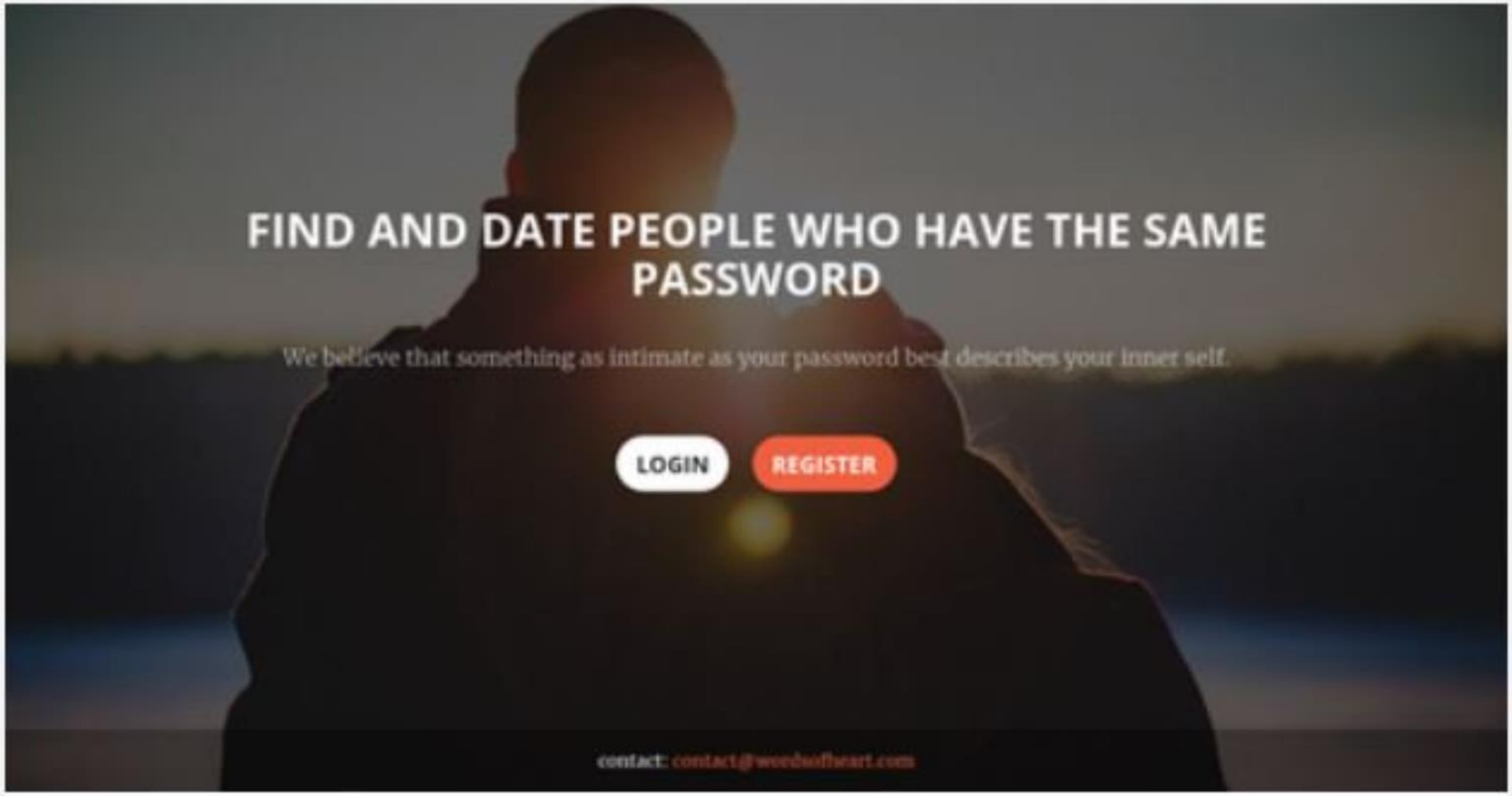


HVORFOR er beredskab vigtigt?



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.

