CENTER FOR CYBERSIKKERHED

Vejledning

Cyberforsvar der virker

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

4. udgave juli 2023.

Indledning

Cybertruslen er et grundvilkår for danske myndigheder og virksomheder. Populært sagt så er det ikke et spørgsmål om en myndighed eller virksomhed bliver ramt, men om hvornår.

Cyberforsvar der virker indeholder seks trin, som myndigheder og virksomheder kan bruge til at opbygge et grundlæggende cyberforsvar. Hvis vejledningens trin implementeres, vil det være muligt at forhindre en markant andel af de cyberangreb, som myndigheder og virksomheder løbende er udsat for, samt være i stand til effektivt at håndtere de angreb, der lykkes.

6 trin til et cyberforsvar der virker

1. Ledelsens værktøjskasse
2. Teknikken der hjælper os
3. Det handler om adfærd
4. Opdag fjenden
5. Vær beredt!
6. Find huller i cyberforsvaret

Topledelsens bevågenhed er den vigtigste forudsætning for et cyberforsvar der virker. Ledelsen skal styre cyber- og informationssikkerheden ved løbende at støtte, prioritere og følge op på målsætninger og strategier efter samme principper som inden for f.eks. økonomi og HR. Et effektivt cyberforsvar er ikke et projekt, men en løbende proces, hvor der hele tiden skal evalueres og optimeres. Det gælder for alle seks trin i denne vejledning. Derfor skal ledelsen prioritere løbende opfølgning og forbedring.

Vi anbefaler, at myndigheder og virksomheder tager udgangspunkt i internationale standarder og best practice. I Danmark anvendes ofte ISO 27001, NIST Cybersecurity Framework, SANS og CIS 18. Ved at efterleve standarder og best practice skabes der et fundament for at etablere faste processer hos myndigheder og virksomheder til gavn for cyber- og informationssikkerheden.

Læsevejledning
Cyberforsvar der virker henvender sig til alle offentlige myndigheder og virksomheder, der har komplekse it-systemer, men den kan med fordel læses af alle, der interesserer sig for god cyber- og informationssikkerhed. Vejledningen henvender sig primært til ledelsen og cyber- og informationssikkerhedsmedarbejdere.

Myndigheder og virksomheder kan være underlagt specifikke krav til cyber- og informationssikkerheden. Det kan være krav om at følge en bestemt standard eksempelvis ISO 27001 eller implementere specifikke tekniske foranstaltninger, som eksempelvis de tekniske minimumskrav, der begge gælder for statslige myndigheder.

Cyberforsvar der virker erstatter ikke sådanne krav, men skal ses i sammenhæng til disse.

Trin 1

Ledelsens værktøjskasse

Et cyberforsvar der virker er forankret i topledelsen. Det handler grundlæggende om, at ledelsen skal styre cyber- og informationssikkerhedsområdet på lige fod med andre områder som for eksempel økonomi, HR, udvikling og forskning. Ligeledes er behandling af personoplysninger blevet et område, som kræver styring fra ledelsen. Uden forankring i topledelsen fejler selv de bedste hensigter om god cybersikkerhed.

Som leder er det vigtigt at forstå cybertruslen. Det er ikke mindst vigtigt at indse, at cybertruslen er et grundvilkår for myndigheder og virksomheder i dagens Danmark. Topledelsen skal tage ejerskab for myndighedens eller virksomhedens målsætninger og strategier på cyber- og informationssikkerhedsområdet. Ledelsens strategier og målsætninger skal udmøntes i politikker, procedurer og retningslinjer. Disse skal anvendes til at styre cyber- og informationssikkerhedsområdet i hele organisationen.

Det er vigtigt, at ledelsen prioriterer etablering af faste processer i organisationen, som understøtter strategien på cyber- og informationssikkerhedsområdet. Uden faste og dokumenterede processer er der en risiko for, at håndtering af cyber- og informationssikkerhedsrisici bliver ad hoc baseret og personafhængigt. Ledelsen skal i den forbindelse sikre, at de etablerede processer løbende kontrolleres og forbedres for at sikre deres effektivitet.

Der er også en særlig vigtig situation i forhold til at højne cyber- og informations-sikkerheden, når myndigheder og virksomheder udvikler og implementerer ny infrastruktur, systemer og applikationer. Derfor skal ledelsen sikre, at der er en fast proces for, at cyber- og informationssikkerhed tænkes ind fra starten af nye projekter.

Generelt skal ledelsen prioritere og støtte cyber- og informationssikkerhedsområdet. Det er i den forbindelse vigtigt, at ledelsen sikrer, at der er adgang til de rette kompetencer. Kompetencerne kan være til stede i egen organisation eller være tilknyttet mere løst som eksterne konsulenter eller rådgivere.

Formulering af målsætninger og strategier, prioritering af ressourcer, etablering af faste processer samt løbende opfølgning, er ledelsens vigtigste værktøjer til at styre cyber- og informationssikkerhedsområdet.

Vi anbefaler, at ledelsen stiller otte spørgsmål til sig selv og seksten til sin organisation. Svarene på spørgsmålene, kan være med til at give ledelsen et indtryk af, hvordan organisationen arbejder med cyber- og informationssikkerhed.

