Building Today's and Tomorrow's IT. Together.

itm8®

Rapport

//Cybersikkerhed_2025
Trends, trusler og taktikker

// Bidragsydere

Denne cybersikkerhedsrapport er blevet til med bidrag
fra følgende personer:

Martin Kofoed
Nicklas Persson
Thomas Öberg
Niclas Hedam
Jesper Højslev Madsen
Shadi Domat
Janeli Sula
Hannes Edström
Rikard Burman
Kent Ekensteen
Erik Bandholm
Simon Krogh Bjerre
Christoffer Bech

Redaktion
Louise Nissen
Julie Blond Andersen
Maria Schlosser
Philip Christiansen - layout

// FORORD

2025 er året, hvor du skal tage cybersikkerhed alvorligt

Håndteringen af trusler relateret til cybersikkerhed kan ofte virke som en uoverskuelig opgave – særligt for små og mellemstore virksomheder (SMV'er). Manglende ressourcer, tid eller teknisk ekspertise betyder, at mange virksomheder forsømmer kritiske sikkerhedsopgaver – og det udnytter de cyberkriminelle.

Med truslen om cyberangreb på et fortsat meget højt niveau bør der ikke være undskyldninger for manglende ansvar og handling.

Hos itm8 oplever vi, at alle typer af virksomheder – både store, små og mellemstore – er udsatte for cyberangreb. Ofte fordi de mangler ressourcer, processer og bedre systemer. Men med enkle og målrettede tiltag kan virksomheder beskytte sig mod trusler og reducere risikoen for store økonomiske tab.

2025 er året, hvor din virksomhed skal tage cybersikkerhed alvorligt. Og du kan begynde lige her.

Sammen med vores kolleger i Sverige har vi udarbejdet en fremadskuende rapport, der skildrer de nyeste metoder, som de cyberkriminelle benytter, og de tendenser, vi i itm8 ser inden for cybersikkerhed. Du får præsenteret vores erfaringer, indsigter og forudsigelser om den komplekse verden omkring cybersikkerhed – og jeg kan garantere, at artiklerne i rapporten giver stof til eftertanke.

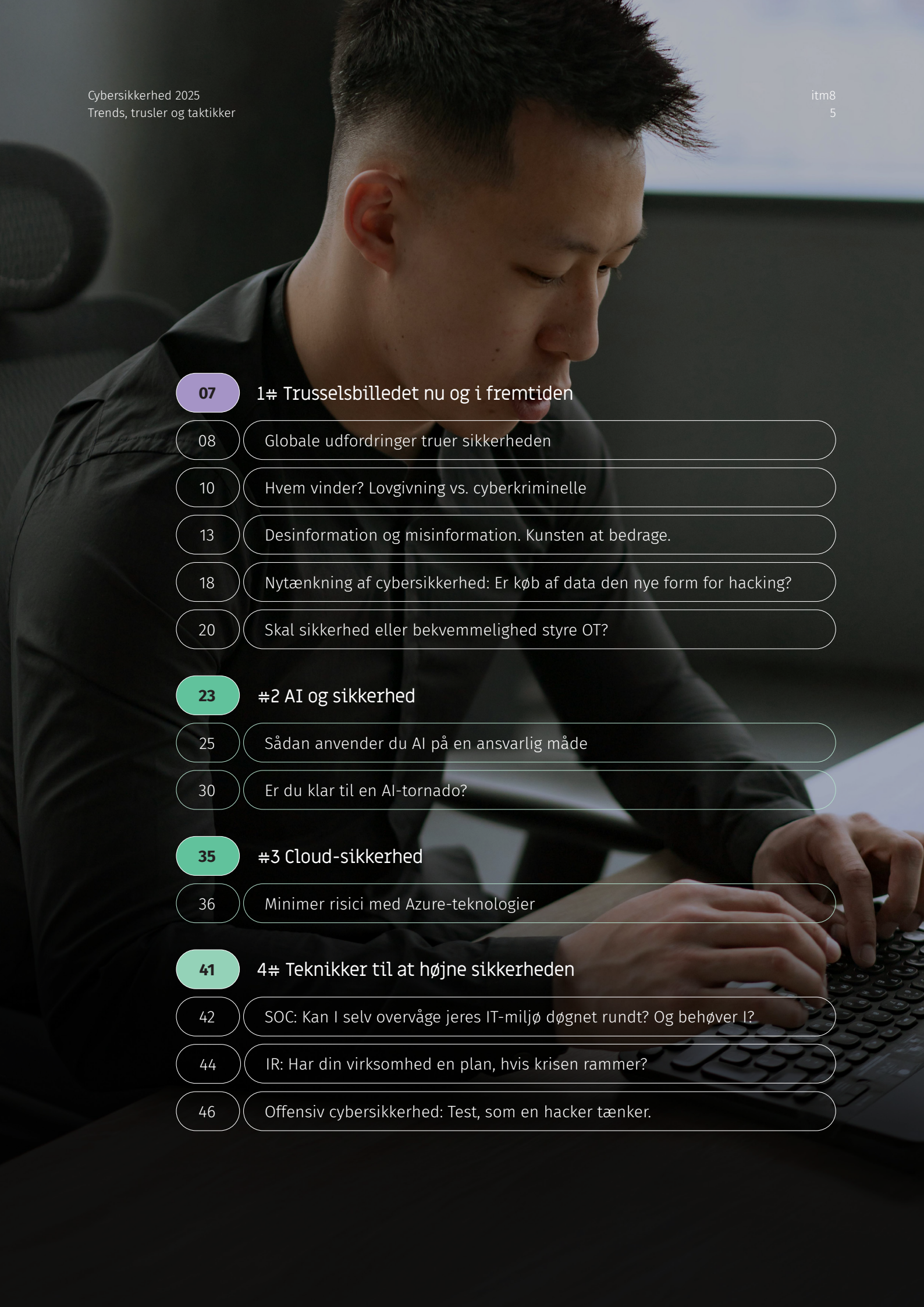
I rapporten kan du dykke ned i forskellige emner relateret til cybersikkerhed. Du kan bl.a. andet læse om kunstig intelligens (AI), og hvordan denne teknologi kan ændre og endda forpurre cybersikkerheden. Ikke kun fra et lovgivningsmæssigt perspektiv, men også set med defensive og offensive øjne. Du kan bl.a. også læse om desinformation, trusselslandskabet i dag, cloud-sikkerhed og OT-sikkerhed. Og hvad dine taktikker til beskyttelse bør være.

Husk, cybersikkerhed er ikke kun en udgift – det er en investering i virksomhedens eksistensgrundlag og robusthed.

Jeg vil hermed ønske god læselyst.

Martin Kofoed
Partner & Chief Cyber Security Officer, itm8 Danmark

// Indhold



1

Trusselsbilledet nu og i fremtiden

I dette kapitel kan du glæde dig til at læse om cybertrusler

[Side 8-9] Globale udfordringer truer sikkerheden i Norden og vores måde at leve på. Virksomheder, myndigheder og enkeltpersoner er afhængige af digital infrastruktur. Men samtidig står vi overfor voksende trusler fra cyberangreb. Bliv klogere på, hvilke proaktive foranstaltninger henholdsvis virksomheder, myndigheder og stater bør tage for at styrke cybersikkerheden. *Læs artiklen af Nicklas Persson på side 8.*

[Side 10-11] Hvem vinder? Lovgivning vs. cyberkriminelle. Cybersikkerhed er et stigende fænomen og faktisk verdens tredje største økonomi. Men hvem driver egentlig udviklingen inden for cybersikkerhed – Lovgivning eller de kriminelle? *Det giver Martin Kofoed et bud på i artiklen på side 10.*

[Side 13-17] Desinformation og misinformation: Kunsten at bedrage. Mængden af misinformation og desinformation, der bliver spredt på sociale medier, traditionelle medier og via regeringsorganer er overvældende. Det skaber forvirring mellem sandhed og fakta. Men hvordan løser vi problemet om Zero Trust? *Læs Thomas Öbergs betragtninger på side 13.*

[Side 18-19] Er køb af data den nye form for hacking? Nytænkning af cybersikkerhed. Ikke alle trusler kommer fra mørke skikkelser. Nogle gange er den største trussel mod virksomhedens data lige for øjnene af dig – i bestyrelseslokalet. Man behøver nemlig ikke altid at hacke en virksomhed for at få fat i dens data. I nogle tilfælde kan man bare købe dem. *Læs betragtninger om den moderne og lovlige hackingmetode i artiklen med Niclas Hedam på side 18.*

[Side 20-21] Skal sikkerhed eller bekvemmelighed styre OT? Operational Technology (OT) spiller en central rolle i at overvåge og styre industrielle systemer og kritisk infrastruktur. Fra SCADA-systemer til PLC'er bruges OT til at sikre effektiv drift. Men truslerne vokser, og sikkerheden er på spil. *Læs artiklen på s. 20, hvor Jesper Højslev Madsen sætter fokus på, hvordan man bedst balancerer sikkerhed og driftseffektivitet.*

// INDFLYVNING TIL CYBERUDFORDRINGER

Globale udfordringer truer sikkerheden i Norden og vores måde at leve på

Nordiske virksomheder, myndigheder og enkeltpersoner, som er kendt for deres store afhængighed af digital infrastruktur, står overfor voksende trusler fra cyberangreb. De vigtigste tendenser og trusler omfatter ransomware, angreb på forsyningskæden og statssponsorerede aktiviteter.

Nicklas Persson
Executive Partner & Country Manager, itm8 Sverige.

Alle virksomheder kan blive ramt af cyberangreb. Men de kritiske sektorer som finans, energi og sundhed er især mål for ransomware-grupper. Angreb på forsyningskæden er stigende, og angribere udnytter sårbarheder hos tredjepartsleverandører til at bryde ind i større organisationer. Brancher, der er kritiske for den nationale sikkerhed, er samtidigt primære mål for spionage, især midt i geopolitiske spændinger, der driver statssponsorerede angreb.

Lovgivning, phishing og krige

Regeringerne i Norden investerer kraftigt i rammerne for cybersikkerhed, men der er stadig udfordringer. Beskyttelse af valgsikkerheden for at sikre demokratiske processer er en prioritet, især i lyset af desinformationskampagner fra udenlandske aktører. Kritisk infrastruktur, herunder nationale net, transportsystemer og offentlige tjenester, er under konstant trussel og kræver avanceret beskyttelse. Overholdelse af lovgivningen skal også styrkes, især med EU's GDPR og NIS2-direktiv, for at harmonisere standarder for cybersikkerhed i hele regionen.

Fra et individuelt perspektiv bliver borgerne i stigende grad udsat for phishing, identitetstyveri og desinformationskampagner. De største udfordringer er begrænset bevidsthed om nye trusler som deepfake-svindel og socialt bedrageri samt sårbarheder i digitale betalingssystemer, der er udsat for svindel.

Globalt set forværres udfordringerne med cybersikkerhed af begivenheder som krigen i Ukraine og Mellemøsten, der har optrappet cyberkrigen. Ruslands invasion har udløst en stigning i cyberangreb rettet mod Ukraine og dets allierede med afsmittende virkninger, der forstyrrer de globale cybernormer og påvirker de nordiske lande.

Cyberspionage af NATO-medlemmer

Cyberangreb på energinet, finansielle systemer og kommunikationsnetværk udført i stor skala har udvisket grænserne mellem statslige og ikke-statslige aktører. Det har gjort lande som Finland, Sverige og Danmark – der alle er NATO-medlemmer – til mere værdifulde mål for cyberspionage. Da Norden er stærkt afhængig af stabile energiforsyninger, påvirker cyberangreb på olie og gasinfrastruktur i Mellemøsten også den nordiske modstandskraft.

Stærkere cybersikkerhed

Ved at træffe proaktive foranstaltninger kan de nordiske lande styrke deres cybersikkerhed i et ustabilt globalt landskab, der er præget af konflikter og trusler i hastig udvikling:

- **Virksomheder** bør investere i sikkerhedsforanstaltninger i flere lag, f.eks. zerotrust-arkitektur og endpoint detection-systemer. De bør også gennemføre regelmæssige vurderinger af cyberrisici og styrke tredjeparts risikostyring.

- **Myndigheder** bør styrke offentlig-private partnerskaber for at opbygge et fælles cybersikkerhedsforsvar. Samt udvikle mekanismer til deling af efterretninger i realtid i Norden og blandt NATO's allierede.

- **Fra et statsligt perspektiv** er det vigtigt at styrke internationale aftaler for at etablere klare normer for cyberkrigsførelse. Samt at støtte den globale indsats for at bekæmpe cyberkriminelle netværk og fremme modstandsdygtige digitale økosystemer.

Når du læser denne rapport om cybersikkerhed, tager du allerede et vigtigt skridt mod at sikre de nødvendige forholdsregler.

Husk: Intet er statisk, når vi taler om cybersikkerhed – trusselsbilledet ændrer sig konstant.

// TRUSSELSBILLEDET

Hvem vinder? Lovgivning vs. cyberkriminelle

Når man læser både skandinaviske og internationale medier, kan man ikke undgå at bemærke, at fænomenet "cybersikkerhed" i stigende grad skaber overskrifter i nyhederne.

