conscia

Cyber Security Rapport 2024

TRENDS OG ANBEFALINGER

CYBER SECURITY MONTH

CYBER SECURITY MONTH

Indhold

Klik på tallet, for at gå til det kapitel, du vil læse

Kapitel

Cyber Security Rapport **2024**

Forord

2024 har båret præg af en stigning i antallet af cyberangreb, og specifikt ransomware-angreb. Vi har desuden set, at flere ransomware-grupper nøjes med at stjæle data uden at kryptere dem, og at de har fundet nye måder at angribe og true deres ofre på.

Et af de offentligt kendte eksempler er den danske distributionsvirksomhed Skanlog, der er blandt de største tredjeparts logistikvirksomheder i Skandinavien, som blev lagt ned af et nordkoreansk ransomwareangreb i april måned. I løbet af en nat blev alle IT-systemer ubrugelige og selskabet måtte fra næste morgen benytte manuelle processer, papir og blyant for at betjene kunder og samarbejdspartnere. Skanlog iværksatte en forberedt nødprocedure, der inkluderede kontakt til politiet, Datatilsynet og Center for Cybersikkerhed, og de betalte ikke ransom, men reetablerede infrastrukturen fra bunden.

Eksemplet er på ingen måde enestående. Der er mange flere alene fra i år. Nogle er offentligt kendte, og andre er holdt internt i de berørte virksomheder, men konklusionen er entydig: Vi har set en vækst i omfanget af angreb, og ingen virksomhed er udenfor målgruppen for de cyberkriminelle.

2024 er desuden et år, hvor compliance har fået endnu mere fokus. Øgede krav til offentlig rapportering presser sig på og udfordrer balancen mellem at levere og dokumentere. Danmarks offentlige sektor og danske virksomheder er på forkant med digitaliseringen. Det afspejles både i FN's digitaliseringsindeks og OECDs Digital Government Index, hvor Danmarks offentlige digitalisering ligger i den absolutte top. Vi ser dog et skred i forhold til Danmarks digitale konkurrenceevne, hvor Danmark i 2023 mistede sin førsteplads og måtte se sig forvist til fjerdepladsen[1] i IMDs World Digital Competitiveness Ranking. Danmark ligger dog stadig i den rigtig gode ende, og det kan tolkes som positivt, for det skaber konkurrencefordele.

Samtidig åbner de digitale fremskridt også op for sårbarheder, for den omfattende digitalisering gør os ekstra sårbare for cyberangreb både på vores kritiske infrastruktur, vores produktions- og servicevirksomheder samt organisationer. Cyberangreb afvikles hurtigere, rammer bredere og bliver konstant mere sofistikerede. Vores arbejde med at forsvare os mod cyberangreb skal følge trit med den voksende cybertrussel, og vi skal samtidig håndtere den kraftigt øgede regulering som

Fortsættes →

1: https://www.danskindustri.dk/di-business/arkiv/nyheder/2023/11/dansk-forsteplads-er-tabt-grundigt/

Cyber Security Rapport **2024**

Forord

fx NIS2-, DORA- og CER-direktiverne varsler. Dette øger behovet for endnu mere struktur i arbejdet med cybersikkerhed. Direktiverne er ikke kun en reaktion på den stigende cybertrussel, men er også en proaktiv foranstaltning til at sikre vores digitale fremtid.

I de seneste år har vi set, at truslen mod Danmark og danske virksomheder er steget, og dermed er alvoren og kritikaliteten i Center for Cybersikkerheds trusselsvurderinger øget.

Anbefalingen er at undlade at gå i panik og kaste sig over endnu flere nye sikkerhedsprodukter, som mange ikke får det fulde udbytte af. Nej, erfaringen er snarere, at alle trusselsaktører også har svagheder, uanset om de er statsstøttede aktører eller cyberkriminelle.

Og de svagheder kan udnyttes, når man opbygger og vedligeholder et godt og effektivt cyberforsvar.

Med denne rapport ønsker vi hos Conscia at give vores syn på sikkerhedssituationen set med danske øjne. Vi dykker ned i aktuelle tendenser og anbefalinger, som vi ser, er særligt vigtige netop nu. Og vi håber at bidrage med viden om, hvordan virksomheder og organisationer kan styrke deres cybersikkerhed for – ikke kun at overleve – men også trives i det digitale landskab, som er en præmis for vores fælles fremtid.

God læselyst,
Thomas Grønne,
Direktør for Sikkerhedsområdet i Conscia

Thomas Grønne
Direktør for Sikkerhedsområdet, Conscia Danmark
TG@conscia.com

Thomas har en kandidatgrad fra DTU og mere end 25 års erfaring med IT-sikkerhed. Han har grundlagt IT-sikkerhedsvirksomheden RespektIT, der senere fusionerede med Credocom og blev opkøbt af Conscia . Thomas er direktør for sikkerhedsområdet i Conscia, og han formidler nye trends og tendenser indenfor IT-sikkerhed, udstikker Conscias retning på sikkerhedsområdet og sikrer, at vores kunder forstår hele det komplekse billede omkring IT-sikkerhed.

1. Hybrid arbejdsplads

Netværk og sikkerhed i skyen

Den hybride arbejdsplads er efterhånden ikke længere en ny virkelighed – men hverdagens realitet. Applikationer leveres fleksibelt fra lokale datacentre eller offentlige skyer. Virksomheder bør derfor være i stand til at beskytte og kontrollere adgangen til alle data og applikationer, uanset hvor de er placeret, samtidig med at de opretholder en god brugeroplevelse. Hybridt arbejde har skabt nye udfordringer for sikkerhed og adgangsstyring, og det er blevet klart, at den traditionelle perimeterbaserede arkitektur ikke dækker de nye behov, der er opstået.

Secure Access Service Edge (SASE) og Secure Service Edge (SSE) tilbyder en konvergens af netværks- og sikkerhedsfunktioner i en samlet cloud-leveret platform. Det gør det muligt for organisationer at administrere adgangen til applikationer og data på en sikker og effektiv måde, uanset brugerens placering.