De gode spørgsmål er vigtige værktøjer

Svarene på disse spørgsmål kan være med til at give ledelsen en indikation af, i hvor høj grad myndigheden eller virksomheden har implementeret passende sikkerhedsmæssige tiltag. Inden for begge kategorier skal det være forventningen, at dels ledelsen selv, dels organisation kan svare på spørgsmålene. Rækkefølgen og nummereringen af spørgsmålene er ikke udtryk for en prioritering eller rangordning af de enkelte spørgsmål.

8 spørgsmål topledelsen bør stille til sig selv

1. Ved vi, hvilke data og informationer der understøtter vores forretningskritiske aktiviteter?
2. Hvilke konsekvenser har det for forretningen, hvis data og informationer, der understøtter vores forretningskritiske aktiviteter, ikke er tilgængelige, ændres eller lækkes?
3. Er vi overbevist om, at vores informationer er tilstrækkeligt beskyttet i forhold til kendte trusler?
4. Har vi i topledelsen defineret målsætninger, strategier eller politikker på cyber- og informationssikkerhedsområdet, som vi aktivt prioriterer og støtter?
5. Har vi en sikkerhedsorganisation, der er forankret i topledelsen?
6. Modtager vi løbende rapportering om status på strategier og målsætninger inden for cyber- og informationssikkerhedsområdet?
7. Har topledelsen taget stilling til myndighedens eller virksomhedens risikoappetit?
8. Har vi gjort os klart, at topledelsen selv er et oplagt mål for cyberangreb (eksempelvis CEO-fraud, og spear-phishing)?

16 Spørgsmål topledelsen bør stille til sin organisation

1. Hvilke it-systemer understøtter vores forretningskritiske aktiviteter?
2. Hvor opbevares vores vigtigste data og informationer?
3. Hvordan holder vi os orienteret om cybertruslen og de metoder, som anvendes til blandt andet cyberspionage og cyberkriminalitet?
4. Hvordan beskytter vi os mod cyberangreb, såsom phishing-angreb og CEO-fraud?
5. Skal vi efterleve eksterne krav til cyber- og informationssikkerheden (eksempelvis standarder eller tekniske foranstaltninger)?
6. Hvilke metoder anvender vi for at kontrollere adgang til it-systemer, data og informationer?
7. Hvilke særlige forholdsregler tager vi i forbindelse med rejser?
8. Hvordan sikrer vi, at it-systemer, computere og telefoner er opdaterede?
9. Hvordan sikrer vi, at der anvendes sikre passwords til it-systemer, computere og telefoner?
10. Hvordan kontrollerer vi anvendelse af brugerkonti med privilegerede rettigheder?
11. Har vi adgang til de kompetencer og ressourcer, som er nødvendige for at indfri vores strategier og målsætninger inden for cyber- og informationssikkerhedsområdet?
12. Hvordan uddanner vi vores medarbejdere inden for cyber- og informationssikkerhedsområdet?
13. Opfordrer vi til, at relevante medarbejdere udveksler viden og erfaringer med medarbejdere fra andre organisationer?
14. Hvornår har vi senest testet, at vores beredskab til at styre organisationen igennem en krise virker?
15. Gennemføres der løbende egenkontrol, audits eller revisioner på cyber- og informationssikkerhedsområdet?
16. Hvordan sikrer vi, at vores samarbejdspartnere og leverandører beskytter de data og informationer, som vi deler med dem?

Svarene på spørgsmålene vil være med til at synliggøre for ledelsen, hvis der er områder i organisationen eller hos ledelsen selv, der trænger til at blive prioriteret. Dermed fungerer spørgsmålene som værktøj for ledelsens styringen af cyber- og informationssikkerhedsområdet.

Du kan finde yderligere hjælp til at forstå og besvare ovenstående spørgsmål på sikkerdigital.dk, hvor der samlet vejledninger, skabeloner og lignende materiale, som myndigheder, virksomheder og borgere frit kan anvende.

Trin 2

Teknikken der hjælper os

De rette tekniske tiltag kan markant reducere risikoen for at blive ramt af et cyberangreb. De kan også gøre det nemmere at opdage og håndtere cyberangreb, som er brudt igennem forsvaret. Vi anbefaler, at myndigheder og virksomheder prioriterer implementering af tekniske tiltag højt i arbejdet med cyber- og informationssikkerheden.

Vi har udarbejdet en liste med ti områder, hvor implementering af tekniske tiltag bør prioriteres. De ti områder og tiltag er ikke listet i en prioriteret rækkefølge, men bør alle implementeres som en del af et cyberforsvar der virker.