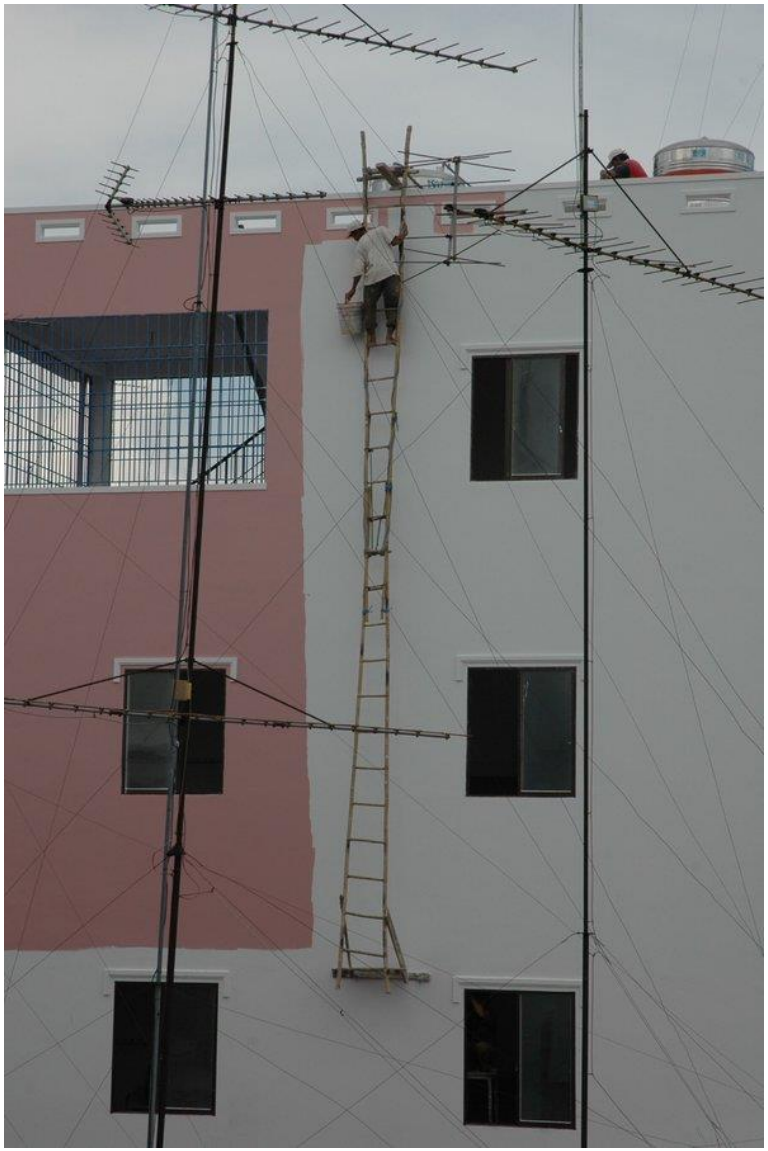
Pause



Words of Heart: Dating app matching people through their passwords

Risikovurdering

Risikovurderingen



Sikkerhedsmål

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

Risiko

En psykolog kan miste sin laptop under transport
Hvor alvorligt er det, hvad er sandsynligheden?

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

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?

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.

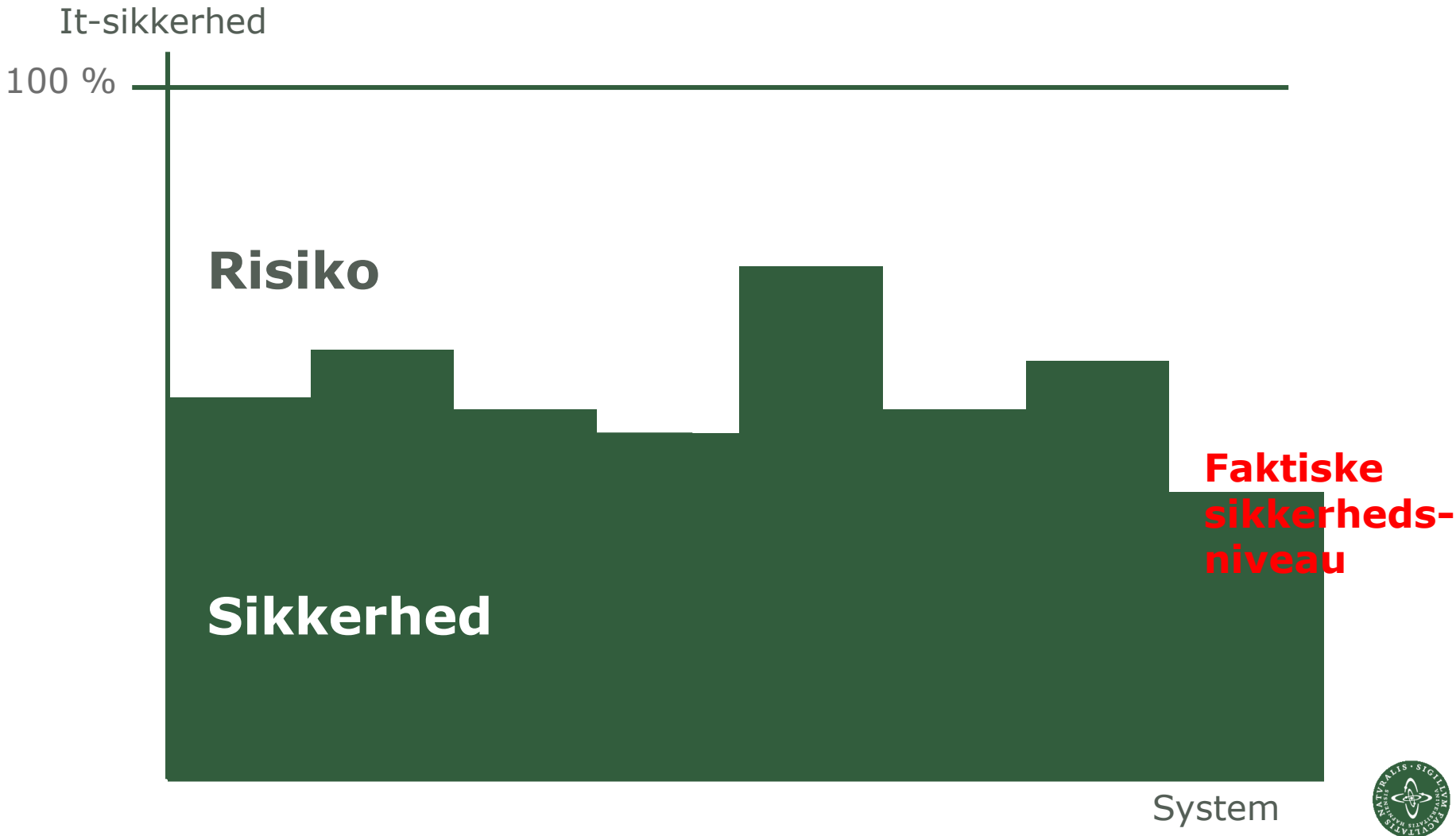
Undgår ting som ”Er internettet sikkert?”

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?"