Der er store gevinster at hente i omstillingen til den nye decentrale arkitektur, men det er ikke en nem øvelse. Det er en af de største ændringer, der er sket inden for netværk og sikkerhed i de sidste 20 år.

Organisationer bør allerede have en plan på plads for, hvordan den nye decentrale arkitektur skal anvendes, fordi dette ikke er et midlertidigt modefænomen.

Fordele ved fremtidens sikre infrastruktur:

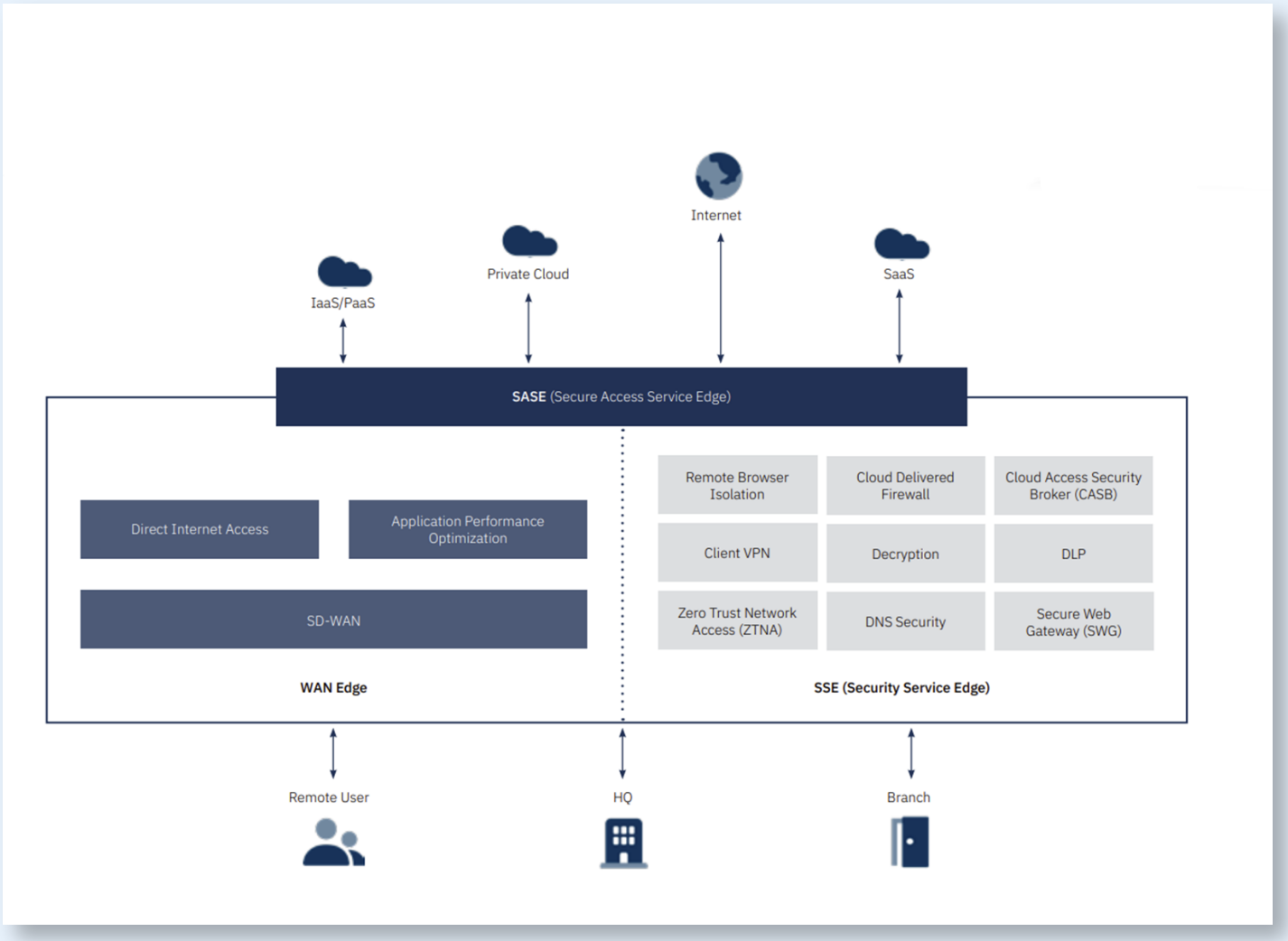
- Skalérbarhed – både økonomisk og teknisk
- Forbedret brugeroplevelse
- Cloud-leveret infrastruktur, der dækker alle kontinenter
- Konsolidering af netværk og sikkerhed

Kristian Von Staffeldt
Sikkerhedsevangelist, Conscia Danmark
KVS@conscia.com

Kristian er **Sikkerhedsevangelist** hos Conscia og arbejder til daglig med at oversætte teknikken bag digitale sikkerhedsløsninger og forklare deres værdi til ledelseslaget hos vores kunder. Kristian er nemlig typen, der har en dyb teknisk forståelse – uddannet fra DTU, har de højeste certificeringer fra Cisco (CCIE), Palo Alto Networks (CNSE) og VMware (VCP-NV) og er AWS architect, men trods hans dybe tekniske kunnen, så forstår han at forklare IT-sikkerhed og dens værdi, så alle kan være med.

1. Hybrid arbejdsplads

En centraliseret sikkerhedsstruktur



Illustrationen skitserer fremtidens arkitektur, der kombinerer netværks- og sikkerhedsfunktioner i en enkelt cloud-baseret tjeneste.

2. Zero Trust

Zero Trust: Stol ikke på nogen

Omkring 2010 begyndte John Kindervag at mistænke, at klienter, applikationer og servere ville blive udbredt til steder uden for virksomhedens kontrol. Tjenester på internettet ville udfordre den hidtil eneste mulighed: at huse alle vigtige data i egne datacentre. Således opstod ideen om Zero Trust Architecture, der oprindeligt blev designet til at udfordre traditionel perimeter-beskyttelse.