Nr.	Område og tiltag	Beskrivelse
1	Opdater operativsystemer og applikationer	Alt software, herunder operativsystemer, applikationer og firmware på klienter, mobile enheder, servere, netværksudstyr mv. skal opdateres, når nye versioner eller sikkerhedsopdateringer frigives fra leverandøren. Opdateringen skal følge en fastlagt proces, der sikrer, at eventuelle kompatibilitetsproblemer eller uhensigtsmæssigheder afdækkes, inden opdateringen overføres til produktionsmiljøet. Der skal fastlægges frister for, hvor hurtigt sikkerhedsopdateringer skal idriftsættes efter frigivelse.
2	Segmenter netværk og begræns trafik imellem segmenter	Organisationens interne netværk skal fysisk eller logisk opdeles i netværkssegmenter, således at en enhed (klienter, mobile enheder, servere eller netværksudstyr) kan placeres på et segment i henhold til enhedens anvendelse og sensitivitet. Netværkstrafikken mellem de enkelte netværkssegmenter skal samtidig begrænses til det nødvendige og om muligt beskyttes samt monitoreres.
3	Beskyt klienter med anti-virus og firewall	Alle klienter skal beskyttes med en anti-virus-løsning og en lokalt installeret firewall.
4	Styr brugerkonti og rettigheder	Oprettelse, brug og nedlæggelse af brugerkonti skal ske på baggrund af en ledelsesgodkendt proces. Tildelingen af rettigheder, herunder privilegerede rettigheder, må kun ske på baggrund af arbejdsbetingede behov. Rettighederne skal løbende gennemgås, opdateres og godkendes i forhold til eventuelle ændringer i roller og ansvar. Tildeling af privilegerede rettigheder til klienter, applikationer og systemer må kun ske til konti, der udelukkende anvendes til opgaver, som kræver sådanne rettigheder.

5	Anvend sikre passwords og flerfaktor-autentifikation	Adgangen til enhver konto skal beskyttes ved brug af sikre passwords, og hvis muligt suppleres med flerfaktor-autentifikation. Adgangen til konti, der er tildelt privilegerede rettigheder, skal beskyttes med flerfaktor-autentifikation. Det gælder også konti, der anvendes i forbindelse med ekstern adgang til organisationens systemer.
6	Tag backup af data og konfigurationer, og test reetablering	Der skal tages backup af data fra forretningskritiske it-systemer. Backup skal foretages i overensstemmelse med en politik på området, der tager hensyn til konsekvensen for organisationen, hvis data i produktionsmiljøet går tabt. Konfigurationer og systemer, der er nødvendige for retablering efter et en større sikkerhedshændelse, skal ligeledes inkluderes i backup. Det bør regelmæssigt testes, at backupindholdet er komplet, og at data og konfigurationer kan indlæses fra backup. En kopi skal opbevares offline.
7	Etabler logning af ændringer og sikkerhedshændelser	Der skal etableres logning af adgang til vigtige systemer, herunder succesfulde og fejlede login forsøg. Logning af konfigurationsændringer og adgang til sensitive data eller systemer skal også logges. Logs skal opbevares separat med begrænset adgang og gennemses regelmæssigt. Logs skal opbevares i en tilstrækkelig periode.
8	Beskyt fjernadgang til systemer	Fjernadgang til organisationens systemer skal beskyttes med flerfaktor-autentifikation. Kommunikationens integritet skal beskyttes med kryptering, f.eks. ved anvendelse af HTTPS eller en VPN-tjeneste.
9	Krypter data på klienter og mobile enheder samt kommunikationen over andre netværk	Data på klienter og specielt på bærbare klienter, der anvendes uden for organisationens område, skal beskyttes med fuld disk kryptering. Data på mobile enheder skal ligeledes beskyttes med kryptering, og evt. administreres i en MDM (Mobil Device Management) platform, der også giver mulighed for fjernsletning. Al kommunikation med organisationens systemer over andre netværk udenfor organisationens kontrol skal krypteres.
10	Udarbejd en positivliste over applikationer (whitelisting)	Installation og afvikling af applikationer på organisationens klienter skal begrænses til de forhåndsgodkendte.

Det vil typisk være en it-afdeling eller eksterne konsulenter, der er udførende i forhold til at implementere de tekniske tiltag i it-miljøet. Det er vigtigt, at it-afdelingen eller de eksterne konsulenter arbejder systematisk med implementering og løbende vedligeholdelse af de tekniske tiltag. Vi anbefaler, at standarder og best practice følges. Det kan eksempelvis være ITIL og CIS 18 til at sikre en systematisk implementering, dokumentation og løbende vedligeholdelse.

For myndigheder og virksomheder, der i høj grad har outsourcet it-afdelingen, er det nødvendigt at kontrollere, at leverandøren implementerer de tekniske tiltag. Vi anbefaler, at der stilles krav om løbende rapportering fra leverandøren. Dels i forhold til myndighedens eller virksomhedens it-miljø og dels i forhold til leverandørens eget it-miljø. En svaghed i leverandørens eget it-miljø vil kunne skade myndigheden eller virksomheden. Vi har udgivet en vejledning om sikkerhed i leverandørforhold, der beskriver nogle af problemstillingerne, som bør håndteres i forbindelse med anvendelse af it-leverandører (CFCS & DIGST, *Cybersikkerhed i leverandørforhold*, 2022). Hvis der er tale om cloud-sourcing henviser vi til vores vejledning om anvendelse af cloud (CFCS & DIGST, *Vejledning i anvendelse af cloudservices*, 2020).

Teknikken skal udgøre et stærkt bolværk mod cyberangreb – det er med andre ord teknikken, der hjælper os. Teknikken kan dog ikke stå alene. Medarbejdernes adfærd skal udgøre et ligeså stærkt bolværk mod cyberangreb som teknikken.

