Cybersikkerhed for ledelsen

10 essentielle spørgsmål om Cybersikkerhed, som virksomhedsledelsen bør stille sig selv.

Christian Schmidt
CEO Dediko A/S, chr@dediko.dk

INDHOLD

#1 Hvor stor er risikoen for, at virksomheden bliver offer for et Cyberangreb?.....2

#2 Hvad er konsekvensen af et Cyberangreb mod virksomheden? 3

#3 Hvem ejer risikoen for at undgå, at virksomheden bliver offer for et Cyberangreb? 4

#4 Hvad gør andre virksomheder for at håndtere risikoen for et Cyberangreb?.....5

#5 Hvad koster det at beskytte virksomheden mod et Cyberangreb?.....6

#6 Hvor sikre er vi (A), hvor sikre skal vi være (B) og hvordan kommer vi fra A til B?.....7

#7 Hvad er forskellen på Informationssikkerhed, IT-Sikkerhed og Cybersikkerhed? 8

#8 Kan ISO27001, IT-Revision, 3402 erklæringer og GDPR compliance bruges til at forhindre et Cyberangreb?.....9

#9 Tildeler bestyrelsen de ressourcer, der er nødvendige for at mitigere risikoen for et Cyberangreb? 10

#10 Hvordan skaber vi et effektivt Cybersikkerhedsprogram med effektiv Cyberkommunikation i virksomheden? 11

FAQ vedr. ledelseskommunikation af Cybersikkerhed. 12

#1 Hvor stor er risikoen for, at virksomheden bliver offer for et Cyberangreb?

En dansk undersøgelse* pegede i 2021 på, at risikoen for et Cyberangreb lå på 56%, mens en ny international undersøgelse** fra 2022 peger på, at risikoen for et Cyberangreb er 87% over en periode på 3 år og at antallet af angreb er stigende***. Center for Cybersikkerhed har de seneste 3 år angivet Cyberkriminalitet som en af de største trusler mod Danmark og 78% af virksomhedsledere anser nu organiserede Cyberkriminelle som den største Cybertrussel mod virksomheden.

Der er baggrund for at konkludere, at der er en overvældende sandsynlighed for, at din virksomhed bliver ramt af et Cyberangreb i den nærmeste fremtid. Det kan virksomheden dog arbejde aktivt med at håndtere ved at nedsætte sandsynligheden for og konsekvensen af at blive offer for et succesfuldt Cyberangreb.

Eksempler på danske virksomheder der har været i medierne i forbindelse med, at de er blevet ofrer for Cyberangreb: NRGi, Mærsk, ISS, Demant, Vestas, Würth, AK Techotel, Bauhaus, Coop, Nationalbanken, SAS, Dansk Energi, Kompan A/S, Illum, Jobnet.dk, Nybolig, Estate mæglerne. Før 2021: Forsvarsministeriet, Skat, Nets, Desmi, Ritzau.

> **Tiltag**: Bl.a. anti-spam, anti-phishing, webfilter, rettigheder, flerfaktorgodkendelse, sårbarheder, anti-malware, awarenesstræning, backup og Incident response.

*PwC Cyber Crime Report 2021 & 2022
**Anomali Cybersecurity Insights report 2022
***Checkpoint Software 2022 Security Report

#2 Hvad er konsekvensen af et Cyberangreb mod virksomheden?

Et succesfuldt Cyberangreb vil ofte føre til flere af følgende begivenheder som i særlig grad bekymrer ledelsen*:

A. Nedsat produktivitet

B. Produktionsstop

C. Tab af sensitive data
(herunder immaterielle rettigheder og persondata)

D. Tab af omdømme

E. Negativt påvirket aktiekurs over længere tid, udskiftninger i ledelsen, ødelagt digital infrastruktur og store omkostninger til eksterne konsulenter, der skal redde virksomheden samt betaling af store løsesummer og evt. bøder.

Regningen kan løbe op i mange millioner kroner og for nogle virksomheder vil det være en eksistenstruende begivenhed.

> **Tiltag**: Bl.a. regelmæssig backup, test gendannelse aktivt og målrettet og sikr den mod ransomware, hav et godt gennemprøvet beredskab, gennemfør pen-tests og trykprøvninger af organisationens Cyberforsvar.

*PwC Cyber Crime Report 2022

#3 Hvem ejer risikoen for at undgå, at virksomheden bliver offer for et Cyberangreb?