Zero Trust blev endnu mere relevant i 2020, da Covid19-pandemien brød ud, og den hybride arbejdsplads blev en naturlig del af hverdagen for næsten alle virksomheder og organisationer. Året efter udstedte USA's præsident Joe Biden: "Executive Order on Improving the Nation's Cybersecurity". Bekendtgørelsen betød, at alle amerikanske myndigheder skulle begynde at implementere Zero Trust.

Principperne bag Zero Trust er enkle:

- Verificér alt, stol ikke på nogen eller noget. Der skal sættes spørgsmålstegn ved al adgang, og det skal altid sikres, at det er den korrekte identitet, enhed og placering, der anmoder om oplysninger, før der gives adgang.
- Minimum adgang. Hvis der skal gives adgang, er det vigtigt, at adgangen begrænses så meget som muligt.
- Segmentér. Isolér systemer så meget som muligt i forskellige zoner. Jo mindre zoner, jo bedre.
- Antag, at der er sket et brud. I stedet for at antage, at din beskyttelse er tilstrækkelig.

Kristian Von Staffeldt
Sikkerhedsevangelist, Conscia Danmark
KVS@conscia.com

Kristian er sikkerhedsevangelist hos Conscia og arbejder til daglig med at oversætte teknikken bag digitale sikkerhedsløsninger og forklare deres værdi til ledelseslaget hos vores kunder. Kristian er nemlig typen, der har en dyb teknisk forståelse – uddannet fra DTU, har de højeste certificeringer fra Cisco (CCIE), Palo Alto Networks (CNSE) og VMware (VCP-NV) og er AWS architect, men trods hans dybe tekniske kunnen, så forstår han at forklare IT-sikkerhed og dens værdi, så alle kan være med.

2. Zero Trust

Zero Trust: Stol ikke på nogen

Sådan starter du din Zero Trust-rejse:

1.
Identificér systemer, hvor implementering af en Zero Trust-strategi gør den største forskel. Det er noget, hele virksomheden skal være enige om. IT-organisationen er ofte ikke den bedste til at identificere, hvilke systemer, der er mest kritiske fra et forretningsmæssigt perspektiv. Her er det i stedet ledergruppen og dem, der bruger systemerne, der er bedst informeret.

2.
Rangér systemerne, hvad vil forårsage mest skade på virksomheden?

3.
Identificer, hvordan systemet bedst beskyttes. Det behøver ikke at være en fysisk firewall. I stedet handler det om at styrke identitetsstyring, uddanne brugere, bruge operativsystemets firewall eller isolere serveren på sit eget segment. Hvis vi kan komme hele vejen med at isolere systemets processer, er det endnu bedre!

True Zero Trust

True Zero Trust betyder, at et system eller flere systemkomponenter kan implementeres sikkert hvor som helst. Stil dig selv spørgsmålet: *"Kan jeg implementere dette i skyen eller i et fremmed land og stadig føle mig sikker?"* Sandsynligvis ikke. Det kræver tillid og ofte en masse kompromiser. Derfor er det vigtigt altid at træffe bevidste valg og at gøre én ting ad gangen.

Klienterne bør være relativt højt oppe på listen over identificerede systemer. De er trods alt i daglig kontakt med forretningskritiske data – og de er overalt. For at bringe dem under kontrol skal al deres kommunikation være omfattet af et enkelt sæt regler, som skal sikre fuld gennemsigtighed omkring, hvilke data, der sendes, fra hvem til hvad, og hvor det er gjort.

Det er præcis, hvad SASE/SSE kan tilbyde, og det er det, der gør teknologien så eftertragtet. SASE (Secure Access Service Edge) handler om at sende trafik til en Secure Service Edge (SSE), der fungerer som en cloud-baseret firewall. Det er med SASE/SSE som med mange andre produkter, der lanceres: Der skabes et behov.

Men er det virkelig det, din organisation har brug for? Start altid med at sikre, hvilke sikkerhedsudfordringer du har, og hvordan det stemmer overens med dine forretningsmål. Først da er det tid til at evaluere hvilke produkter og løsninger, der er tilgængelige. Hvis du i stedet starter med at vurdere, hvad der er tilgængeligt, er det nemt at blive farvet og dermed begrænset til, hvad de adspurgte leverandører præsenterer.

John Kindervag kom på ideen om Zero Trust gennem et digt skrevet af Joseph Rudyard Kippling, der skrev den noget mere berømte Junglebogen.

I keep six honest serving-men.
(They taught me all I knew);
Their names are What and Why and When
And How and Where and Who.
I send them over land and sea,
I send them east and west;
But after they have worked for me,
I give them all a rest.

I let them rest from nine till five,
for I am busy then,
As well as breakfast, lunch and tea,
For they are hungry men.
But different folks have different views;
I know a person small
– She keeps ten million serving-men,
Who get no rest at all!

She sends'em abroad on her own affairs,
From the second she opens her eyes
– One million Hows,
two million Wheres,
And seven million Whys!

The Elephant's Child

3. Cyberresiliens

Cyberresiliens

Cyberresiliens, eller på engelsk Cyber resilience, refererer til en organisations evne til at forberede sig på, håndtere og komme sig efter cyberangreb, og det bør være en central del af enhver organisations sikkerhedsstrategi. Især i en tid, hvor cybertrusler konstant udvikler sig og bliver mere og mere sofistikerede. Cyberresiliens handler ikke kun om at beskytte information og systemer mod angreb, men også om evnen til at opretholde forretningsdriften og beskytte data, under et cyberangreb eller en anden krise.

For at imødekomme de voksende udfordringer og for at sikre danske og europæiske organisationer bliver bedre rustet til at operere i dette øgede trusselsbillede, har EU Parlamentet den 10. november 2022 vedtaget et "direktiv om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen" også kendt som NIS2. Formålet med NIS2-direktivet er at styrke og ensarte cybersikkerheden og effektiviteten af organisationers informationssikkerhed på tværs af landene i EU og herunder Danmark. Blandt andet pålægges de omfattede organisationer ("enheder") i NIS2 direktivet "at træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre sikkerhedsrisici og begrænse skaderne i tilfælde af en sikkerhedshændelse"

Til implementering af "passende foranstaltninger", i forbindelse med NIS2, anbefaler den Europæiske Unions Agentur for Cybersikkerhed (ENISA) organisationer at benytte sig af Sikkerhedsrammeværket fra Center for Internet Security (CIS).