Martin Kofoed
Partner & Chief Cyber Security Officer, itm8 Danmark

Hvis det ikke handler om virksomheder, der bukker under for cyberangreb, eller meldinger om tab af følsomme data, er det annonceringer af nye lovkrav, direktiver og forordninger fra både EU og den danske stat. Dette kan lede til refleksionen: "Hvem driver egentlig udviklingen inden for cyber"?

Cyberkriminalitet er verdens[3.] største økonomi

Hvis vi kigger på den økonomi, der er forbundet med cyberangreb og cyberkriminalitet, er det massive midler, der er tale om. I 2023 udgav World Economic Forum en artikel ([1]), der angav, at hvis cyberkriminalitet var en nation, ville det være verdens 3. største økonomi kun overgået af Kina og USA's nationale økonomier.

Derudover kan vi kigge på udviklingen de senere år. Særligt fra midten af 2017, hvor vi blandt andet oplevede cyberangreb, der påvirkede Mærsk-koncernen og førte til et tab på mere end 300 millioner USD. Her kan man antage, at den økonomiske påvirkning er en væsentlig driver for fokus på området. Både for lovgiver og virksomheder, men i særdeleshed også for de kriminelle.

Øget trusselsvurdering

Siden krigen i Ukraine brød ud i 2022, har vi kunne observere en trusselsvurdering, som løbende er forøget. Dette til trods for, at Center for Cybersikkerhed siden

2016 har vurderet, at truslen for cyberkriminalitet og spionage er på et "meget højt" niveau, som er det højeste niveau, CFCS arbejder med.

Vi bliver altså løbende mindet om, at de kriminelle står og banker på, og at vi skal forberede os. Senest også på såkaldte destruktive angreb. Det er et udtryk for, at krigsførende nationer som eksempelvis Rusland har suppleret våbenarsenalet med "cybervåben".

På den anden side ser vi lovgiver – både på nationalt og internationalt niveau. Over de seneste år er der udgivet mere end 20 forskellige forordninger og direktiver på europæisk niveau. Alle sigter mod, at virksomheder og organisationer øger deres modenhed og modstandsdygtighed over for de digitale angreb. Cybersikkerhed er blevet en "license to operate" og i nogle tilfælde "license to exist".

NIS2-direktivet kræver dokumentation, træning og beredskabsplaner

Et eksempel er NIS2-direktivet, der i år implementeres i dansk lov. Som det foreskriver, skal aktører inden for kritisk og væsentlig infrastruktur – såsom sundhed, finans, tele, transport, energi og forsyning – kunne dokumentere, at de er klar til angreb.

Der skal blandt andet findes veldokumenterede og gennemafprøvede beredskabsplaner. Organisationen skal sikre relevant ledelsesinformation om risici forbundet med cybertruslen. Og det skal sikres, at både ledelse og medarbejdere er tilstrækkeligt trænede i "cyber". Dette er blot for at nævne nogle få elementer, der skal prioriteres et øget fokus på.

EU vs. de cyberkriminelle

Så hvor stiller det virksomhederne, og hvem driver egentlig udviklingen – staten/EU eller de kriminelle? Svaret ligger nok midt imellem.

Det er et konstant udviklingskapløb, og med mængden af sager og den massive økonomi der er forbundet med området, vil min personlige vurdering være, at det er de kriminelle, der driver udviklingen, mens os, der er eller potentielt bliver forurettet, halsende forsøger at følge med.

Nordiske virksomheder halter bagefter på sikkerhedsområdet

itm8's egne hackere og sikkerhedsstrategiske konsulenter er løbende ude og se på virksomheder. Det, de ser, er, at virksomheder og organisationer i overvejende grad er bagud.

De fleste virksomheder mangler den nødvendige modenhed til at imødegå trusler. Og der er lang vej igen, før de kan leve op til kravene i lovgivningen.

Hvis virksomheder vil være på forkant eller endda foran deres modstandere, er de nødt til at foretage investeringer og uddanne deres medarbejdere i cybersikkerhed. Det skal selvfølgelig ske på en afbalanceret måde og i overensstemmelse med virksomhedens risikovillighed – man kan hurtigt "købe sig fattig", når det gælder cybersikkerhed.

Men den pris og konsekvens man kan risikere at skulle møde, ser vi desværre bare alt for mange eksempler på. Og det kan de færreste tåle. For ikke alle er Mærsk.

[1] Cybersikkerheden skal strammes op i en tid med mange kriser | World Economic Forum (weforum.org)
[2] BNP-data for USA og Kina er baseret på rapporter fra Verdensbanken (2022). Det økonomiske omfang af cyberkriminalitet er estimeret ud fra en artikel fra World Economic Forum (2023) og Cybersecurity Intelligence.

// DESINFORMATION OG MISINFORMATION

Kunsten at bedrage

Misinformation, fejlinformation og desinformation flyder frit i vores digitale verden og kan blive en stor trussel i fremtiden for både virksomheder og samfund. Men hvordan skelner vi sandhed fra manipulation? Gennem samarbejde, gennemsigtighed og et nyt syn på tillid kan vi måske finde vejen til at bekæmpe løgnens kunst.

Thomas Öberg
CTM, Cyber Security, itm8 Sverige

Lad mig forklare, hvad misinformation egentlig er, før vi går i dybden med kunsten at bedrage:

- **Misinformation** er falsk information, men ikke skabt eller delt med henblik på at forårsage skade.
- **Fejlinformation** er baseret på fakta, men bruges uden for kontekst til at vildlede, skade eller manipulere.
- **Desinformation** er bevidst skabt for at vildlede, skade eller manipulere en person, en social gruppe, en organisation eller et land.[1]

De to primære faktorer, der adskiller forskellige former for desinformation, er hensigt og tilsløring (forvirring). Jeg mener dog, at der er en anden vigtig faktor, der skal tages i betragtning; den tilsigtede målgruppe.

- **Enkeltpersoner** kan være et mål, primært af økonomiske årsager med svigagtige hensigter.
- **Nationer** og dens offentlighed kan være målet for at påvirke meninger og så frø af usikkerhed.
- **Virksomheder** kan også være et mål, igen af økonomiske årsager, men i en anden skala.

Medmindre du har levet under en sten i det sidste årti, har du formentlig opdaget, at mængden af misinformation, der er blevet spredt på de sociale medier, gennem traditionelle medier og faktisk også via regeringsorganer, mildest talt været overvældende.

De fleste mennesker kan gennemskue det mest åbenlyse vrøvl, som teorien om at jorden er flad og andre lignende konspirationsteorier. Men det bliver stadig sværere, fordi nogle af historierne har udviklet sig til at indeholde en lille kerne af sandhed, som er blevet fordrejet for at fremme en bestemt fortælling.

[1] Kilde: CISA, Foreign Influence Operations and Disinformation

På et individuelt plan er virkningen ret begrænset, men når man anvender denne måde at arbejde på i større skala, kan virkningen faktisk være betydelig.

Forvirring i stor skala

Så hvem er dommer over sandheden? Er det regeringen, medierne, det videnskabelige samfund eller måske religion? Der kan argumenteres for og imod for hvert af disse tilfælde, men for at få noget ud af det er det vigtigt at forstå forskellen mellem begreberne **sandhed** og **fakta**.

Fakta er indiskutabelt, objektivt bekræftet og bevist gennem evidens. Sandhed er derimod en subjektiv beskrivelse af virkeligheden, som kan være baseret på fakta, overbevisninger, erfaringer eller andre faktorer, men den behøver ikke nødvendigvis at være logisk eller endda verificerbar. Baseret på dette rationale kan der ikke rigtig være en dommer over sandheden – og det er her, problemet ligger.

I takt med at offentlighedens tillid til regeringen, medierne og andre instanser er blevet mindre i de senere år, er det blevet sværere og mere tidskrævende at afgøre, hvilke oplysninger der er faktuelle, og hvilke der er nonsens. Det blev smerteligt tydeligt under den seneste pandemi og fortsatte med andre store begivenheder som f.eks. de igangværende krige i Ukraine og Israel. Så spørgsmålet, vi som samfund må stille os selv, er: Vil vi have et sandhedsministerium, der håndhæver en bestemt fortælling og dermed pålægger afvigende stemmer censur, eller er der en anden måde at gøre det på?

Fupnumre i virksomheder

Virksomheder har i årevis været udsat for desinformation på den ene eller anden måde, da de er mere lukrative

for organiserede trusselsaktører. Metoder som Business E-mail Compromise (BEC) og phishing er de facto standarden i dag, hvilket resulterer i økonomiske tab, produktionsforstyrrelser og informationslækager for blot at nævne nogle få konsekvenser.

Men en ny trussel truer i horisonten. En, der ikke bare er sværere at forstå, men også meget vanskelig at håndtere. Faktisk er denne trussel allerede til stede i et vist omfang, men endnu mørkere og mere uhyggelige skyer nærmer sig med foruroligende hast.

Tre casehistorier, der illustrerer, hvad vi har set indtil nu

 # 1. Produktfejl
Den kommercielle afdeling i en virksomhed var ikke i stand til at sælge et ellers populært produkt, som de selv fremstillede, fordi produktet efter sigende led af defekter, der kunne føre til katastrofale fejl. Der gik flere uger, før der blev foretaget en undersøgelse, da ingeniørafdelingen ikke kunne finde problemet. Det viste sig så, at selskabet havde været udsat for en desinformationskampagne. Flere interne og eksterne konti var blevet kompromitteret, hvilket førte til, at troværdige rygter blev spredt af folk med autoritet, der antydede problemer med det pågældende produkt. Virksomheden gik glip af flere forretningsmuligheder og led et betydeligt knæk i deres indtægtsstrøm.

 # 2. Påstand om brud på sikkerheden
En berygtet trusselsaktør offentliggjorde oplysninger om et virksomhedsbrud på deres darknet-lækageside, hvor de delte skærmbilleder af dokumenter og interne systemer. Nyheden om bruddet spredte sig hurtigt på sociale medier, da selskabet var associeret med højt profilerede kontrakter. Mainstream-nyhedsmedier bragte også historien, men den berørte virksomhed forblev tavs og hverken bekræftede eller benægtede bruddet. Tiden gik, og til sidst begyndte regeringen at stille spørgsmål, da selskabet faktisk arbejdede sammen med forskellige instanser både inden for retshåndhævelse og militæret. Grunden til, at selskabet ikke kommenterede bruddet, var, at deres kontrakter med de retshåndhævende myndigheder foreskrev, at de ikke måtte kommunikere med medierne under nogen omstændigheder. Bruddet viste sig til sidst at være falsk, men skaden var allerede sket.

 # 3. Kriminel pligtforsømmelse
En CISO fra en stor, global virksomhed blev ikke blot fyret, men også anklaget for kriminelle aktiviteter med formodet hensigt at stjæle og potentielt sælge virksomhedens fortrolige oplysninger. Det startede med, at 'en whitehat hacker' rapporterede en sårbarhed i virksomhedens hovedapplikation til CISO'en. Efter afsløringen af sårbarheden fik whitehat hackeren en belønning for at have handlet ansvarligt. Sårbarheden blev rapporteret opad i hierarkiet sammen med forslag til afhjælpende procedurer. Det var her, tingene blev værre: Kendskabet til sårbarheden blev offentliggjort, og bestyrelsen handlede på baggrund af dårlig information. Dette resulterede i en heksejagt.

Kan du stole på, at det er sandheden?
Nogle af disse historier er sande, og andre er ikke. Eller er de? Hvordan kan du stole på, at min sandhed er sandheden og intet andet end sandheden? Og selv hvis de alle er sande, er de så baseret på fakta eller en anden forestilling, der passer ind i min fortælling?