Det er virksomhedens ejere, ledelse og bestyrelse, der burde eje det fulde ansvar! Men i mange organisationer er det ikke (helt) tilfældet, hvorfor det de fakto er de udførende afdelinger som fx IT-afdelingen, der i praksis ejer ansvaret. Men IT-afdelingen kan og skal aldrig eje ansvaret, fordi der efter al sandsynlighed ikke er det fornødne overblik, den nødvendige indsigt og tilstrækkelige ressourcer i IT-afdelingen til at mitigere Cyberrisikoen for hele virksomheden.

Dette faktum er den grundlæggende årsag til, at mange virksomheder har et utilstrækkeligt Cyberforsvar og Cyberparathed, hvilket øger sandsynligheden for et succesfuldt Cyberangreb.

> **Tiltag**: Brug Dediko's modenhedsmodel for Ledelsen og Bestyrelsen til at vurdere, om dette er et problem i din virksomhed. Hvis det viser sig at være tilfældet, kan vi hjælpe dig aktivt på vej til at løse denne udfordring.

#4 Hvad gør andre virksomheder for at håndtere risikoen for et Cyberangreb?

Meget tyder på, at mange virksomheder stadig har for utilstrækkelig en Cybersikkerhed og derfor skal man passe på med, hvilke andre virksomheder man sammenligner sig med! De virksomheder, der har succes med at håndtere risikoen for Cyberangreb, gør bl.a. følgende:

A) De forankrer Cyberrisikoen i ledelsen.

B) Gør Cybersikkerheden målbar.

C) Implementerer en flerårig Cybersikkerhedsprogram.

D) Outsourcer de Cyberdiscipliner som virksomheden ikke selv kan håndtere.

E) Sørger for at kommunikere Cybersikkerheden til/fra ledelsen og resten af organisationen.

F) Lærer af de hændelser som virksomheden udsættes for.

> **Tiltag**: Brug Dediko's modenhedsmodel for Cyberprogrammet til at vurdere, om dette er håndteret professionelt i din virksomhed. Se vores YouTube video om GAP analyse på https://youtu.be/hTJPuIzv3lU

#5 Hvad koster det at beskytte virksomheden mod et Cyberangreb?

Omkostningerne ved Cyberangreb afhænger af mange faktorer**, som fx hvor godt du er forberedt på et angreb, hvor hurtigt du opdager du et Cyberangreb, virksomhedens Cyberforsvar af cloud systemer (!) og hvad du er ramt af som fx ransomware. Angreb med ransomware opdages i gennemsnit i løbet af 4-5 dage mens andre typer af angreb i Europe har en "dwell time" på 48 dage i gennemsnit (tal fra 2023 – Mandiant M-trends og Verizon DBIR).

Et større angreb mod en mellemstor dansk virksomhed kan nemt koste 10-20 millioner kroner (eller mere) plus tabt fortjeneste ved et længere produktionsstop. Dertil kommer et milliontab pga. en faldende aktiekurs, tabt salg og kundeflugt som følge af tabt omdømme. Den forlangte løsesum ved et ransomware angreb er steget mere end 500%* over de seneste 3 år og er som udgangspunkt på mange millioner kroner. I 2023 tyder tal på at den gennemsnitligt forlangte løsesum er 16 millioner DKK mens den udbetalte løsesum er 5 millioner DKK og mere end 50% er nødsaget til at betale.

Gennemsnitsomkostningen ved et Cyberangreb med tab af mange sensitive data er i Skandinavien** 18 millioner kroner og på verdensplan i gennemsnit 30 millioner kroner. De tilsvarende tiltag, der skal beskytte virksomheden mod Cyberangreb, består normalt af dedikerede medarbejdere, de rette kompetencer, processer og kontroller samt software og hardware

Vores **CIS GAP Analyse** afslører ofte en teknologisk gæld, der for mindre virksomheder kan være fra ca. ½ til 1 million kroner og for større virksomheder normalt ligger på 5-10 millioner kroner. For meget store virksomheder er dette beløb væsentligt højere, men deres teknologiske gæld er ofte mindre. Du kan se vores Cybersikkerhedsanalyse på Youtube (17 minutter).

> **Tiltag**: Se vores video om omkostningerne ved et Cyberangreb og implementer et robust og målbart Cyberforsvar, der passer til trusselsbilledet for din virksomhed. Er du i tvivl om hvordan du gør det i praksis, kan vi hjælpe med at give dig et godt overblik.

* Unit 42 Ransomware Report 2022
** IBM The Cost of a Data Breach 2023

#6 Hvor sikre er vi (A), hvor sikre skal vi være (B) og hvordan kommer vi fra A til B?

