CENTER FOR CYBERSIKKERHED

Center for Cybersikkerhed
- FGU-Festival 2024

Emil og Dean
Rådgivning, CFCS

1. oktober 2024

CENTER FOR CYBERSIKKERHED

Forventninger

	ER BEKENDT MED	FORSTÅR	KAN ANVENDE
Om CFCS og den aktuelle trusselsvurdering			
Vigtigheden af god cyberhygiejne og menneskelige adfærdstiltag			
Cybersikkerhed i sin beredskabsplanlægning- og styring			

Cybertruslen mod Danmark - aktuelle trusselsniveauer

CYBERSPIONAGE
MEGET HØJ

CYBERKRIMINALITET
MEGET HØJ

CYBERAKTIVISME
HØJ

DESTRUKTIVE
CYBERANGREB
MIDDEL

CYBERTERROR
INGEN

Cybertruslen mod Danmark - øvelse

Hvad er jeres største bekymringer?

Tal sammen i 2 minutter

Kort opfølgning

Risikostyring – hvorfor?

Ungdomsuddannelser lagt ned af it-kriminelle

Himmerlands Erhvervs- og gymnasieuddannelser er uden internet, og en del af deres it-infrastruktur er blevet ramt af et ransomwareangreb

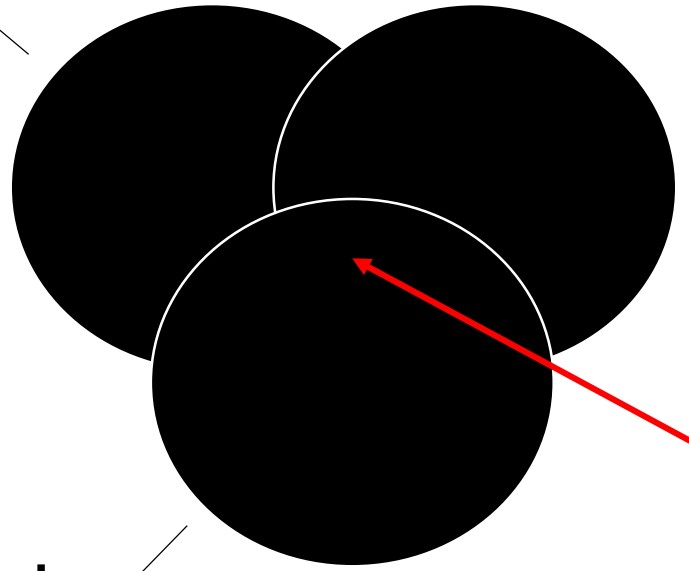
Ransomware-angreb mod sønderjyske skoler vokser: 40.000 underretninger om datalæk udsendt

GDPR | 2. oktober 2023 kl. 10:57 | 1

Risikostyring – Hvad er en risiko?

Aktiv

- Data
- Forretningsproces
- Nøglemedarbejder
- Forretningshemmelighed
- It-system
- Arbejds-pc
- Fysiske dokumenter



Trussel

- Statslig / ikke-statslig aktør
- Kriminalitet / Sabotage / Spionage
- Bevidst insider
- Phishing / DDoS / Malware / Brute force / supply chain attack

RISIKO

Sårbarhed

- Manglende adgangsstyring
- Manglende backup
- Ikke opdaterede systemer
- Svage passwords
- Manglende retningslinjer
- Mangelfuld leverandørstyring

Risikostyring – Hvor lander bekymringerne?