Implementering af selv basale tekniske tiltag kræver de rette tekniske kompetencer. Derfor er det vigtigt, at der er nogen i organisationen, der forstår og kan implementere tiltagene. Hvis dette ikke er tilfældet, så er det ledelsens ansvar at prioritere og sikre, at kompetencerne kan tilgås eksempelvis hos eksterne konsulenter og rådgivere.

Trin 3

Det handler om adfærd

Medarbejdernes adfærd og kompetencer indgår som en aktiv og væsentlig del af et cyberforsvar der virker. Internationale undersøgelser anslår, at størstedelen af alle hackerangreb og informationssikkerhedsbrud skyldes menneskelige fejl[1].

De fleste medarbejdere ansættes ikke ud fra deres viden om cyber- og informations-sikkerhed, men på grund af deres kompetencer inden for myndighedens eller virksomhedens kerneforretning. Det kræver meget af den enkelte at ændre adfærd og vaner. Især inden for et område der ligger uden for deres primære funktion.

Dette bør der tages højde for i arbejdet med at opbygge en god sikkerhedskultur for organisationen.

Fem essentielle faser til at skabe en god sikkerhedskultur
Vi anbefaler, at topledelsen i myndigheden eller virksomheden efterspørger og igangsætter disse aktiviteter med henblik på at skabe den ønskede adfærd på sikkerhedsområdet:

Det er vigtigt, at myndigheden eller virksomheden har kendskab til, hvilke adfærdsudfordringer de har på sikkerhedsområdet, og arbejder med dem adfærdsvidenskabeligt.

Karakteren af den konkrete adfærdsindsats, der skal gennemføres, afhænger selvfølgelig af det identificerede problem hos målgruppen. Plakater, nyhedsbreve og informationsmøder kan være en god start til at opnå kendskab til emnet, men de er sjældent adfærdsændrende i sig selv. For at opnå en varig adfærdsændring skal indsatsen derfor sigte efter at håndtere de identificerede adfærdsproblemer med specifikke adfærdsgreb. Et identificeret adfærdsproblem kunne f.eks. være ”vedholdenhed”. Det vil sige, at målgruppen har udfordringer med at fastholde de sikkerhedsmæssigt ønskede valg over tid på grund af manglende motivation, eller fordi den ønskede adfærd er i konflikt med andre ønsker. Et adfærdsgreb kunne i denne sammenhæng være at formindske barrierer ved f.eks. at reducere antal klik man skal foretage for at træffe de gode sikkerhedsvalg. Det kunne også være at indføre systematisk feedback, når gode sikkerhedsvalg træffes – f.eks. real-time feedback ved indrapportering af phishing-mails.

[1] https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/

God sikkerhedsadfærd handler ikke om, hvad medarbejderne ved, men om hvad de gør.

Det er vigtigt, at adfærdsindsatsen bygger på et solidt analysearbejde, som diagnosticerer årsagerne til adfærdsproblemet. Ellers vil man sjældent lykkes med en adfærdsindsats. Derudover er det afgørende, at organisationen sørger for at teste adfærdsindsatsen, inden den gennemføres i fuld skala. Formålet her er også at identificere eventuelle sideeffekter. Når man intervenerer i menneskers adfærd, bør etiske overvejelser være en del af udarbejdelsen af indsatsen. Her kan organisationen eventuelt lade sig inspirere af "Kodeks for gennemførelse af sikkerhedstests", som kan findes på digst.dk.

Endelig er det selvfølgelig vigtigt, at organisationen sørger for at evaluere og følge op på adfærdsindsatsen, så der kan bygges videre, og så arbejdet med en god sikkerhedskultur bliver et kontinuerligt og tilbagevendende arbejde (CFCS & DIGST, *Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed,* 2021).

Trin 4

Opdag fjenden

For at kunne opdage cyberangreb kræves det, at myndigheder og virksomheder aktivt anvender monitorering til at opdage afvigelser fra normalbilledet eller andre tegn på potentielle cyberangreb. Monitorering er en væsentlig del af et cyberforsvar der virker. Derfor handler dette trin primært om, hvilke politikker, processer og procedurer der skal være på plads for at kunne opdage et cyberangreb.

Monitorering

For at kunne anvende monitorering til at opdage cyberangreb kræver det, at myndigheder og virksomheder har identificeret de it-aktiver, som er kritiske for kerneforretningen (forretningskritiske aktiver).

For det første skal det sikres, at de forretningskritiske it-aktiver monitoreres, og at det er de rette aspekter (parametre), der monitoreres på. Monitorering bør som udgangspunkt ske på alle niveauer lige fra netværkslaget til applikationslaget og på organisationens it-enheder. Vær omhyggelig med at finde de rette aspekter at monitorere på, da eksempelvis monitorering af krypteret trafik ikke nødvendigvis er informativt. Bemærk at sikkerheds-monitorering ofte dækker andre aspekter end den typiske driftsmonitorering af it-løsninger.

Dernæst skal det sikres, at der er opsat "alarmer", som aktiveres hvis der observeres hændelser, der afviger fra normalbilledet, ligner kendte angrebsmønstre eller ligger uden for nogle fastlagte grænseværdier. Det kan eksempelvis være mange afviste logins som følge af forkert afgivne passwords. I den sammenhæng skal man være indstillet på, at man særligt indledningsvis vil få en række falske alarmer, som følge af at registrerede afvigelser rent faktisk høre til normalbilledet.