CIS Sikkerhedsrammeværket er en anerkendt, praktisk og prioriteret sikkerhedsramme som anses for "Best Practise" for tekniske sikkerhedskontroller, og benyttes af mange organisationer til at måle og planlægge deres cybersikkerhedsinitiativer og roadmap. DORA er en lignende lovgivningsmæssig ramme for på lignende vis at styrke den finansielle sektors modstandsdygtighed overfor cyberangreb.

Ronnie Abrahamsen
Salgsspecialist, Conscia Danmark
ROAB@conscia.com

Ronnie er Salgsspecialist indenfor Strategisk og Offensiv sikkerhed. Her hjælper han vores kunder med at identificere huller og sårbarheder i deres aktuelle informationssikkerhed og, på en struktureret måde, guide dem til hen imod en sikkerhedsløsning med større, bedre og mere effektiv beskyttelsesevne - på både et teknisk og strategisk niveau. Ronnie har, med +25 år i IT-branchen, bred erfaring med forskellige aspekter indenfor sikkerhed - bl.a. sårbarhedshåndtering, penetrationstests, samt sikkerhedsassessments baseret på anerkendte sikkerhedsrammeværk som CIS-rammeværket. Han opretholder desuden CISSP- og CEH-certificeringer samt udvalgte certificeringer fra vores producenter.

3. Cyberresiliens

CIS-kontrollerne

CIS-kontrollerne består af 18 hovedkontroller med i alt 153 tilhørende beskyttelsesforanstaltninger (safeguards) og tre implementeringsgrupper, der angiver forskellige ambitionsniveauer for beskyttelse. Kontrollerne skal enten udføres som tekniske kontroller – eksempelvis brugen af en aktiv scanner, der identificerer al hardware på netværket – eller de skal udføres som menneskelige kontroller, hvor nogen aktivt skal tage stilling til noget – eksempelvis identifikation af, hvem i organisation der har ansvaret for en computer, et budget eller en forretningsproces. I CIS-rammeværket er hver kontrol udstyret med en titel og en beskrivelse, så det ikke kan misforstås, hvordan kontrollen skal udføres.

Vel vidende at der er forskel på virksomheders størrelse, sikkerhedsbudgetter og modenhedsniveauer deler CIS virksomheder ind i tre implementeringsgrupper: IG1, IG2 og IG3. Det fremgår tydeligt af oversigten i CIS-rammeværket, hvilke beskyttelsesforanstaltninger virksomheder tilhørende henholdsvis implementeringsgruppe 1, 2 og 3 anbefales at udføre.

En virksomhed bør som det første identificere, hvilken implementeringsgruppe de selv tilhører baseret på deres risikoprofil og tilgængelige sikkerhedsressourcer. Hovedkontrollerne og beskyttelsesforanstaltningerne i hver implementeringsgruppe bygger videre på implementeringen af de forrige, således at IG2 indeholder alle hovedkontroller og beskyttelsesforanstaltninger i IG1, og IG3 indeholder alle hovedkontroller og beskyttelsesforanstaltninger i IG1 og IG2.

Center for Internet Security (CIS)

Center for Internet Security (CIS) blev etableret i 2000 som en nonprofitorganisation af en flok sikkerhedseksperter og tæller i dag bidragydere såsom NSA Red Team and Blue Team, Homeland Security, US-CERT, US DoD Computer Network Defense Architecture Group, US DoD Joint Task Force – Global Network Operations, US DoD Defense Cyber Crime Center, The SANS Institute samt en lang række virksomheder indenfor blandt andet det offentlige, militæret samt forsynings-, finans-, transport- og uddannelsessektoren. CIS-kontrollerne understøtter forskellige lovmæssige og regulatoriske rammeværktøjer og gør det mere simpelt at efterleve compliance indenfor cybersikkerhed.

4. Regulatoriske **krav**

Direktiver og forordninger

Den geopolitiske situation, der er kendetegnet ved øgede spændinger mellem stormagter og indvirkning på handel og teknologisk dominans, intensiverer usikkerheden i det globale IT-økosystem. Rusland, Kina og Iran agerer mere offensivt, hvilket, kombineret med øget digitalisering, gør, at cybersikkerhed og informationsintegritet i stigende grad er koblet til geopolitiske forandringer.

Cyberangreb accelerer i både kompleksitet og beskyttelsesomkostninger og er i dag en sikkerhedstrussel drevet af aktører med politiske, militære eller økonomiske motiver. Desuden er cyberangreb en af de hurtigst voksende former for kriminalitet, og EU spiller en vigtig rolle som vejviser.

ENISA, EU's myndighed for net- og informationssikkerhed, har rapporteret, at de gennemsnitlige omkostninger ved en IT-relateret hændelse i EU steg til ca. 1,3 mio. DKK i 2022, hvilket er en fordobling af omkostninger i forhold til det forgangne år.

Indførelsen af regler som NIS2

NIS2-direktivet eller DORA-forordningen er politiske forsøg på at reagere på det voksende trusselsbillede, da virksomheder og samfund ikke har været i stand til at forbedre deres cybersikkerhed tilstrækkeligt i takt med digitaliseringen. Det gør lovgivning til et af de få redskaber, som politikerne kan bruge til at håndtere denne udfordring.

Peter Koch
Sikkerhedsevangelist, Conscia Danmark
PKO@conscia.com

Peter har travlt med at gøre vores kunders digitale rejse sikker og beskytte forretningsværdien fra digitaliseringen af kunders forretning. Han fører an, når det kommer til at hjælpe kunderne med en mere struktureret tilgang til cybersikkerhed gennem udførlig planlægning og brug af CIS-kontrollerne. På samme tid hjælper han dem med at drage fordel af Zero Trust - cybersikkerhedsstrategien - som et fokuspunkt for en gennemprøvet sikkerhedsstrategi.

