Lederens guide til NIS2

Du har ikke tid til å vente

Hva betyr det nye EU-direktivet for deg og hvordan kommer du i gang?

ATEA

INNHOLD

Thomas Tømmernes, konserndirektør for IT-sikkerhet i Atea

Nå er IT-sikkerhet ditt ansvar

Sikkerhet er ikke lenger noe IT-avdelingen bare fikser for deg. Det er et lederansvar. Det nye EU-direktivet, NIS2, krever at du som leder har god kontroll og styring. Du må kunne svare på hvor virksomheten er sårbar, hva du gjør for å redusere risiko – og hvordan du dokumenterer dette.

NIS2-direktivet, som ble innført i alle EU-land i oktober 2024, vil få store ringvirkninger her hjemme. Det er forventet at det norske regelverket vil oppdateres så snart som mulig, og allerede nå er mange virksomheter omfattet av regelverket fordi de leverer til EU-land.

Likevel viser ferske tall, fra vår egen sikkerhet-sundersøkelse, at mange fortsatt tror at NIS2-direktivet ikke angår dem. Direktivet er ment å beskytte kritisk infrastruktur og samfunnsviktige tjenester, og mange ser kanskje ikke sin rolle i dette. Andre forstår alvoret, men tenker at de har god tid.

Sannheten er at du ikke har tid til å vente, og at det nye regelverket vil gjelde de aller fleste virksomheter. Direkte eller indirekte.

Du må ha kontroll på verdikjeden din

NIS2-direktivet får nemlig konsekvenser også for virksomheter som ikke omfattes direkte. Leverer du til offentlig sektor, er du garantert berørt. Leverer du til noen, som leverer til noen, som defineres som en del av den kritiske infrastrukturen og samfunnsviktige tjenester i et EU- eller EØS-land, er du også berørt. Dette betyr at om du skal kunne levere dine tjenester i fremtiden, må du sørge for å etterleve NIS2-kravene.

«Det nye regelverket vil gjelde de aller fleste virksomheter. Direkte eller indirekte.»

> **«Om du skal kunne levere dine tjenester i fremtiden, må du sørge for å etterleve NIS2-kravene.»**

Det nye direktivet krever at du har kontroll på hele verdikjeden din. Du må ha robuste planer, prosesser og rutiner for å sikre at virksomheten din er forberedt dersom du utsettes for et cyberangrep.

Du kan få sikkerhetskrav fra kunder, leverandører og partnere du samarbeider med, og du bør stille tilsvarende krav til ditt økosystem. Din IT-sikkerhet er ikke sterkere enn ditt svakeste ledd, og du må vite hvor risikoen ligger.

Du risikerer å tape omdømme – og oppdrag

Kan du ikke dokumentere at du opererer i samsvar med NIS2-regelverket, kan dette føre til sanksjoner fra myndighetene, blant annet i form av bøter, stans av drift, offentlig kritikk, ordre om retting eller pålegg om opplæring i IT-sikkerhet.

Men enda verre er jo risikoen for omdømmetap eller tap av oppdrag, fordi du ikke har tatt IT-sikkerheten på alvor.

Denne guiden er laget for deg som er leder – for å gi overblikk og retning i en kompleks virkelighet. Den gir deg innblikk i hvordan NIS2-direktivet påvirker norske virksomheter, hvilke grep vi anbefaler, og hvordan du selv kan komme i gang – uavhengig av om du er leder i en offentlig virksomhet, en underleverandør eller et konsern.

> **«NIS2 er mer enn et direktiv. Det er en ny måte å tenke sikkerhet på.»**

Sammen med våre teknologipartnere gir vi deg våre beste sikkerhetsråd, om hvordan du kan gå fra usikkerhet til kontroll, fra å være reaktiv til å bli proaktiv.

NIS2 er mer enn et direktiv. Det er en ny måte å tenke sikkerhet på, og det starter med at du tar styring og ansvar. Du har ikke tid til å vente.

Thomas Tømmernes
Konserndirektør for IT-sikkerhet i Atea

NIS2-direktivet: Hva betyr det for deg?

NIS2 er en oppdatering av det opprinnelige NIS-direktivet (Network and Information Security Directive) fra 2016. Det er EUs mest omfattende regelverk for digital sikkerhet til dags dato, og målet er å sikre et jevnt og tilstrekkelig sikkerhetsnivå på tvers av medlemsland og sektorer, for både private og offentlige virksomheter.

NIS2 ble innført i alle EU-land i oktober 2024, og det er forventet at det norske regelverket vil oppdateres så snart som mulig. Allerede i dag er mange norske virksomheter som leverer til EU-land omfattet av regelverket.

Manglende samsvar med NIS2 kan medføre bøter, stans av drift, ordre om retting eller pålegg om bedre opplæring for ledelsen. Med NIS2 får styret og daglig leder et særskilt ansvar for å etterleve kravene.

På sikt vil de aller fleste norske virksomheter omfattes av direktivet, enten direkte – eller indirekte gjennom verdikjeden.

I første omgang har EU som mål å sikre kritisk infrastruktur innen energi, transport, vann- og matforsyning, romfart, helsevesen, offentlig administrasjon, digitale tjenester og finanssektoren.

Dette er de viktigste kravene i NIS2:

- God kontroll på beredskap, risikovurdering og hendelseshåndtering
- Tydelige regler for ansatte og god opplæring til ledelsen
- God kontroll på kryptering og tilgangsstyring
- Plikt til å rapportere alvorlige hendelser innen 24 timer
- Kontroll på sikkerheten i hele verdikjeden, ikke bare i egen organisasjon
- Måle effekt av sikkerhetstiltak og justere det som ikke fungerer
- Alltid kunne dokumentere hva du gjør og hvordan du tenker rundt sikkerhet

«Har du ikke kontroll på sikkerheten, har du heller ikke kontroll på fremtiden.»

Olof Eilertsson, jurist og forretningsutvikler for IT-sikkerhet i Atea-konsernet

Et varslet veiskille for IT-sikkerheten

Det nye EU-direktivet, NIS2, krever at virksomheter og myndigheter jobber tettere sammen for å beskytte kritisk infrastruktur. Dette får følger for mange norske virksomheter.

– Det handler ikke lenger bare om IT. Det handler om ledelse og ansvar, sier Thomas Tømmernes, konserndirektør for IT-sikkerhet i Atea.

Tenk deg en motorvei. På overflaten flyter trafikken som normalt. Varer transporteres, informasjon flyter, alt ser ut til å fungere. Men under overflaten skjer det noe. Kode og kontrakter, leveranser og beslutninger, kryper inn og ut av digitale systemer, som er tett sammenvevd. Ett hull, én åpen dør og hele kjeden kan stoppe opp.

Fem grep du som leder bør ta nå

1. **Få oversikt**
   Hvilke krav gjelder for din virksomhet, direkte eller indirekte?
2. **Plasser ansvaret**
   Sett sikkerhet på agendaen i ledergruppen
3. **Se på leverandørkjeden**
   Hvilke krav kommer fra dine kunder og hvilke må du stille til dine partnere?
4. **Bruk det du har**
   Har du aktivert to-faktor, tilgangsstyring og bevisstgjøring? Start der
5. **Dokumenter alt**
   Skriv ned vurderingene dine. Ikke bare hva du gjør – men hvorfor

Thomas Tømmernes, konserndirektør for IT-sikkerhet i Atea

Følgende sektorer berøres av NIS2

- Energi
- Transport
- Bank og finans
- Helse
- Drikkevann
- Avløpsvann
- Digital infrastruktur
- IKT-tjenester
- Offentlig forvaltning
- Romfartsvirksomhet

Følgende tilbydere berøres av NIS2

- Post - og kurertjenester
- Avfallshåndtering
- Produksjon og distribusjon av kjemikalier
- Matproduksjon
- Produsenter av medisinsk utstyr, IKT-utstyr, kjøretøy, elektronikk, maskiner, transportutstyr
- Tilbydere av digitale tjenester
- Forskning

– Dette er virkeligheten EU prøver å møte med det nye NIS2-direktivet. Mange tror at kravene ikke gjelder dem, men det gjør de i aller høyeste grad. Nå som fokuset er rettet mot hele verdikjedene, for å tette mulige sikkerhetshull, viser det seg at det er mange som bidrar til kritisk infrastruktur, enten direkte eller indirekte, sier han.

Hva er NIS2 og hva krever det av deg?

NIS2 er en oppdatering av det opprinnelige NIS-direktivet (Network and Information Security Directive) fra 2016. Det er EUs mest omfattende regelverk for digital sikkerhet til dags dato, og målet er å sikre et jevnt og tilstrekkelig sikkerhetsnivå på tvers av medlemsland og sektorer.

Den første versjonen av direktivet ga landene stort rom til å definere sikkerhetsnivå selv, mens NIS2 stiller langt strengere og mer konkrete krav. Det er forventet at det norske lovverket vil oppdateres med NIS2-kravene så fort det lar seg gjøre.

– Det EU gjør nå, er å definere et minstekrav for digital sikkerhet på tvers av landegrenser. Dette er ikke en veileder. Det er bunnplanken, sier Olof Eilertsson, som er jurist og forretningsutvikler for IT-sikkerhet i Atea-konsernet.

Som EØS-medlem har Norge forpliktet seg til å innføre direktivet i nasjonal lov. For deg som leder betyr dette blant annet at:

- du må ha kontroll på beredskap, risikovurdering og hendelseshåndtering
- du må ha god tilgangsstyring og sørge for opplæring av alle ansatte
- du har plikt til å rapportere alvorlige hendelser innen 24 timer
- du må ha kontroll på sikkerheten i hele verdikjeden, ikke bare i egen organisasjon
- du har et personlig og juridisk ansvar for å etterleve kravene
- du må vite om tiltakene du innfører har effekt og justere det som ikke fungerer
- manglende samsvar kan medføre bøter, stans av drift, offentlig kritikk, ordre om retting eller pålegg om bedre opplæring

> **«Det EU gjør nå, er å definere et minstekrav for digital sikkerhet på tvers av landegrenser.»**
>
> *Olof Eilertsson, Atea*

> **«De IT-kriminelle venter ikke på at lovverket skal være ferdig behandlet i Norge. De utnytter svakhetene dine nå.»**
>
> *Thomas Tømmernes, Atea*

Hvem må forholde seg til NIS2?

Direktivet gjelder ikke bare store nasjonale aktører. Selv om det ofte er disse som berøres direkte av direktivet, er det mange i økosystemet rundt som også må forholde seg til kravene. I første omgang har EU som mål å forbedre sikkerheten innen energi, transport, vann- og matforsyning, romfart, helsevesen, offentlig administrasjon, digitale tjenester og finanssektoren.

– Mange ledere i mindre virksomheter tror de er for små til å omfattes. Det stemmer ikke. NIS2 handler om verdikjeden du er en del av, ikke hvor stor du er, sier Tømmernes.

Han påpeker at NIS2-kravene ikke bare skal følges, men også forstås. Det handler om å ta eierskap til virksomhetens digitale risiko. Dette innebærer å gjøre løpende vurderinger, dokumentere valg og følge opp tiltak. Ikke én gang, men som en del av den daglige styringen.