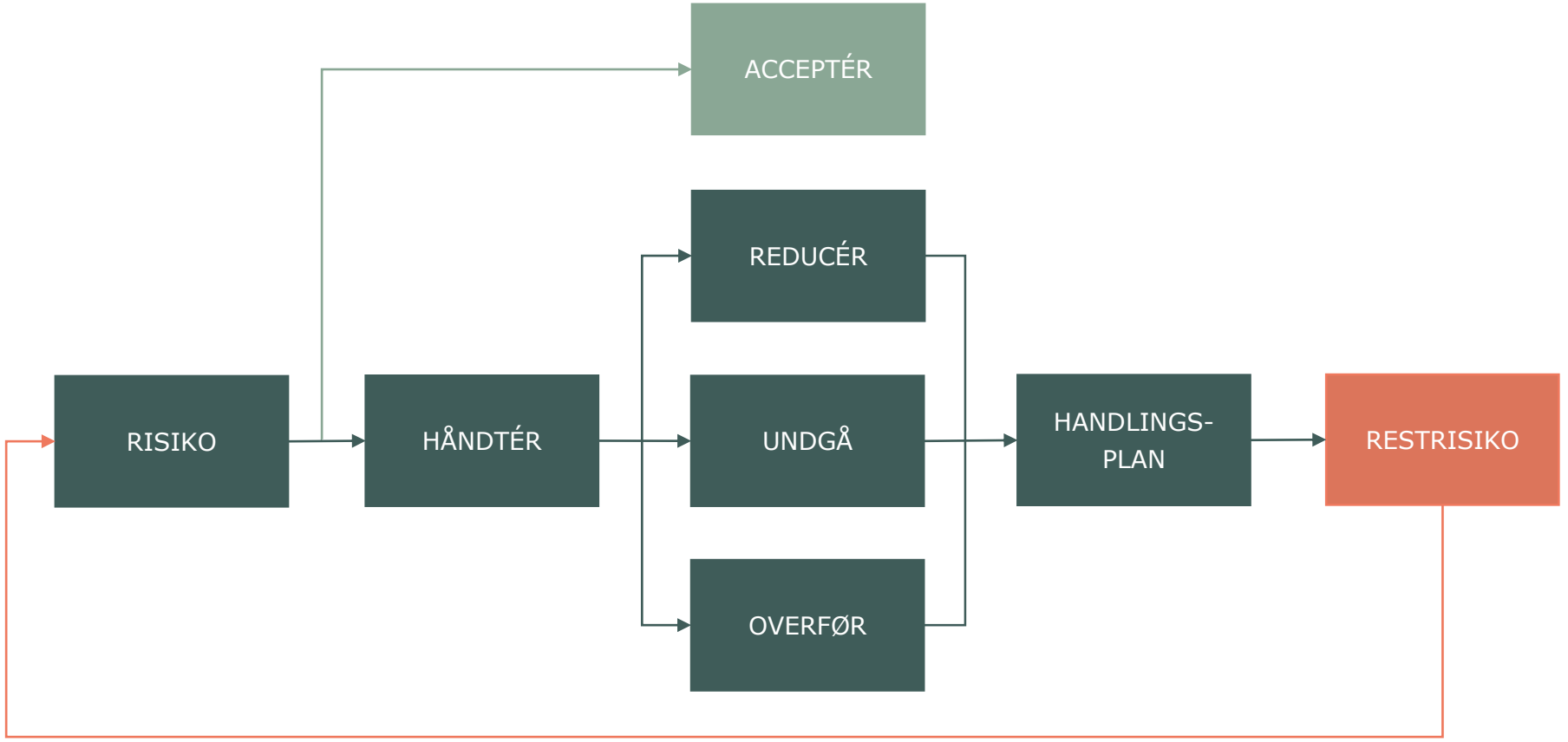


Illustration af beslutningsmodel fra sikkerdigital.dk:
https://sikkerdigital.dk/myndighed/iso-27001-implementering/risikostyring/beslutning