Kan du ikke svare på de helt grundlæggende spørgsmål, der er forbundet med Cybersikkerhed, bliver det meget svært at nå et passende niveau af sikkerhed, som ikke er baseret på et gæt. Derfor skal Cybersikkerhed gribes meget metodisk an, hvor en Cybersikkerheds GAP Analyse typisk baseret på CIS kontrollerne bliver virksomhedens pragmatiske og praktiske navigation og søkort samlet i Cybersikkerhedsprogrammet. Det handler ikke om at blive eller være perfekt (100% sikkerhed), men at nedsætte risikoen til et acceptabelt niveau (”Den accepterede Cyberrisiko”).

> **Tiltag**: Få gennemført Dediko’s CIS baserede GAP analyse som i detaljer giver en målbar plan for at komme frem til den accepterede Cyberrisiko. Analysen tager typisk 5-10 dage og går i dybden med målbarheden, modenheden samt behovet for processer, kontroller, kompetencer, medarbejdere
> og software til at automatisere Cybersikkerhedsprogrammet og gøre det robust. Se YouTube video.
>
> Du får et fuldstændigt indblik i hvor lang tid det vil tage at komme i mål samt et detaljeret overblik over, hvad det vil koste i ressourcer. Undgå at vælge en Cybersikkerheds GAP Analyse hvis resultat præsenteres i en ”200 siders rapport” uden klare, prioriterede praktiske tiltag. Den kan være nok så teknisk korrekt, men hvad skal du bruge den til?

#7 Hvad er forskellen på Informationssikkerhed, IT-Sikkerhed og Cybersikkerhed?

Informationssikkerhed er en overordnet betegnelse, som ofte har et væsentligt element af compliance fx med ISO27001. En stor del af Informationssikkerheden kan karakteriseres som IT-Sikkerhed, som har både fysiske og virtuelle elementer og som ofte er systemspecifikt. Som en del af IT-Sikkerheden finder du den digitale Cybersikkerhed, der dækker Cyberkriminelle og insider trusler

Det giver således ingen mening at sige, at "vi interesserer os ikke for it-sikkerhed eller Cybersikkerhed, men kun Informationssikkerhed". Hvis du anlægger en synsvinkel fokuseret på rammeværk, udgør CIS version 7.1 kontrollerne (Cybersikkerhed) 66 ud af de 114 kontroller i ISO27001 hvilket svarer til 58%. Altså udgør CIS Cybersikkerheds kontrollerne mere en ½ af alle Annex A kontroller i ISO27001. Den "nye" CIS 18 indeholder 154 subkontroller og er koblet ISO27002:2022.

Se https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-iso-iec2-27002-2022.

> **Tiltag**: Vær sikker på at du ikke (kun) bekæmper Cybertruslen med politikker, hensigter, formodninger og "Word dokumenter". Vælg en praktisk og pragmatisk funderet ramme som fx Center for Internet Security's (CIS) 20/18 kritiske kontroller. Dediko's **Cybersikkerheds GAP analyse** bruger netop denne metodik. Se YouTube video.

#8 Kan ISO27001, IT-Revision, 3402 erklæringer og GDPR compliance bruges til at forhindre et Cyberangreb?

Det er højest usandsynligt at compliance relaterede tiltag og IT-revisionserklæringer i praksis kan bruges som effektive våben mod cyberkriminalitet og hackerangreb. Det kræver væsentligt dybere og mere nuancerede tiltag med en meget hyppigere kontrolfrekvens

Fx står der i ISO27001 Annex A 9.2.3 under Privilege Access Management: ”The conditions for the expiry of the privilege of access rights should be defined”, mens CIS kontrollernes Password Policy Guide kommer med helt specifikke råd til password længde, kompleksitet, skift, 2FA og meget mere. Compliance rammeværk som fx ISO27001 kan være nødvendige, fordi det er et krav fra virksomhedens kunder (ligesom revisionserklæringer) men det er ikke muligt at bygge et effektivt Cyberforsvar på disse tiltag

> **Tiltag**: Brug konkrete målinger til at udføre Cybersikkerhedskontroller og vær sikker på, at virksomheden følger bedste praksis i stedet for ”best effort”.

#9 Tildeler bestyrelsen de ressourcer, der er nødvendige for at mitigere risikoen for et Cyberangreb?