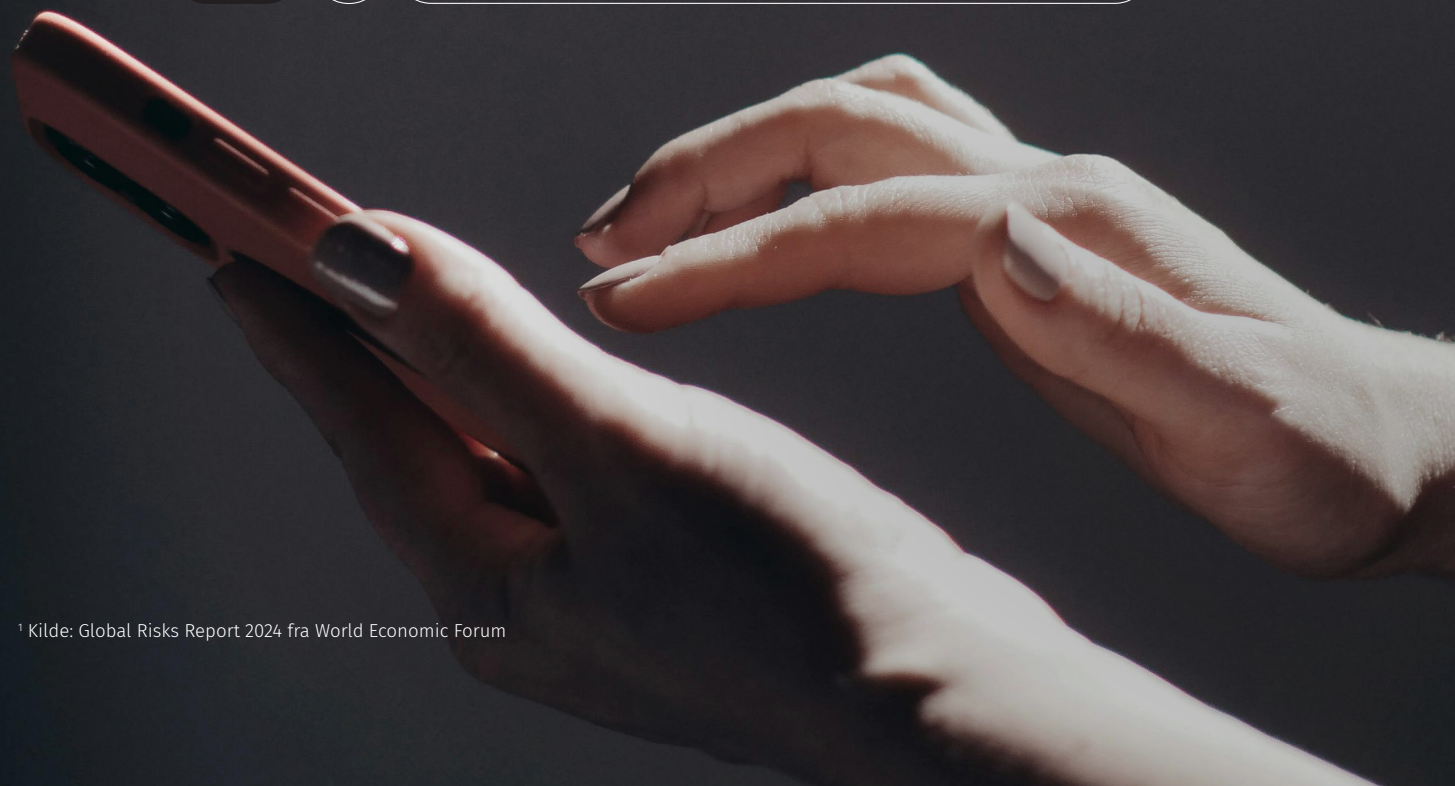
Uanset hvad er en virksomhed ikke kun en finansiel enhed, et kontor eller en produktionshal. Det er først og fremmest en gruppe mennesker med personligheder, følelser og alt det, der udgør et menneske. Og ligesom alle mennesker har deres fejl, har virksomhederne det også. Det gælder ikke kun medarbejdere i en virksomhed, men også partnere, leverandører, kunder og offentligheden. Så den logiske konklusion er, at hvis en person kan udsættes for og i sidste ende blive narret af desinformation, så kan en virksomhed også.

Desinformation er den største trussel
Desinformation bliver det sværeste emne at tackle fremover, ikke kun for enkeltpersoner, men også for nationer, virksomheder og andre organisationer. Men tag ikke blot *mit* ord for det; Global Risks Report 2024 fra World Economic Forum viser tydeligt, at et stort flertal af verdens ledere faktisk rangerer dette emne som den største trussel i de kommende år.

Det spørgsmål, vi alle må stille os selv, er, hvad vi skal gøre ved det. Personligt afskyr jeg enhver forestilling om en dommer over sandheden. På et samfundsmæssigt plan er det blevet forsøgt og har slået fejl ved adskillige lejligheder. Når alt kommer til alt, er der ingen ved deres fulde fem, der ønsker at være en del af et 1984-lignende samfund. Selvom en virksomhed i sig selv langt fra er et demokrati, tror jeg heller ikke, at en dommer over sandheden vil være mulig i den sammenhæng. Min begrundelse er, at det ikke er den interne tillid, der udgør det meste af vores hovedpine, men den eksterne og offentlige tillid. Og dermed nærmer vi os det, jeg anser for at være en væsentlig del af løsningen.

Desinformation bliver det sværeste emne at tackle fremover

1. **Misinformation og desinformation**
2. Ekstreme vejrbegivenheder
3. Samfundsmæssig polarisering
4. Cyber-usikkerhed
5. Væbnet konflikt mellem stater
6. Mangel på økonomiske muligheder
7. Inflation
8. Ufrivillig migration
9. Økonomisk nedtur
10. Forurening



[1] Kilde: Global Risks Report 2024 fra World Economic Forum

Sandheden er derude

I årevis har jeg, samt mine kollegaer inden for cybersikkerhed, understreget værdien af Zero Trust. Men det er vigtigt at forstå, at det ikke betyder, at der ikke er tillid at hente. Det betyder, at man begynder uden tillid og opbygger tillid baseret på flere uafhængige kilder med det mål at nå et punkt, hvor man opnår et acceptabelt og rimeligt niveau af tillid. Tiden fra rekognoscering til et kompromitteret miljø under hændelser bliver kortere for hvert år. Derfor er hastighed også en faktor, der skal tages i betragtning, når man udnytter Zero Trust.

Så kan vi håndtere misinformation på samme måde?

Zero truth

Forestil dig et spil, hvor du er i et rum med fire andre spillere, og hvor I hver især har et skjult kort. Der er ti kort i alt, hvoraf fem er grønne (gode), og fem er røde (dårlige). Alt er godt, indtil en ny spiller kommer ind i lokalet og påstår, at han har et grønt kort, samtidig med at han antyder, at du har et rødt kort. Det lægger op til følgende spørgsmål:

- Hvordan kan du se, hvilket kort den nye spiller har, eller hvilken som helst spiller for den sags skyld?
- Hvorfor antyder den nye spiller, at du har fået et rødt kort?
- Hvorfor føles det, som om alle i lokalet beskylder dig for noget?

I dette scenarie skal du forestille dig, at de andre spillere består af en kunde, en myndighed, en partner og et medlem af offentligheden, mens den nye spiller er en dårlig aktør. Det ville ikke gå godt for dig. Men hvad nu, hvis alle spillerne viste hinanden, hvilket kort de har i hånden, lige før den nye spiller kommer ind i lokalet? Og at det viser sig, at alle har et grønt kort. Hvad ville udfaldet af dette scenarie så være?

- Den nye spiller kan ikke have et grønt kort, da de alle fem allerede er taget.
- Alle ved allerede, at du har et grønt kort, så den nye spiller lyver tydeligvis.
- Alle i lokalet vil kigge anklagende på den nye spiller.

Den nye spiller bliver straks identificeret som en dårlig aktør, da spillerne på forhånd har været åbne over for hinanden og er blevet enige om en sandhed baseret på fakta.

Men hvordan oversætter vi dette spil til den virkelige verden?

Samarbejde er nøglen

Den første opgave er at identificere troværdige kilder og at etablere sig selv som en troværdig kilde. Det skal ske i flere netværk med et udvalg af aktører, der spænder over både private og offentlige interesser:

- Virksomheder i specifikke markedssegmenter
- Leverandører, partnere og sælgere af produkter og tjenester samt offentlige myndigheder, som måske ligger inden for specifikke forretningsområder
- Offentlige medieplatforme

En troværdig kilde skal være tilstrækkelig gennemsigtig og konsekvent over tid med en klar vilje til at samarbejde og dele viden med andre aktører.

Indrømmet, det kan være en udfordring i konkurrenceprægede markedssegmenter, men det er langt fra umuligt, og det behøver ikke nødvendigvis at påvirke forretningen, hvis det gøres rigtigt. Det samme kan siges om forskellige regeringsorganer, som normalt ikke ønsker at samarbejde. Men der er en ændring på vej, da det er blevet klart, at misinformation er et nationalt problem og skal håndteres som sådan.

Gevinst for virksomheder, myndigheder og samfundet

Når vi først har etableret et rimeligt niveau af tillid til flere kilder med en åben og gennemsigtig kommunikation, vil det være svært for dårlige aktører at få forfalskede oplysninger ind i vores netværk, da det straks vil blive afsløret. Det vil være en gevinst for virksomheder, offentlige myndigheder og vores samfund som helhed.

Jeg tror, at samarbejde i denne slags netværk er en af de vigtigste nøgler til succes i kampen mod den uundgåelige bølge af misinformation. Og hvis du ikke er overbevist endnu, vil jeg slutte af med følgende:

- Det er nemt at sprede misinformation, da det hverken kræver særlige færdigheder eller avancerede værktøjer.
- Udbyttet er potentielt gigantisk, da der stort set ikke er nogen omkostninger forbundet med en desinformationskampagne.
- Endelig er det desuden lovligt at have mindre evne til at tænkte kritisk, så det er stort set risikofrit at udføre disse handlinger.

Kombinationen af avanceret generativ AI og desinformationskampagner kan ved første øjekast se ud som en trussel uden nogen form for forsvarsmuligheder. Jeg håber dog, at en fælles indsats med fokus på fakta og fornuft vil sejre i sidste ende.

Desinformation er bevidst skabt for at vildlede, skade eller manipulere en person, en social gruppe, en organisation eller et land.

// NYTÆNKNING AF CYBERSIKKERHED

Er køb af data den nye form for hacking?

Den klassiske hacker-myte er ikke længere den eneste, der eksisterer.

Niclas Hedam
Cyber Security Advisor, itm8 Danmark

Når du tænker på cybersikkerhed, ser du måske den velkendte Hollywood-kliché for dig: en ensom hacker, der sidder bøjet over tastaturet i et mørkt rum, omgivet af skærme, der flimrer med grøn kode. Eller måske ser du et højteknologisk driftscenter, hvor et team af specialister hjælpeløst ser til, mens hackeren bryder ind i deres systemer – en firewall ad gangen.

Og selv om de billeder måske ikke er helt forkerte, er de kun en del af historien. Som tekniske konsulenter bruger vi masser af tid på at beskytte netværk, lukke sårbarheder og styrke sikkerheden. Vores opgave er at sikre, at uvedkommende ikke kommer ind – uanset hvor dygtige, motiverede eller velfinansierede de måtte være.

Men udfordringen er, at ikke alle trusler kommer fra mørke skikkelser i svagt oplyste rum. Nogle gange er den største trussel for virksomhedens datasikkerhed lige for øjnene af os – i bestyrelseslokalet.

Ikke hacking, men køb

Det er her, strategiske konsulenter kommer ind i billedet. Mens tekniske konsulenter bygger mure og barrierer for at beskytte mod cyberangreb, arbejder strategiske konsulenter på at forhindre, at dine data slipper ud på lovlig vis. Ja, på lovlig vis.

Man behøver nemlig ikke altid at hacke en virksomhed for at få fat i dens data. I nogle tilfælde kan man bare købe dem.

Lovlige læk af data

Der kan være tale om "lovlige læk", hvor data kan ende i hænderne på en helt ny – og potentielt meget interesseret – ejer gennem helt legitime kanaler.

Det er ikke datalækager i traditionel forstand, hvor oplysninger slipper ud gennem et hul i en firewall. Nej, disse "læk" sker gennem salg, fusioner, partnerskaber eller endda outsourcede serviceaftaler.

Tænk over det: Hver gang du indgår en aftale med en leverandør eller samarbejdspartner, er dine forretningsdata – markedsindsigter, kundeoplysninger, konkurrencemæssige oplysninger – på spil. Disse interaktioner kan åbne døren til din virksomheds hemmeligheder, uden at der bliver knækket nogen som helst form for kode.

Man behøver nemlig ikke altid at hacke en virksomhed for at få fat i dens data. I nogle tilfælde kan man bare *købe* dem. På lovlig vis.

Beskyt data uden for firewallen

Strategiske konsulenter arbejder for at forhindre, at den slags læk sker. De fokuserer på compliance, kontrakter og datadelingspolitikker, der styrer, hvem der har adgang til hvilke oplysninger – og hvor meget de kan gøre med dem.

De beskytter ikke kun dine data mod uautoriserede hackere, men også mod autoriserede. Og du kan roligt regne med, at de "autoriserede" datajægere kan være lige så udspekulerede som de mørkklædte hackere.

23andMe-sagen: Pionerer inden for DNA-test

Tag for eksempel 23andMe. Som en af pionererne inden for DNA-test til private ligger 23andMe inde med en guldgrube af følsomme og meget personlige genetiske data.

Med millioner af kunder, der deler deres DNA for at få indsigt i deres ophav, sundhedsrisici og genetiske træk, er 23andMe nødt til at opretholde strenge sikkerhedsforanstaltninger for at beskytte disse data mod nysgerrige blikke.

Men nu kommer det afgørende: Selv om 23andMe måske er gode til at holde hackere ude (det var de faktisk ikke – de blev hacket i 2024 og gav endda brugerne skylden for det), står de over for en anden risiko – hvad sker der, hvis de får økonomiske problemer?

I øjeblikket har 23andMe svært ved at skabe overskud og ville kunne risikere at gå konkurs. Hvis det kommer så vidt, kan en køber træde til og opkøbe hele virksomheden (og dens database) til en brøkdel af den oprindelige værdi. Og hvem kan den køber være?

Forestil dig et forsikringsselskab, som gerne vil forbedre sine risikovurderinger, og som køber 23andMe billigt.

Erfaringer fra RadioShacks databasesalg

Og det er ikke bare et tankeeksperiment. Tilfælde fra den virkelige verden har vist, at kundedata kan være kronjuvelen i opkøb – nogle gange lige så eksplicit, som hvis det var en post i balancen.

Tag f.eks. tilfældet med RadioShack. RadioShack, som engang var en velkendt elektronikforhandler, havde økonomiske problemer og endte med at gå konkurs i 2015. Under afviklingsprocessen viste det sig, at et af RadioShacks mest værdifulde aktiver ikke var det resterende varelager eller varemærket – det var kundedatabasen.