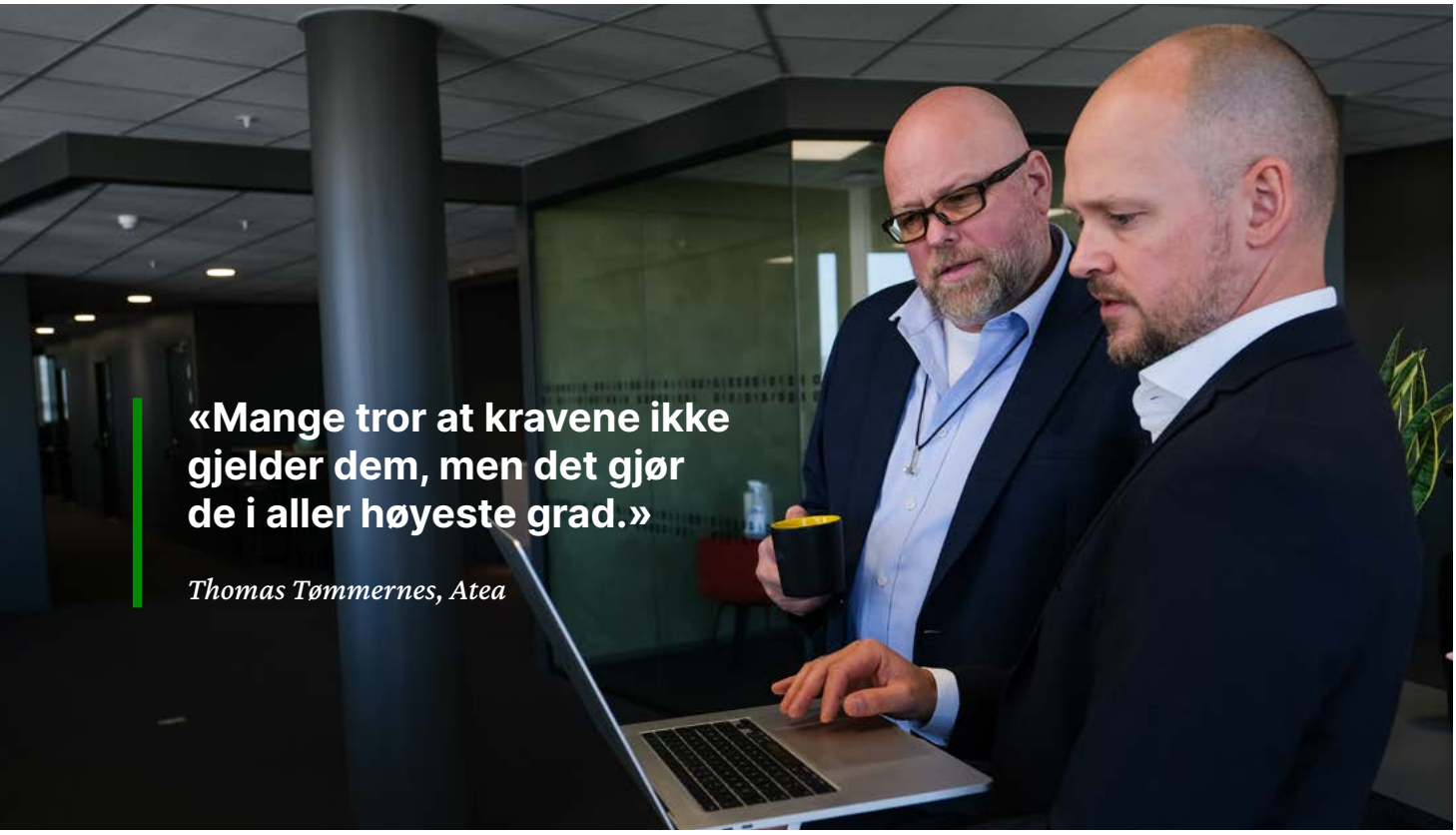
– Du kan ikke gjøre det halvveis og håpe det holder. Dette er et varslet veiskille for hvordan du som leder må jobbe med IT-sikkerhet. Og husk at de IT-kriminelle ikke venter på at lovverket skal være ferdig behandlet i Norge. De utnytter svakhetene dine nå. Og går de ikke direkte på deg, finner de kanskje et smutthull gjennom en av leverandørene dine, sier Tømmernes.

Den usynlige kjeden du er en del av

Han beskriver det som en dominoeffekt: Én svak aktør i verdikjeden kan sette mange i fare.

– Vi ser gang på gang at angrepene starter hos noen med lav modenhet og få ressurser, men ender hos en kritisk virksomhet. NIS2 forsøker å gjøre noe med den risikoen. Du må forstå din del av ansvaret, sier han.

> **«Har du ikke dokumentasjonen klar, kan du miste oppdrag.»**
>
> *Olof Eilertsson, Atea*



> **«Mange tror at kravene ikke gjelder dem, men det gjør de i aller høyeste grad.»**
>
> *Thomas Tømmernes, Atea*

> **«Vi ser gang på gang at angrepene starter hos noen med lav modenhet og få ressurser, men ender hos en kritisk virksomhet.»**
>
> *Thomas Tømmernes, Atea*

Selv om din virksomhet ikke blir nevnt eksplisitt i lovteksten, kan direktivet treffe deg gjennom økosystemet ditt. Store aktører, som selv er regulert, vil måtte dokumentere sikkerheten i sin verdikjede. Og det ansvaret vil de sende videre til deg.

– Du kan bli bedt om å dokumentere hvordan du håndterer digital sikkerhet, fordi du leverer til noen som er regulert av NIS2. Har du ikke denne dokumentasjonen klar, kan du miste oppdrag, sier Eilertsson.

Han ser allerede nå at store aktører i Europa har begynt å stille formelle krav til underleverandører. Det norske "pusterommet" før direktivet blir innført i norsk lov, er i realiteten bare en utsettelse.

– Vi ser at mange sitter på gjerdet og venter. Men det er et farlig selvbedrag. Skal du være konkurransedyktig i tiden som kommer, vil det kreve handling nå. Når kravet om samsvar fra en viktig kunde kommer, er det trolig for sent å sette i gang tiltak, sier han.

Sunt digitalt bondevett

En sentral del av NIS2-direktivet er ikke bare hvilke tiltak du har gjort, men hvordan du har tenkt. Myndighetene krever at du dokumenterer vurderingene dine. Hvorfor gjør du som du gjør? Hvorfor lar du være?

– Det handler ikke nødvendigvis om å kjøpe nytt. Mange har allerede verktøyene, men de har kanskje ikke slått på tofaktor-autentisering, de mangler rutiner for onboarding og offboarding, eller de har ikke opplæring som treffer, sier Eilertsson.

Han kaller det digitalt bondevett. Å bruke det du har, og å bruke det riktig. Innsikten du får må du bruke til å ta avgjørelser som er rimelig ut ifra din virksomhets størrelse, risiko og funksjon. Du må ta bevisste valg og dokumentere hvordan du resonnerer.

NIS2 som mulighet, ikke bare plikt

For ledere som tenker fremover, gir NIS2-direktivet en strategisk mulighet. Det tvinger frem en dialog mellom

Olof Eilertsson, jurist og forretningsutvikler for IT-sikkerhet i Atea-konsernet

> **«Det handler ikke nødvendigvis om å kjøpe nytt. Mange har allerede verktøyene.»**
>
> *Olof Eilertsson, Atea*

IT-avdelingen og ledelsen, og gjør sikkerhet til en del av forretningsstrategien. Dette er et godt utgangspunkt for å digitalisere virksomheten på en trygg måte og å bygge langsiktig konkurransekraft.

– God IT-sikkerhet i henhold til NIS2 er en forutsetning for å bruke AI, for å skalere digitale tjenester og for å beholde tillit hos kunder og partnere. Har du ikke kontroll på sikkerheten, har du heller ikke kontroll på fremtiden, sier Eilertsson.

– Om IT-sikkerhet behandles som et IT-problem, overser du noen viktige realiteter. I dag handler IT-sikkerhet om omdømme, økonomi og evne til å levere tjenester. Ledere som ser IT-sikkerhet som en mulighet, kommer til å vinne kampen om oppdragene i tiden som kommer. Og så er jo dette også en veldig smart måte å øke sikkerheten i hele samfunnet på, avslutter Tømmernes.

> **«Du kan ikke gjøre det halvveis og håpe det holder.»**
>
> *Thomas Tømmernes, Atea*

Du må vite hvem som har tilgang. Hele tiden

Alt sikkerhetsarbeid må starte med tilgangsstyring. For IT-kriminelle bryter seg ikke lenger inn. De logger seg bare på.

Hva har en koffertfabrikk, et TikTok-innlegg og en skybasert app til felles? Alt og alle kan utnyttes i et angrep hvis du ikke har kontroll på hvem som har tilgang til hva.

Cecilie Andersen er løsningsrådgiver for sikkerhet i Atea, og har jobbet med fagfeltet i over 25 år. Hun var tidlig involvert i de digitale ID-løsningene til Norsk Tipping og Altinn, og jobbet med konseptet lenge før det fikk et navn. Hun mener fortsatt at nøkkelen til sikkerhet starter med ett ord: identitet.

– I gamle dager visste vi hvor serverne våre sto. Nå er alt i skyen, og du kan ikke bare ringe Microsoft og si at noe "føles rart", sier hun.

Zero Trust, enkelt forklart

Zero Trust kan høres ut som enda en trend. Men Andersen forklarer det enkelt:

– Du skal aldri stole på noen før de har bevist hvem de er. Ikke mennesker, ikke apper, ikke maskiner.

Alt handler om å vite hvem som får tilgang, og hvorfor.

– De fleste angrep skjer ikke med brekkjern, men med pålogging. Passordlekkasjer er overalt. Det er flaut enkelt. Derfor må identitet være selve navet i sikkerhetsarbeidet, påpeker hun.

Cecilie Andersen, løsningsrådgiver for sikkerhet i Atea

Et typisk angrep kan se slik ut:

En ansatt får en e-post fra det som ser ut som "IT-drift". Den inneholder en lenke til det som ligner SharePoint. Personen logger inn. Det virker ikke. Vedkommende prøver på nytt. Ingenting skjer.

Samtidig har en angriper nå fått tak i brukernavn og passord. Kanskje er tofaktor-autentisering slått av for akkurat denne ansatte. Kanskje vedkommende har flere eller høyere tilganger enn det som er riktig.

Nå har angriperen fått fotfeste i systemet ditt, og det tok bare 30 sekunder.

– Hvis den ansatte har for vide rettigheter, kan en IT-kriminell bevege seg videre i systemet. Du har da en alvorlig hendelse før noen har rukket å forstå at noe er galt, sier Andersen.

Hun mener derfor at du som leder må tenke kontinuerlig risikovurdering. Det er ikke ett stort prosjekt, men mange små, riktige valg i hverdagen.

Bare det å ha tofaktor-autentisering, eller aller helst multifaktor, på plass kan stoppe over 99 prosent av angrepene. Likevel er det mange norske virksomheter som fortsatt ikke har skrudd på denne sikringen. Andersen mener det burde være et absolutt minstekrav, spesielt for virksomheter som skal etterleve det nye EU-direktivet, NIS2.

Multifaktor-autentisering

Multifaktor-autentisering, eller flerfaktor-autentisering, er en sikkerhetsmetode som krever at ansatte bekrefter sin identitet ved å oppgi flere uavhengige bevis eller "faktorer". Dette gir et ekstra lag med beskyttelse utover bare brukernavn og passord.

Vanligvis brukes tre kategorier av faktorer for å autentisere en ansatt:

1. **Noe du vet:** Dette er vanligvis et passord eller en PIN-kode
2. **Noe du har:** Dette kan være en fysisk gjenstand, som en smarttelefon, en sikkerhetsnøkkel eller en kodebrikke
3. **Noe du er:** Dette er en biometrisk faktor som fingeravtrykk, ansiktsgjenkjenning eller iris-gjenkjenning

> **«Du skal aldri stole på noen før de har bevist hvem de er. Ikke mennesker, ikke apper, ikke maskiner.»**

Ikke perfeksjon, men bevissthet

IT-sikkerhet handler ikke om å gjøre hverdagen vanskeligere for de ansatte. Heller det motsatte.

– Når vi vet hvem som er hvem, kan folk jobbe fra Karasjok eller Kuala Lumpur. På kontoret, på hytta eller i feriemodus. Det gir trygghet og frihet, sier hun.
Når sikkerhet bygges rundt identitet, kan hverdagen faktisk bli enklere. Ingen behov for å bytte passord hver måned. Ingen frustrasjon over feiltilganger. Bare full kontroll.