”Hvornår er nok nok?” og hvordan måler ledelsen at de ressourcer, der tildeles Cybersikkerhed, bruges bedst? Det kræver i første omgang, at virksomheden har foretaget en analyse af, hvor sikker virksomheden er (A), hvor sikker den skal være (B) og hvad det kræver at nå dette mål (C). Målet er at nå og forstå den accepterede risiko, som typisk ikke er 100% Cybersikkerhed. Til dette mål er der tildelt et budget og sammen med de tiltag, der er planlagt, måler man om de indførte kontroller viser, at virksomheden har nået et bestemt stykke på vejen mod den accepterede risiko

> **Tiltag**: Dediko’s CIS Analyse indeholder ledelses-dashboards, benchmarking mod andre virksomheder, KPI for ressourceforbrug og kontroller, så du kan sikre at de mange ressoucer bruges optimalt. Det officielle Danmarks dokument på dette område hedder Cybersikkerhed for Bestyrelsen og kan hentes på https://bestyrelsesforeningen.dk/vejledninger-og-anbefalinger/. Vores ledelsesmodenhedsmodeller og model for at måle styrken af Cyberprogrammet kan også hjælpe her.

#10 Hvordan skaber vi et effektivt Cybersikkerhedsprogram med effektiv Cyberkommunikation i virksomheden?

Det er ledelsens rolle at eje og mitigere den accepterede risiko, men alle i virksomheden skal bidrag til at nå dette mål. Derfor skal de udførende afdelinger, som typisk er IT og SecOps have klare mål, tidslinjer og KPI/KRI, som rapporteres tilbage til ledelsen. Men hele organisationen skal hjælpe kontinuerligt til med at nå dette mål og derfor er det vigtigt med et målbart awareness program implementeret efter bedste praksis (SANS MGT433) som udspringer fra ledelsen.

> **Tiltag**: Brug Dediko's awareness profil til at måle modenheden af virksomhedens awarenessprogram og automatisere awareness med vores programmer og målrettede tiltag. Se mere på https://dediko.dk/emner/awareness.

FAQ vedr. ledelseskommunikation af Cybersikkerhed.

1. **Hvad er sandsynligheden for at blive ramt af et Cyberangreb**
   Afhængigt hvilken typer af virksomhed man er, hvor i verden man er repræsenteret og hvad niveauet af Cybersikkerhed er der større eller mindre sandsynlighed. De seneste tal fra PwC's undersøgelse af Cybersikkerhed i 2022 peger på ca. 1/5 virksomheder har været ramt det seneste år, men Internationale undersøgelser Deloitte og Anomali peger på 4/5 har været ramt. Det er sikkert at konstatere at det er et spørgsmål om hvornår og ikke om. Det er naturligvis også er spørgsmål om hvordan man definerer "har været ramt af et Cyberangreb".

2. **Hvad koster det at blive ramt af er Cyberangreb**
   Dette afhænger også meget af virksomhedstypen og hvad man er ramt af, men et større Cyberangreb fulgt af ransomware, tab af sensitive data og DDoS kan løbe op i mange millioner kroner som fordeles på:
   * Driftstab (90%)
   * Omkostninger til oprydning (10%)
   * Omkostninger til etablering af et effektivt Cyberprogram (herunder medarbejdere, uddannelse, software, eksterne konsulenter og outsourcing)
   * Tab af sensitive data og immaterielle rettigheder
   * Påvirkning af aktiekursen i flere år
   * Udskiftning af medarbejdere (og på ledelsesgangen)
   * Betaling af løsesum
   * Cyberforsikring
   * Bøder som følge af non-compliance (fx GDPR, NIS2 og andre standarder)

3. **Hvad er de hyppigste årsager til et Cyberangreb**
   Et Cyberangreb forårsages hyppigst af følgende:
   * Lækkede rettigheder (konti og passwords) med eller uden 2FA (Kør SpyCloud eller SpecOps Password Policy Auditor for at se situationen i din organisation)
   * Phishing angreb – fører til ovenstående eller direkte installation af malware
   * Misbrug af administrative rettigheder
   * Sårbarheder på kritiske systemer
   * Usikker ekstern adgang til virksomhedens systemer
   * Usikker opsætning af Cloud systemer
   * Usikker OT, manglende mitigering af OT Cyber risk og hardening
   * Insider trusler (sjusk eller forsætlige)
   * Eksterne / tredjeparter

4. **Hvor er overlappet mellem privatsfæren og virksomheden når det gælder Cyberrisiko**
   Brug af samme passwords fx på sociale medier privat og i virksomheden samt manglende brug af en passwordmanager og 2FA skaber en meget farlig situation. Brug ALDRIg din password cache i browsen som password vault! Desuden har det vist sig at risikoen for et Cyberangreb er væsentligt større ved hjemmearbejde og i stressede situationer