I auktionen over RadioShacks aktiver var kundedatabasen udtrykkeligt en del af handlen. Den indeholdt personlige data om millioner af kunder, der havde handlet hos RadioShack, fra e-mailadresser og telefonnumre til transaktionshistorik.

De potentielle købere så denne database som en guldgrube for målrettet markedsføring, og det blev den primære motivation for de virksomheder, der overvejede et køb. Og det til trods for at RadioShack tidligere havde forsikret kunderne om, at de satte en ære i "ikke at sælge vores private mailingliste".

De strategiske dataaftalers rolle

RadioShack- og 23andMe-sagerne er perfekte eksempler på, hvorfor virksomheder har brug for strategiske konsulenter, der kan forudse og beskytte mod denne type risici.

Disse konsulenter hjælper virksomheder med at oprette dataaftaler, der sætter klare grænser for, hvordan kundedata kan bruges, også i tilfælde af salg eller konkurs. Uden disse beskyttelsesforanstaltninger kan en virksomheds mest følsomme aktiv – kundedata – blive solgt uden ret meget kontrol, så de nye ejere kan bruge dem på måder, som de oprindelige kunder aldrig havde forudset.

Disse cases illustrerer, hvorfor datastrategi ikke bare er "nice-to-have" men derimod afgørende for den etiske og langsigtede beskyttelse af kunderelationer og tillid.

Ved at udarbejde datapolitikker, der beskytter kundernes interesser, kan strategiske konsulenter hjælpe virksomheder med at undgå faldgruberne ved et uønsket salg af databasen – og sikre, at selv hvis virksomheden skifter hænder, forbliver kundedataene utilgængelige for en eventuel køber, der har planer om at udnytte dem.

Måske er den største risiko for din virksomhed ikke hackergrupper, der bryder ind i dine systemer, men andre virksomheder, der har til hensigt at købe og udnytte dine data?

// OT-SIKKERHED

Skal sikkerhed eller bekvemmelighed styre OT?

I mange OT-miljøer prioriteres drift og effektivitet over sikkerhed. Multifaktorautentificering fravælges, systemopdateringer udskydes, og gamle systemer holdes i live, fordi de "stadigvæk virker." Men bekvemmelighed har en pris.

Jesper Højslev Madsen
Lead Cybersecurity Strategist, Cyber Defence Center, itm8 Danmark

Når sikkerheden nedprioriteres, øges risikoen for cyberangreb, der kan lamme produktionen og true kritisk infrastruktur. Især med det øgede fokus på kritisk infrastruktur blusser debatten om OT atter op igen. Så hvordan balancerer vi sikkerhed og driftseffektivitet?

Hvad er Information Technology, Operational Technology & Internet of Things?

Det er vigtigt at holde tungen lige i munden, når vi planlægger og designer vores kritiske infrastruktur, industrielle miljøer eller produktionssystemer. Det kan være en svær balancegang både at opbygge og opretholde sikkerheden på tværs af IT, OT og IoT. Denne udfordring bliver ofte overset, selvom den kan have enorme økonomiske konsekvenser for virksomhederne.

Forskellene på IT, OT og IoT – helt kort

IT (Information Technology): Informations- og kommunikationsteknologi, som omfatter computere, netværk, software og systemer, der bruges til at behandle og lagre data i virksomheder og organisationer.

OT (Operational Technology): Driftsteknologi, der refererer til hardware og software, som overvåger og styrer industrielle systemer, processer og fysiske enheder, såsom SCADA-systemer (Supervisory Control And Data Acquisition) og PLC'er (Programmable Logic Controllers) i produktion og kritisk infrastruktur.

IoT (Internet of Things): Tingenes internet, hvor fysiske enheder (fx sensorer, smart home-enheder og andet) er forbundet til internettet for at indsamle og udveksle data.

Det kan være svært at kigge i krystalkuglen og forudsige fremtiden, når en virksomhed i sin spæde opstart skal planlægge, hvordan infrastrukturen på tværs af systemer skal hænge sammen – samtidig med at systemerne fortsat skal fungere optimalt.

Vores miljøer skal gerne være skalerbare og fleksible nok til, at vi kan tilføje eller fjerne komponenter over tid, uden at det går ud over sikkerheden. Desværre ser vi ofte, at skellet mellem brugerne i deres daglige drift af f.eks. SCADA-systemer og ledelsen fører til, at man vælger ikke at implementere eksempelvis multifaktorautentificering for ikke at besværliggøre medarbejdernes hverdag. Dette skaber en markant sikkerhedsrisiko.

En voksende trussel

Senest har Center for Cybersikkerhed d. 22. januar 2025 vurderet truslen mod den danske vandsektor som MEGET HØJ[1]. De skriver:

"Truslen udspringer primært fra ransomware-aktører, der krypterer IT-systemer og data med henblik på at afpresse ofre for løsesummer."

I deres publikation understreges det yderligere:

"Som følge af den globale sikkerhedspolitiske situation står Danmark over for et mere sammensat trusselsbillede end i mange år. Det, der foregår i den fysiske verden, smitter også af på cyberdomænet, og den danske vandsektor står derfor, ligesom mange andre dele af det danske samfund, over for et dynamisk trusselslandskab."

Selvom denne beskrivelse fokuserer på den danske vandsektor, er der ingen tvivl om, at alle danske virksomheder med eksponeret OT – helt eller delvist – bør tage den aktuelle trussel alvorligt.

Hvad kan vi gøre

Hvilke forbehold bør vi tage, og hvilke grundige overvejelser kræver det, når vi sidder med et eksisterende miljø, hvor vi ikke har mulighed for at starte forfra?

Det handler, som så ofte før, om at styrke den eksisterende løsning først. At danne sig et overblik, vurdere sin risiko og afgøre, hvor risikovillig man som virksomhed er. I virkeligheden adskiller det sig ikke meget fra generelle sikkerhedsdiscipliner som backup-strategier – det er et spørgsmål om at "spise elefanten en bid ad gangen," som man siger.

Udfordringerne i OT-miljøer er dog ekstra komplekse af flere årsager. Det kan blandt andet være:

- Leverandørejede systemer, hvor virksomheder ikke har fuld kontrol over sikkerhedsopdateringer eller adgange.
- Driftskritiske systemer, der kører på operativsystemer, som for længst har mistet support og opdateringer.
- Manglende dokumentation og uklare ansvarsfordelinger.

Ved at have en systematisk tilgang til OT-sikkerhed kan virksomheder reducere risikoen og øge modstandsdygtigheden over for cybertrusler. Det kræver en kombination af tekniske løsninger, organisatoriske tiltag og et tæt samarbejde med leverandører og interessenter. Selvom udfordringerne er komplekse, er en struktureret indsats nøglen til at beskytte sig selv imod eksterne trusler.

[1] Kilde: https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/vandsektoren/

2

AI og sikkerhed

I dette kapitel kan du glæde dig til at læse om:

[Side 25-30] Sådan anvender du AI ansvarligt. Interessen og investeringen i AI stiger. Men hvilken betydning har det for cybersikkerheden? Få bedste praksis og overvejelser, forstå AI's potentielle faldgruber, hvad AI-loven indebærer, og indsigt i hvordan vejen frem ser ud. *Læs artiklen af Shadi Domat, Janeli Sula og Hannes Edström på side 25.*

[Side 30-33] Er du klar til en AI-tornado? Det stormer udenfor. Er det en normal storm eller en AI-tornado, der er parat til at ødelægge alt, hvad vi kender til? Bliv klogere på de største trusler, og hvad du som organisation bør prioritere at beskytte. *Læs artiklen af Rikard Burman på side 30.*

// AI, SIKKERHED OG COMPLIANCE

Sådan anvender du AI på en ansvarlig måde

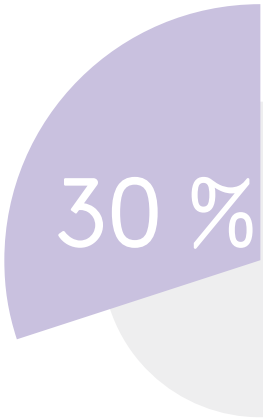
2024 har markeret et vendepunkt for, hvordan vi opfatter og anvender AI. Det seneste år har budt på øget interesse for generativ AI og en stigning i investeringerne.

Shadi Domat, Janeli Sula, Hannes Edström
Management Consultants, Governance, Risk Management & Compliance, itm8 Sverige

Gartner forudsiger, at 30 % af de generative AI-initiativer vil blive opgivet efter proof-of-concept, hvilket understreger behovet for en robust tilgang, der er baseret på datakvalitet. Fremover vil fokus ikke kun være på at udvikle AI-løsninger, men på at gøre det med en forståelse for deres etiske, operationelle og strategiske konsekvenser.

Når organisationer forsøger at navigere i direktiver og forordninger som NIS2, CER, DORA og AI-loven, er spørgsmålet ikke bare, hvordan man udnytter AI, men også hvordan man gør det på en ansvarlig måde.

Lad os nu udforske det neurale netværk i din organisations fremtid.



af de generative AI-initiativer vil blive opgivet efter proof-of-concept.

Mandatet til at kende dine data

Ethvert AI-initiativs succes begynder med en omfattende forståelse af de data, det bygger på. Selv om generativ AI er revolutionerende, er det grundlæggende en transformation af allerede eksisterende information. Det betyder, at kvaliteten af outputtet er direkte proportional med kvaliteten af inputtet. Inkonsekvent, forældede eller modstridende data kan føre til fejlbehæftede resultater, der underminerer beslutningstagningen og driftseffektiviteten.

Vi kan allerede se, at organisationer, der ikke foretager en grundig opgørelse af deres informationsaktiver, forlader AI-skibet på grund af kritiske problemer, der opstår under implementering og tilpasning.

Nogle af de tiltag, som organisationer bør have fokus på – men som de oftest ikke har – er:

- **Identificering af vigtig data (Key Information Assets):** Udpegning af de mest kritiske data, uanset om det er proprietære datasæt, kundeoplysninger eller tredjeparts datafeeds.
- **Kortlægning af datakilder:** Forstå, hvor dataene stammer fra, hvordan de opbevares, og hvordan de flyder i organisationen.
- **Vurdering af dataintegritet:** Sikre, at dataene er nøjagtige, komplette og pålidelige for at bevare troværdigheden, når de indføres i AI-systemer.
- **Håndtering af rettigheder og tilladelser:** Sikre, at kritiske og fortrolige dokumenter eller oplysninger aldrig føres ind i det neurale netværks tomrum.

Nogle vil måske genkende disse nødvendige trin fra arbejdet med standarder inden for informations-sikkerhed, og det er med rette. Ligesom når man arbejder med informationssikkerhed, er det at tage strategisk kontrol over sin organisations information og data også et fundament, når vi taler om AI-governance.

Bedste praksis og overvejelser

Når din organisation har forstået sine data, er det næste skridt at sikre, at implementeringen af AI er baseret på sikkerhed, etik og driftseffektivitet. Selvom AI-systemer lover hidtil uset produktivitet og innovation, følger der et betydeligt ansvar:

- **Databeskyttelse og compliance:** Overholdelse af databeskyttelsesregler, såsom GDPR, er ikke til forhandling. Det betyder anonymisering af persondata og anvendelse af robuste modeller inden for data governance for at undgå overtrædelser og bøder for manglende overholdelse.

- **Overvejelser om træningsdata:** AI-modeller, der er trænet på bias eller ufuldstændige data, kan fastholde eller forstærke eksisterende bias. Derfor skal dataudvælgelsen ske med gennemsigtighed og overblik for at mindske potentielle risici.

- **Uddannelse og bevidstgørelse af medarbejdere:** Det er afgørende at uddanne medarbejderne i, hvordan de skal interagere med AI-systemer og forstå deres begrænsninger. Det hjælper med at forhindre overdreven afhængighed af AI og fremmer et samarbejdsmiljø, hvor menneskeligt tilsyn supplerer de teknologiske muligheder.

I et stykke tid har teknologi ikke kun været et anliggende for IT-afdelingen, og tilføjelsen af AI gør dette endnu mere tydeligt. AI kræver en mangefacetteret tilgang, der tager højde for lovgivning, etik, mennesker og teknologi. Så lad være med at presse din IT-chef til at slå Copilot til, før du er godt forberedt.

AI's potentielle faldgruber

AI's transformerende kraft er forbundet med betydelige risici. Beslutningstagere skal være opmærksomme på de potentielle faldgruber ved implementering af AI:

- **Sikkerhedstrusler:** Implementering af AI i din organisation, uanset om det er et internt system eller et tredjepartssystem, kan åbne for nye og muligvis ukendte angrebsvektorer, som du er nødt til at tage højde for.

- **GDPR og juridiske konsekvenser:** I øjeblikket er det status quo blandt AI-udviklere, at jo større modellen er, jo bedre er den. Dette medfører dog yderligere risici i forbindelse med persondata. Mange AI-modeller, især store sprogmodeller, kræver en masse data for at forbedre deres nøjagtighed. Men den kompleksitet, der er forbundet med disse modeller, er de principper, der er kernen i GDPR, såsom retten til at blive glemt og dataminimering for blot at nævne nogle få.