4. Regulatoriske **krav**

NIS2-direktivet: Højere krav og skærpede sanktioner

I august 2018 blev NIS-direktivet sat iværk for at højne sikkerhedsniveauet af kritiske net- og informationssystemer i EU. Med digitaliseringens fremskridt og de forbundne risici besluttede Europa-Kommissionen, at det var på tide med en opdatering. Resultatet blev NIS2-direktivet.

I 2025 vil NIS2-direktivet blive implementeret i dansk lovgivning. En vigtig opdatering er, at CER-direktivet (direktiv for styrket modstandsdygtighed i samfundsmæssigt vigtige aktiviteter) vil blive implementeret samtidig med NIS2. Relevante aktører bør derfor arbejde parallelt med begge direktiver.

Her følger en kort opsummering af NIS2

Formål:
- Styrke sikkerheden for organisationer, der spiller en afgørende rolle for det europæiske samfunds funktion

Ændringer fra tidligere direktiver:
- Forøgelse fra syv til 11 sektorer under »væsentlige enheder«
- Indførelse af syv nye sektorer som "nøgleenheder"

Nye tilføjelser:
- Blandt andet offentlig forvaltning og rumfartsindustrien som væsentlige tjenester
- Blandt andet produktion, forarbejdning og distribution af fødevarer, post- og kurertjenester og affaldshåndtering som væsentlige tjenester
- Øgede krav til sikkerhed og hændelsesrespons
- Krav til forsyningskæde og styring
- Yderligere rapporteringskrav
- Sanktioner og tilsyn
- Øgede krav til ledelsen

Resultat
- Markant flere virksomheder og organisationer er omfattet af NIS2 end forgængeren NIS-direktivet

4. Regulatoriske **krav**

10 tin til NIS2 compliance

De tekniske minimumskrav listet i NIS2-regulativet til at opnå bedre cyberresiliens, er følgende:

1 Risikostyring og Sikkerhedspolitikker

Organisationer skal udvikle og implementere omfattende risikostyringspolitikker, der omfatter vurdering og styring af cybersikkerhedsrisici. Disse politikker skal dække teknologiske, operationelle og organisatoriske risici.

2 Incident Response (hændelseshåndtering)

Organisationer skal have etableret processer og værktøjer til effektivt at identificere, rapportere og reagere på sikkerhedshændelser. Dette inkluderer oprettelse af incident response-teams, kontinuerlig overvågning og logging af aktiviteter samt udarbejdelse af handlingsplaner for forskellige typer af hændelser.

3 Driftskontinuitet

Organisationer skal etablere solide backup- og recovery-processer for at sikre, at data kan gendannes i tilfælde af en hændelse, såsom ransomware-angreb eller datatab. Dette omfatter regelmæssige backups, offsite-lagring og test af gendannelsesprocedurer.

4 Sikkerhed i forsyningskæden

Organisationer skal sikre, at leverandører og partnere overholder bestemte sikkerhedskrav. Dette indebærer risikovurderinger og indførelse af kontraktuelle forpligtelser for at sikre, at forsyningskæden ikke udgør en svaghed i den overordnede sikkerhed.

5 Netværks- og Informationssystemers sikkerhed

Der skal etableres effektive foranstaltninger for at sikre netværks- og informationssystemers fortrolighed, integritet, tilgængelighed og robusthed. Dette inkluderer implementering af passende tekniske og organisatoriske foranstaltninger til at beskytte mod cyberangreb.

6 Sikkerhedsrevision og testning

Der skal udføres regelmæssige sikkerhedsrevisioner og penetreringstests for at evaluere effektiviteten af de eksisterende sikkerhedsforanstaltninger. Resultaterne skal bruges til at forbedre sikkerhedspraksis og afhjælpe eventuelle svagheder.

4. Regulatoriske **krav**

10 tin til NIS2 compliance

7 Awareness training (bevidsthedstræning)

Organisationer skal uddanne deres personale i cybersikkerhedspraksis, så de kan genkende og reagere på potentielle trusler. Dette inkluderer regelmæssige træningsprogrammer, phishing-tests og opdateringer om de nyeste trusler.

8 Kryptering

Organisationer skal etablere procedurer for brug af kryptografi og kryptering til beskyttelse af data.

9 Adgangskontrolpolitikker og forvaltning af aktiver

Organisationer skal etablere foranstaltninger, der adresserer personalesikkerhed, adgangskontrolpolitik og forvaltning af aktiver.

10 Multifaktor autentificering

Der skal etableres foranstaltninger, som omfatter brug af MFA m.v., beskyttelse af kommunikation og etablering af nødkommunikation, hvor det er relevant.

> *Disse er som nævnt de tekniske minimumskrav for at "træffe passende og forholdsmæssige tekniske og organisatoriske foranstaltninger for at styre sikkerhedsrisici". Men hvad der er passende og forholdsmæssige foranstaltninger kan være vanskeligt for den enkelte organisation at vurdere. Conscia anbefaler at læne sig op af et anerkendt sikkerhedsrammeværk – som eksempelvis CIS rammeværket.*
>
> **Peter Koch**
> **Sikkerhedsevangelist, Conscia Danmark**