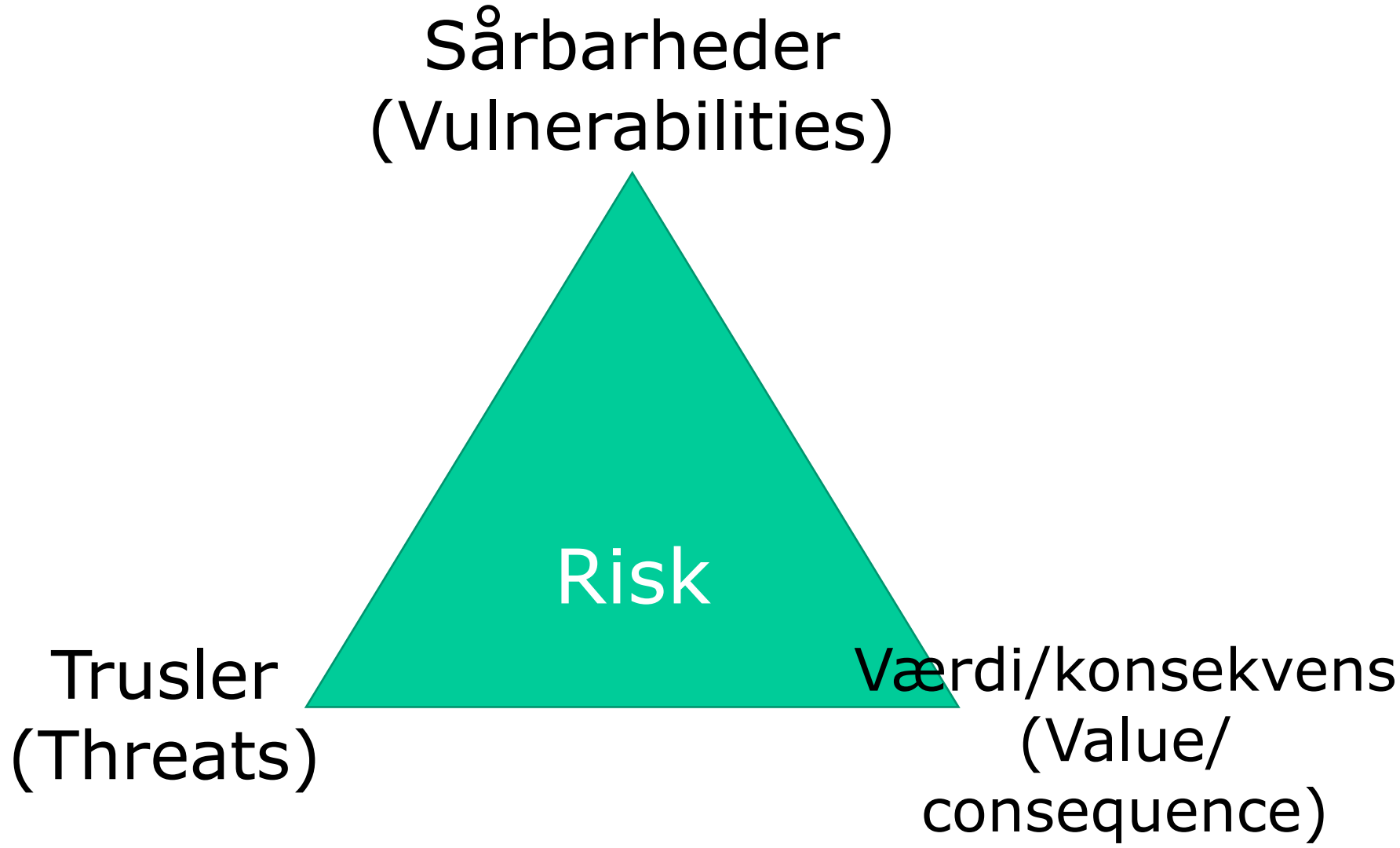
Risk assessments asks
"how much should I care?"

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

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

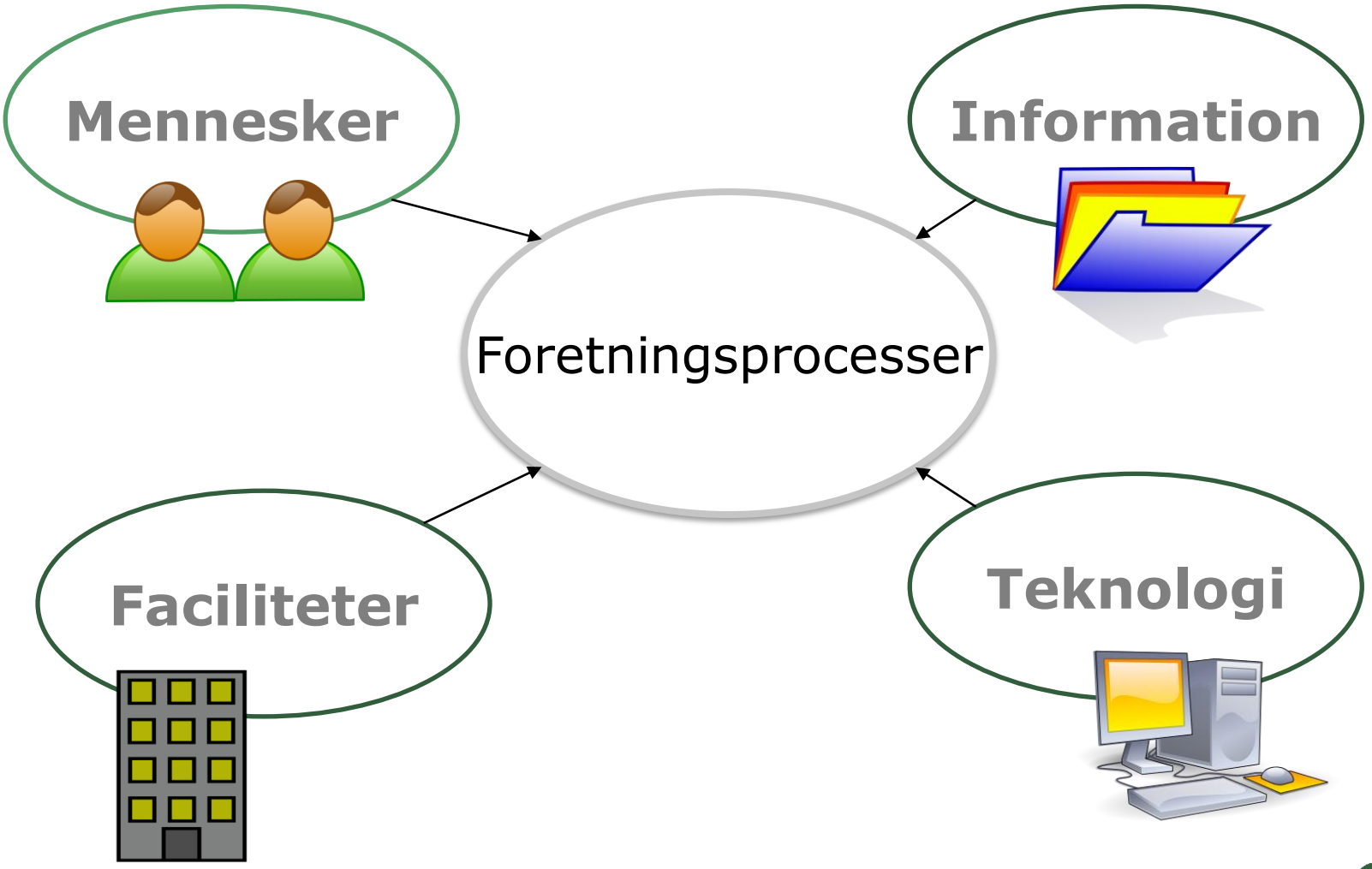
Uheld
- Brand
- Oversvømmelse
- Lynnedslag
- Strømafbrydelse
- Fejl på hardware
- Fejl i software
- Menneskelige fejl
- Tab af nøglepersoner
- Tab af netværksforbindelse