- **Bias og diskrimination:** AI-modeller afspejler de data, de er trænet på. Hvis disse data er biased, vil modellens output også være biased, hvilket fører til beslutninger, der kan være diskriminerende eller uetiske.

Hypen og begejstringen omkring generativ AI lever stadig i bedste velgående, men det er vigtigt at bevare en sund skepsis. Med det mener vi, at man skal holde forventningerne til AI realistiske. Selv om det kan løse mange problemer og forbedre effektiviteten, er det ikke en løsning på alt, men snarere en funktion blandt andre.

Det, der virkelig betyder noget, er resultatet. Vil det gøre processen hurtigere, billigere eller mere præcis? Løser vi reelle problemer, eller falder vi bare for hypen? Det er vigtigt at identificere din organisations behov, de problemer, du vil løse med AI, og om det overhovedet er muligt.

Etablerede standarder er nøglen til succes

I takt med at implementeringen af AI bliver mere og mere kompleks, kan nøglen til succes være at udnytte allerede etablerede standarder og retningslinjer.

Blandt al den støj, der har været omkring AI i de sidste to år, har der været en betydelig udvikling af AI-governance i løbet af 2024. Der findes veletablerede standarder, der fortsat fungerer som pålidelige vejledninger til styring af data og AI, herunder ISO27001.

Der er også nye modeller og ny lovgivning, som aktivt tager højde for de komplicerede forhold i AI-systemer, der ikke er omfattet af traditionelle IT-standarder som AI Act og ISO42001.

AI kræver en mangefacetteret tilgang, der tager højde for lovgivning, etik, mennesker og teknologi. Så pres ikke din IT-chef til at slå Copilot til, før du er godt forberedt.

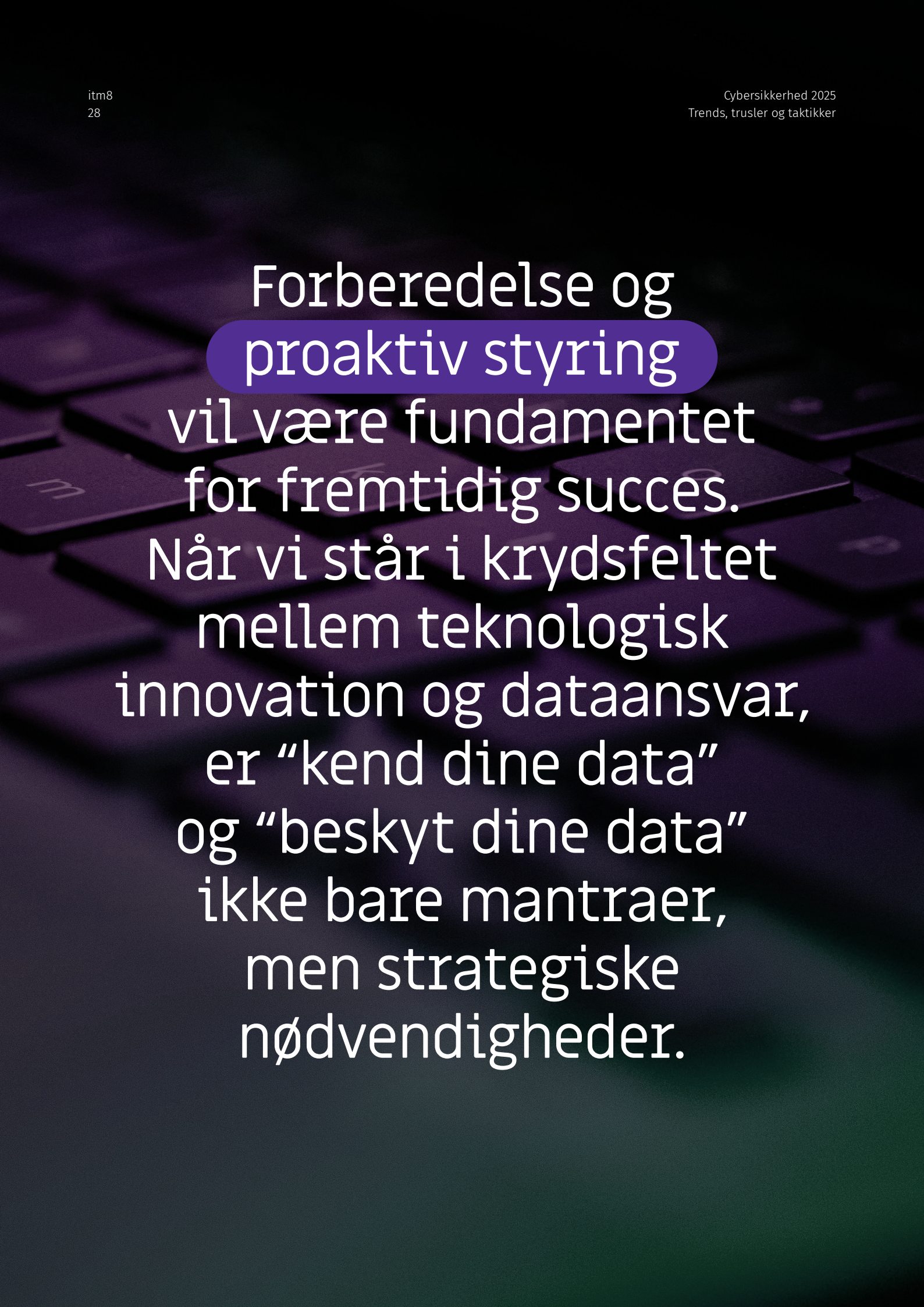
Lov om kunstig intelligens

Den 1. august 2024 trådte AI-loven i kraft, den første af sin slags inden for AI. Loven indfører en firedelt risikobaseret model for AI-systemer: forbudte systemer, højrisikosystemer, systemer med begrænset risiko og systemer uden risiko – og med særlige overvejelser i forhold til generelle AI-systemer som ChatGPT.

Mens hovedparten af loven medfører flere forpligtelser for udbydere af AI-systemer, er deployers (brugere af AI-systemer i en professionel sammenhæng) også underlagt nogle forpligtelser i henhold til loven, afhængigt af risikoniveauet for de AI-systemer, der bliver brugt i organisationen.

Nogle af forpligtelserne i henhold til loven for en deployer inkluderer at sikre AI-kendskab blandt de interessenter, der arbejder med AI-systemerne, samt sikre overholdelse af privatlivsregler som GDPR i forbindelse med brugen af AI.

Mens de fleste organisationer, der ønsker at bruge AI, vil blive betragtet som brugere af generelle, begrænsede eller ikke-risikobetonede AI-systemer, betyder det ikke, at det er krystalklart, at loven og dens udvikling ikke er noget, man skal følge med i. For eksempel er afklaringen af forpligtelser og ansvar ikke så klar i loven, hvor brugere i visse tilfælde kan blive udbydere af AI-systemet. Derfor bør kontrakter og licenser med tredjepartsleverandører af AI-systemer tjekkes grundigt for at forstå, hvor ansvaret ligger i situationer med manglende overholdelse, og for at sikre en klar ansvarsfordeling mellem alle interessenter, når der indgås aftaler.



Forberedelse og proaktiv styring vil være fundamentet for fremtidig succes. Når vi står i krydsfeltet mellem teknologisk innovation og dataansvar, er “kend dine data” og “beskyt dine data” ikke bare mantraer, men strategiske nødvendigheder.

Standardisering af AI-adoption, -governance og -sikkerhed

Den Internationale Standardiseringsorganisation (ISO) har også gjort fremskridt med at håndtere AI-governance. I 2024 er der udgivet nye AI-specifikke standarder og retningslinjer, f.eks. ISO42001 til udvikling af et AI Management System.

Standarden henvender sig til et bredt publikum bestående af brugere, udviklere og udbydere af produkter og tjenester, der anvender AI. Den giver også vejledning om de kontroller og kontrolmål, der skal implementeres i systemet, skræddersyet til problemer, der er specifikke for AI-systemer som f.eks:

- automatiseret beslutningstagning og databehandling
- manglende gennemsigtighed og forklaring
- AI-teknologiernes brede anvendelsesområde og anvendelighed
- de adfærdsændringer, der kan opstå på grund af deres kontinuerlige læringsevner

Det er vigtigt at præcisere, at selv om der findes modeller for udvikling af et AI Management System, fokuserer de ikke specifikt på AI-sikkerhed. For eksempel giver ISO42001 en struktur til håndtering af AI. Men for at opnå omfattende sikkerhed er det nødvendigt at integrere yderligere sikkerheds-standarder som ISO27001, hvilket AI-standarden opfordrer til.

Til håndtering af risici, der er unikke for AI, findes der nyere retningslinjer for AI-specifik risikostyring, men de omhandler ikke specifikt AI-sikkerhedsproblemer. I øjeblikket er specialiserede vejledninger skræddersyet til AI-sikkerhed, som ISO27090 og ISO27091, under udvikling og forventes at blive offentliggjort i løbet af 2025. Disse kommende vejledninger vil give organisationer et stærkere grundlag for at sikre grundig beskyttelse af både organisationen og deres AI-systemer.

Vejen frem

Mens fremskridtene inden for AI giver stærke værktøjer til effektivitet, innovation og forbedret cybersikkerhedsforsvar, kommer de også med en nedarvet risiko: den hastighed, hvormed nye angrebsvektorer og sårbarheder kan opstå.

AI's hurtige udvikling betyder, at ondsindede aktører kan udvikle og implementere trusler i et hidtil uset tempo, hvilket udfordrer de traditionelle sikkerhedsstandarders evne til at virke effektivt. Dette dynamiske miljø kræver et paradigmeskift i vores tilgang til sikkerhed. Reaktive strategier er ikke længere tilstrækkelige. Derimod er proaktive, AI-integrerede forsvarsmekanismer og løbende tilpasning afgørende.

Når vi omfavner AI's potentiale, må vi også forberede os på den ubarmhjertige hastighed, hvormed de tilknyttede risici udvikler sig, og sikre, at vores sikkerhedsprocedurer er lige så agile og intelligente som selve teknologien.

Fremover vil de organisationer, der klarer sig godt, være dem, der tager principperne om at kende og beskytte deres data til sig og integrerer dem dybt i AI-strategier. Forberedelse og proaktiv styring vil være fundamentet for fremtidig succes. Når vi står i krydsfeltet mellem teknologisk innovation og dataansvar, er "kend dine data" og "beskyt dine data" ikke bare mantraer, men strategiske nødvendigheder.

Beslutningstagere skal prioritere disse principper for at udnytte AI's potentiale effektivt og etisk. Ved at gøre det vil de ikke kun beskytte deres organisationer mod potentielle faldgruber, men også ansvarligt positionere sig selv i spidsen til den næste store digitale transformation.

// AI-UDVIKLINGEN

Er du klar til en AI-tornado?

Der opstår bange anelser, når det stormer vildt omkring os. Er det bare en normal storm, eller er der en AI-tornado på vej, som er parat til at ødelægge alt, hvad vi kender til?

Rikard Burman
Lead Architect, Cyber Security, itm8 Sverige

Når tornadoer klassificeres, vurderes de efter den skade, de kan forårsage. En F1-tornado kan sammenlignes med et dårligt udført phishing-angreb, mens en F5-tornado er beslægtet med et meget avanceret ondsindet AI-angreb. Et sådant angreb udnytter sårbarheder, der er ukendte for dig, dine leverandører eller udviklerne, og trænger ind i det forsvar, der skal sikre dine oplysninger.

Kan vi klassificere disse AI-drevne trusler som zero-days, eller kræver de en helt ny klassificering?

Vi kan ikke stoppe udviklingen

Jeg vil sige, at det er det trusselsbillede, vi nærmer os: et, hvor ondsindet AI kan angribe enhver tjeneste, applikation eller digital identitetsbeskyttelse. En verden, hvor hackere opererer uden regler eller juridiske begrænsninger, hvilket gør dem til ubarmhjertige modstandere.

Skal vi finde sølvpapirshattene frem? Eller er det virkelig det, der venter os? I mine ører lyder det som Skynet fra filmen Terminator, men med deepfakes, virtuelle kidnapninger og AI-drevet malware. Så er vi virkelig så langt fra en sådan virkelighed?

Den vigtigste pointe her er, at vi ikke kan stoppe udviklingen af AI. Den er her allerede. I stedet skal vi omfavne den og bruge den til at identificere og håndtere sårbarheder, vi ikke vidste eksisterede, og beskytte os selv mod "dårlig" AI.

Ubalance og udfordringer

Det er afgørende at holde sig opdateret om de nyeste trends, patches og sikkerhedskonfigurationer. Men mens vi forvalter begrænsede budgetter og ressourcer, behøver angribere kun at udnytte én sårbarhed for at få adgang. Denne ubalance får mange til at føle sig overvældede.

Det er den virkelighed, vi står over for i dag, og som vi fortsat vil stå over for i morgen. En verden, hvor nye CVE'er, zero-days-sårbarheder og menneskelige fejl skaber udfordringer på flere fronter. Selv avancerede beskyttelsessystemer mod trusler kommer nogle gange til kort og kræver manuel trusselsjagt for at opdage snigende, avancerede trusselsaktører, der bruger værktøjer i konstant udvikling.

Sikkerhed eller trussel?