Monitoreringen kan foretages af myndigheden eller virksomheden selv – men det kræver særlige kompetencer. Derfor anbefaler vi, at monitorering outsources såfremt disse kompetencer ikke er tilstede i organisationen.

Undersøgelser af mulige hændelser

Af hensyn til afdækning af mulige hændelsesforløb skal myndigheden eller virksomheden tage stilling til, hvordan data fra monitoreringen indgår i organisationens samlede logning. Vi anbefaler, at relevant monitoreringsdata samt logning fra relevante netværksenheder med videre indsamles og behandles centralt. Det kan både ske internt hos myndigheden eller eksternt ved at købe ydelserne hos en leverandør. Læs mere om, hvilken type af logning der kan være nødvendig i forbindelse med undersøgelser af mulige hændelser, i CFCS' vejledning "Logning – en del af et godt cyberforsvar (2023)".

Situationscenteret i CFCS består af en døgnbemandet vagt, som kan kontaktes i forbindelse med it-sikkerhedshændelser.[2]

[2] https://www.cfcs.dk/da/om-os/netsikkerhedstjenesten/situationscenter/

Trin 5

Vær beredt!

Uanset hvor mange tekniske og organisatoriske tiltag, der er implementeret, og uagtet hvor godt et uddannelsesprogram der kører, så er det kun et spørgsmål om tid, før jeres myndighed eller virksomhed rammes af et cyberangreb.

Det vigtige er derfor at være godt forberedt på, hvad der skal gøres i en situation, hvor et cyberangreb rammer og lammer dele af organisation. Det gælder også, hvis cyberangrebet rammer en leverandør eller samarbejdspartner.

I forhold til alvorlige cyberhændelser, der ikke kan håndteres inden for rammerne af den normale drift, er det først og fremmest vigtigt, at myndigheder og virksomheder ved, hvornår og hvordan de indkalder deres kriseberedskab. Beredskabets primære formål er at sikre håndteringen af den pågældende krise og genetablere en normal drift så hurtigt og effektivt, som muligt. En forudsætning herfor er, at de rigtige medarbejdere med de rigtige kompetencer er medlemmer af krisestaben. Vi anbefaler, at der tilknyttes eksterne medlemmer såfremt myndigheden eller virksomheden ikke selv råder over de nødvendige kompetencer.

I en krise er det vigtigt, at myndigheder og virksomheder tænker på krisehåndtering bredt. Således vil en krise på baggrund af en cyberhændelse medføre krisestyring inden for IT, kommunikation og forretning.

Et effektivt kriseberedskab kræver en operationel beredskabsplan, der er ajourført, afprøvet og ledelsesgodkendt. Vi anbefaler, at beredskabsplanen bygges op omkring fem faser.

Aktivering
Myndigheder og virksomheder skal fastlægge hvilke specifikke kriterier, der medfører, at kriseberedskabet aktiveres. Det skal også fastlægges, hvem i organisationen der har mandat til at aktivere og indkalde kriseberedskabet.

Myndigheder og virksomheder kan med fordel bygge bro mellem beredskabsplanen og eksisterende processer for it-hændelseshåndtering. Der vil ofte være en kategori af it-hændelser, der hedder ”major incident” eller ”alvorlig hændelse”. Det er ved alvorlige it-hændelser, som falder inden for de fastlagte kriterier, at myndigheder og virksomheder bør overveje om kriseberedskabet skal aktiveres.

Mobilisering
Når kriseberedskabet er aktiveret skal medlemmerne af krisestaben mobiliseres. Beredskabsplanen skal indeholde en beskrivelse af, hvordan krisestaben mobiliseres

og samles. Det skal derfor være angivet forholdsvis detaljeret, hvordan medlemmer af krisestaben kontaktes og af hvem, hvor hurtigt de skal mødes og hvor de mødes. Det kan overvejes, om krisestaben skal mødes fysisk eller virtuelt. Hvis krisestaben mødes fysisk, skal adresse, lokale og evt. adgangsforhold være kommunikeret tydeligt til medlemmerne af krisestaben.

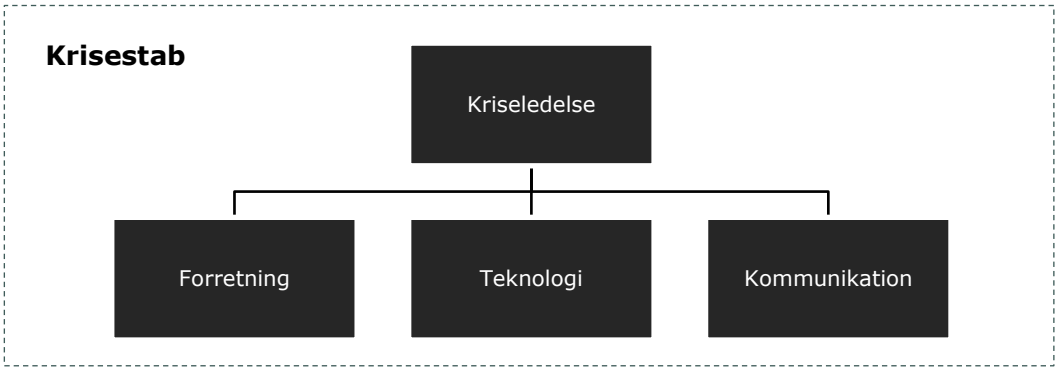
Digitaliseringsstyrelsen har udarbejdet en skabelon til en miniberedskabsplan, som den enkelte organisation kan udfylde og anvende. Den kan benyttes af medlemmer af krisestaben til hurtigt at orientere sig i f.eks. kontakt-informationer, mødested og første skridt i forbindelse med en hændelse.