CIA

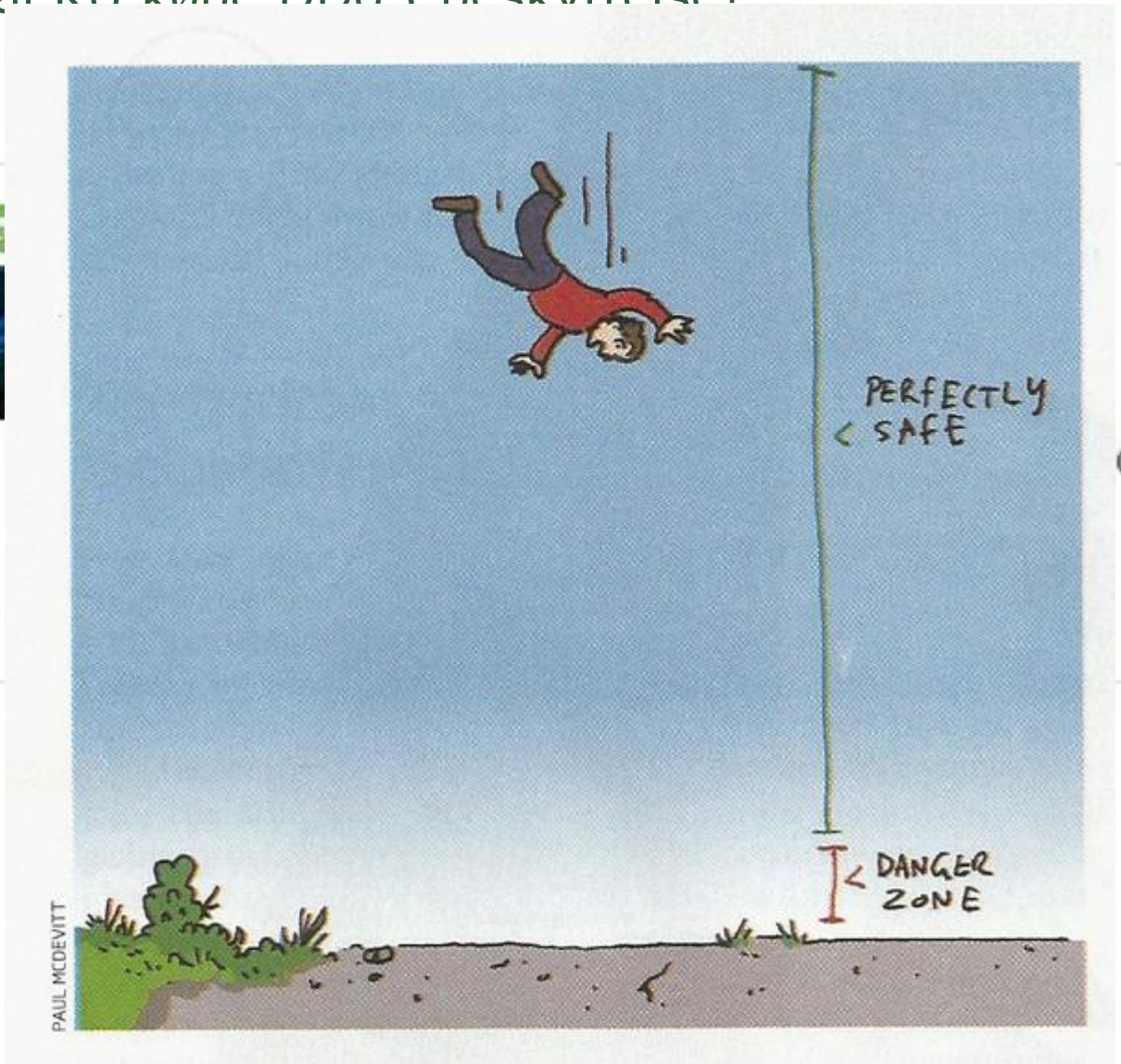
(Confidentiality, Integrity, Availability)

	Mennesker	Teknologi
Externe	... ...	... ...
Interne	... ...	... ...

Typer af aktiver



Skal DanID købe DDoS-beskyttelse?
Skal KU 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.

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?