> **«Når vi vet hvem som er hvem, kan folk jobbe fra Karasjok eller Kuala Lumpur.»**

Fem gode råd for sikker tilgangsstyring

- Slå på multifaktor-autentisering. Alltid. Det stopper 99 prosent av alle angrep
- Velg passordløs der du kan. Bruk biometri eller annen sikker pålogging
- Innfør betinget tilgang. Folk skal bare ha tilgang til det de faktisk trenger
- Oppdater systemene dine. Det virker, selv om det er kjedelig
- Snakk om sikkerhet. Hele tiden. Ikke gjør det skummelt, gjør det kjent

– Det finnes alltid et smutthull. Poenget er å gjøre det vanskelig nok til at angriperen gir opp, og samtidig enkelt nok til at ansatte faktisk følger reglene, sier hun.

Hun kaller det pragmatisk sikkerhet. Ikke perfeksjon, men bevissthet. Ledelsen må eie sikkerhetsarbeidet, ikke bare delegere det.

– Hvis du som leder ikke vet hvilke verdier du beskytter, hvilke ansatte som har tilgang, eller hvem som har sluttet uten å bli fjernet fra systemene, da har du et problem. Ikke IT. Du, sier hun med tydelig tonefall.

Hvem klikker, og hvem betaler?

– Det er ikke alltid du vet at du har blitt angrepet. Det skjer i det stille, poengterer Andersen.

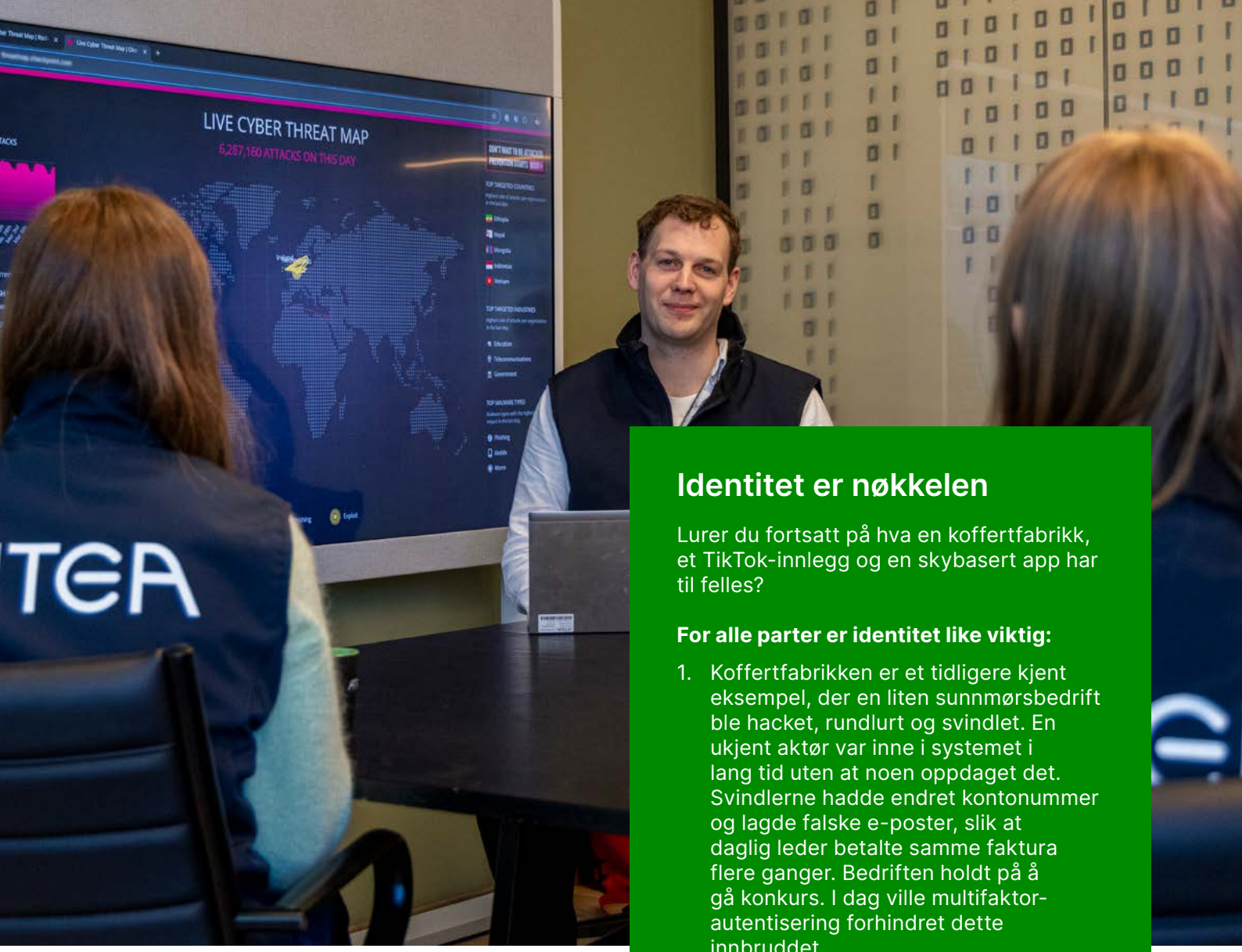
Hun beskriver hvordan norske virksomheter blir lurt: Kanskje lures du til å betale en faktura, men pengene sendes til feil konto. Da kan dine midler ende opp i hender som sprer desinformasjon.

– Du tror du har gjort en liten feil. Men du risikerer å bli en del av noe langt større, uten å vite det.

Når penger havner i feil hender, er det ikke lenger bare en regnskapsmessig feil. Midlene kan gå til trollfabrikker som sprer desinformasjon i sosiale medier som TikTok og Snapchat. Eller videre til stater som Russland eller Nord-Korea, som bruker midlene til å utvikle mer avanserte angrep.

– Det handler ikke bare om datasikkerhet. Det handler om samfunnssikkerhet. Om å beskytte statlige selskaper, strømleverandører og samfunnskritiske funksjoner fra å bli utnyttet i geopolitiske kampanjer, forklarer hun.

«Det er ikke alltid du vet at du har blitt angrepet. Det skjer i det stille.»



Sikkerhetskultur handler også om det usynlige

– Det er her kultur kommer inn, sier Andersen.

Hvis løsningene dine er for rigide, vil folk finne snarveier. De vil sende dokumenter via Messenger, bruke private e-poster eller lagre ting på måter som ikke er sikre, bare for å få jobben gjort.

Slike omveier skjer ikke fordi ansatte er uansvarlige, men fordi sikkerhetsopplegget ikke henger sammen med hverdagen deres.

– Du har allerede tapt hvis folk føler at de må omgå systemene for å få gjort jobben sin, sier hun.

God sikkerhet handler derfor like mye om rutiner og roller, som om teknologi. HR og ledelsen må involveres.

– IT-sikkerhet må inn i styrerommet. Det er daglig leder som får boten hvis noe går galt. Da bør sikkerhet være en del av ryggmargen, på lik linje med budsjettrutiner, oppfordrer hun.

Identitet er nøkkelen

Lurer du fortsatt på hva en koffertfabrikk, et TikTok-innlegg og en skybasert app har til felles?

For alle parter er identitet like viktig:

1. Koffertfabrikken er et tidligere kjent eksempel, der en liten sunnmørsbedrift ble hacket, rundlurt og svindlet. En ukjent aktør var inne i systemet i lang tid uten at noen oppdaget det. Svindlerne hadde endret kontonummer og lagde falske e-poster, slik at daglig leder betalte samme faktura flere ganger. Bedriften holdt på å gå konkurs. I dag ville multifaktor-autentisering forhindret dette innbruddet.

2. Et TikTok-innlegg er også avhengig av en kjent identitet for å være troverdig. Når norske influensere rått kopierer amerikanske medier eller andre kilder, er det lett for mottaker å tro at innholdet er sant. Men når identiteten til de som står bak budskapet er skjult, risikerer vi å bli utsatt for en påvirkningskampanje, uten å vite det. Dette er farlig i en urolig verden.

3. Når du logger inn i en app, må du være sikker på at du bruker riktig app. Det er forholdvis lett å kopiere utseende til kjente og troverdige apper, og dermed risikerer du å logge inn og gi fra deg persondata, før du forstår at du er på feil sted. Det samme gjelder for QR-koder. Du vet aldri hva som ligger bak en slik kode. Vær forsiktig, den kan være lenket til noe helt annet enn det du tror!

Mia Mathilde Steien, markedssjef for sikkerhet i Microsoft Norge

AI og NIS2 tvinger frem ny sikkerhetstenkning i norske virksomheter

Kunstig intelligens forbedrer sikkerhetsarbeidet, men endrer også trusselbildet. Samtidig strammes kravene om kontroll inn. Derfor må virksomheter bygge IT-sikkerheten rundt automatisert tilgangsstyring og kontinuerlig risikovurdering.

Når NIS2-direktivet nå blir del av norsk lovgivning, skjerpes kravene til hvordan virksomheter organiserer sin digitale sikkerhet. Ikke bare må du ha kontroll på egen butikk. Du må også sikre at hele verdikjeden din opererer i samsvar med det nye EU-direktivet.

– Mange ledere tror fremdeles at sikkerhet er noe IT-avdelingen fikser, men sikkerhet er et lederansvar. Når noe skjer, er det lederne som må stå til ansvar for om virksomheten har gjort det som er nødvendig, sier Mia Mathilde Steien, markedssjef for sikkerhet i Microsoft Norge.

> **«Etter hvert vil det bli vanskelig å samarbeide med partnere som ikke holder samme sikkerhetsnivå som deg.»**

Slik bygger du god IT-sikkerhet

- **Bevissthet og kunnskap:** Sørg for at alle ansatte kjenner sin rolle i sikkerhetsarbeidet
- **Samsvar og styring:** Velg verktøy som gir styret og ledelsen oversikt over status og risiko i sanntid
- **Risiko og praksis:** Bruk teknologi som AI, Zero Trust og betinget tilgang for å vurdere risiko kontinuerlig
- **Forankring og samarbeid:** Sikre at leverandørkjeden og samarbeidspartnerne følger samme høye sikkerhetsstandard som du gjør

> **«Mange ledere tror fremdeles at sikkerhet er noe IT-avdelingen fikser, men sikkerhet er et lederansvar.»**

For ledere som skal navigere i dette nye landskapet, handler sikkerhetsarbeidet derfor like mye om kultur og ledelse, som om teknologi. I Microsoft har de integrert sikkerhet som tema i alle medarbeidersamtaler.

– Vi flytter ikke ansvaret vekk fra sikkerhetsteamet, men vi gir alle ansatte et medansvar for å tenke sikkerhet i sitt arbeid. Når du vet at du skal snakke med lederen din om sikkerhet, får alle et større eierskap til risikohåndteringen, sier Steien.

Stol aldri på noen eller noe

Zero Trust har for lengst gått fra å være et teknologibegrep til å bli et styringsprinsipp for moderne sikkerhet. Kort fortalt handler det om å aldri stole på noen eller noe, men å kontinuerlig verifisere alle forsøk på å få tilgang til virksomhetens ressurser.

– Conditional access, eller betinget tilgangsstyring, er i praksis motoren som håndhever dette prinsippet. Hver gang en ansatt prøver å logge inn, vurderes en rekke faktorer i sanntid: hvem den ansatte er, hvor vedkommende befinner seg, hvilken enhet som brukes, om denne er oppdatert og mye mer. Basert på dette kan systemet gi tilgang, be om ekstra verifisering, begrense tilgangen eller i verste fall nekte tilgang, forklarer Steien.

Der tradisjonell tilgangsstyring ofte har vært mye enklere – du har tilgang eller ikke – gjør betinget tilgang det mulig å tilpasse tilgangsstyringen etter den faktiske risikoen i øyeblikket. Dette gjør også at tilganger kan revideres fortløpende, for eksempel når noen bytter rolle, eller når utstyr blir utsatt for risiko eller skade.

I praksis betyr dette også at tilgangsstyring ikke alltid trenger å være et IT-ansvar alene.

– Flere virksomheter har automatisert tilgangsprosesser slik at det er nærmeste leder som godkjenner eller reviderer hvem som skal ha tilgang til hvilke systemer. På den måten flyttes ansvaret til de som faktisk kjenner rollen og behovene til den enkelte ansatte, mens IT sikrer at prosessen skjer sikkert og sporbart, forklarer Steien.