5. **Kan man få sine data tilbage ved at betale løsesum ved et ransomwareangreb**
   Det viser sig at omkring 50% af de virksomheder der rammes at et ransomware angreb betaler løsesum af forskellige årsager. Når de får koderne kan 68% (!) ikke re-etabe alle data. Og retter du ikke de grundlæggende årsager til det, der forårsagede angrebet, er der ca. 50% risiko for at blive ramt igen i løbet af få måneder

6. **Hvordan måler man Cybersikkerhed og hvorfor gør man det (Hvad er en CIS analyse - https://www.youtube.com/watch?v=hTJPuIzv3lU)**
   Brug en mitigering af CIS 18 implementeringsgruppe 2 som en grundlæggende og pragmatisk standard til at måle niveauet af Cybersikkerhed i virksomheden. Hvis Cybersikkerheden ikke er målbar kan virksomheden grundlæggende ikke svare på hvor den er på Cyberrejsen.

7. **Kan virksomheden outsource Cybersikkerheden helt til tredjepart**
   Ja og det kan anbefales, men på en struktureret og målrettet facon. Specielle områder som fx CIS analyse, SIEM, Incident Response og pentest egner sig rigtigt godt til outsourcing. Men det er ikke en god idé at outsource hele it-sikkerheden til en ekstern part. Hvis du forsøger dette så skal du være 110% sikker på hvad du får i din oursourcingaftale (Brug MITRE ATT&CK som reference for TTP)

8. **Hvad er benchmark tal for brugen af ressourcer på Cybersikkerhed (gør vi mere eller mindre end "de andre")**
   * Omkostning til Cybersikkkerhed pr. medarbejder 15-18.000+ DKK pr. bruger pr år
   * 0,48% af årsomsætningen
   * 15-18%+ i forholdet mellem it-budget og cybersikkerhedsbudget
   (Tal fra Deloitte)

9. **Hvordan kommunikerer ledelsen med de udførende dele af organisationen og visa versa om Cybersikkerhed**
   Se vores videoer og webinarer om dette emne på vores webiarportal: https://www.gotostage.com/channel/dediko

10. **Hvad er de vigtigste KPI når det gælder Cybersikkerhed og ledelseskommunikation**
    Se punkt 9. Eksempler er:
    * MTTD, MTTR og MTTM (opdage, svar og mitigeringstid)
    * Antallet og type af hændelser
    * Cybersikkerhedsprofil (fx målt efter CIS 18)
    * Cybersikkerhedsrobusthed (fx målt efter NIST CSF eller ISO27002:200)
    * Sårbarheder på kritiske systemer (SLA for mitigeringstid)
    Når KPI sættes i relation til forretningen går de fra at være Key Performance Indicators til at være Key Risk Indicators
    Få en idé om virksomheden set udefra via fx SecurityScoreCard

11. **Hvad er de konkrete tiltag der skal indføres for at mindske risikoen for og konsekvensen af et Cyberangreb**
    Det er summen af alle tiltag der udgør Cybersikkerhedsprofilen hvilket kan oversættes til opfyldelsen af CIS 18 implementeringsgruppe 2 for de fleste virksomheder og offentlige institutioner. Cybersikkerheden skal indtænkes i en proces der understøttes af NIST CSF eller ISO27002:2022 samlet i et Cybersikkerhedsprogram for virksomheden.

12. **Er der en konkurrencemæssig fordel i at være Cybersikker**
    Når flere og flere virksomheden bliver beviseligt mere ”Cybersikre” kan det være et udvælgelseskriterie i forbindelse med udbud og salg. Desuden er det et krav i fx NIS2 at virksomheden kan dokumentere sit niveau af Cybersikkerhed. Brug fx D-mærket som et bevis på virksomhedens engagement og niveau af Cybersikkerhed (men brug IKKE CIS 18, da dette er for konkret)

13. **Hvad er NIS2 (CIS, ISO27002:2022 og NIST CSF)**
    NIS2 er en EU-forordning for entiteter der er væsentlige eller vigtige for infrastrukturen i EU og i den enkelte lande i EU. Forordningen skal udmøntes senest i oktober 2024 og du se mere om dette på vores YouTube kanal og evt. bruge vores NIS2 modenhedsmodel som du kan hente gratis fra vores hjemmeside.

14. **Kom godt i gang med at blive Cybersikker og diskussion i forum**
    Se vores dokumenter ”Cyberråd” og ”Staldtips fra Cyberhesten” som du kan hente gratis fra vores hjemmeside. Her får du gode råd og vejledning til at komme i gang. Du kan desuden se mere på sikkerdigital.dk

Ledelsens kommentarer:

Forslag til særlige tiltag:

Videresendt til:

Christian Schmidt
Direktør, DEDIKO
chr@dediko.dk