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
	Comments: 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
	Comments: 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

Risiko = Sandsynlighed x Konsekvens

Sandsynlighed kan kategoriseres som:		Konsekvens kan kategoriseres som:	
Meget Sandsynlig	(4)	Katastrofal	(4)
Sandsynlig	(3)	Kritisk	(3)
Mindre Sandsynlig	(2)	Skadelig	(2)
Ikke sandsynlig	(1)	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

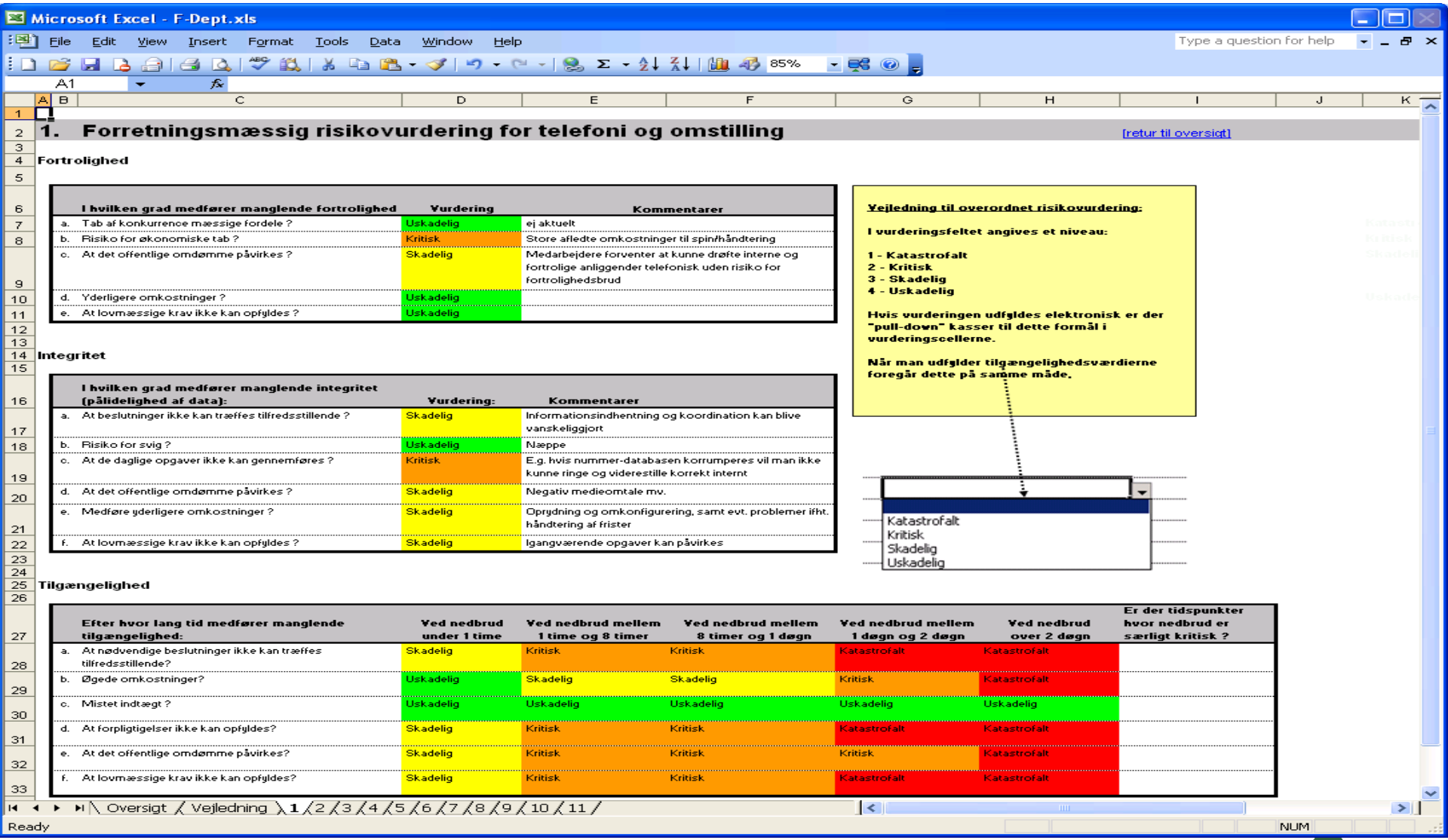
	No/low consequence	Medium consequence	High consequence
No/low probability	1x1=1	1x2=2	1x3=3
Medium Probability	2x1=2	2x2=4	2x3=6
High probability	3x1=3	3x2=6	3x3=9

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
	Comments:	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
	Comments:	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

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 spin/håndtering
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 korrumperes vil man ikke kunne ringe og viderestille 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