– Vi setter den ansatte i sentrum og vurderer hele tiden om omgivelsene har endret seg. Dette gir oss en langt mer fleksibel og presis sikkerhetsmodell, som også er godt tilpasset kravene i NIS2, sier hun.

AI som verktøy både for deg og de kriminelle

Parallelt med at sikkerhetskravene strammes inn, rulles det nå ut stadig mer kunstig intelligens (AI) i virksomhetene. Dette gir både nye muligheter og nye utfordringer.

Ifølge Steien brukes AI allerede i betydelig grad i sikkerhetsarbeidet, selv om mye av teknologien opererer i

bakgrunnen. Hun peker på hvordan AI både kan oppdage avvik, analysere tilgangsmønstre og avdekke blindsoner i sikkerhetsoppsettet.

– Det vi ser nå, er at AI også i større grad blir synlig som operative sikkerhetsagenter. Disse kan utføre hele oppgaver – som å analysere tilgangsrettigheter eller simulere hendelser – fra start til slutt, uten at du trenger store sikkerhetsteam for å overvåke alle detaljer. For mange norske virksomheter som ikke har store interne sikkerhetsmiljøer, kan dette bli en viktig ressurs, sier hun.

> **«Når noe skjer, er det lederne som må stå til ansvar for om virksomheten har gjort det som er nødvendig.»**

Men kunstig intelligens åpner også nye angrepsflater. Bruk av åpne eller dårlig kontrollerte AI-verktøy kan skape risiko dersom ansatte for eksempel deler sensitiv informasjon uten tilstrekkelige sikkerhetsmekanismer.

– Du må forstå at ny teknologi alltid åpner for nye trusler. Det krever at sikkerhetsmiljøet involveres tidlig i AI-prosjektene, og at du setter tydelige rammer for hva som er lov og ikke lov. Ansatte må forstå at hvis du blir blokkert fra å gjøre noe, skal du ikke forsøke å finne kreative omveier via andre AI-tjenester, sier Steien.

Hun legger til at ledere og sikkerhetsfolk må engasjere seg i AI og ikke vente:

Underinvestering i IT-sikkerhet

40 prosent av norske virksomheter bruker under fem prosent av IT-budsjettet sitt på sikkerhet.

Investeringene står på stedet hvil, til tross for økende trusler.

Kilde: Atea sikkerhetsrapport 2025

– Ledere må tilby trygge løsninger som samsvarer med selskapets sikkerhetskrav, og det finnes flere måter å administrere bruk av AI som gjør det trygt og sikkert, uten risiko for at de ansatte driver med skygge-AI.

Leverandørkjeden – den skjulte risikoen

Med NIS2 følger også ansvaret for hele leverandørkjeden. Mange sikkerhetsbrudd skjer i dag via tredjepartsleverandører som har fått tilgang til dine interne systemer. Steien understreker at selv om mange virksomheter har gode ytre forsvar, er det ofte begrenset innsikt i hvordan tilganger forvaltes internt og hos samarbeidspartnere.

– Det handler ikke bare om å beskytte seg mot at informasjon blir stjålet. Du må også beskytte deg mot at informasjon manipuleres. Hvis for eksempel noen forurenser dataene du bruker i produksjonen, kan det få like store konsekvenser som et produksjonsstopp. Denne innside-risikoen er det ikke alle som tar like alvorlig, sier hun.

Med Zero Trust og betinget tilgang kan du kontrollere leverandørtilganger langt mer presist. Gjester og partnere kan få begrenset tilgang til kun de ressursene de trenger, i avgrensede tidsperioder, og med krav om flerfaktor-autentisering og godkjente enheter. Samtidig loggføres all aktivitet, slik at du har full kontroll.

Steien peker på at dette snart vil bli en konkurransefaktor.

– Etter hvert vil det bli vanskelig å samarbeide med partnere som ikke holder samme sikkerhetsnivå som deg. Mange ser allerede nå at god IT-sikkerhet kan være et konkurransefortrinn. På sikt vil det bli et krav for å kunne levere i det hele tatt, sier hun.

Sørg for at ledelsen sover godt om natten

For ledere som skal sørge for samsvar med NIS2-regelverket, er det lett å tenke at du bare må krysse av for regelverkets krav. Men Steien mener det er viktig å løfte blikket.

– Når du jobber godt med sikkerhet, sover både du og lederen din litt bedre om natten. Ingen kan garantere at ingenting vil gå galt, for det vil oppstå hendelser. Men du kan da dokumentere at du har gjort de tiltakene som er mulig. Og hvis noe skjer, blir det langt enklere å reise seg igjen, sier hun.

Steien advarer også mot å vente på at alt skal bli ferdigdefinert fra myndighetenes side.

– Zero Trust er ikke en knapp du skrur på. Det handler om å bygge stein på stein. Det beste tidspunktet å starte er nå, for dette arbeidet er en prosess, hvor du hele tiden må tilbake og vurdere om tiltakene står seg etter hvert som trusselbildet og beste praksis endres. Adopter det som en arbeidsmetodikk fremfor å se det som et arbeid du skal bli ferdig med, avslutter hun.

Når det smeller, hvem ringer du da?

– Det er ikke spørsmål om det skjer, men når. Og hvor forberedt du faktisk er, sier Vegard Kjerstad, ansvarlig for hendelseshåndtering i Atea.

Sammen med kollega Kristin Vegsund Brennan har han vært tett på mange alvorlige sikkerhetshendelser i både offentlig og privat sektor. Erfaringen er tydelig: Beredskap er ferskvare. Og du må ha trent før det smeller.

Med det nye NIS2-direktivet, som innføres i alle EU- og EØS-land, blir det enda viktigere for norske virksomheter å øve og ha kontroll på beredskapen.

> **«Det som virkelig skaper trygghet, er når ledelsen vet hva som skal skje og hvem som skal ta beslutningene i en reell situasjon.»**
>
> *Kristin Vegsund Brennan, Atea*

Fra reaktiv panikk til profesjonell håndtering

Det sitter mange ledere rundt om i landet med ansvar for beredskapsplaner som er skrevet, godkjent og arkivert. Men vet du faktisk hva som står der? Hvem som gjør hva? Og hvem som tar telefonen når nasjonale myndigheter ringer?

– Vi hadde nylig et tilfelle hvor tilsynsmyndighetene kontaktet en kommune om en pågående trussel. Kommunen visste akkurat hva de skulle gjøre. Hvorfor? Fordi de hadde hatt et stort fokus på sikkerhet og beredskap i tiden før angrepet, forteller Brennan, som er rådgiver for IT-sikkerhet i Atea.

Det er dette som skiller reaktiv panikk fra profesjonell håndtering: Tydelige roller. Oppdaterte planer. Trening.

Vegard Kjerstad, ansvarlig for hendelseshåndtering i Atea

Kristin Vegsund Brennan, rådgiver for IT-sikkerhet i Atea

Tre grep for bedre beredskap

1. Øv på realistiske situasjoner som faktisk kan skje, med hele virksomheten
2. Oppdater planverket og sørg for at det er kjent og forstått av alle involverte
3. Klargjør roller og ansvar med konkrete navn og kontaktinformasjon, ikke bare stillingstitler

En annen kommune hadde øvd på sine beredskapsplaner fra A til Å. De hadde involvert kommuneledelse, ansatte og leverandører. Foreldre i skoler og barnehager hadde fått god informasjon på forhånd. Kommunikasjon med mediene var trent på, og ordføreren hadde deltatt i en simulert pressekonferanse der spørsmålene satt løst.

– Jeg har aldri sett noen andre ta det til det nivået. Flere tusen mennesker ble berørt av øvelsen. Kommunen satte seg ikke bare rundt et bord og snakket. De involverte hele organisasjonen og samfunnet rundt, sier Kjerstad.

> **«I kriser er det ofte det enkle som svikter først.»**
>
> *Kristin Vegsund Brennan, Atea*

Og det skapte ringvirkninger i lokalsamfunnet. Etterpå satt flere organisasjoner og vurderte hvordan de skulle klare å fungere uten IT-systemene sine. Kjerstad er klar på at ikke alle beredskapsøvelser må føre til perfekte svar. Men den må belyse det som kan forbedres, og bidra til bedre forståelse hos ledelsen om hva et angrep kan bety for virksomheten.

I Ateas sikkerhetsrapport fra 2025 svarer 62 prosent av respondentene at de har en beredskapsplan. Men hvor god den er, varierer i praksis. Les rapporten her.

– Ingen kan håndtere en alvorlig hendelse alene. Du trenger støtte fra leverandører og samarbeidspartnere, og i noen tilfeller myndighetene. Gjerne fra naboene dine også. Det er summen av relasjoner og forberedelser som avgjør hvor hardt du blir rammet av et angrep, sier han.

Når rollen din er uklar, blir alt kaos

Brennan påpeker at tilsynelatende små ting kan utgjøre en stor forskjell. Som å velge ett felles språk som alle involverte kan forstå, og å sørge for at alle roller er tildelt navngitte personer. Det handler ikke bare om teknisk sikkerhet, men om å trygge hele organisasjonen og alle rundt.

– Det som virkelig skaper trygghet, er når ledelsen vet hva som skal skje og hvem som skal ta beslutningene i en reell situasjon. Ikke bare i teorien, men i praksis, sier hun.

I mange tilfeller skjer angrepet før du vet at det er et angrep. Det er ikke en blinkende rød alarm, men kanskje en e-post. En uventet innlogging. Et system som oppfører seg annerledes.

– Det er ikke dramatisk i starten. Men det utvikler seg, og hvis du ikke tar grep tidlig, kan konsekvensene bli store. Derfor må både tekniske og administrative grep være på plass, legger Kjerstad til.

Atea øver ofte med kundene sine på scenarioer knyttet til løsepengevirus. Hendelsene er realistiske, de berører hele virksomheten, og setter ledergruppen i en situasjon der de må svare på hva som skjer om IT-systemene er nede. Hvordan skal ledelsen håndtere hendelsen? Hvem skal ta de viktige avgjørelsene? Det er en stor sannsynlighet for

> **«Det er ikke dramatisk i starten. Men det utvikler seg.»**
>
> *Vegard Kjerstad, Atea*

at personopplysninger er på avveie. Hvordan håndterer vi dette?

– Det er lett å glemme hvor følsom informasjonen vi forvalter, faktisk er. Det kan være helsedata, økonomiske forhold, konfidensielle kontrakter eller identiteter som kan misbrukes. Dette er informasjon som – hvis den slippes ut – kan føre til utpressing, tap av tillit og konsekvenser langt utover det tekniske, forteller Kjerstad.

Du må øve på å ta beslutninger under press

Han viser til flere eksempler på at norske virksomheter har opplevd dette. Informasjon som ikke burde vært ute, blir offentlig. Og da er det for sent å hente den tilbake.

Sensitiv medisinsk informasjon kan bli brukt til utpressing. Det samme kan innsikt i personlige økonomiske forhold. Slike opplysninger er ikke bare ubehagelige å få på avveie, de kan få langvarige og personlige konsekvenser for den enkelte.

Målet er imidlertid ikke å ha en tykk perm med alle mulige scenarioer du kan stå overfor. Det du trenger er å ha et oppdatert planverk og realistiske øvelser, der du øver på å ta beslutninger under press.

– Det er ikke antall dokumenter som teller. Det er om folk vet hvor planene finnes, hva som står der og at de faktisk har øvd på dem, sier Brennan.

Beredskap er ikke et ansvar IT-avdelingen kan bære alene. Det må være en sentral del av virksomhetsstrategien. Du som leder må stille deg selv følgende spørsmål:

- Hva gjør jeg hvis noe skjer?
- Vet jeg hvem som har ansvar?
- Vet jeg hvem vi ringer først?

– Det høres banalt ut, men i kriser er det ofte det enkle som svikter først. Derfor må det enkle sitte, poengterer hun.

Et godt planverk er et konkurransefortrinn. Ikke minst sett i lys av kravene i NIS2-direktivet. Ikke fordi du har en plan, men fordi du har brukt den. Virksomheter som trener, samarbeider og evaluerer jevnlig, kommer seg raskere på beina etter et angrep. Og når viktige kunder eller partnere krever at du kan dokumentere god IT-sikkerhet, så har du svaret klart.