Forebyg med god cyberhygiejne – cybertruslen mod Danmark 2024

Sårbarheder

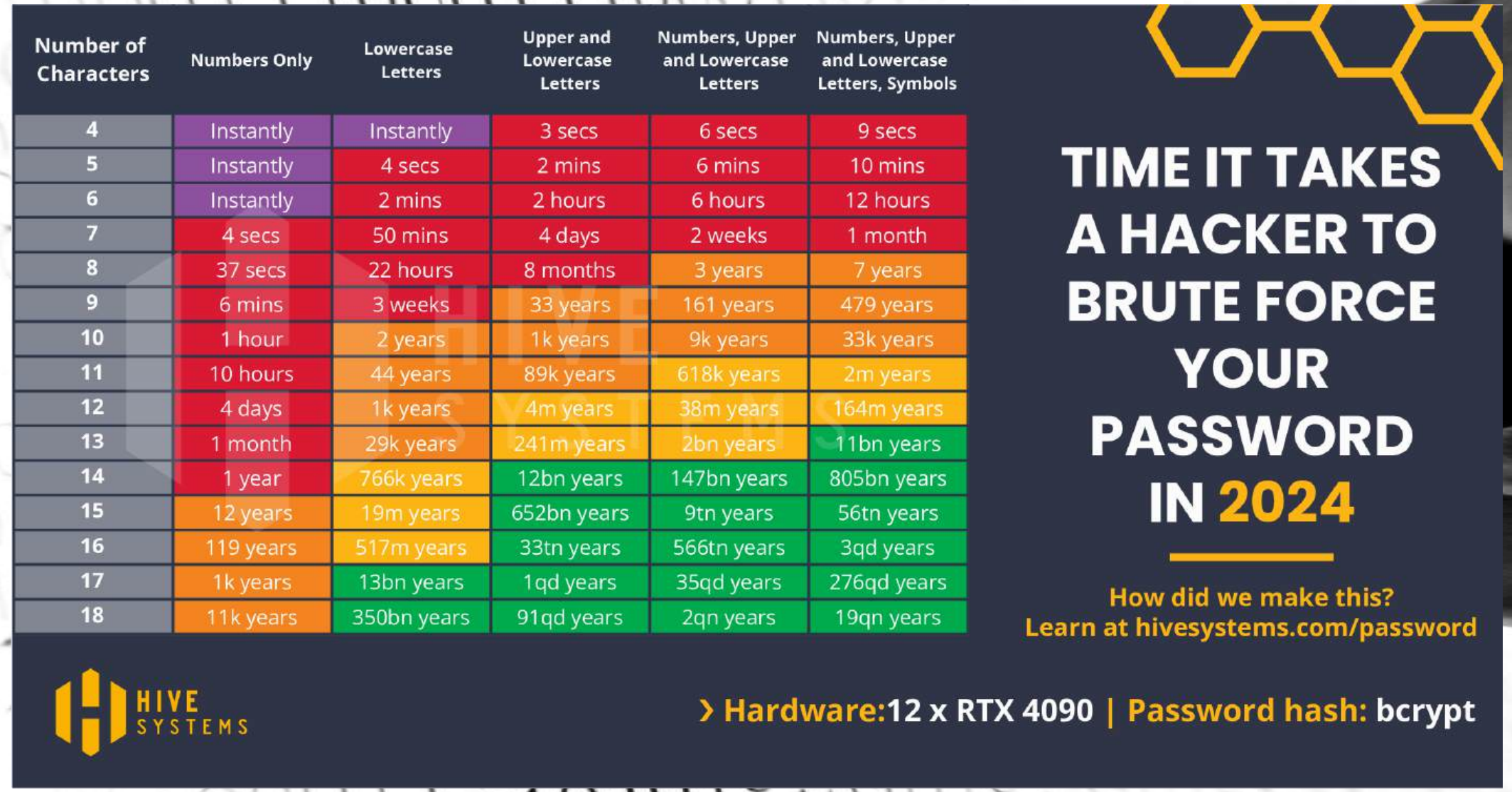
Cyberkriminelle angriber ofte via kendte sårbarheder i software

Phishing

Phishing-mails er fortsat blandt hackeres fortrukne værktøjer.

Passwords

Brute force-angreb er stadig en anvendt og effektiv angrebsmetode.



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

Phishing

BESKYT

- DMARC
- DNSSEC
- Mailfilter

"ENABLE"

- Uddannelse og træning
- Sikkerhedskultur
- Fremhæv potentielt farlige links/indhold

BEGRÆNS

- Flerfaktor-autentifikation (MFA)
- Opdateret og hærdet browser
- Antivirus

90%

I en verden af **komplekse og foranderlige cybertrusler,** hvor op til **90 procent** af alle cyberangreb skyldes **menneskelige fejl**, er det vigtigt at øge vores forståelse for det menneskelige aspekt i cybersikkerhed og se på, **hvorfor mennesker fejler.**

Kilde: The Global Risks Report 2022, World Economic Forum

CENTER FOR CYBERSIKKERHED

Adfærdsindsats - case

Scenarie 1

I modtager veludførte phishingforsøg der kan forbigå jeres sikkerhedssoftware.

Hvordan hjælper I medarbejderne, så de undgår at falde for phishingmails?

Scenarie 2

Medarbejdere rapporterer sjældent phishingforsøg, selvom I har kendskab til at de forekommer.

Hvordan hjælper I medarbejderne til at blive bedre til at rapportere phishingforsøg?

Hvilke tiltag vil I indføre?