En hændelse viser, hvordan sikkerhedsværktøjer i sig selv kan blive til en trussel. En defekt CrowdStrike-opdatering resulterede i, at Windows-systemerne fik en blå skærm og ikke kunne starte op, hvilket førte til et af de største IT-nedbrud i historien. IT-teams over hele verden var derfor nødsaget til at udføre manuelle rettelser for at genoprette driften.

Dette scenarie kan ske for hvilket som helst værktøj med højtprivilegeret software. Det kan være en tredjepart eller indbygget af leverandører, det kan være antivirus, beskyttelse- eller styringsværktøjer som Intune, Kaseya eller Configuration Manager. De kan alle bruges til at indsætte en ondsindet kode eller deaktivere sikkerhedsfunktioner. De samme værktøjer, der er designet til at beskytte os, kan vende sig mod os.

// En F1 tornado:
Et dårligt udført phishing-angreb.

// En F5 tornado:
Et meget avanceret ondsindet AI-angreb,
der udnytter ukendte sårbarheder.

De samme værktøjer, der er designet til at beskytte os, kan også vendes mod os, hvilket gør tillid, robust identitetsbeskyttelse og proaktive sikkerhedsforanstaltninger til hjørnestenen i at navigere i dagens skiftende trusselslandskab.

Identitetsbeskyttelse

Når man ser på nutidens trusselsbillede, står det klart, at organisationer ikke kun skal sikre deres eget miljø. De skal også sikre, at leverandørerne har kontrakter, der sikrer deres kunders miljø såvel som deres eget.

Sikkerhedsløsninger beskytter vores enheder, men tilbyder de avancerede muligheder for at opdage mistænkelige aktiviteter, der er rettet mod vores identiteter?

I dag er identitetsbeskyttelse hovedsageligt baseret på brugernavn + adgangskode + multifaktorautentificering (MFA). Men token-tyveri og Adversary-in-the-Middle (AitM)-angreb har gjort denne tilgang utilstrækkelig. Når man ser tilbage på 2024, har antallet af konti, der er blevet kompromitteret gennem disse angrebsvektorer, været overvældende.

Det er tydeligt, at autentificering uden adgangskode, FIDO2-nøgler og kompatibel enhedsteknologi er vejen frem for at forhindre identitetstyveri.

Den største trussel

Informationslandskabet udvikler sig. Men det gør hackerne også. Truslerne kan kategoriseres som flere typer, der hver især udgør sin egen trussel og løsning.

SOCIAL ENGINEERING

Social engineering er et bredt begreb, der omfatter forskellige aktiviteter. Disse angreb har til formål at udnytte menneskelig adfærd til at få adgang til information eller tjenester. Dette omfatter angreb som virtuel kidnapning, scareware, phishing, spear-phishing, whaling, smishing og vishing.

AI har forbedret disse angreb, hvilket gør dem endnu mere effektive til at udnytte menneskelige fejl og sværere for organisationer at forsvare sig imod.

Social engineering bruges primært til at få et indledende fodfæste, men kan også anvendes i senere faser af et sikkerhedsbrud, der involverer efterligning, forfalskede oplysninger eller Business E-mail Compromise (BEC). Med avanceret AI, der manipulerer video og stemme, er det ikke længere science fiction, men en reel trussel mod organisationer.

Sådan beskytter du dig mod **social engineering:**

- Træn alle brugere regelmæssigt i, hvad de kan forvente, og hvordan trusselsbilledet udvikler sig.
- Implementer adgangskontrol og “passwords” mellem medarbejderne for at verificere identiteter.

RANSOMWARE

Ransomware kan enten være det endelige mål for et angreb eller blot begyndelsen.

At tage systemer og informationer som gidsler i bytte for penge har været en udbredt trussel i mange år og er stadig et af de mest ødelæggende angreb, en organisation kan opleve.

Sådan beskytter du dig mod **ransomware**:

- Sørg for, at dine enheder er opdaterede med de nyeste patches.
- Sørg for, at sikkerhedsløsningerne er oppe at køre, og at de er konfigureret med fokus på sikkerhed.
- Sørg for, at backups er sikre og uforanderlige.

MALWARE
Malware eller ondsindet kodning er ganske enkelt software eller firmware, der udfører uautoriserede handlinger på de systemer, der er blevet angrebet.

Mens ransomware har sin egen kategori i denne artikel, er spyware, command and control og meget andet samlet i Malware-kategorien.

Sådan beskytter du dig mod **Malware:**

- Sørg for, at dine enheder er opdateret med de nyeste patches.
- Sørg for, at sikkerhedsløsningerne er oppe at køre, og at de er konfigureret med fokus på sikkerhed.

DATABRUD
I takt med at organisationer i stigende grad benytter sig af cloud-tjenester, er sårbarhederne i cloud-infrastrukturen blevet mere tydelige. Fejlkonfigurationer og utilstrækkelig adgangskontrol viser, hvor let cloud-tjenester kan misbruges, og hvordan simple fejl kan føre til uautoriseret adgang og brud på datasikkerheden.

For eksempel har usikre S3-bokse – en central lagerressource i Amazon – ført til betydelige datatab for store organisationer, simpelthen fordi grundlæggende sikkerhedsforanstaltninger ikke var implementeret.

Sådan beskytter du dig mod **databrud:**

- Sørg for, at produkter er konfigureret med sikkerhed for øje med private endpoints og ingen offentlig adgang som grundlæggende princip.
- Krypter følsomme data, og implementer netværkssegmentering.
- Sørg for, at adgang som minimum kræver multifaktorautentificering og adgangskontrol.

Hvad bør du som organisation prioritere at beskytte?

 # 1. Identiteter
Multifaktor med SMS og godkendelsesapps er simpelthen ikke godt nok længere. At arbejde "passwordless" med passkeys er vejen frem. Applikationer, der ikke understøtter multifaktorautentificering, bør tages ud af drift så hurtigt som muligt eller sikres på anden måde.

 # 2. Backup
Det er afgørende at sikre korrekt og beskyttet backup af alle virksomhedens oplysninger. Dette omfatter også behovet for at teste sikkerhedskopierne regelmæssigt. Ikke kun enkeltfiler – der bør også blive udført disaster recovery-tests hvert år på kritiske systemer.

 # 3. Opdater operativsystemer og applikationer
Sørg for, at systemer og apps er opdateret med de nyeste patches. Overvåg CVE-trusler i applikationer og operativsystemer.

 # 4. Offentlig adgang
Sørg for, at systemer ikke bliver gjort offentligt tilgængelige uden ordentlig beskyttelse. Når du bruger Microsoft Azure, skal du sikre dig, at der er en Cloud Adaption-model på plads, så du er beskyttet mod fejlkonfigurationer. VPN-løsninger bør udskiftes med mere robuste fjernadgangsløsninger uden risiko for eksponering af offentlige endpoints.

Og som altid:

Stol ikke på nogen, mistænk alle, og sæt spørgsmålstegn ved alt.

Cloud-sikkerhed og trusler

I dette kapitel kan du glæde dig til at læse om:

[Side 36-39] Minimer risikoen med Azure-teknologier. Det er mere kritisk end nogensinde før at sikre sin infrastruktur – både lokalt og i public cloud som Azure. Forstå SaaS, Defender for Cloud, Azure Arc. Og lær, hvordan du kan undgå eksponering af offentlige IP-adresser og garantere sikre forbindelsesmuligheder. *Læs artiklen med Kent Ekensteen på side 36.*

// CLOUD-SIKKERHED

Minimer risici med Azure-teknologier

I 2024 stod det klart, at public cloud tilbyder større effektivitet, fleksibilitet og sikkerhed, end private datacentre nogensinde vil kunne opnå. Og alligevel har vi aldrig set så meget aktivitet fra "the dark side". Sikring af infrastruktur – både lokalt og i public cloud som Azure — er mere kritisk end nogensinde.

Kent Ekensteen
Lead Architect Azure Infrastructure og Cloud Security, itm8 Sverige

Forstå SaaS' betydning

Den nemme anvendelse af SaaS-tjenester kombineret med en manglende forståelse af grundlæggende netværk og ansvarsfordeling giver ondsindede aktører optimale angrebsmuligheder. Det har aldrig været vigtigere at tage ejerskab over sine identiteter, data og infrastruktur, uanset hvor dine systemer er hostet.

Kunderne har tillid til, at du har fuld kontrol over din webshop, selv om du bruger en billig SaaS-løsning. Burde du ikke først undersøge, hvordan denne SaaS-tjeneste fungerer? Hvordan er dine data sikret? Og endnu vigtigere, hvordan kan du afvikle eller skifte løsning (med din data i behold), hvis det bliver nødvendigt?

Husk, at SaaS kan optræde i mange former. Det kan være en app service-ressource i dit Azure-abonnement eller en tjeneste, der er købt hos en lokal hosting-udbyder. Begge markedsføres muligvis som SaaS, men hvilken skal du vælge?

Pålidelighed, tilgængelighed og sikkerhed er vigtige overvejelser. Kan en lille, lokal hosting-udbyder f.eks. tilbyde samme oppetid og sikkerhed som Azure? Hvor vigtig er denne service for din virksomhed? Hvordan håndterer udbyderen sikkerhed?

En væsentlig fordel ved at bruge Azure er muligheden for at bruge SaaS inden for dit private netværk via private endpoints og sikkerhedsgrænser for netværket og på den måde undgå eksponering på internettet. Dette er en enestående funktion, som øger din sikkerhed. Men husk på: at købe SaaS fritager dig ikke for dit ansvar – eller risikoen for badwill.

Defender for Cloud

Det kan være svært at sikre miljøer – både i skyen og lokalt. I Azure har vi et praktisk værktøj, der hedder Defender for Cloud. Men hvad kan det gøre for dig? Og giver det værdi, hvis du primært arbejder med lokale datacentre? Læs videre og få svarene – måske bliver du overrasket over værktøjets evne til at forbedre dit miljø.

Defender for Cloud består af tre hovedkomponenter:

1. **Indsigt i kodepipeline:** Beskytter pipelinen fra kode til cloud og understøtter Azure DevOps, GitHub eller almindelig Infrastructure as Code.

2. **Cloud Security Posture Management (CSPM):** Giver handlingsorienteret indsigt for at forhindre brud.

3. **Cloud Workload Protection Platform (CWPP):** Giver specifik beskyttelse til forskellige arbejdsområder f.eks. servere, databaser og meget mere.

Når du skal sikre din infrastruktur, kræver det værktøjer som Azure Defender for Cloud og Azure Arc til at beskytte arbejdsopgaver og reducere sårbarheder.

Nogle af disse funktioner er gratis, så lad os starte med de gratis funktioner i Cloud Security Posture Management.

Noget af det første, du lægger mærke til, er dashboardet med en Secure Score, som mange af os kender fra andre Microsoft-portaler. Dette smarte lille værktøj opsummerer din sikkerhedsstatus baseret på Microsofts anbefalinger og hjælper dig med at prioritere dine forbedringer. Start med de "lavthængende frugter" og de højest vurderede scores, hvis du hurtigt vil forbedre den samlede score.

Styrket sikkerhed på tværs af multicloud-miljøer

Du vil også se understøttelse af multicloud-dækning. Defender for Cloud kan oprette forbindelse til Amazon Web Services (AWS) og Google Cloud og integrere dem i Secure Score og sikkerhedsanbefalinger.

En anden gratis, men værdifuld funktion er centraliseret styring af politikker, som giver dig mulighed for at definere betingelser på tværs af dit miljø og bruge indbyggede sikkerhedsstandarder. Disse politikker vil fortælle dig, hvor compliant du er, og hvilke ressourcer du skal sikre for at være compliant.

Alt i alt får du en masse sikkerhedsinformation om jeres Azure- eller multicloud-miljø bare ved at se på Defender for Cloud.

Ved at bruge den licenserede cloud-beskyttelse kan du beskytte forskellige arbejdsopgaver i Defender-løsningen. Bortset fra servere kan Regular Defender for Endpoint også beskytte:

- Native Azure-ressourcer som blob- og fillagring
- Databaser som Azure SQL og Cosmos DB
- Open source relationsdatabaser
- Containers
- App-tjenester
- Key vaults
- Mistænkelig aktivitet inden for ressourcehåndtering i Azure-portalen
- Unormale DNS-aktiviteter

Alt sammen inden for Defender for Cloud ved hjælp af Defender-produkter.

Lokal cloud-sikkerhed med Azure Arc

Mens den offentlige cloud vinder terræn for AI, ML og big data, er mange organisationer stadig afhængige af kritisk lokal infrastruktur. Hvis du foretrækker lokal drift, vil du måske stille følgende spørgsmål: "Hvad får jeg ud af det? Hvilke værktøjer kan jeg bruge til at forbedre sikkerheden for servere i vores lokale datacenter?

I Defender for Cloud kan du oprette forbindelse til andre cloud-udbydere som AWS eller Google, men du har også en anden mulighed: at bygge bro mellem dine lokale miljøer og Azure med noget, der hedder **Microsoft Azure Arc.**

Azure Arc er et gratis produkt, som forbinder dine lokale servere med Azure. Ved at installere en agent på dine fysiske eller virtuelle maskiner kan du få vist disse ressourcer i Azure-portalen. Det bedste ved det hele er, at de også integreres med Defender for Cloud, så du kan se sikkerhedsproblemer, patchniveauer og uregelmæssigheder i et enkelt dashboard. Du vil modtage handlingsrettede anbefalinger og en sikker score, som kan hjælpe dig med at øge og vedligeholde sikkerheden.