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

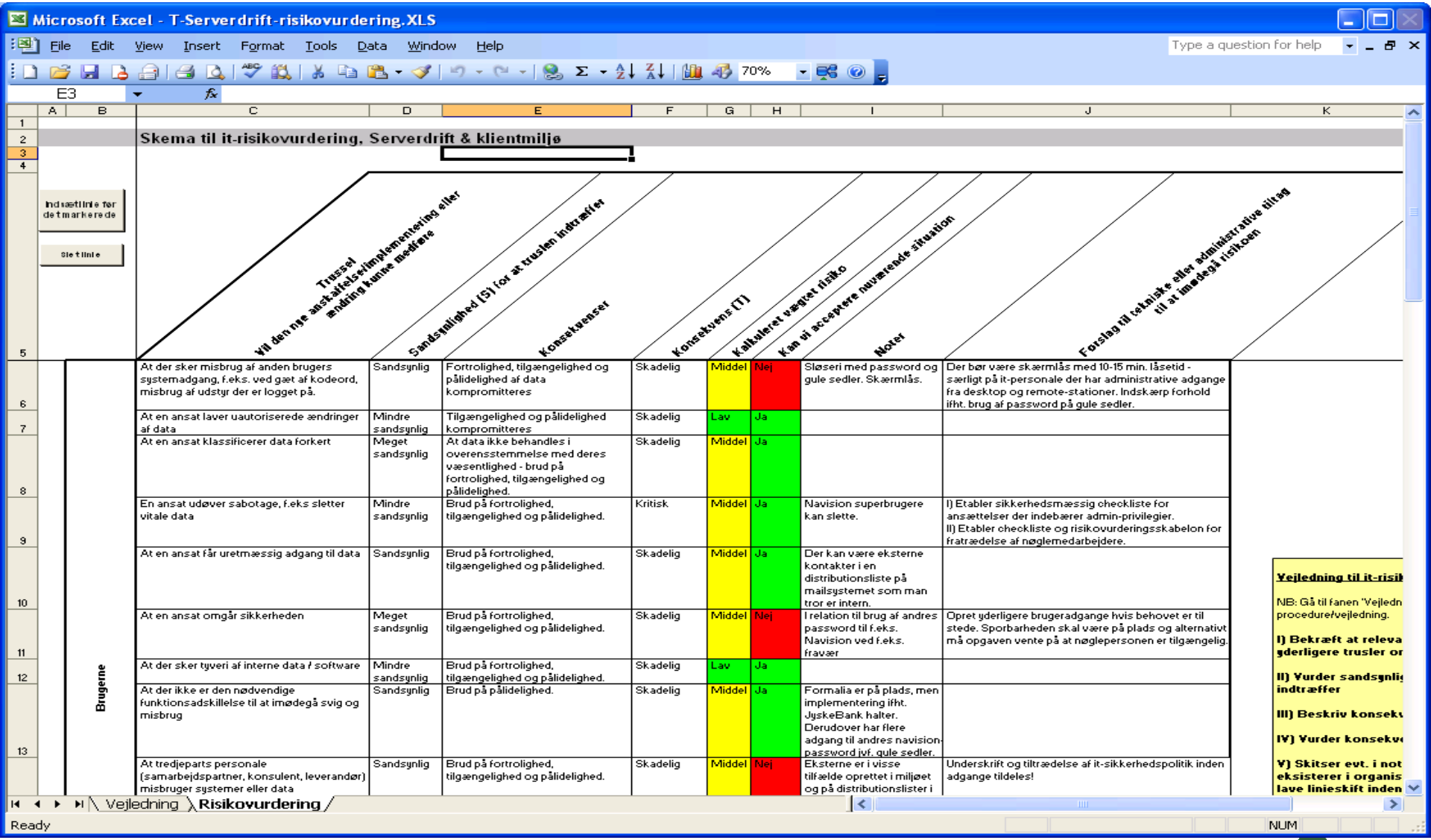
Tilgængelighed

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	

Oversigt / Vejledning / 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

Skema til it-risikovurdering, Serverdrift & klientmiljø

	Trussel: Vil den nye anskaffelse/implementering eller ændring kunne medføre	Sandsynlighed (S) for at truslen indtræffer	Konsekvenser	Konsekvens (T)	Kalkuleret vægtet risiko	Kan vi acceptere nuværende situation	Noter	Forslag til tekniske eller administrative tiltag til at imødegå risikoen
Brugerne	At der sker misbrug af anden brugers systemadgang, f.eks. ved gæt af kodeord, misbrug af udstyr der er logget på.	Sandsynlig	Fortrolighed, tilgængelighed og pålidelighed af data kompromitteres	Skadelig	Middel	Nej	Sløseri 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.
	At en ansat laver uautoriserede ændringer af data	Mindre sandsynlig	Tilgængelighed og pålidelighed kompromitteres	Skadelig	Lav	Ja		
	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		
	En ansat udøver 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 risikovurderingsskabelon for fratrædelse af nøglemedarbejdere.
	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.	
	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.
	At der sker tyveri af interne data *I software*	Mindre sandsynlig	Brud på fortrolighed, tilgængelighed og pålidelighed.	Skadelig	Lav	Ja		
	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 gderligere trusler or

II) Vurder sandsynlig indtræffer

III) Beskriv konseku

IV) Vurder konseku

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

DIKUcorp har en årlig omsætning på 100 mio DKR.
Virksomhedens webserver har en kendt RCE (Remote Code Execution) sårbarhed i virksomhedens CMS, der vil kunne udnytes til at tage fuld control over serveren.

En opdatering har været tilgængelig i 18 måneder men er endnu ikke rullet ud fordi virksomheden normalt venter til leverandøren har en samlet sevicepack opdatering klar.

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

Threat Assessment:
Risk 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 udnytes 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 omking 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 udnytes 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 omking 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 udnytes 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 omking 80% af virksomhedens omsætning, ligger på serveren. Der ligger en række databaser på serveren, flere indeholder persondata om virksomhedens 800.000 kunder.

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

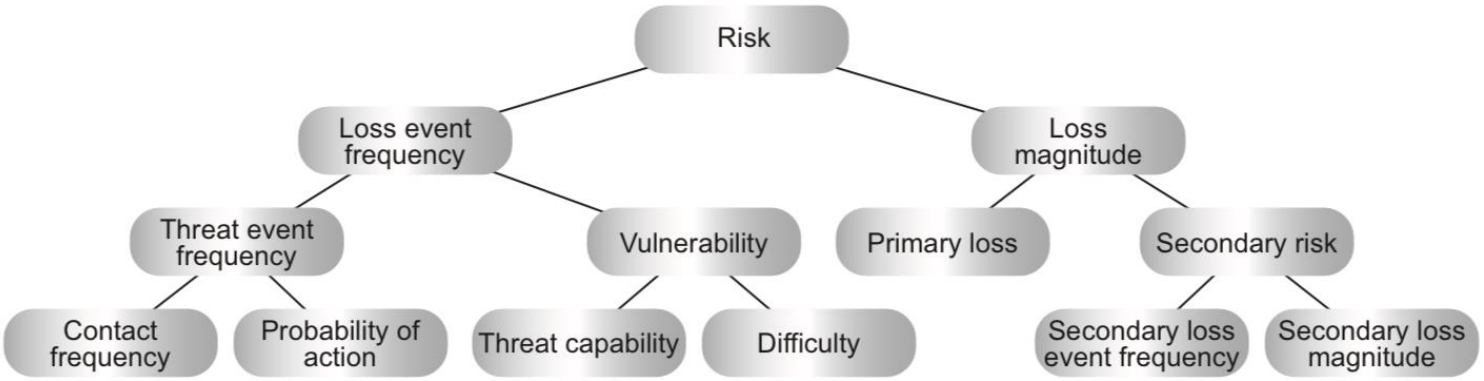
Hvad er sandsynligheden for vi bliver hacket?