– Du må bygge motstandsdyktighet i fredstid. For når det først smeller, er det for sent å google ”beredskapsplan”, avslutter Brennan.

NIS2 endrer spillereglene:

Ta styring før myndighetene griper inn

Charlotte Hovring, sikkerhetsekspert i Cisco

NIS2-direktivet flytter ansvaret for IT-sikkerhet fra serverrommet til styrerommet. Toppledelsen blir personlig ansvarlig for virksomhetens evne til å håndtere risiko – og tilsyn kan komme uten forvarsel.

I en tid preget av økende geopolitisk usikkerhet og der det meste av samarbeid og kommunikasjon foregår digitalt, stilles det nå strengere krav til styring, kontroll og oversikt enn noen gang før. EUs nye NIS2-direktiv treffer også norske virksomheter hardt, når det blir en del av det norske lovverket. Da er det viktig å være forberedt.

Sikkerhetsekspert Charlotte Hovring i Cisco er tydelig på at NIS2 må forstås som et paradigmeskifte i måten virksomheter håndterer risiko på.

– Vi snakker ikke lenger om IT-sikkerhet som en avdeling i kjelleren. Vi snakker om forretningskritisk styring av risiko, sier hun.

Mens det tidligere var vanlig at sikkerhetsansvaret lå hos IT-avdelingen, sikkerhetsansvarlig eller driftssjef, flytter innføringen av NIS2 dette ansvaret opp til toppledelse og styre. Både daglig leder og styret blir personlig ansvarlige for at virksomheten etterlever kravene i det nye direktivet. Denne utviklingen innebærer at alle virksomheter må tenke nytt om hvordan sikkerhet organiseres og følges opp.

> **«De fleste norske virksomheter omfattes av det nye regelverket, enten direkte eller indirekte.»**
>
> *Charlotte Hovring, Cisco*

– De fleste norske virksomheter omfattes av det nye regelverket, enten direkte eller indirekte. Men mange har fortsatt ikke tatt innover seg at dette ansvaret ikke kan dyttes videre. Du kan sette ut oppgaver, men ikke ansvar. Styret og daglig leder eier risikoen, understreker Hovring.

Kompleksitet skaper risiko

I praksis er det ikke bare ansvarsfordelingen som blir utfordrende for mange ledere.

De siste årene har mange virksomheter bygget opp IT-miljøer med ulike sikkerhetsløsninger fra forskjellige leverandører – ofte anskaffet for å beskytte enkeltområder. Dette gir økt kompleksitet, fordi løsningene i liten grad er koblet sammen og ikke gir et samlet risikobilde.

> **«Styret og daglig leder eier risikoen.»**
>
> *Charlotte Hovring, Cisco*

Et typisk eksempel er virksomheter som har én løsning for e-postsikkerhet, en annen for mobilbeskyttelse og separate innloggingssystemer for ulike forretningsapplikasjoner. Når sikkerheten styres i ulike spor, blir det vanskelig for ledelsen å få oversikt – og desto mer krevende å vurdere og rapportere risiko på en helhetlig måte.

– Har du for mange ulike systemer og leverandører blir det veldig vanskelig å få overblikket du trenger for å rapportere på risiko. Jo mer kompleksitet, jo mer risiko tar du, sier Hovring.

Du må redusere antall ansvarsområder

Ciscos filosofi er derfor bygget rundt ideen om å samle flere sikkerhetsfunksjoner i en integrert løsning. I stedet for å ha separate løsninger for hvert enkelt område, bør du sørge for at datasenter, nettverk, samarbeidsløsninger og sikkerhet henger sammen.

– Det handler ikke nødvendigvis om å ha færre leverandører eller samarbeidspartnere, men om å redusere antall ansvarsområder. Når ansvaret for IT-sikkerheten er fordelt på mange ulike ansatte, øker risikoen for at ledelsen mister oversikt og styring. Med en helhetlig sikkerhetsplattform får ledelsen et samlet risikobilde, forklarer Hovring.

Dette gjør det enklere å få oversikt, og gir et bedre grunnlag for å vurdere risiko og håndtere hendelser – helt i tråd med de nye kravene i NIS2.

– Vi ser at jo mer helhetlig virksomheten tenker og opererer, desto enklere blir det å oppfylle kravene til oversikt, dokumentasjon og kontinuerlig forbedring, sier Hovring.

> **«Jo mer kompleksitet, jo mer risiko tar du.»**
>
> *Charlotte Hovring, Cisco*

Tor Geir Rosseid, strategisk rådgiver i Atea

En ny type kontroll fra myndighetene

En av de mest krevende endringene som kommer med NIS2 er at tilsynsmyndighetene kan gjennomføre proaktive kontroller. Du trenger ikke lenger ha opplevd et sikkerhetsbrudd for å bli kontrollert. Finner tilsynsmyndighetene mangler i dine rutiner, kan det i seg selv medføre sanksjoner.

– Vi snakker om bøter, pålegg om retting, tvangsmulkt, offentlig kritikk, suspensjon av tjenester, strengere tilsyn og i verste fall strafferettslig ansvar. Dette er en helt ny virkelighet for norske ledere, sier Hovring.

Desto viktigere er det at du kommer i gang med NIS2-arbeidet tidlig. Å vente til kravene trer formelt i kraft kan bli både dyrt og krevende.

Slik kommer du i gang: Fra kartlegging til forbedring

Sammen med Cisco har Atea utviklet en metodikk for å hjelpe ledere i arbeidet med NIS2. Første steg handler om å få oversikt. Hovring forklarer at ledelsen bør etablere en arbeidsgruppe som setter seg inn i direktivet, analyserer hvilke krav som gjelder egen virksomhet og kartlegger dagens situasjon.

Strategisk rådgiver Tor Geir Rosseid i Atea utdyper:

– Vi starter ofte med en modenhetsanalyse basert på Nasjonal sikkerhetsmyndighet sine grunnprinsipper. De dekker cirka 90 prosent av det NIS2 krever. Resten handler om lederansvaret: At ledergruppen må eie og forankre risikostyringen.

– Videre bør du gjennomføre en grundig analyse av nåsituasjonen og utarbeide en handlingsplan for hvordan du skal lukke eventuelle avvik. Her er det viktig at toppledelsen involveres aktivt i prosessen, sier Rosseid.

Du har ansvar for dine leverandører

Det som er spesielt med NIS2-direktivet er hvordan ansvaret forplanter seg gjennom hele verdikjeden. I det forrige EU-direktivet var det i hovedsak din egen infrastruktur som var regulert, men med NIS2 må du også ta ansvar for hvordan leverandører, underleverandører og deres leverandører igjen håndterer risiko.

– Det er ikke lenger nok å ha kontroll på eget hus. Du må ta ansvar for hele verdikjeden din. Du må vite at dine leverandører oppfyller kravene i NIS2. Gjør de ikke det, er heller ikke du i samsvar, sier Hovring.

Her er samarbeidet mellom Cisco og Atea en sterk kombinasjon. Gjennom felles rammeverk, modenhetsvurderinger og leverandøranalyser får du hjelp med å evaluere sikkerheten – også hos partnerne og leverandørene dine.

> **«En modenhetsanalyse basert på Nasjonal sikkerhetsmyndighet sine grunnprinsipper dekker rundt 90 prosent av det NIS2 krever.»**
>
> *Tor Geir Rosseid, Atea*

Fallgruvene: Hva gjør du feil?

Gjennom arbeidet med norske kunder har Cisco og Atea identifisert flere typiske feil ledere gjør i møte med NIS2. Mange mangler grunnleggende forståelse av direktivet og undervurderer ressursbehovet som kreves for å kartlegge og lukke avvik. Det er også vanlig at rollene er uklare, og at ansvar skyves nedover i organisasjonen – noe NIS2 eksplisitt forbyr.

Og kanskje viktigst av alt: Mange utsetter arbeidet, i håp om at kravene ligger lenger frem i tid.

Hovring understreker samtidig at sikkerhet også handler om organisasjonskultur:

– Opplæring, bevisstgjøring og kultur er avgjørende. Dette handler ikke bare om teknologi, men om hvordan hele organisasjonen jobber med risiko i hverdagen.

Kan du fortsette driften om IT-systemene går ned?

EUs nye direktiv, NIS2, er en god målestokk for minimumsnivået du må legge deg på for å holde virksomheten trygg.

– NIS2 er et enormt løft. Før ble sikkerhet ofte sett på som noe "IT må fikse". Nå blir det regulert av loven og forankret i styret. Det handler om ledelse, sier Jacob Järte, IT-direktør i Atea.

Järte viser til at direktivet flytter IT-sikkerhet opp på toppledernes bord. Det er ikke IT-avdelingen som skal avgjøre om folk må sendes hjem eller om forretningen kan drives videre om et angrep inntreffer.

– Dette er det vi i ledelsen som må ta stilling til. Vi må kunne svare på: Hvem tar beslutningen hvis systemene går ned? Hva gjør vi da? Har vi alternative rutiner? Dette er ingen IT-beslutning, det er en forretningsbeslutning, sier han.

Atea har selv tatt konsekvensene av dette. Hele konsernledelsen har fått opplæring i NIS2 og står ansvarlig for risikostyringen. Ettersom sikkerhet alltid har vært en del av DNA-et i Atea, har det ikke vært den største omveltningen, men Järte understreker viktigheten av å snakke om det: Sikkerhet er nå et fast punkt på agendaen i ledermøter, og det rapporteres kvartalsvis til konsernledelsen.

En sunn sikkerhetskultur krever mer enn teknologi

God risikoforståelse for Järte, er å gå fra å tenke "hva hvis en meteoritt faller ned på kontoret vårt" til å identifisere realistiske, sannsynlige og alvorlige scenarioer.

Det handler om styrt beslutningstaking: Hva slags risiko er du villig til å ta? Når går du over en grense?

«NIS2 er et enormt løft.»

Jacob Järte, IT-direktør i Atea

Ledergruppen må ha en felles forståelse for hvilken risiko virksomheten faktisk lever med, og hva du vil gjøre med det.

Han advarer mot å være naiv. Angrepene mot norske virksomheter er ofte målrettede, avanserte og det er menneskene, ikke teknologien, som feiler.

– Dette er baksiden av kunstig intelligens. Svindel har blitt ekstremt avansert med AI. Du kan bli ringt opp av det du tror er barnebarnet ditt, med helt riktig dialekt, men så blir du lurt av svindlere til å oppgi kortnummer og PIN-kode, sier han.

Og nettopp der ligger kjernen: den vanvittig raske teknologiutviklingen. Folk flest klarer ikke skille såkalte deep fakes fra hva som er ekte. Det florerer av AI-genererte bilder, videoer og tekster overalt. Og alt dette gjør oss enklere å lure, også når vi er på jobb.