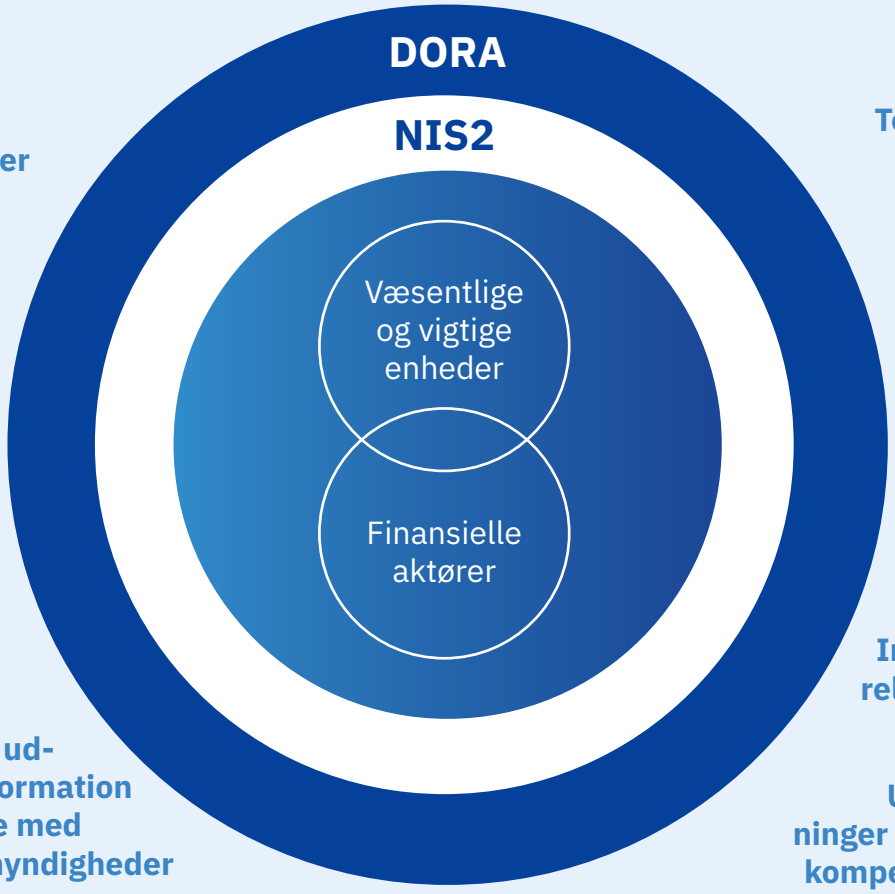
4. Regulatoriske **krav**

Nye EU-krav til øget sikkerhed

Figuren illustrerer de krav og regler, der følger med NIS2 og DORA. Det viser Den Europæiske Unions igangværende bestræbelser på at imødegå de voksende cybertrusler og sikre en sikker digital fremtid for alle medlemsstater.

NIS2-krav

- Sikkerheds-foranstaltninger
- Risiko-vurdering
- Styring
- Sikkerhed for leverandører
- Håndtering af hændelser
- Rapportering, udveksling af information og samarbejde med kompetente myndigheder



DORA-krav

- Test af digital operationel robusthed
- Informations- og kommunikations-teknologi risiko-vurdering (IKT)
- IKT-styring
- Håndtering af IKT-tredjepartsrisici
- Indberetning af IKT-relaterede hændelser
- Udveksling af oplysninger og samarbejde med kompetente myndigheder

4. Regulatoriske **krav**

DORA og ISO

Digital Operations Resilience Act (DORA)

Digital Operations Resilience Act (DORA) er en forordning, der har til formål at begrænse digitale trusler i bank- og finansverdenen. DORA trådte i kraft i begyndelsen af 2023, men finansielle virksomheder skal først overholde de nye regler fra januar 2025.

DORA - et skræddersyet reguleringsværktøj

DORA- og NIS2-reglerne følger stort set den samme tidslinje og har flere overlapninger. DORA forventes dog, for finanssektoren, at overskygge NIS2's mere generelle bestemmelser. DORA er ved at udvikle sig til et mere skræddersyet reguleringsværktøj, der har til formål direkte at imødekomme de specifikke behov og udfordringer, som finansielle institutioner står overfor. Når vi gennemgår NIS2 og DORA, kan vi tydeligt se, at de har flere fælles mål, når det kommer til at styrke den digitale sikkerhed i EU.

NIS2 og DORA repræsenterer således EU's igangværende bestræbelser på at imødekomme de voksende cybertrusler og sikkerhedstrusler samt skabe en sikker digital fremtid for alle medlemsstater. For organisationer, navnlig i de relevante sektorer, indebærer disse forordninger et behov for at revurdere, styrke og standardisere deres sikkerhedsforanstaltninger og -strategier.

Hvorfor er begge dele vigtige?

I en verden, hvor digitaliseringen er stigende, bliver netværk og informationssystemer stadig vigtigere for samfundsfunktioner, og vi bliver mere og mere afhængige af sikre og pålidelige digitale systemer. NIS2 og DORA arbejder sammen om at styrke cybersikkerheden og den operationelle modstandsdygtighed i EU især i kritiske sektorer og finansielle tjenesteydelser, hvor det kan have store konsekvenser i tilfælde af forstyrrelser.

Standardiserede rammer gør det nemmere

ISO 27001 er en international standard for informationssikkerhed, der hjælper organisationer med at implementere og vedligeholde deres informationssikkerhedsstyringssystem (ISMS). Den fokuserer på at sikre nøjagtighed, fortrolighed og tilgængelighed af oplysninger gennem en systematisk og risikobaseret tilgang.

ISO 27001 understøtter implementeringen af DORA og NIS2 ved at tilvejebringe en ramme for standardiserede sikkerhedsforanstaltninger, risikostyring, hændelsesstyring og forretningskontinuitet. Det understreger vigtigheden af at håndtere tredjepartsrisici, som kræver omhyggelig dokumentation og revision for at demonstrere overholdelse. Derudover er ISO 27001's kontinuerlige forbedringer i overensstemmelse med den løbende tilpasning, som DORA og NIS2 kræver.

5. AI

AI i Den Europæiske Union

AI spiller en central rolle i samfundets digitale transformation. Det er svært at forestille sig en tilværelse uden AI's forskellige produkter og services, både i privatlivet og arbejdslivet. I sin digitale strategi, Forordningen om kunstig intelligens (AI), sigter EU mod at regulere kunstig intelligens for at optimere udviklingen og anvendelsen heraf.

Teknologien kan give flere fordele, og for at fremme en sikker og innovativ udvikling har EU foreslået visse regler:

Risikobaseret tilgang
AI-systemer kategoriseres ud fra deres risikoniveau:
- Begrænset risiko
- Høj risiko
- Uacceptabel risiko

Forbud mod visse anvendelser
Applikationer, der anses for at udgøre en trussel mod mennesker, betragtes som uacceptabel og vil blive forbudt. Dette omfatter fx AI-systemer, der bruges til manipulation, social pointscoring og biometrisk identifikation i realtid, med visse undtagelser.