Skabelon til miniberedskabsplanen kan findes på **sikkerdigital.dk**

For nogle myndigheder og virksomheder kan det være relevant at udpege en sekundær lokalitet, hvor krisestaben kan mødes. Som udgangspunkt anbefaler vi, at krisestaben mødes på myndighedens eller virksomhedens normale lokaliteter. Vælges i stedet et virtuelt møde, skal platformen, hvad enten det er video-opkald eller et chat-forum, være aftalt på forhånd og let tilgængelig for medlemmerne af krisestaben. Læs mere om, hvordan der arbejdes sikkert på virtuelle mødeplatforme i CFCS' vejledning "Råd om sikkerhed på virtuelle mødeplatforme", som kan findes på cfcs.dk.

Organisering
Krisestaben skal sammensættes af relevante repræsentanter fra forskellige dele af myndigheden eller virksomheden. Krisestaben skal kunne bruge ekstraordinære ressourcer og træffe beslutninger, som kan påvirke myndigheden og virksomheden væsentligt. Derfor skal repræsentanterne i kriseledelsen have beslutningsmandat, herunder mulighed for at disponere over økonomiske og personalemæssige ressourcer.

Organisationsdiagrammet for en krisestab afhænger af myndighedens eller virksomhedens organisering, men der kan tages udgangspunkt i følgende model:

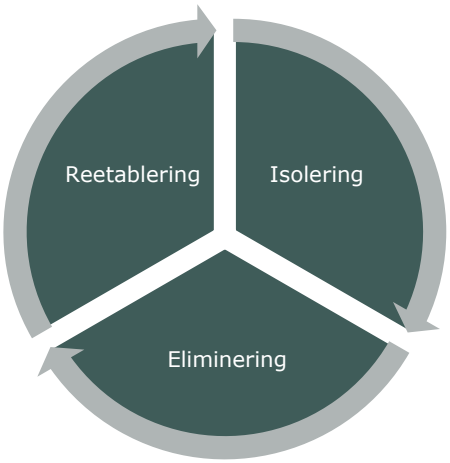


Det er væsentligt, at undergrupperne bemandes med medarbejdere, der har et indgående kendskab til de respektive undergruppers områder. Vi anbefaler, at der inddrages medarbejdere fra leverandører og samarbejdspartnere, som indgår i driften og kritiske forretningsområder, der er berørt af krisen.

Husk at en krise kan tage lang tid. Derfor er det vigtigt at tænke noget så banalt som forplejning, rengøring mv. ind i organiseringen.

Håndtering
Når krisestaben er samlet, skal den sikre, at de relevante stabsfunktioner er tilstede, og rollerne er fordelt. Herefter aftales en fast kadence og dagsorden for krisestabens møder. Formålet med møderne er at danne sig et situationsoverblik og at træffe passende beslutninger for at håndtere krisen hurtigst muligt.

Der bør løbende skrives og fordeles resumeer af møderne, så krisestaben ikke er i tvivl om opgavefordelingen frem til næste møde.



■ Vi anbefaler, at kriseberedskabet følger denne cyklus i krisehåndteringsfasen. Først afgrænses og isoleres årsagen til drifts-forstyrrelsen. Dernæst fjernes og elimineres årsagen. Endelig igangsættes reetableringen af de berørte systemer og netværk. Denne fremgang gentages og kan skaleres på system- og netværksniveau efter behov.

I denne fase er det væsentligt, at der er adgang til tilstrækkelige logs. Disse skal anvendes til at undersøge, i hvilket omfang organisationens it-aktiver er ramt af angrebet. Det er også væsentligt, at det er muligt at genetablere relevante opsætninger og data ved hjælp af backup. Undersøgelse af logs og monitorering bidrager til at identificere, hvor langt tilbage i tid der skal genetableres fra for at undgå kompromitteringen. Vi anbefaler, at myndigheder og virksomheder, der ikke selv råder over kompetencer inden for såkaldt forensics og remediering, tilknytter eksterne konsulenter, som kan løse opgaven.

Afslutning
Når der er foretaget en effektiv isolering, eliminering og reetablering, skal beredskabet afsluttes, og normal drift genindføres. Inden krisestaben opløses og kan erklære krisen for løst, bør følgende bekræftes:

- At reetableringen af it-systemer er gennemført, eller at der er en tydelig tidsplan for, hvornår den er gennemført.
- At relevant dokumentation fra krisehåndteringen, både fra undergrupper og krisestaben, er sikret, og at der er aftalt en plan for udarbejdelse af kriserapporten.
- At krisekommunikationen til interne og eksterne interessenter er afsluttet

Endelig bør krisestaben aftale et opfølgningsmøde, hvor kriserapporten gennemgås. Relevante læringspunkter bør afstedkomme konkrete handlinger, som f.eks. ændringer i eksisterende forretningsprocesser, iværksættelse af træningsforløb eller revidering af risikovurderinger og reducerende sikringstiltag.