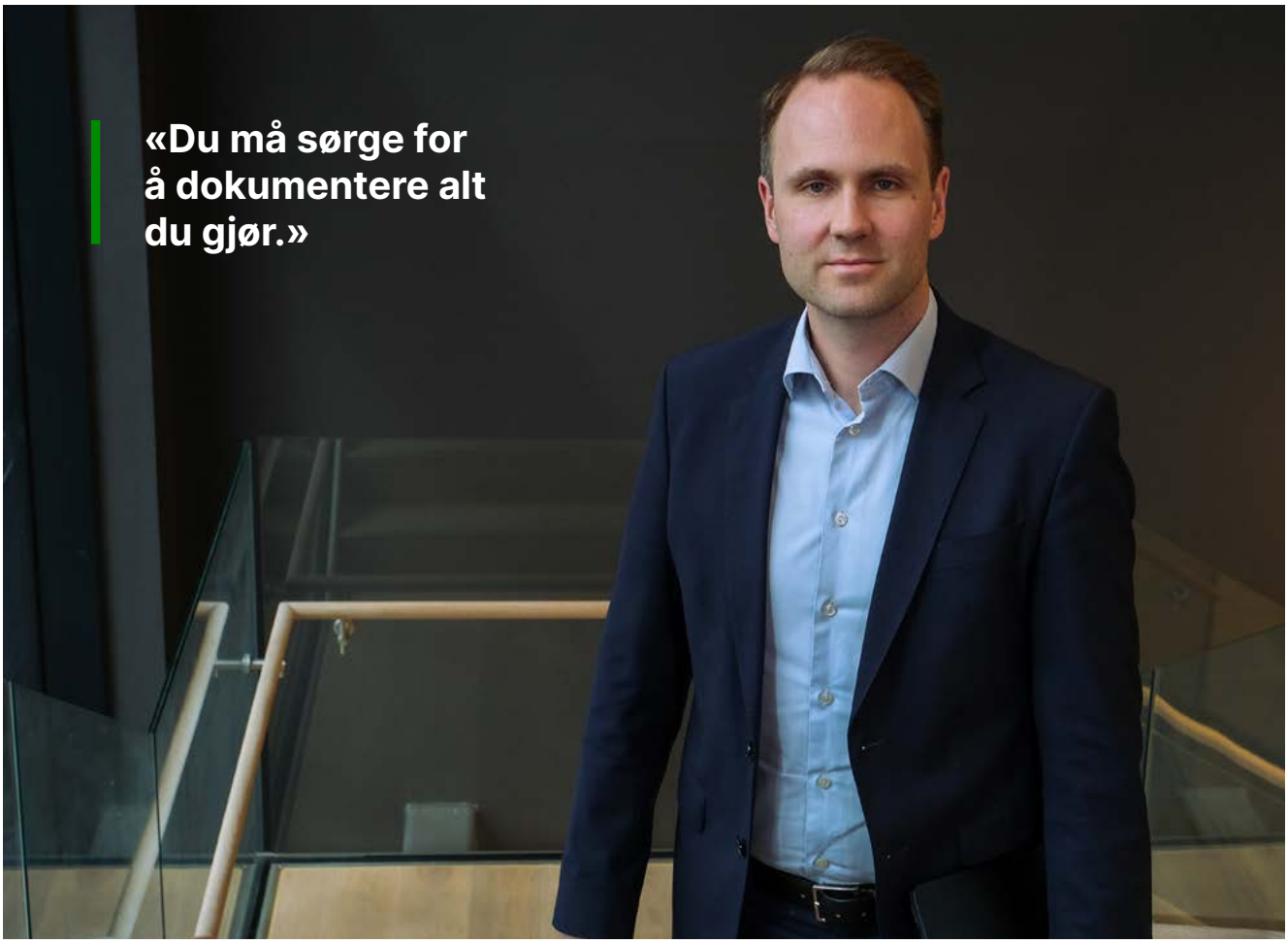
Derfor handler ledelse om å kommunisere risiko på en forståelig måte, trene ansatte og bygge en kultur som gjør det naturlig å tenke sikkerhet i det daglige. Uten å skape frykt for å gjøre feil, mener Järte.

– Vi må trene på disse tingene. Vi må kunne kjenne igjen når en deep fake-video av sjefen sirkulerer. Eller når noen kloner stemmen hennes for å få en falsk faktura utbetalt.

«Svindel har blitt ekstremt avansert med AI.»

Han peker på hvordan trusselbildet har endret seg fra dårlig formulerte Nigeria-brev og e-poster til IT-kriminalitet og profesjonelt bedrageri i stor skala. Dette krever mye av både ledere og myndigheter.

– Akkurat nå kommer det ekstremt mye fra svindelfabrikkene i Sørøst-Asia. Vi må få opp kunnskapen om dette i norsk arbeidsliv, og staten må følge opp AI-strategien med bedre rammebetingelser for digital infrastruktur. Norge kan bli verdensledende med både grønn strøm og trygge datasentre, sier han.



Tre råd for å lykkes med NIS2

- **Løft diskusjonen til toppledelsen.** Sett sikkerhet på agendaen
- **Sørg for grunnleggende IT-regler.** Gå gjennom dokumentasjon, rutiner og praksis
- **Be om hjelp.** Bruk noen som kan regelverket og vet hva som skal til
- **Sørg for god opplæring.** Husk at gode verktøy og maler ikke virker uten forståelse og eierskap fra ledelsen og ansatte

Et kollektivt sikkerhetsløft gagner både deg og fellesskapet

Järte mener at arbeidet med NIS2-kravene er en gylden mulighet for å få orden på både dokumentasjon og rolleavklaringer, og til å sikre forretningskontinuitet i virksomheten.

Og det finnes gode løsninger.

Det å få på plass et sikkerhetsoperasjonssenter (SOC) hjelper organisasjonen med å overvåke, oppdage og respondere på sikkerhetstrusler i sanntid. Dette kan enten være noe du etablerer internt eller kjøper inn som en tjeneste. Overvåkning og håndtering i sanntid er avgjørende for å forberede deg på sikkerhetsangrep.

Han forteller at en slik tjeneste også bidrar til å opplyse resten av organisasjonen om hva som skjer. Det å dele og lære fra tidligere hendelser og angrep, er gull verdt.

Han avslutter med en oppfordring:

– Du må også sørge for å dokumentere alt du gjør. God dokumentasjon er en investering som gjør at deg i stand til å ta beslutninger basert på reell risiko. Bruk kravene i NIS2-direktivet til å gjøre virksomheten din tryggere, mer robust og konkurransedyktig. Det er nå du har muligheten til å bli med på et enormt kollektivt sikkerhetsløft, som gagner både deg og fellesskapet, sier han.

«Bruk kravene i NIS2-direktivet til å gjøre virksomheten din tryggere, mer robust og konkurransedyktig.»

Totalforsvar er eneste realistiske vei for å møte kravene i NIS2

Poul Kjeldgaard, teknologidirektør for kundeløsninger i Dell Technologies

NIS2-direktivet er ikke vanskelig fordi kravene er uklare, men fordi de er krevende i praksis.

– Du kan ikke lene deg på enkeltstående sikkerhetsverktøy, som hver for seg løser én spesifikk utfordring eller risiko. Du må bygge et totalforsvar, fastslår Poul Kjeldgaard, teknologidirektør for kundeløsninger i Dell Technologies.

Det nye direktivet fra EU skal gjøre europeiske virksomheter bedre rustet mot cyberangrep. Det krever mer enn teknologi – det stiller også krav til prosesser, ledelse og leverandører. Likevel møter mange virksomheter kravene med gamle metoder og silotankegang.

– Mange tror dette handler om å legge til et nytt sikkerhetsprodukt eller å skrive en prosedyre. Men det handler ikke om punktvise tiltak. NIS2 er et skifte i tankesett. Og det krever en helhetlig tilnærming, sier Kjeldgaard.

Kompleksitet bak enkle krav

NIS2-direktivet stiller ti tydelige minstekrav. På overflaten virker de overkommelige – men for mange virksomheter er dette et minefelt i praksis.

– Det ser kanskje enkelt ut å lage en risikovurdering eller etablere sikkerhetsregler. Men i realiteten er det få som har oversikt over hvilken informasjon de har, hvor den er lagret, og hvordan den sikres. Mye eksisterer bare på papiret, sier Kjeldgaard.

Han trekker spesielt frem dataklassifisering som en utfordring. Altså det å identifisere hvilken informasjon

> **«Du kan ikke sette ut ansvar. NIS2 krever at du selv vurderer sikkerhetsnivået hos alle leverandører.»**

> «NIS2 er et skifte i tankesett.»

som er kritisk for virksomheten, og sikre at den beskyttes i tråd med hvor viktige den er.

– Jeg har aldri sett en virksomhet som faktisk har dette i orden. Informasjon flyter rundt: i gamle e-postkontoer, i backup-systemer og i mapper ingen har kontroll over. Og likevel tar man sikkerhetskopi av alt. Da mister du oversikt over hva som faktisk er kritisk, sier han.

Kjeldgaard mener dette er fundamentalt for å forstå hvorfor enkeltstående sikkerhetsløsninger ikke fungerer:

– Det hjelper ikke å sikre ett system. Når informasjonen ligger overalt, må sikkerheten være helhetlig.

Et annet aspekt som ofte glemmes, er opplæring og grunnleggende digital hygiene:

– De fleste virksomheter vet at opplæring er viktig, men de mangler rutiner for å sikre at det faktisk skjer. Uten bevissthet og gode vaner hos ansatte hjelper ingen teknologi, sier Kjeldgaard.

Uten innsyn, ingen kontroll

Et av de mest krevende punktene i NIS2 er kravet om kontroll og sikkerhet i hele leverandørkjeden.

– Du kan ikke sette ut ansvar. NIS2 krever at du selv må kunne vurdere sikkerhetsnivået hos alle leverandører – og det gjelder også infrastrukturen i skyen. Men hvordan skal du vurdere sikkerheten i alle ledd bak en offentlig sky? spør Kjeldgaard.

Dette dilemmaet har fått mange til å revurdere skystrategien:

– Vi ser at flere vurderer å hente hjem systemer og informasjon. Ikke fordi skyen er usikker, men fordi det er praktisk talt umulig å dokumentere det totale sikkerhetsnivået hos alle underleverandører. Uten innsyn, ingen kontroll. Uten kontroll, ingen NIS2-etterlevelse, sier han.

Styret er ofte fraværende i kriseøvelser

Kun fem prosent av norske virksomheter involverer styret i beredskapsøvelser.

Ledelse og IT-avdeling deltar langt oftere (77 prosent), men NIS2-direktivet krever også at styret er aktive i sikkerhetsarbeidet.

Kilde: Atea sikkerhetsrapport 2025

> **«I realiteten er det få som har oversikt over hvilken informasjon de har, hvor den er lagret, og hvordan den sikres.»**

Dell Technologies svarer blant annet med egne standarder for maskinvaresikkerhet. Det betyr at hver eneste datamaskin sjekker sine egne komponenter mot det som er forhåndsgodkjent – og nekter å starte opp hvis noe er endret eller mistenkelig. Dette forhindrer at ondsinnet kode eller uautoriserte deler tar kontroll over maskinen.

– Dette er sikring i praksis. Ikke bare et dokument. Ikke bare et løfte. Men noe som faktisk fungerer når det gjelder.

Kjeldgaard trekker frem at lovgivningen i NIS2-direktivet er godt ment, men i praksis ofte umulig å gjennomføre slik det står skrevet. Særlig når ansvaret ikke kan settes ut, og kontrollen i mange tilfeller er umulig å oppnå.

Når alt faller – hva prioriterer du først?

En annen utfordring er kravet om plan for gjenopprettelse. Mange virksomheter tenker at en sikkerhetskopi alene er tilstrekkelig. Det er det ikke, ifølge Kjeldgaard:

– Du må ha en plan for hva du må få opp først – hva som er ditt «minimum viable company». Hvis du mister Microsoft 365 – med e-post, Teams, OneDrive, SharePoint – hva gjør du da? Har du tenkt gjennom hvilke funksjoner som må opp først, og hvor lang tid det faktisk vil ta?

Han mener mange har en beredskapsplan, men at få reelt har testet den. Og enda færre har kontroll på hvordan de prioriterer i en krisesituasjon.

– Det står i NIS2-direktivet at du skal kunne dokumentere dette. Men i realiteten vil mange oppdage at de ikke har verktøyene, oversikten eller rutinen til å få driften raskt tilbake.

Du må evaluere om det virker

NIS2 handler ikke bare om å ha tiltak på plass, men også om å evaluere hvor godt de virker. Her svikter mange, mener Kjeldgaard:

– Sikkerhetsansvarlige må kunne vise til hvordan sikkerhetstiltak fungerer i praksis. Derfor har vi bygget inn muligheten for sikkerhetsscore direkte i de større systemene våre. Du trykker på en knapp, og får en score fra en til ti – og konkrete forslag til hva du kan forbedre. Det gir et reelt beslutningsgrunnlag.

Det kan bli dyrt å være uforberedt
Den største endringen NIS2 fører med seg, er at sikkerhet nå er et lederansvar.

– Tidligere var dette IT-sjefens bord. Nå er det styret og toppledelsen som eier risikoen. Og det ansvaret kan ikke skyves bort eller delegeres. Det må forstås og følges opp, sier Kjeldgaard.