Strenge krav
AI-systemer, der anses for at være højrisikosystemer, skal opfylde strenge krav. Disse krav omfatter høje niveauer af robusthed, cybersikkerhed, databeskyttelse, detaljeret dokumentation og menneskeligt tilsyn.

Gennemsigtighed
Generativ AI, såsom ChatGPT, skal tydeligt informere brugerne om, at de interagerer med AI. Dette krav har til formål at sikre gennemsigtighed og brugerbevidsthed.

Overvågning og rapportering
Virksomheder og organisationer, der udvikler eller bruger AI, skal følge overvågnings- og rapporteringsprocedurer for at sikre overholdelse af loven.

De nationale tilsynsmyndigheder
Hvert EU-medlemsland skal oprette tilsynsmyndigheder til at overvåge overholdelsen af AI-forordningen.

Sanktioner
Overtrædelser af EU's AI-forordning kan føre til store bøder: For brug af forbudte AI-applikationer kan bøden være op til 35 mio. EUR eller 7 % af den globale omsætning. For andre overtrædelser kan bøden være op til 7,5 mio. EUR eller 1,5 % af den samlede omsætning.

5. AI

AI i Danmark

Den danske regering har udviklet en omfattende AI-strategi for at udnytte potentialet i kunstig intelligens inden for forskellige sektorer.

Strategien fokuserer på fire hovedområder: sprogteknologi, data, kunstig intelligens og digital inklusion. Når det kommer til sprogteknologi, sigter regeringen mod at etablere en fælles dansk sprogressource for at understøtte udviklingen af sprogteknologiske løsninger som talegenkendelse og sprogforståelse. Strategien lægger også vægt på åbne offentlige data, hvor fem offentlige datasæt vil blive gjort tilgængelige for virksomheder, forskere og offentlige myndigheder til udvikling af kunstig intelligens.

Desuden implementerer regeringen signaturprojekter i samarbejde med kommuner, regioner og private virksomheder inden for sundhed, socialområdet og tværgående sagsbehandling for at opnå erfaring med implementering af kunstig intelligens i den offentlige sektor. Strategien inkluderer også tiltag til at styrke investeringerne i danske virksomheder med forretningsmodeller baseret på kunstig intelligens gennem en dansk investeringspulje. Alt i alt stræber den danske regerings AI-strategi efter at fremme udviklingen og anvendelsen af kunstig intelligens i landet.

Allan Møller
Konsulentchef, Cloud
ALMO@conscia.com

Allan, Cloud Konsulentchef Conscia, har mere end 10 års erfaring med cloud-teknologi og softwareudvikling på tværs af forskellige cloud-miljøer og har blandt andet en baggrund fra Microsoft. Han har via sin uddannelse og karriere arbejdet med at forskellige AI- teknologier i cloud. Allan er chef for Conscias Cloud-team og hjælper Conscias kunder at designe, implementere og administrere cloudbaserede løsninger, der passer ind i den enkelte virksomheds digitale rejse.

5. AI

AI som hjælp

Den hurtige udvikling af AI kræver et nyt niveau af årvågenhed og tilpasning fra virksomheder og organisationer. Efterhånden som kunstig intelligens fortsætter med at udvikle sig, skal vi også være opmærksomme og forberedte på de potentielle risici, AI udgør. På trods af disse risici er kunstig intelligens også et vigtigt aktiv i kampen mod cyberkriminalitet. Dets evne til hurtigt og effektivt at identificere trusler bidrager til stærkere og mere tilpasningsdygtige cybersikkerhedssystemer.

AI-teknologier som maskinlæring er allerede etableret på cybersikkerhedsområdet og rummer fortsat potentiale til at forbedre sikkerhedsforanstaltningerne. Disse systemer, som løbende lærer af nye data, har evnen til ikke kun at forudsige og forhindre trusler, men også løbende at forbedre deres beskyttelse. Med sin evne til at strømline overvågningsprocesser og identificere afvigelser i store mængder af data, spiller kunstig intelligens en vigtig rolle med hensyn til at muliggøre en hur-tig og effektiv reaktion på sikkerhedstrusler. Fremskridt inden for AI giver også potentiale for mere sofistikeret risikoanalyse og automatiseret trusselsdetektion. Det giver virksomheder mulighed for at reagere på og neutralisere trusler hurtigere. Dette er især vigtigt i en tid, hvor cyberangreb stadig bliver mere komplekse og vanskelige at opdage, samtidig med, at de bliver større i omfang. På den følgende side finder du en række anbefalinger til, hvordan kunstig intelligens som værktøj kan bruges i kampen mod AI-baserede trusler.

5. AI

AI i praksis

Anbefalinger til, hvordan kunstig intelligens som værktøj kan bruges i kampen mod AI-baserede trusler.

1 Bekæmp AI med AI:

Brug AI-baserede cybersikkerhedsværktøjer, der blandt andet bruger maskinlæring til at opdage trusler og markere mistænkelig kommunikation. Sådanne værktøjer kan mere effektivt identificere og reagere på komplekse trusler.

2 AI i cybersikkerhedsstyring:

AI-baserede assistenter som værktøjer til cybersikkerhed er et nyt koncept, der er muliggjort af udviklingen af generativ AI-teknologi. Denne type værktøjer er i en tidlig udviklingsfase, men har et lovende potentiale til at ændre sikkerhedslandskabet. Fremtidens AI-assistenter kan spille en central rolle i at identificere og adressere sikkerhedssårbarheder såsom fejlkonfigurationer, automatisere komplekse sikkerhedsopgaver og tilbyde dybere indsigt i potentielle trusler. Det er vigtigt for organisationer at følge med i udviklingen på dette område og undersøge, hvordan disse værktøjer kan integreres i eksisterende sikkerhedssystemer. De bør også forberede sig på at udnytte det fulde potentiale af AI-teknologi inden for cybersikkerhed.