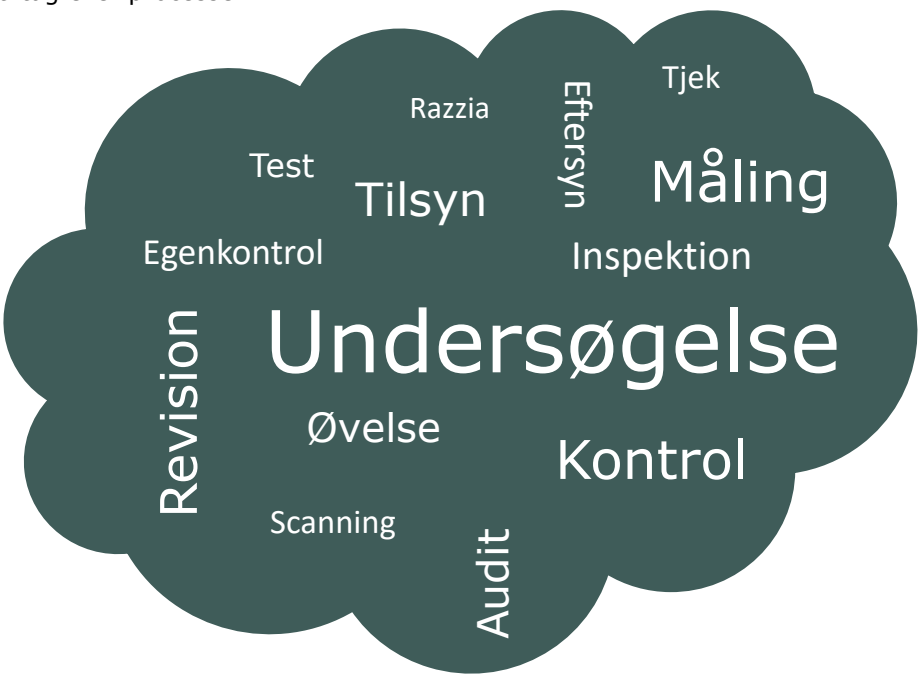
Trin 6

Find huller i cyberforsvaret

Cyber- og informationssikkerhedsområdet udvikler sig med stor hast. Det gælder derfor om hele tiden at lede efter hullerne i cyberforsvaret. De sikkerhedstiltag en myndighed eller virksomhed implementerede i går eller i dag er muligvis ikke tilstrækkelige i morgen.

Et vigtigt element i et cyberforsvar der virker er derfor, at der løbende gennemføres undersøgelser af de eksisterende sikkerhedstiltag, der er implementeret af myndigheden eller virksomheden.

Vi anbefaler, at der løbende gennemføres undersøgelser for at vurdere om de tiltag og processer, der er implementeret, har den ønskede effekt, samt om der er behov for nye tiltag eller processer.



Forskellige typer af undersøgelser
Afhængig af, hvilket område der skal undersøges, vil der være forskellige metoder til at finde hullerne. Eksempelvis vil der inden for teknologiområdet kunne gennemføres sårbarhedsscanninger og såkaldte pentests. Undersøgelser af organisationen og processer vil typisk have karakter af egenkontrol, audit eller revision. Undersøgelser om adfærd typisk vil have karakter af målinger eller tests – eksempelvis en phishing-test. Nogle typer af undersøgelser, som eksempelvis egenkontrol, eftersyn, tjek og interne audits vil myndigheder og virksomheder i vid udstrækning selv kunne gennemføre. Andre typer af undersøgelser vil kræve assistance fra eksterne – eksempelvis certificerede auditører, revisorer, it-eksperter og lignende. Inden for de mere tekniske undersøgelser, bør der løbende foretages scanninger af de væsentlige it-aktiver for at konstatere om der er kendte sårbarheder – såkaldte CVE'er (Common Vulnerabilities and Exposures).

Der eksisterer en række tilgængelige værktøjer, som kan anvendes til at foretage såkaldte sårbarhedsscanninger. Gennemførelse af sådanne scanninger kræver dog særlige kompetencer. Derfor anbefaler vi, at sårbarhedsscanninger outsources såfremt disse kompetencer ikke er tilstede in-house.

Myndigheder og virksomheder kan også overveje at få gennemført såkaldte penetrationstest. Det er tests, hvor udefrakommende forsøger at bryde ind i myndighedens eller virksomhedens netværk, enheder, systemer og applikationer, som en kriminel eller spion ville gøre det. I den forbindelse gælder det samme i forhold til kompetencer som i tilfældet med sårbarhedsscanninger.

Topledelsen i myndigheder og virksomheder skal prioritere ressourcer til løbende at gennemføre undersøgelser på cyber- og informationssikkerhedsområdet. Det indbefatter, at de rette kompetencer er tilstede internt eller tilgængelig via eksterne konsulenter og samarbejdspartnere.

Uanset hvilken undersøgelse en myndighed eller virksomhed gennemfører, er det centrale måden, hvorpå resultatet af undersøgelsen anvendes.