Kan man overhovede beregne sandsynligheder indenfor sikkerhed?

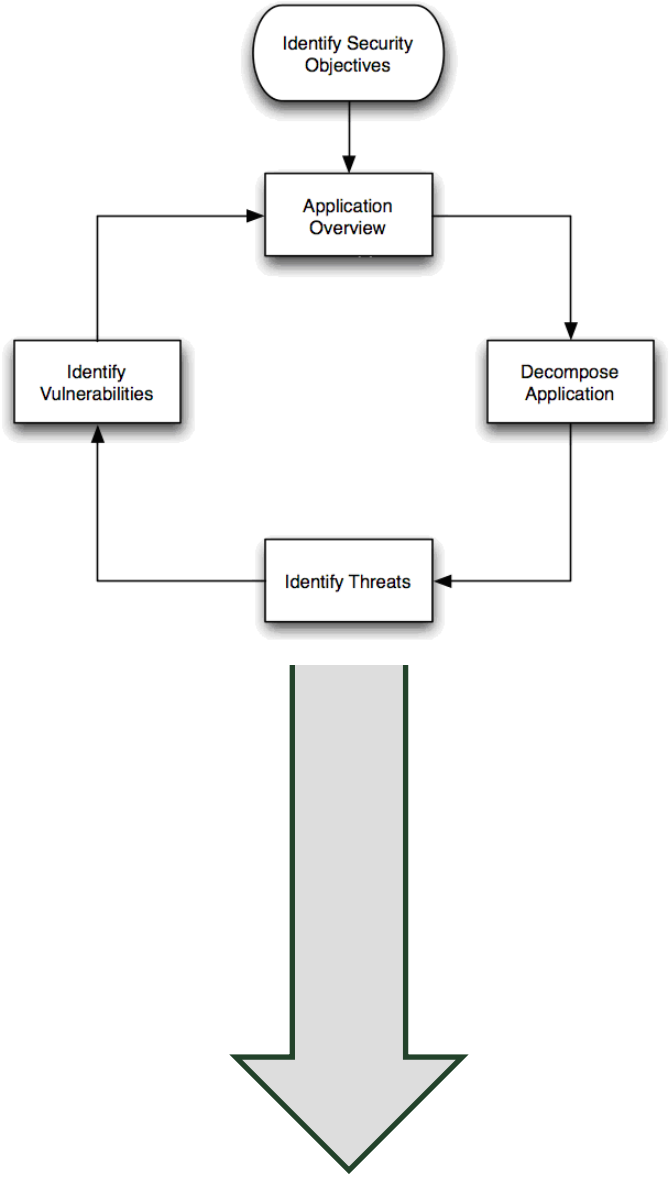
SANDSYNLIGHED OG SIKKERHED ("FAIR")

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

Men hvis man opdeler i relevante komponenter kan man – væsentligt bedre end med de traditionelle vurderinger - lave en vurdering og f.eks. vise ændringer i riskobilleder



http://en.wikipedia.org/wiki/Factor_analysis_of_information_risk



Løsningen	Hardware, software, interfaces, people, mission, system- and data classification
Overvej trusler	Tidligere angreb, vurdering af potentielle trusler
Find Sårbarheder	Krav, sikkerhedstests, potentielle sårbarheder
Vurder sandsynlighed	Angriber motivation, sikkerhedsmekanismer, typer af sårbarheder
Vurder Konsekvens	Hvad er den samlede risiko?

Opsummering

IT-sikkerhedsledelse, incl. risikovurderinger, er en kritisk del af it-sikkerheden – og et stærkt redskab

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

”Den menneskelige firewall”

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

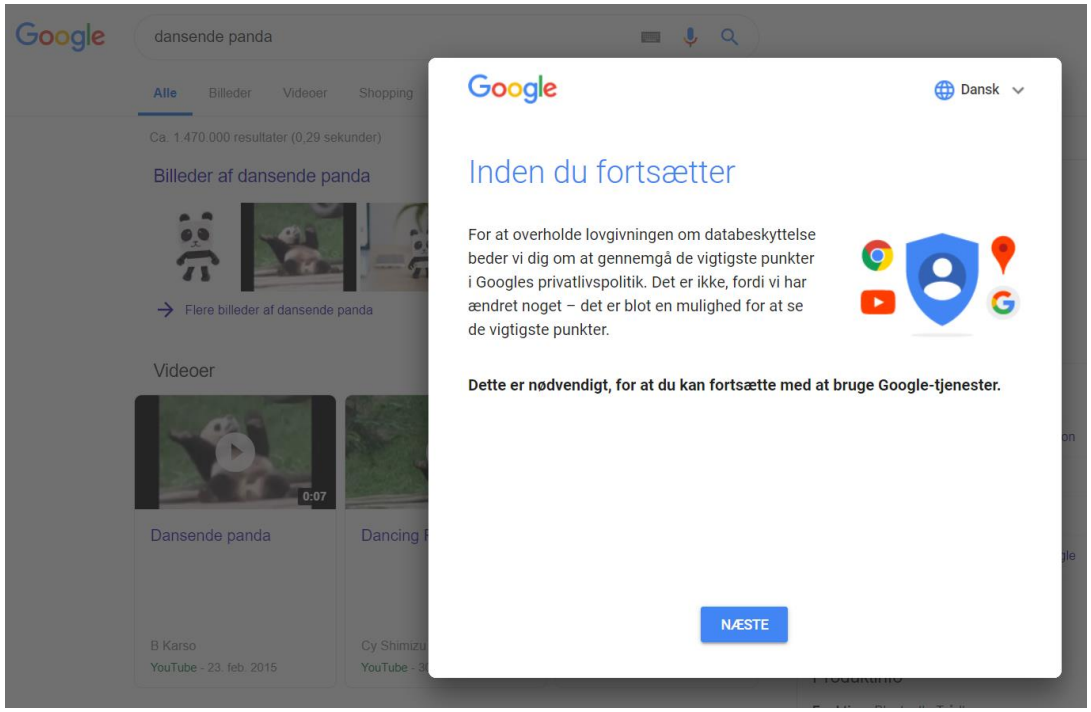
sikkerdigital.dk

Sikkerhedspakken 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**.