3 Identificér AI med AI:

Brug AI-baserede værktøjer til at registrere, når e-mails og andet tekst er skrevet af andre generative AI-værktøjer. Ved at integrere sådanne værktøjer kan organisationer lettere identificere og handle på potentielt skadelig AI-genereret kommunikation.

4 AI-phishing-simulering:

Brug værktøjer som Chat-GPT i phishing-simuleringer for at hjælpe deltagerne med at vænne sig til den højere kvalitet og tonen i AI-genereret kommunikation. Dette hjælper medarbejderne med at blive mere opmærksomme på sofistikerede forsøg på svindel.

5 AI-cyber-træning:

Tilføj generativ AI-bevidsthedstræning til cybersikkerhedsprogrammer og lær om alle de mange måder, hvorpå AI kan bruges af trusselsaktører. Det er vigtigt at uddanne medarbejderne i de forskellige metoder, hvorpå AI kan bruges til at kompromittere informationssikkerheden.

5. **AI**

AI som trussel

I en verden, hvor den teknologiske innovation accelerer, er AI dukket op som et tveægget sværd inden for cybersikkerhed. På den ene side giver kunstig intelligens uovertrufne muligheder for beskyttelse og effektivitet, og på den anden side bringer den også nye sofistikerede trusler med sig.

Misbruget af AI kan ses i udviklingen af avancerede værktøjer til phishing-teknikker og -kampagner, generering af falske nyheder og tekster samt facilitering af cyberangreb. Disse AI-drevne metoder er ikke kun en risiko for informationssikkerheden, men også for, hvordan offentligheden danner deres meninger. Der er voksende bekymring omkring AI-værktøjer, der kan automatisere og optimere cyberangreb, hvilket gør det muligt for mindre dygtige angribere at udføre mere avancerede angreb.

Her er nogle af de trusler, AI-udvikling medfører:
Automatisering og skalerbarhed: AI-baserede værktøjer gør det muligt for cyberkriminelle at automatisere forskellige trin i angrebsprocessen. Denne automatisering gør det lettere for trusselsaktører at udføre angreb i stor skala og målrette dem mod flere personer på én gang.

Deepfake-trusler:
AI-algoritmer kan generere realistiske medier, såsom manipuleret lyd- og videoindhold. Trusselsaktører udnytter deepfake-teknologi til at udgive sig for at være betroede personer, skabe manipuleret indhold, der narrer medarbejdere til at afsløre følsomme oplysninger, eller foretage ondsindede handlinger.

Avanceret phishing med målrettet profilering:
AI-baserede værktøjer giver cyberkriminelle mulighed for at indsamle store mængder information fra flere kilder, fx sociale medier, offentlige databaser og lækkede data, som kan bruges til at designe personlige spear phishing-emails, der virker legitime og troværdige. Disse målrettede angreb øger trusselsaktørernes chancer for succes og udgør en alvorlig trussel mod enkeltpersoner og organisationer.

> *Det er vigtigt at understrege AI's dobbelte karakter inden for cybersikkerhed. På trods af dens potentiale til at forbedre vores digitale sikkerhed skal vi også være på vagt over for de trusler og risici, som AI medfører. Indsigt i AI's muligheder og begrænsninger vil derfor være vigtig. Dette inkluderer behovet for løbende at opdatere og tilpasse organisationens sikkerhedsstrategier, så de matcher den hurtige teknologiske udvikling.*
> **Allan Møller, Konsulentchef, Cloud**

Cyber Security Rapport **2024**

Afsluttende indsigter

Ransomware med forskellige metoder til afpresning, social engineering og phishing fortsætter med at **koste virksomheder milliarder i løsepenge, bøder og tabt omsætning.** Den hastigt accelererende udvikling af AI vil gøre disse typer angreb endnu mere sofistikerede og sværere at beskytte sig imod.

Etableringen af den **hybride arbejdsplads som en langsigtet løsning indebærer nye udfordringer** for at etablere en sikker og robust infrastruktur. Samtidig er den geopolitiske situation inden for cybersikkerhed blevet mere og mere kompliceret og anspændt. **Statsstøttede cyberangreb er steget med det formål at påvirke det politiske landskab,** udføre spionage og destabilisere lande og vigtige organisationer.

Cybertruslerne stiger, mens der er **global mangel på færdigheder inden for cybersikkerhed.** Det skaber en langt fra ideel situation. Der tages dog store og vigtige initiativer for at øge organisationers modstandsdygtighed. Det ses for eksempel med **nye EU-direktiver** om strengere sikkerhedskrav, risikostyringsforanstaltninger og rapporteringsforpligtelser. Samtidig sker der fremskridt inden for kunstig intelligens, som kan hjælpe med at styrke organisationers cyberrobusthed gennem innovative løsninger.

Afslutningsvis kan vi konstatere, at nutidens cybersikkerhedslandskab er i konstant forandring. **Fremadrettede og innovative tilgange er derfor et must for at tackle disse nye udfordringer.**

Conscia er en førende europæisk IT-specialist inden for netværk, cybersikkerhed og cloud. Vi leverer sikre infrastrukturløsninger og managed services 24/7 til kunder med komplekse netværks-, datacenter-, cloud-, IoT- og mobility-krav. Som en betroet rådgiver stræber vi efter at understøtte kundernes forretningskritiske IT-systemer gennem hele livscyklussen fra design, implementering og drift til optimering. Med et Security Operation Center (SOC), hvor sikkerhedseksperter udnytter AI's kraft, beskytter vi kunderne mod trusler og angreb døgnet rundt, året rundt. Conscia blev grundlagt i 2003 og har i dag over 1.100 medarbejdere.

Vi betjener nogle af de største virksomheder inden for finansielle tjenesteydelser, sundhedspleje, den offentlige sektor, produktion, forsyning og detailhandel fra vores kontorer i Danmark, Sverige, Norge, Tyskland, Holland, England og Slovenien. Vi sigter mod at være det bedste sted at arbejde i Europa for talentfulde IT-specialister med dyb teknisk ekspertise.

CYBER SECURITY MONTH