Tal sammen i 2 minutter

CENTER FOR CYBERSIKKERHED

Adfærdsindsats - case

Scenarie 1

I modtager veludførte phishingforsøg der kan forbigå jeres sikkerhedssoftware.

Hvordan hjælper I medarbejderne, så de undgår at falde for phishingmails?

Scenarie 2

Medarbejdere rapporterer sjældent phishingforsøg, selvom I har kendskab til at de forekommer.

Hvordan hjælper I medarbejderne til at blive bedre til at rapportere phishingforsøg?

Rapporteringsknap

Medarbejdere får mulighed for at **indmelde** phishingforsøg. Rapporteringer anvendes til at forbedre jeres mailfiltre

”Bid ikke på!” - Kampagne

I indkøber en **generisk** awareness-kampagne. Kampagnen skal øge medarbejdernes viden om phishing

Analyse

For at komme problemets omfang nærmere **analyserer** I processer der er sårbare over for phishing

CENTER FOR CYBERSIKKERHED

Adfærdsindsats - case

Scenarie 1

I modtager veludførte phishingforsøg der kan forbigå jeres sikkerhedssoftware.

Hvordan hjælper I medarbejderne, så de undgår at falde for phishingmails?

Scenarie 2

Medarbejdere rapporterer sjældent phishingforsøg, selvom I har kendskab til at de forekommer.

Hvordan hjælper I medarbejderne til at blive bedre til at rapportere phishingforsøg?

Rapporteringsknap

Medarbejdere får mulighed for at **indmelde** phishingforsøg. Rapporteringer anvendes til at forbedre jeres mailfiltre

”Bid ikke på!” - Kampagne

I indkøber en **generisk** awareness-kampagne. Kampagnen skal øge medarbejdernes viden om phishing

Analyse

For at komme problemets omfang nærmere **analyserer** I processer der er sårbare over for phishing

Analysen viser

- Medarbejdere kan ikke genkende phishingmails
- Nogle medarbejdere anvender arbejdsmail til tredjeparts services/apps hvor flere er har haft datalæk
- En række forretningsprocesser foregår over mailkorrespondance

CENTER FOR CYBERSIKKERHED

Adfærdsindsats - case

Scenarie 1

I modtager veludførte phishingforsøg der kan forbigå jeres sikkerhedssoftware.

Hvordan hjælper I medarbejderne, så de undgår at falde for phishingmails?

Scenarie 2

Medarbejdere rapporterer sjældent phishingforsøg, selvom I har kendskab til at de forekommer.

Hvordan hjælper I medarbejderne til at blive bedre til at rapportere phishingforsøg?

Rapporteringsknap

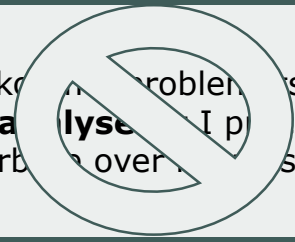
Medarbejdere får mulighed for at **indmelde** phishingforsøg. Rapporteringer anvendes til at forbedre jeres mailfiltre

”Bid ikke på!” - Kampagne

I indkøber en **generisk** awareness-kampagne. Kampagnen skal øge medarbejdernes viden om phishing

Analyse

For at kv[illegible]roblem[illegible]s omfang nærmere **a[illegible]lyse**[illegible] I p[illegible]esser der er sårb[illegible] over [illegible]shing



Phishingtræning

I indkøber en **målrettet** phishing-træningspakke der træner medarbejdere i at identificere phishingforsøg

Tilpasning af retningslinjer

I indskærper **retningslinjer** for brug af arbejdsmails. Dispensation kræves ved brug af tredjeparts services/apps

Tilpasning af processer

I styrker forretningsprocesserne, ved at tilføje krav om at **verificering** ikke alene er mailbaseret

Adfærdsindsatser starter med at lytte og lære

ADFÆRDSINDSATSENS FEM FASER:

1. HVAD ER PROBLEMET?
   IDENTIFICÉR PROBLEMET OG SÆT MÅL FOR ØNSKET ADFÆRD
2. HVAD FORSØGER VI AT LØSE/ÆNDRE?
   ANALYSÉR OG IDENTIFICÈR ADFÆRDSPROBLEMET
3. HVORDAN VIL VI ÆNDRE DET?
   UDARBEJD ADFÆRDSINDSATSEN
4. LYKKEDES VI? HVIS IKKE, HVORFOR?
   TEST ADFÆRDSINDSATSEN
5. IMPLEMENTÉR/RAPPORTÉR
   IMPLEMENTÉR ADFÆRDSINDSATSEN OG FØLG OP

https://www.cfcs.dk/globalassets/cfcs/dokumenter/vejledninger/adfaerdsindsatser-cyber-og-informationssikkerhed-juni-2021.pdf

Adfærdsindsatser starter med at lytte og lære

Find det rette niveau for
adfærdsindsatsen baseret på:

RISICI	KAPABILITET	KAPACITET
RISIKOAPPETIT	KOMPETENCER	RESSOURCER

Niveau 1
Ikke fokus på det menneskelige aspekt

Niveau 2
Compliance fokuseret

Niveau 3
Promoverer awareness, uddannelse og træning

Niveau 4
Indsigt i menneskelig adfærd

Niveau 5
Metodisk styrke og støjfrie vurderinger

TLP:GREEN

All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvnmwk.onion/?E3D94FA5
    This link only works in Tor Browser!
| 3. Follow the instructions on this page

Attention!
Do not rename encrypted files.
Do not try to decrypt using third party software, it may cause permanent data loss.
Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
Tor Browser user manual https://tb-manual.torproject.org/about

!!! We also download huge amount of your private data, including finance information, clients personal info, network diagrams, passwords and so on.
Don't forget about GDPR.

TLP:GREEN

Kilde: https://arstechnica.com/information-technology/2020/05/lockbit-the-new-ransomware-for-hire-a-sad-and-cautionary-tale/

Beredskabets faser – et konkret afsæt for beredskabsplanlægningen

Aktivér → Mobilisér → Organisér → Håndtér → Afslut

En beredskabsplan **skal** være

- Ajourført
- Afprøvet
- Ledelsesgodkendt

Beredskabsplanen **bør** være

- Handlingsorienteret
- Overskuelig
- Realistisk
- Tilgængelig
- Læst og forstået

TLP:GREEN

Fastlæg hvornår beredskabet aktiveres

- Klare aktiveringskriterier
- Mandat til aktivering
- Bygge bro til hændelseshåndtering

TLP:GREEN

Hav styr på hvordan beredskabet mobiliseres

- Kontaktlister og kommunikationsform
- Mødefaciliteter og tidspunkt
- Alternative lokationer, kommunikationskanaler mv.

Aktivering | Mobilisering | Organisering | Håndtering | Afslutning

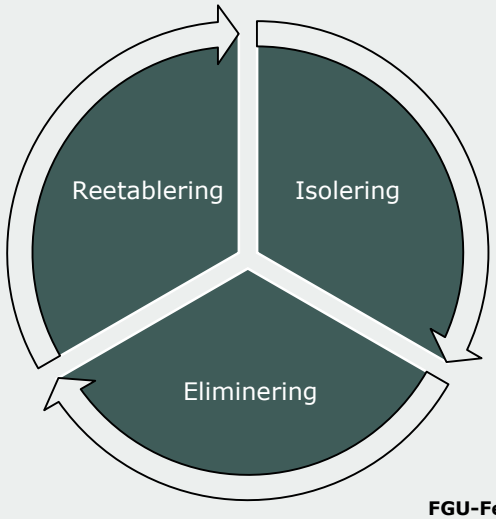
Hvem gør hvad i beredskabet?

- Roller og ansvar, herunder beslutningsmandat
- Interessenter og leverandører
- Incident response team (evt. eksternt)
- Intern/ekstern kommunikation

TLP:GREEN

Få styr på hændelsen

- Situationsoverblik: Antagelser, fakta og vedtagne beslutninger
- Kommunikation
- Isolér, eliminér, reetablér



TLP:GREEN

Tilbage til normalen – med ny viden

- Opfølgning og læring
- Fastlæg kriterier og rammer for afslutning
- Test og øvelser

CENTER FOR CYBERSIKKERHED

Hvor kan jeg finde mere information?

- Vejledninger
- Trusselsvurderinger
- Temaartikler
- Undersøgelsesrapporter og meget mere

www.cfcs.dk

Center for Cybersikkerhed

@cybersikkerhed
@CFCSsitcen

BEMÆRK: Trusselsniveauet varierer på tværs af sektorer