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 sikkerheds-budskaberne

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.”

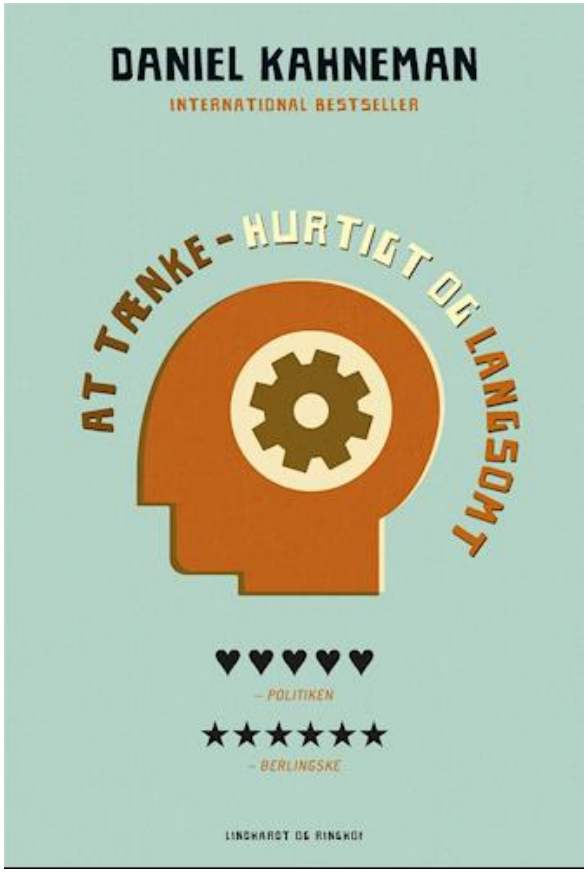
Problemet er, at mange sikkerhedshændelser starter med en trigger-hændelse, som vi reagerer på.

Når mennesker træffer beslutninger

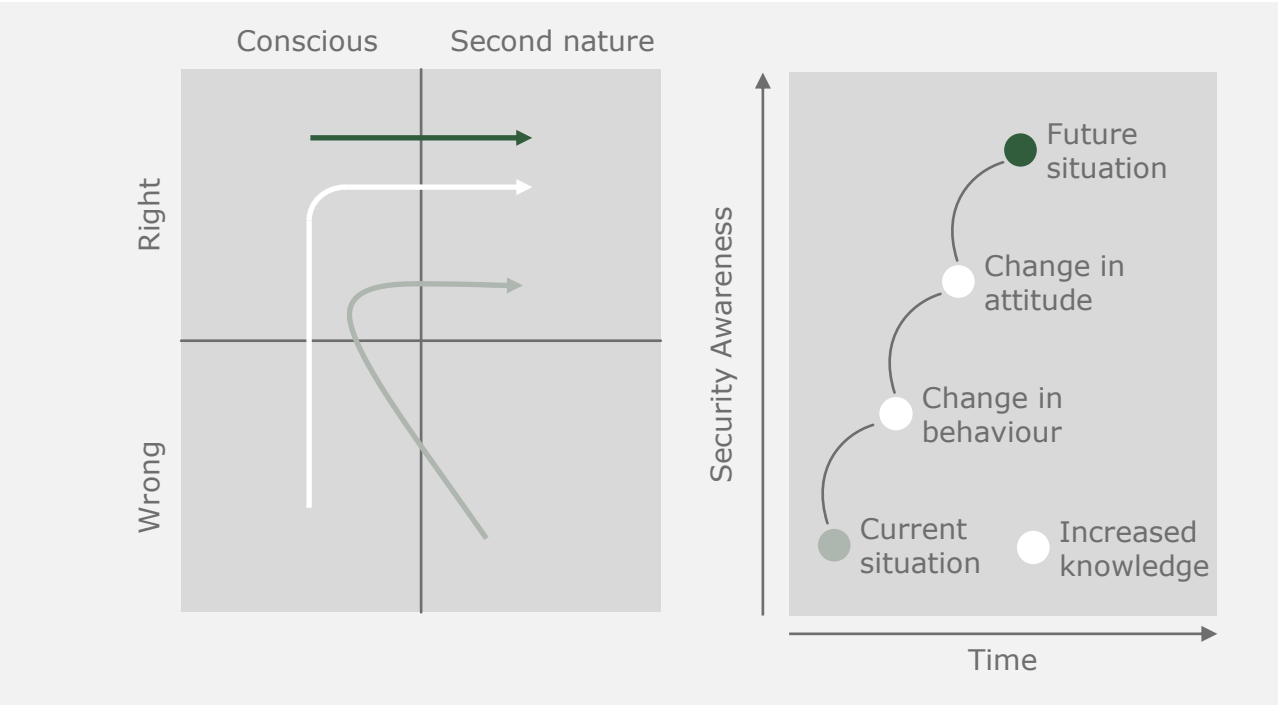
Daniel Kahneman beskriver i ”At tænke – hurtigt og langsomt”, hvordan, hvorfor og hvornår mennesker træffer beslutninger.

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.

ENISA 2016

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:
Lav en awareness-kampagne for universitetsstuderende

- Hvad er de 3 vigtigste sikkerhedsbudskaber for studerende?

- Hvilken adfærd ønsker I at se?
- Hvad kan være effektive midler til at opnå det (plakater?)

Brug 2 min til at overveje

Spørgsmål