Azure Arc kan også bruges til at gennemgå dine SQL-servere, Kubernetes clusters, Hyper-V- og VMware-miljøer. Du kan faktisk bruge Azure-portalen til at udrulle VM'er i et lokalt VMware-miljø og få en samlet, overskuelig styring direkte fra Azure-portalen.

Undgå eksponering via offentlige VPN

Et stort problem for mange i dag er eksponeringen af offentlige IP-adresser. Fjendtlige angreb kan komme indefra – men du har den klare fordel, at du har mulighed for at kontrollere identiteter, enheder og data. Du bør selvfølgelig kun bruge private IP-adresser til dine tjenester og håndhæve private endpoints og deaktivere offentlig adgang for alle PaaS/SaaS.

Men hvad med alt det, der bliver eksponeret via en offentlig IP? Du kan være sikker på, at alle offentlige IP-adresser løbende bliver scannet for sårbarheder, så sørg for at holde dem på et minimum. Og brug altid sikkerhedsprodukter mellem de offentlige IP-adresser og jeres systemer.

Det er ingen overraskelse, at SSL VPN lokalt er et populært mål for de kriminelle. Det er stadig udbredt, det er offentligt tilgængeligt og er ofte bygget på x64-arkitektur med sårbarheder, der opstår næsten dagligt – ofte med store portåbninger indefra. Det er næsten som at hænge et netværkskabel ud ad vinduet.

Siden Covid-19 er vi mere end nogensinde vant til at arbejde hvor som helst. Men i 2024 nedlagde vi også flere SSL VPN'er end nogensinde før til fordel for andre teknologier. Du kan selvfølgelig tilføje MFA til din SSL VPN, men tænk på al den tid, der går, fra en hacker finder en sårbarhed, til du har opdateret din enhed – og din leverandør har leveret ny firmware.

Sikre forbindelsesmuligheder

Azure tilbyder flere alternativer til at reducere netværkseksponeringen – uden omdannelse af offentlige IP-adresser til dit interne netværk:

1. **Global sikker adgang – privat adgang:** Dette er ideelt til Entra-relaterede enheder og giver mulighed for detaljeret adgangskontrol baseret på destinationer, porte, protokoller og regler for betinget adgang. Det er en mere sikker afløser til traditionelle SSL VPN'er.

2. **Azure Virtual Desktop:** Denne giver en fuldt administreret Windows-klient i Azure. Eksterne brugere kan få sikker adgang til ressourcer uden at eksponere interne netværk. I hybride opsætninger kan virtuelle klienter oprette forbindelse til lokale netværk og samtidig drage fordel af funktioner som automatisk nedlukning for at spare på omkostningerne.

3. **Azure Bastion Host:** Muliggør sikker, browserbaseret adgang til VM'er i Azure eller lokale miljøer uden direkte netværksforbindelse. Funktioner som sessionsoptagelse giver sporbarhed og kontrol til en brøkdel af prisen for traditionelle løsninger.

Kort sagt:

- Brug Defender for Cloud og sikr dine lokale enheder på samme måde gennem Azure Arc.
- Udskift forældede SSL VPN'er med moderne løsninger som Entra Global Secure Access, Azure Virtual Desktop eller Bastion Host.

Ved at minimere din angrebsflade og udnytte Azures værktøjer kan du være et skridt foran nye trusler.

4

Teknikker til at højne sikkerheden

I dette kapitel kan du glæde dig til at læse om:

[Side 42-43] SOC: Kan I selv overvåge jeres IT-miljø døgnet rundt? Og behøver I? Det stigende trusselniveau kræver, at du ikke sover i timen. Men hvad stiller du op, hvis din virksomhed ikke er i besiddelse af de rette ressourcer? *Et Security Operations Center (SOC) kan være løsningen, og i denne artikel giver Erik Bandholm dig en indføring.*

[Side 44-45] IR: Har din virksomhed en plan, hvis krisen rammer? Et Incident Response (IR) team kan bedst beskrives som virksomhedens redningshold ved cyberangreb. På samme tid er det også en disciplin, der gør din virksomhed stærkere efter hver hændelse. Et professionelt IR-team reagerer hurtigt, identificerer skjulte trusler og sikrer, at din virksomhed lærer og forbedrer sig kontinuerligt. *Læs om Incident Response-disciplinen, og de 5 største fordele ved at have et professionelt IR-team tilknyttet, i artiklen af Simon Krogh Bjerre på side 44.*

[Side 46-49] Offensiv cybersikkerhed: Test, som en hacker tænker. Mange virksomheder føler sig overvældede af opgaven med at sikre sig mod cyberangreb. Ofte er IT-infrastrukturen forældet og flere år bagud i forhold til de metoder, som hackere bruger i dag. Med en Assume Breach-test kan I afdække skjulte svagheder og sikre, at I er på forkant – allerede før problemerne opstår. *Bliv klogere på testmetoden "assume breach". Læs artiklen af Christoffer Bech på side 46.*

// SECURITY OPERATIONS CENTER (SOC)

Kan I selv overvåge jeres IT-miljø døgnet rundt? Og behøver I?

Intet IT-miljø er 100 % sikkert 100 % af tiden. Hver måned opdages sikkerhedshuller i selv nogle af de bedste IT-systemer. Ja, faktisk blev der ifølge Verizons Data Breach Investigations Report fra 2024 analyseret 30.458[1] sikkerhedshuller i netop 2024. Derfor er det vigtigt altid at have et opdateret indblik og evner til at sætte ind, hvis det lykkes de cyberkriminelle at komme på indersiden af jeres systemer. Også på de tidspunkter, hvor den normale IT-afdeling er gået hjem.

Erik Bandholm
Partner, Cyber Security, Cyber Defence Center, itm8 Danmark

Et stigende trusselsniveau

Behovet for et øget sikkerhedsniveau er tydeligt. Fra 2022 til 2023 steg antallet af anmeldelser om cyberkriminalitet i Danmark hele 30 % - fra 27.038 anmeldelser til 35.254[2] – i følge Center for Cybersikkerhed.

De største virksomheder med store IT-afdelinger har ofte selv et cybersikkerhedsben – men for små og mellemstore virksomheder er situationen en ganske anden.

Hvad er løsningen, hvis man ikke selv har ressourcer in house?
IT-sikkerhed kræver oftest specialistviden. Derfor kan det ofte betale sig at kigge i retning af en partner, der har et professionelt setup specifikt designet til at holde sig up-to-date og overvåge virksomheders sikkerhedssystemer i døgndrift. Har du ikke ressourcerne, kan et Security Operations Center være løsningen.

Hvad er Security Operations Center (SOC)?
Security Operations Center, eller SOC i daglig tale, er et område – eller den enhed – der er ansvarlig for at overvåge og reagere på IT-sikkerhedshændelser. Det sker blandt andet ved at indsamle og analysere store mængder data fra forskellige sikkerhedskilder. Derfra er det muligt at identificere og reagere på potentielle trusler og cyberangreb.

Uden en SOC tilknyttet er du henvist til din egen reaktive respons på sikkerhedshændelser. Det vil sandsynligvis betyde, at du først opdager en hændelse, efter den er indtruffet. Det er både for langsomt og ineffektivt og betyder høj risiko for tab af data eller skader på virksomhedens omdømme.

Investeringen i et 24/7 sikkerhedssetup, der både overvåger de seneste trends, teknologier og sikkerhedshuller og virksomhedens egen infrastruktur, er et kæmpe ressourcetræk, hvis man ikke selv har de rigtige kompetenceprofiler ansat.

Business Email Compromise (BEC) - ét eksempel
Danske virksomheder udsættes løbende for Business Email Compromise (BEC)-angreb, hvor hackere får adgang til e-mailkonti – ofte i topledelsen – og begynder at sende tilsyneladende troværdige mails til

medarbejdere. SOC-teamet alarmeres i disse tilfælde af unormal login-adfærd og mistænkelig mailaktivitet og reagerer hurtigt, så angrebet kan stoppes, før skaden sker. Uden SOC-overvågning kan kompromitteringen forblive ubemærket i længere tid og føre til alvorlige sikkerhedsbrud. Dette er blot ét af mange eksempler på, hvordan en SOC kan være forskellen mellem hurtig inddæmning og omfattende konsekvenser.

4 gode grunde til at vælge en professionel sikkerhedspartner

At vælge en professionel sikkerhedspartner – itm8 eller andre – giver jer en række fordele frem for selv at skulle hyre et hold af sikkerhedseksperter:

1. **Sikkerhedskonsulenter, der hver dag arbejder med at forhindre angreb, holder sig skarpe**
   Præcis som en sportsudøver har sikkerhedseksperter ikke godt af at sidde for længe på bænken. At afværge et aktivt cyberangreb er ofte et spørgsmål om minutter – det er hektisk, krævende, kræver koordination og et roligt mindset. Og den slags skal tryktestes. Ofte. Ellers risikerer man, at kniven er sløv, når situationen er skarp.

2. **Del udgifterne for 24/7 overvågning med andre virksomheder**
   At overvåge IT-miljøer 24/7 er en ressourcetung opgave, hvis man har én person til ét miljø. Ved at have en SOC-partner med et professionelt monitoreringssetup slipper I for at betale hele regningen selv – og får de rigtige ressourcer stillet til rådighed det sekund, der er brug for dem.

3. **Rådgivning om og implementering af de seneste sikkerhedskrav**
   En professionel sikkerhedspartner lever af at overvåge og implementere de seneste teknologier og krav til overholdelse af lovgivningen. Derfor bliver du varslet og kan nemt få hjælp til implementeringen af de nyeste sikkerhedstiltag fra en partner, der kender dig og dit it-miljø.

4. **Proaktiv overvågning af trusselsbilledet**
   For at være klar til at modgå de seneste former for cyberangreb bruger professionelle sikkerhedspartnere meget tid på at holde sig opdateret om de seneste teknologier, hackergrupper og udviklinger inden for både cybersikkerhed og IT generelt.

Skal du investere i dit eget sikkerhedssetup eller finde en ekstern partner?

Om det kan betale sig for dig at samarbejde med en ekstern partner eller selv investere i et internt IT-sikkerhedssetup, afhænger af en række forhold. Kompleksiteten af jeres it-miljø, hvor kritisk jeres IT-systemer er for jeres daglige drift og mængden af systemer, der er tilgængelige online, spiller alle ind. Det vigtigste er, at I får taget aktivt stilling til, hvor godt I er beskyttet, hvor kritisk IT er for jeres daglige drift, og hvor risikovillige I er.

For i en verden, hvor systemer opdateres løbende, og nye sikkerhedshuller identificeres hver eneste dag, er det nødvendigt at forholde sig til, hvordan I hurtigst muligt får lukket ned, hvis cyberkriminelle får adgang til jeres systemer.

[1] Kilde: Verizon's 2024 Data Breach Investigations Report
[2] Kilde: Center for Cybersikkerhed, Cybertruslen mod Danmark, 2024

// INCIDENT RESPONSE

Har din virksomhed en plan, hvis krisen rammer?

Et Incident Response-team sikrer, at din virksomhed ikke kun kan håndtere cyberkriser, men efterfølgende også bliver bedre rustet til at forebygge fremtidige angreb. Spørgsmålet er: Har du og din virksomhed en plan for, hvad I gør, hvis krisen rammer?

Simon Krogh Bjerre
Security Advisor, Incident Responder, itm8 Danmark

Hvis du nogensinde har spekuleret over, hvad et Incident Response (IR) team egentlig laver, kan det bedst beskrives som virksomhedens redningshold ved cyberangreb. For mange er det nemt at forestille sig IR-teamet som en digital brandbil, der suser afsted for at slukke en akut ransomware-brand. Denne metafor holder, men kun til en vis grad. For bag kulisserne udfører et IR-team langt mere end blot brandslukning.

Hvad gør et Incident Response-team?

Kernen i Incident Response handler om hurtigt at identificere, begrænse og løse sikkerhedshændelser, så virksomheden kan vende tilbage til normal drift. Men arbejdet for incident response teamet slutter ikke der. Bag kulisserne fortsætter IR-processen som en kontinuerlig cyklus af analyse, forbedring og forberedelse.

Efter en hændelse: Læring og optimering

Når det akutte efterforskningsarbejde er afsluttet, og kunden er i gang med reetablering, foretager IR-teamet altid et "After-Action Review". Dette indebærer blandt andet:

- Analysere holdets håndtering af hændelsen.
- Identificere nye metoder benyttet af trusselsaktører.
- Udvikle konkrete forbedringer i processer og procedurer.

Derefter træner hele teamet i de nye løsninger, så de er klar til fremtidige incidents. Den konstante læring sikrer, at teamet kan reagere endnu hurtigere og mere effektivt næste gang.

Skjulte trusler: Når én hacker afslører en anden

Som analytiker på et IR-team beskæftiger man sig med nogle af de mest dybdegående tekniske aspekter af operativsystemer, filsystemers indre funktioner og meget mere. Den dybe indsigt kombineret med en analytisk og struktureret efterforskningsplan betyder, at man ofte finder ting, som ikke bliver opdaget af traditionelle sikkerhedsværktøjer. Lad mig komme med et eksempel:

En større landsdækkende kæde kontaktede Incident Response-teamet hos itm8 efter at have taget en aktør på fersk gerning, som var i gang med at køre malware på en server. Kunden tog den fornuftige beslutning at få undersøgt hændelsen for at finde måden, aktøren var kommet ind på, og om der var blevet stjålet data.