Han mener at de som tar NIS2 på alvor, vil bruke det som en anledning til å rydde – og bygge et sterkere og fremtidsrettet forsvar:

> **«Det hjelper ikke å sikre ett system. Når informasjonen ligger overalt, må sikkerheten være helhetlig.»**

– Ingen kommer til å levere perfekt på alle punkter. Men forskjellen mellom dem som gjør NIS2 til en skrivebordøvelse, og dem som faktisk bygger totalforsvar – den blir tydelig. Og denne forskjellen vil kunne koste de uforberedte dyrt, sier han.

– Vi skal være ærlige: NIS2 er ambisiøst. Men det er også nødvendig. Du kan ikke bygge en ny sikkerhetskultur med gårsdagens tankesett. Og du kan ikke møte komplekse krav med enkeltstående løsninger. Du må bygge et totalforsvar. Det er det eneste realistiske svaret for å møte kravene i NIS2, avslutter han.

Slik får du full kontroll på NIS2:

Automatisk oppfølgning – døgnet rundt

Med EUs nye sikkerhetsdirektiv på vei inn i norsk lovverk, vil det bli krevende for mange virksomheter å oppfylle kravene. IBM tilbyr nå et verktøy som oversetter lovverk direkte til tekniske tiltak – og hjelper både ledelse og IT-avdelingen med å jobbe smartere.

Samsvar, eller compliance, betyr ganske enkelt etterlevelse av lover, regler og standarder som gjelder for virksomheten din. Det handler ikke om å ha gode intensjoner, men om å kunne dokumentere at du faktisk følger kravene.

I praksis betyr dette også at virksomheten kontinuerlig må overvåke kjente sårbarheter i systemene, følge med på nye trusler som kan oppstå i skyen eller egne datasentre, og sørge for at regelverket følges selv når det oppdateres. EU-regelverk som NIS2, DORA og GDPR er nemlig i stadig utvikling, og kravene endres hyppig.

I NIS2-sammenheng betyr dette blant annet at du må beskytte dine digitale systemer, ha kontroll på risiko, varsle om sikkerhetsbrudd og kunne vise at du kontinuerlig jobber med å forbedre sikkerheten.

Hvor står virksomheten din i dag?

Jimi Inge anbefaler at ledelsen stiller seg noen enkle, men viktige spørsmål:

- Hvor står vi i dag, og hvor stort er samsvars-gapet?
- Har vi dokumentasjon på samsvar, eller bare en følelse av kontroll?
- Kan vi bruke samsvars-arbeidet til å styrke merkevaren og konkurransekraften?
- Er vi rigget for de regulatoriske endringene som kommer de neste årene?

Jimi Inge, direktør for forretnings-utvikling i finanssektoren i IBM

Samsvar er mer enn en årlig øvelse

– Mange tror fortsatt at samsvar er noe du tar tak i én gang i året i forbindelse med revisjon, men NIS2 handler om kontinuerlig kontroll, hver dag og hele året, sier Jimi Inge, direktør for forretningsutvikling i finanssektoren i IBM.

Det er et tankeskifte mange virksomheter nå må forholde seg til. Der revisjoner tradisjonelt har vært en periodisk sjekk, krever NIS2 at ledelsen har sanntidsoversikt over IT-risiko og sårbarheter.

– Regelverket er der for å beskytte virksomheten din året rundt. Da må du vite når avvik oppstår. Du kan ikke vente til neste revisjon, sier Inge.

Full kontroll når du trenger det

Utfordringen for ledere er at IT-landskapet i de fleste virksomheter er blitt ekstremt komplekst. Informasjon finnes i egne datasentre, flere offentlige skyer, i programvarer levert som tjenester og i ulike kombinasjoner av disse. Nye servere etableres, systemer flyttes, tjenester fases ut og inn. I tillegg oppdateres regelverk og internasjonale standarder fortløpende.

IBM har derfor utviklet verktøyet IBM Cloud Security and Compliance Center Workload Protection (SCC WP), som fortløpende oppdaterer retningslinjene sine slik at du hele tiden kan måle virksomheten opp mot gjeldende krav. Dermed trenger du ikke lenger følge opp manuelt.

> **«Vi ser i dag at noen selskaper budsjetterer for fremtidige bøter. Det er feil tankesett.»**

– Menneskelige prosesser blir ofte flaskehalsen. Derfor handler dette ikke bare om teknologi, men om å automatisere det som må gjøres, slik at du faktisk har kontroll når du trenger det, forklarer Inge.

Regelverk blir til tekniske tiltak

Kjernen i IBM-verktøyet er at det oversetter juridiske krav og regulatoriske rammeverk til konkrete, tekniske sjekklister som kontinuerlig kontrolleres mot IT-infrastrukturen din. Allerede fra dag én kan du bruke verktøyet til å kjøre en automatisk analyse. Det tekniske oppsettet ditt sjekkes opp mot kravene i NIS2 og andre regelverk, og gir et tydelig bilde på hvor du er i rute, og

Fire nøkkelråd for bedre samsvar

- Start arbeidet nå
- Automatiser alt som kan automatiseres
- Gjennomfør en analyse for å se hvor dere står
- Se samsvar som en investering som kan spare virksomheten for både risiko og kostnader

hvor det finnes avvik som må lukkes. På den måten får ledelsen et konkret utgangspunkt for planlegging av videre arbeid.

I tillegg til å kartlegge samsvar-status, gjennomfører verktøyet også sårbarhetsskanning i IT-systemet ditt. Slik oppdages feiloppsett og svakheter tidlig, og IT-avdelingen får konkrete, prioriterte tiltak som kan iverksettes før det oppstår sikkerhetshendelser.

– Vi sier gjerne at verdien i verktøyet ligger i oversettelsen. Regelverkene er i sitt vesen juridiske og forretningsmessige tekster. Men IT-folk snakker ikke det språket, og samsvar-ansvarlige snakker ikke IT-språk. SCC WP gjør om regelverkene til tekniske kontroller som IT-avdelingen forstår og kan forholde seg til, forklarer Inge.

> **«NIS2 handler om kontinuerlig kontroll, hver dag og hele året.»**

> **«Mange tror fortsatt at samsvar er noe du tar tak i én gang i året i forbindelse med revisjon.»**

Verktøyet kobler dermed sammen det som tradisjonelt har vært to adskilte verdener i virksomheten: samsvar og IT-drift. Resultatet er et dashboard som gir en helhetlig sanntidsvisning av virksomhetens samsvar-status.

– Du kan se hvor du har avvik. Kanskje har du 800 kontroller som er godkjente, 20 gule og 10 røde. Da vet du hvor du er i samsvar med regelverket og hvor du har risiko, sier han.

Leverandøruavhengig arkitektur gir komplett oversikt

En viktig styrke med IBM SCC WP er at plattformen fungerer uansett hvor informasjonen din ligger.

– Informasjon finnes i dag over alt. På lokale servere, i skyen, ofte flere skyer, og i ulike programvaretjenester. Derfor må samsvarsverktøyet kunne se alt samlet. SCC WP fungerer uavhengig av leverandør, og samler all informasjon på ett sted, sier Inge.

> **«Regelverket er der for å beskytte virksomheten din året rundt.»**

Denne egenskapen gjør også verktøyet nyttig for virksomheter som har satt ut IT-driften.

– Om du outsourcer IT-driften din, har du fortsatt ansvar for å være i samsvar. SCC WP gir deg innsikten du trenger for å stille krav til dine leverandører, påpeker Inge.

Til tross for kompleksiteten i IT-landskapet trenger ikke innføringen av SCC WP å være omfattende.

– Vi anbefaler å starte smått: velg ett regelverk, ett datasenter, og begynn der. Etter to til fire uker har du et fungerende testmiljø. Deretter kan du utvide stegvis, sier Inge.

Invester nå, og unngå fremtidige bøter

Verktøyet kan fungere som en bro mellom ledelsen og IT. Ledere får trygghet og dokumentasjon for styrerommet, samtidig som IT-avdelingen får konkrete handlingspunkter.

– IT kan vise ledelsen at virksomheten er i samsvar. Ledelsen kan på sin side stille konkrete spørsmål tilbake til IT: Hvorfor er denne kontrollen rød? Hva er planen for utbedring? forklarer Inge.

Han påpeker viktigheten av å investere i proaktiv kontroll, som gir langt bedre beskyttelse, lavere risiko og potensielt også lavere kostnader. Å få løpende kontroll på samsvar kan også være en god investering i virksomhetens merkevare i form av tillit.

– Vi ser i dag at noen selskaper budsjetterer for fremtidige bøter. De forventer at de kommer til å feile. Det er et feil tankesett. Bruk heller disse pengene på å ta kontrollen nå. Dette er et ledelsesspørsmål, og har du ikke løftet denne diskusjonen inn i ledergruppen ennå, er tiden mer enn moden nå, avslutter Inge.

> **«Om du outsourcer IT-driften din, har du fortsatt ansvar for å være i samsvar.»**

Thomas Tømmernes, konserndirektør for IT-sikkerhet i Atea

Med AI som våpen

Det er mandag morgen, og du logger deg på ukas første Teams-møte med avdelingen din. Midt i samtalen plinger det i telefonen din fra administrerende direktør. Du blir litt overrasket over at han ringer deg på Teams, men svarer selvsagt umiddelbart.

«Hei, jeg trenger at du gjennomfører en hastebetaling på 850 000 kroner så raskt som mulig,» sier han alvorlig. «Det haster, så vi kan ikke diskutere det nå, men jeg sender deg betalingsdetaljene på e-post rett etter samtalen».

Som IT-sikkerhetsdirektør i Atea-konsernet, og med over 20 år i bransjen, har jeg sett hvor utrolig lett det er å bli lurt når slike forespørsler kommer brått og troverdig.

Når AI gjør svindelen mer troverdig

Men allerede her er det mange røde flagg, i hvert fall for oss som jobber med IT-sikkerhet på fulltid. Jeg har sett det gang på gang gjennom mine år i bransjen, både som sikkerhetsdirektør i Atea og i møte med virksomheter over hele landet. Men kvaliteten og kreativiteten på det som kalles direktørsvindel er i en enorm utvikling. Mye takket være hjelpen nettkriminelle får fra kunstig intelligens (AI).

Direktørsvindel, også kalt CEO-svindel eller BEC-svindel

> **«Kvaliteten og kreativiteten på det som kalles direktørsvindel er i en enorm utvikling.»**

(Business Email Compromise), innebærer at en ansatt med myndighet til å foreta betalinger lures til å betale en falsk faktura eller foreta en uautorisert overføring fra bedriftens konto.

AI manipulerer både video og lyd

Allerede i 2021 ble det første svindelforsøket med AI-manipulering av både videobilde og lyd utført, og siden den tid har omfanget spredt om seg. Nylig fikk DNB omtale etter at deres toppledere ble misbrukt i et falskt videomøte, der målet var å få DNB-ansatte til å utbetale 24 millioner kroner til svindlerne. DNB gikk ikke på limpinnen, men det finnes mange eksempler der nettkriminelle lykkes også.

Dette er viktig å tenke på:

- AI øker risikoen for avanserte svindelmetoder.
- Det er viktig å utfordre forespørsler og sette klare retningslinjer for håndtering av mistenkelige situasjoner.
- Grunnleggende sikkerhetstiltak, som flerfaktorautentisering, er avgjørende for å beskytte virksomheten mot svindel.
- Opplæring og bevisstgjøring av ansatte er en kontinuerlig prosess som bidrar til å redusere risikoen for svindel.
- Innføring av «Zero Trust»-prinsippet kan være en effektiv strategi for å beskytte virksomheten mot både interne og eksterne trusler.

For eksempel da en finansarbeider i et multinasjonalt selskap ble lurt til å overføre totalt 25,6 millioner dollar. Fremgangsmåten var ganske likt som hos DNB, da offeret ble lurt inn i en videokonferanse hvor han trodde han snakket med selskapets finansdirektør og flere kollegaer. Alle deltakerne i videomøtet viste seg å være «deepfakes» av både ansikter og stemmer skapt ved hjelp av kunstig intelligens.