Det er vigtigt, at ledelsen efterspørger resultater fra undersøgelser om, hvor effektive etablerede sikkerhedstiltag og processer er. Det kan eksempelvis gøres ved, at undersøgelser om cyber- og informationssikkerheden behandles på direktions- eller bestyrelsesmøder på lige fod med undersøgelser om økonomi, forskning og udvikling mv.

Anvendelse af undersøgelsesresultater
Resultaterne skal anvendes til at udarbejde en prioriteret plan for, hvordan hullerne minimeres. I den forbindelse er det væsentligt, at planen i sidste ende godkendes af topledelsen. Ligesom på andre forretningsområder vil der være tale om en prioritering af planens forskellige elementer i overensstemmelse med myndighedens eller virksomheden risikoappetit.

Nogle myndigheder og virksomheder har oprettet en dedikeret sikkerhedsorganisation, hvor topledelsen er repræsenteret. Hos andre er det den almindelige topledelse (direktionen), der behandler denne slags sager. Grunden, til at topledelsen skal involveres i prioriteringen, er, at de skal styre og prioritere cyber- og informations-sikkerheden i myndigheden eller virksomheden i overensstemmelse deres risikoappetit.

Løbende og systematiske undersøgelser, hvad enten der er tale om egenkontrol, audits, tests eller revisioner, er et af de vigtigste redskaber til at styre cyber- og informationssikkerheden hos myndigheder og virksomheder – og dermed til et cyberforsvar der virker.

Litteraturliste

- Australian Cyber Security Center (AU). (2023). *Essential Eight Explained*. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained
- Canadian Centre for Cyber Security (CA). (2021). *Top 10 IT Security Actions to Protect Internet Connected Networks and Information.* *https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089*
- Center for Internet Security. (2021). *CIS Controls V8.* *https://www.cisecurity.org/controls/v8_pre*
- Infosecurity Magazine. (tilgået 2021). *90% of UK Data Breaches Due to Human Error in 2019.* *https://www.infosecurity-magazine.com/news/90-data-breaches-human-error/*
- National Cyber Security Center (UK). (2021). *10 steps to Cyber Security.* *https://www.ncsc.gov.uk/collection/10-steps*
- National Cyber Security Center (UK). (2023). *Board Toolkit v2.* *https://www.ncsc.gov.uk/collection/board-toolkit*
- National Security Agency (US). (2018). *NSA'S Top Ten Cybersecurity Mitigation Strategies*. *https://www.nsa.gov/portals/75/documents/what-we-do/cybersecurity/professional-resources/csi-nsas-top10-cybersecurity-mitigation-strategies.pdf*
- Nasjonal sikkerhetsmyndighet (NO). (2022). *Fem effektive tiltak mot dataangrep.* *https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/5tiltak*
- OECD. (2019). *Tools and Ethics for Applied Behavioural Insights: The BASIC Toolkit.* *https://www.oecd.org/regreform/tools-and-ethics-for-applied-behavioural-insights-the-basic-toolkit-9ea76a8f-en.htm*

Vejledninger til yderligere inspiration

- Bestyrelsesforeningen. (2021). *Cybersikkerhed for bestyrelser.* https://bestyrelsesforeningen.dk/vejledninger-og-anbefalinger/
- Center for Cybersikkerhed. (2023). *Cybertruslen mod Danmark.* https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/cybertruslen-mod-danmark/
- Center for Cybersikkerhed. (2021). *Råd om sikkerhed på virtuelle mødeplatforme.* https://www.cfcs.dk/da/forebyggelse/vejledninger/distancearbejde/rad-om-sikkerhed-pa-virtuelle-modeplatforme/Digitaliseringsstyrelsen og Center for *
- Center for Cybersikkerhed. (2021). *Metode til at arbejde med adfærdsindsatser inden for cyber- og informationssikkerhed.* https://www.cfcs.dk/da/forebyggelse/vejledninger/vejledning-metode-til-at-arbejde-med-adfardsindsatser/
- Center for Cybersikkerhed, Digitaliseringsstyrelsen, KL m.fl. (2021). *Kodeks for gennemførelse af sikkerhedstests.* https://digst.dk/media/23689/kodeks_for_sikkerhedstest_2021_digst.pdf
- Center for Cybersikkerhed. (2023). *Logning – en del af et godt cyberforsvar.* https://www.cfcs.dk/da/forebyggelse/vejledninger/logning/
- Center for Cybersikkerhed. (2022). *Phishing – beskyt organisationen mod phishingangreb.* https://www.cfcs.dk/da/forebyggelse/vejledninger/phishing/
- Center for Cybersikkerhed og Digitaliseringsstyrelsen. (2022). *Cybersikkerhed i leverandørforhold.* https://www.cfcs.dk/da/forebyggelse/vejledninger/informationssikkerhed-i-leverandorforhold/
- Center for Cybersikkerhed. (2022). *Reducer risikoen for falske mails.* https://www.cfcs.dk/da/forebyggelse/vejledninger/reducer-risikoen-for-falske-mails/
- Digitaliseringsstyrelsen og Center for Cybersikkerhed. (2020). *Vejledning i anvendelse af cloudservices.* https://digst.dk/data/vejledning-til-anvendelse-af-cloudservices/
- Digitaliseringsstyrelsen. (2019). *Miniberedskabsplan.* https://sikkerdigital.dk/myndighed/iso-27001-implementering/beredskabsstyring/implementering