Aktøren i dette tilfælde havde været yderst larmende og havde efterladt en lang række af beviser. Dette er typisk, hvad man kan forvente fra f.eks. en ransomware aktør, der sætter hastighed af kompromittering over snilde.

Der, hvor efterforskningen tog en drejning, var, da teamet identificerede et stykke malware, der bruges til at gemme andre ondsindede processer dybt i operativsystemet, hvilket var stik modsat de metoder, som ellers var benyttet af aktøren.

Ved nærmere efterforskning opdagede IR-teamet, at malwaren var blevet placeret på systemet af en anden aktør flere år tidligere, end den kompromittering som teamet originalt efterforskede. Altså var én aktørs uagtsomhed resultat i, at vi opdagede, at virksomheden også tidligere var blevet kompromitteret. Det betød, at vi fik sparket to ondsindede aktører ud af infrastrukturen, og at virksomheden kom tilbage på rette spor.

Forebyggelse og forberedelse

Incident Response er ikke kun reaktivt – det er også proaktivt. IR-teams arbejder løbende på:

- At holde sig opdateret om nye metoder og teknikker, som trusselsaktører bruger.
- Udvikle og optimere egne værktøjer til hurtigere og mere præcis respons.
- Rådgive virksomheder om, hvordan de kan konfigurere deres infrastruktur til hurtigere at kunne efterforskes, hvis uheldet er ude.

Denne kontinuerlige forbedringsproces er en hjørnesten i at opbygge det høje tekniske niveau, det kræves at udføre korrekt incident response.

Det handler om at reagere hurtigt og rigtigt, hvis din virksomhed bliver ramt af et cyberangreb. Jo længere tid ondsindede hackere har adgang til dine systemer, jo større konsekvenser kan det have for din virksomhed. Et Incident Response-team hjælper din virksomhed tilbage til normal tilstand.

5 fordele ved et professionelt IR-team

Et dedikeret IR-team kan være en gamechanger for din virksomheds evne til at overkomme et cyberangreb.

Her er de vigtigste fordele:

#1 Hurtig reaktionstid

Med et IR-team har du en eskaleringsmulighed, der kan spare dig dyrebar tid, når angrebet rammer.

#2 Fjern usikkerheden

Du kan altid ringe og få sikkerhedsråd eller en vurdering fra en ekspert, hvis du er i tvivl, om din forretning er under angreb.

#3 Få klarlagt risici

Når man er ramt af et cyberangreb, er der uvisheder og spørgsmål, men med et specialiseret efterforskningshold har du grundlaget for at tage de rigtige valg og komme bedst muligt videre.

#4 Du kender dit team – og de kender dig

Du får et fast team af eksperter, der ikke laver andet end at arbejde med 'major cyber incident', og som kender din situation og forretning.

#5 24/7 beredskab

Aktiver dit beredskab døgnet rundt 365 dage om året, når din forretning kommer under angreb.

Det kan være en stor omkostning for mange virksomheder selv at have et Incident Response-team, der både altid er klar, men også trænet i relevante incidents.

Et dedikeret Incident Response-team er din partner, når cybertruslen rammer. Det er fundamentalt mere end blot en reaktiv løsning – det er et hold, der laver den nødvendige investering i udvikling og parathed, så din virksomhed kan komme bedst muligt gennem et cyberangreb.

// OFFENSIV CYBERSIKKERHED

Test, som en hacker tænker

"Jamen, de blev jo hjulpet indenfor. Så er det jo lidt snyd, er det ikke?" En sætning vi indimellem hører, når vi har gennemgået resultatet af en teknisk sikkerhedstest – en hacker-test udført som "Assume Breach".

Christoffer Bech
Director og leder af Technical Cyber Risk Advisory, itm8 Danmark

Når den IT-sikkerhedsansvarlige i en virksomhed står med en rapport, der er blodrød med angivelser af en mængde kritiske sårbarheder og fejlkonfigurationer, handler det om at finde en god forklaring overfor virksomhedsledelsen og andre interessenter, hvorfor det ser så skidt ud.

I denne artikel gennemgås vigtigheden af at lave en såkaldt Assume Breach-test – og der sættes lup under, hvorfor du er bagud, hvis I ikke tester sikkerhedsforanstaltninger, ud fra hvad en hacker (formentlig) tænker. Læs videre, hvis du er på udkig efter anbefalinger.

Assume Breach: Er det ikke bare snyd?

I en Assume Breach Test – som navnet antyder – tager man udgangspunkt i, at en hacker kan komme uset inden for muren. Det vil sige, at testen tager udgangspunkt i, at hackeren har fået udleveret en standard laptop eller virtuel maskine sammen med en ganske almindelig brugerkonto. Derfra søger hackeren at bevæge sig rundt i infrastrukturen og finde de krummer, der kan flytte hackeren over på andre enheder eller forøge dennes rettigheder via en lateral og horisontal bevægelse i infrastrukturen.

Målet vil ofte være fuld domæneovertagelse som eks. Domæne Administrator, muligheden for at udtrække følsomme data, ændre i data og lignende. Altså: Målet er at bryde fortroligheden, integriteten og/eller tilgængeligheden.

Men er det ikke snyd, når hackeren bliver hjulpet indenfor? Det korte svar er nej.

Det længere svar er, at vi gerne beviser, at man kan kompromittere en organisation via phishing e-mails, via fysisk kompromittering i en "Black Team"-test eller ved at anvende en ekstern sårbarhed.

Vi kan ikke garantere, at det på det konkrete tidspunkt lykkes inden for et rimeligt forbrug af konsulenttid. Hvis det var så enkelt, ville vi som samfund stå over for meget større udfordringer, end vi trods alt gør. Men er vi først inde, så vil jeg godt garantere, at vi lykkes. Før eller siden.

Supply Chain – den største cybertrussel

Når vi ser på trusselsudviklingen de senere år – særligt de store cyberangreb som Mærsk, SolarWinds-sagen, Coop i Sverige, Move-IT, Odense Universitets Hospital og mange flere – så er der særligt ét fællestræk: at cyberangreb i dag ofte sker via et Supply Chain-angreb.

Angreb via Supply Chain bør anses for den altoverskyggende største trussel, virksomheder i relation til IT- og cybersikkerhed skal håndtere. For principperne om "zero trust" og "trust but verify" lever i overvejende

del på et teoretisk niveau og alt for sjældent i praksis.

Så når en underleverandør bliver hacket og dermed skaffede angriberen en uhindret adgang ind bag borgmuren, er man ofte prisgivet, hvis man ikke har arbejdet struktureret for at imødegå denne trussel.

Det er den barske realitet, at vi ikke længere kan gemme os bag borgmure og voldgrave i forsvaret mod de cyberkriminelle. Hvis du ønsker et effektivt forsvar, både i forhold til økonomi og udbytte i form af læring, så bør du teste ud fra en Assume Breach-tilgang.

Det er den bedste metode til at få indsigt i de nødvendige, mitigerende handlinger og til at forberede sig på den dag, hvor det ikke er en venligsindet konsulent, men en ondsindet hacker, der kommer på besøg.

Flere år bagefter de cyberkriminelle

Opgaven med at forbedre sikkerheden kan for flere synes uoverskuelig. Særligt fordi mange virksomheder og organisationer er flere år bagefter de cyberkriminelle i forhold til evner og modenhed.

Mange anvender stadig infrastruktur, der blev etableret for et årti eller mere siden. Maskinen har måske fået lidt olie undervejs, når det knirkede, men ellers har det overvejende fået lov at passe sig selv. Også selv om der på labels står historiske navne som “NT”, “XP” og “2012r2”. Den løbende rengøring og vedligehold har været stærkt begrænset.

Cyber- og informationssikkerhed handler basalt set om at have styr på mennesker, processer og teknologier. De tre fokusområders formål er at beskytte fortroligheden, integriteten og tilgængelighed for data, systemer og services i eller understøttet af IT.

Det lyder jo umiddelbart enkelt. Ansæt de rette personer og uddan dem. Få styr på processer, procedurer og arbejdsinstruktioner, så man ved, hvem der gør hvad, hvordan og hvornår. Og anvend de relevante teknologier på den korrekte måde.

Fortrolighed, integritet og tilgængelighed

Der skal passes på data, systemer og services. Der skal holdes styr på fortroligheden, så kun de relevante personer og systemer har adgang. Dataintegriteten skal holdes intakt, så vi kan stole på, at indhold er korrekt. Og så skal der være tilgængelighed.

Servicen skal være oppe, så den kan understøtte funktionen. Tænk eksempelvis på MitID, som kan medføre omfattende konsekvenser for borgerne og erhvervslivet, hvis servicen er nede.

Det lyder jo egentlig simpelt nok, det der med at passe på data. Men hvad så med de tests, som både NIS2 og særligt DORA stiller krav om?

Hvordan tester vi evnen til at imødegå cyberangreb mest effektivt – også ud fra et økonomisk perspektiv? Og hvad sker der, hvis hackerne kommer ind i vores systemer? I disse tilfælde er alle de gode politikker nytteløse. En politik nedfældet på papir har aldrig stoppet en hacker.

Vi starter med at teste ud fra en hackers mindset. Den tankegang kan vi så bruge til at definere vores strategi, vores politikker og processer. Når vi kender det aktuelle niveau, kan vi lægge en strategi ud fra dette. Du kan ikke starte omvendt med strategien, hvis du ikke ved, hvor slemt det står til.

En politik nedfældet
på papir har **aldrig**
stoppet en hacker.

Antag det uundgåelige – test som en hacker arbejder

Når det kommer til at definere virksomhedens tekniske teststrategi, er det en klar anbefaling at arbejde modulbaseret frem for at køre det hele i én stor og dyr sikkerhedstest. Det involverer blandt andet følgende steps:

- Teknisk phishing test og awareness
- Assume Breach
- Test af Backup og Restore
- Test af kritiske applikationer

Penetrationstest og "hacking" er sjældent, som man ser det i amerikanske actionfilm. Det er i hvert fald ikke lige så nemt at hacke en virksomhed, som filmkulturen har det med at fremstille det. Det betyder dog ikke nødvendigvis, at der er tale om en høj modenhed.

Overvej scenariet: *En brandbombe eller Molotovcocktail kastes mod en husfacade. Skaden vil som udgangspunkt være begrænset, med mindre særligt uheldige omstændigheder er til stede. Samme brandbombe detoneres i sofaen i stuen. Her er en større brandskade nærmest uundgåelig, og risikoen for total nedbrænding er overhængende. Samme brandbombe, men forskellige steder for detonation.*

Ind skal de nok komme

Det er almindeligt kendt, at en stor del af cyberangreb starter via e-mail phishing. Men hvis e-mail phishing skal anvendes i et målrettet angreb, er der risiko for, at det slår fejl.

Der udsendes millioner af phishingmails på daglig basis. Blandt andet som del af opportunistiske angrebsforsøg via såkaldte "Initial Access Brokers". Organiserede grupper, der har gjort det til en sortbørsforretning at skaffe sig adgang til en hvilken som helst virksomhed eller organisation og så sælge denne adgang på det sorte marked.

Sagt med andre ord: Dét cyberangreb din virksomhed udsættes for, er højst sandsynligt ikke en del af et målrettet komplot. I var blot de uheldige, der var på det forkerte sted på det forkerte tidspunkt – og faldt i fælden.

Det er ikke ualmindeligt, at initial adgang er 9-12 måneder undervejs, før det egentlige angreb som eks. ransomware eller datatyveri og efterfølgende afpresning igangsættes.

Derfor bør I teste ud fra en antagelse om, at nogen kan komme ind ad hoveddøren – eller via et vindue på klem. Test og træning af medarbejderne i at spotte phishing e-mails er fortsat et vigtigt element. Men tag det som et selvstændigt modul, på samme måde som "hacker-testen" bør være det.

Tak, fordi du læste med.

Har du spørgsmål vedrørende cybersikkerhed, er du altid velkommen til at række ud til os.

+45 6916 0004
information@itm8.com
www.itm8.dk

En forbedret cybersikkerhed i dag holder hackerne ude i morgen. Læs mere om, hvordan vi kan styrke dit sikkerhedssetup.

https://itm8.dk/cyber-security

Vi bygger nutidens og fremtidens IT. Sammen.

itm8 er en førende nordeuropæisk IT-servicepartner med over 20 års erfaring i at hjælpe både offentlige og private organisationer med forretningskritisk IT. Vi er mere end 1.700 specialister, der tilbyder alt fra dag-til-dag IT-support og konsultation til avancerede løsninger inden for cybersikkerhed, cloud services og digital transformation.

Vores fokus er altid at levere høj kvalitet, pålidelig service og kompetent rådgivning, der hjælper vores kunder med at optimere forretningsprocesser og vækste i en digital verden. Som en 360 graders IT-partner sikrer vi, at vores kunder får dækket alle deres IT-behov.
Today. Tomorrow. Together.

itm8®

Sverige: +46 4059 2400 // Danmark: +45 6916 0004
information@itm8.com

www.itm8.se // **www.itm8.dk**