Tenk kritisk i møte med uvanlige forespørsler

Som påpekt i den siste trusselvurderingen fra Nasjonal Sikkerhetsmyndighet (NSM), blir generativ kunstig intelligens i økende grad brukt til å lage falsk informasjon, inkludert bilder, videoer, lyd og tekst. Dette gir angripere muligheten til å forvirre, manipulere og påvirke både enkeltpersoner og organisasjoner, noe som øker risikoen for svindel og cyberangrep. Kombinasjonen av å oppleve at man prater med virksomhetens leder, og vårt iboende ønske om å være gode ansatte som hjelper virksomheten ut av en knipe, skaper en skummel situasjon.

Dette vet de IT-kriminelle. Vi må derfor begynne å utfordre ledere som kontakter oss utenom satte rutiner for å få gjennomført oppgaver som kan ha konsekvenser for selskapet.

Dette er ikke nytt

Avanserte og manipulerende svindelforsøk er ikke noe nytt. Svært mange, både ledere og ansatte, kommuniserer

med kompromitterte identiteter på e-post daglig. Men AI gir nye strenger å spille på og gjør det fort vanskeligere å skille. Likevel er det fortsatt slik at grunnleggende sikkerhetstiltak er nødvendige for å senke risikoen her også. Vellykkede svindelforsøk i alle varianter handler først og fremst om at de IT-kriminelle har kommet seg inn i systemet, og har tilgang til virksomhetens egne kommunikasjonskanaler og informasjon.

Hvordan avslører du AI?

Dagens teknologi er knallbra, men vi kan raskt avdekke AI ved å for eksempel stille spørsmål ingen med normal grunnkunnskap klarer å svare på. Dette kan være kompliserte regnestykker, eller mer kuriøse spørsmål som: Hva kona til den femte presidenten i USA heter, eller hvilke land som har vunnet de siste 10 Melodi Grand Prix-konkurransene. Kommer disse svarene kjapt, er det stor sannsynlighet for at du snakker med AI.

> **«Når det kommer henvendelser på intern e-post eller Teams fra ledere, har allerede hackerne tilliten i dialogen, og dette gjør sjansen for å lykkes betydelig høyere.»**

Ikke vær redd for at din leder eller samarbeidspartner opplever at du mistror dem. Om det skulle være en reell samtale, vil de sannsynligvis gi deg ros for å være våken og forsiktig med virksomhetens midler og informasjon.

Slik setter du smarte retningslinjer og prosedyrer

Utover å bevisstgjøre de ansatte, så vil det være vesentlig å sette retningslinjer for hva som er forventet oppførsel, særlig knyttet til utbetalinger av penger. Retningslinjene må kommuniseres ut, og ansatte må få lov å utfordre uten at ledere tar seg nær av det. Alle virksomheter bør etablere en bekreftelsesprosedyre for pengeoverføringer, spesielt der beløp overstiger et visst nivå.

Når en IT-kriminell kontakter offeret på kanaler som ikke normalt blir brukt av virksomheten, eksempelvis «Messenger», «FaceTime» og lignende, vil de aller fleste reagere på dette, og sjansen for å lykkes med

Kompetansemangel i IT-sikkerhet

Kun 28 prosent av norske virksomheter har egne ansatte som jobber dedikert med IT-sikkerhet.

Det er flere i det private næringslivet som kjøper kompetanse eksternt enn virksomheter i offentlig sektor.

Kilde: Atea sikkerhetsrapport 2025

svindelen synker betraktelig. Når det derimot kommer henvendelser på intern e-post eller Teams fra ledere, har allerede hackerne tilliten i dialogen, og dette gjør sjansen for å lykkes betydelig høyere.

Opplæring av ansatte

De ansatte er definitivt virksomhetens viktigste middel i kampen mot IT-kriminelle, men for å kunne holde tritt med et dynamisk trusselbilde og hackere som til stadighet finner nye svindelmetoder, er kontinuerlig kursing et «must». Det finnes mange forskjellige kurs og opplæringsmodeller til dette formålet. Selv foretrekker jeg korte sesjoner med videoklipp og quiz som alle må gjennomføre fortløpende. Gjerne i kombinasjon med «falske» e-poster som sendes ut til de ansatte for å teste at de får med seg innholdet i kursene og holder de på «alerten». Mange av disse kursene tilpasses virksomhetens drift, slik at eksemplene blir relevante og verdifulle for kursdeltagerne.

Hva virksomheter bør ha på plass

Å få på plass grunnleggende sikkerhetshygiene er ingen umulig oppgave, men krever at virksomhetene har en oversikt over egen IT-løsning sett opp mot dagens trusselbilde.I Norge bruker vi gjerne grunnprinsippene fra Nasjonal Sikkerhetsmyndighet som rettesnor for hvilke tiltak en virksomhet bør ha på plass. I EU bruker man blant annet cybersikkerhetsdirektivet NIS2, og den kommende sikkerhetsloven i Norge vil sannsynligvis være preget av en kombinasjon av disse to.

Eksempler på tiltak alle virksomheter bør ha på plass er gode patche-rutiner, kontroll på alle autoriserte og uautoriserte enheter i nettet og flerfaktorautentisering (MFA) på alle systemer, særlig e-post og økonomisystemer.

> **«Det er bedre å bli oppfattet som lettere paranoid enn å bli lurt.»**

«Zero Trust»: Skifte mot total verifisering og sikkerhet

Flere og flere virksomheter innfører også «Zero Trust»-prinsippet, noe jeg anbefaler på det sterkeste. Dette går i all enkelhet ut på at man istedenfor å tro at alt bak bedriftens brannmur er trygt, antar «Zero Trust»-modellen brudd og verifiserer hver forespørsel som om den kom fra et ukontrollert nettverk. Uansett hvor

forespørselen kommer fra eller hvilken ressurs den får tilgang til, lærer «Zero Trust»-modellen oss å aldri stole på, og alltid verifisere. «Zero Trust»-beskytter brukerkontoer, enheter, applikasjoner og data uansett hvor de befinner seg.

Med «Zero Trust» går du bort fra et tillit-ved-standard (som de kriminelle benytter i dag) til et tillit-ved-unntak-perspektiv. Du kan lettere oppdage trusler, reagere på trusler, og forhindre eller blokkere uønskede hendelser på tvers av organisasjonen.

Ja, det kunne skjedd deg

Jeg får ofte spørsmålet «om dette kunne skjedd i min virksomhet», fra bekymrede virksomhetslederes som har lest en artikkel i nyhetene om noen som har blitt kompromittert og hacket av kriminelle.

Svaret er dessverre «Ja», dette kunne skjedd de aller fleste.

Selv om utviklere av sikkerhetsløsninger som skal stoppe hackerne er utrolig dyktige, ligger vi ofte hakket bak de kriminelle. Særlig i møte med oss naive nordmenn, som utpeker oss som et av de mest tillitsfulle folkeslagene i verden. En av de største bekymringene Kripos peker på i sin ferske rapport, er at sanntidsgenererte «deepfakes gjør det vanskeligere å avsløre svindel. Nettopp fordi ofre har mindre tid til å vurdere om en videokonferanse eller telefonsamtale er ekte, men også fordi kvaliteten har blitt så god at det er umulig å skille mellom ekte og falsk.

Som alltid er mitt beste råd: Stopp, tenk og ager. Det er bedre å bli oppfattet som lettere paranoid enn å bli lurt.

Du kan ikke sikre det du ikke ser

For å etterleve NIS2-direktivet må du vite hvor du er sårbar. Med spredte IT-løsninger, uautoriserte AI-verktøy og underleverandører med tilgang til dine systemer, kan dette være krevende.

Det nye sikkerhetsdirektivet fra EU stiller strenge krav til hvordan du må beskytte dine digitale verdier – og hvordan du skal rapportere på arbeidet du gjør. Men i en virkelighet preget av mange ulike IT-systemer og AI-løsninger, blir det stadig vanskeligere å vite hvor du er sårbar.

I Palo Alto Networks starter alt med kartlegging. Du kan ikke beskytte det du ikke vet at du har.

– Dette handler om risikostyring og synlighet. For å sikre noe, må du se det. Skygge-IT er en stor utfordring for mange IT-avdelinger. Kanskje spesielt etter at kunstig intelligens gjorde sitt inntog i arbeidslivet. Uautorisert teknologi utgjør en stor risiko for virksomheten, dersom ikke du får kontroll på disse systemene og verktøyene, sier Ulf Rasmussen, teknisk leder i Palo Alto Networks Norge.

Skygge-IT

Bruk av IT-løsninger, som programvare, apper eller skytjenester, uten at IT-avdelingen er klar over det eller har godkjent og sikret bruken av verktøyet.

Angrepsflaten har eksplodert

I dag jobber ansatte fra ulike steder, på ulike enheter, og med informasjon og programvarer spredt over både tradisjonelle datasentre og offentlig sky. Det har gjort angrepsflaten, steder der en angriper kan forsøke å få tilgang til eller skade et datasystem, langt mer uoversiktlig, og veldig mye større.

Ulf Rasmussen, teknisk leder i Palo Alto Networks Norge

– Mange ledere tror de har kontroll, men i de fleste tilfeller bruker ansatte langt flere verktøy enn du er klar over. En IT-sjef kan si «vi har fem godkjente AI-verktøy», men når vi skanner IT-miljøet, finner vi kanskje over femti i bruk. Da har du kontroll på fem, og null innsikt i resten, sier Rasmussen.

Skygge-IT er ikke nytt, men det har fått en ny dimensjon når ansatte tar i bruk AI-verktøy uten å informere IT-avdelingen. Det gir en risiko for lekkasje av sensitiv informasjon, og gjør det vanskeligere å etterleve NIS2-direktivet.

– Ansatte kan for eksempel lime inn personnummer eller sensitiv kundeinformasjon i verktøy som ikke er godkjent. Da har du ikke kontroll, og det kan få alvorlige konsekvenser – både juridisk og omdømmemessig, sier han.

Underleverandører er ditt svake punkt

Trusselaktørene vet at underleverandører ofte har fått tilgang til interne systemer. Derfor er leverandørkjedene blitt en av de mest brukte inngangsportene for angrep.

> **«Uautorisert teknologi utgjør en stor risiko for virksomheten.»**

Kommunikasjonsavdelingen uteblir fra øvelser

Kun 34 prosent av norske virksomheter involverer kommunikasjonsavdelingen i sikkerhetsøvelser.

Manglende trening på krisekommunikasjon svekker evnen til å håndtere omdømmerisiko ved angrep.

Kilde: Atea sikkerhetsrapport 2025

– Fra et sikkerhetsperspektiv har underleverandør-angrep vært en av de mest brukte metodene de siste årene. Du må vite hvem som har tilgang, hva de har tilgang til, og når. Og du må ha en sikkerhetsmodell som bygger på "Zero Trust". Du kan ikke stole på noen eller noe, derfor må all tilgang verifiseres kontinuerlig, sier Rasmussen.

> **«Mange ledere tror de har kontroll, men i de fleste tilfeller bruker ansatte langt flere verktøy enn du er klar over.»**

Palo Alto Networks fremhever at det ikke er tilstrekkelig å basere seg kun på andres bekreftelser. Du må selv ha systemer og prosesser som kontrollerer og logger tilgang og aktivitet, og du må få dette bekreftet i ettertid.

Flytt sikkerheten til nettleseren

Siden mye av arbeidshverdagen nå foregår i nettleseren, mener Rasmussen at sikkerheten også må flyttes dit.

– Vi snakker mye om bedrifts-nettlesere nå. Der kan du legge inn regler for hva som er lov, og hva som ikke er det. For eksempel at du kan kopiere personnummer mellom visse godkjente apper, men ikke ut i et privat notatverktøy, forklarer Rasmussen.

Denne formen for sikkerhet gir også en bedre opplevelse for de ansatte, fordi kontrollen skjer nærmere der arbeidet faktisk utføres.

AI som verktøy for både angrep og forsvar

Samtidig som AI gir nye trusselflater, er teknologien også en sentral komponent i nye sikkerhetsløsninger.

– Angriperne bruker AI aktivt, da må vi som forsvarere også gjøre det. I Palo Alto Networks oppdager vi over sju millioner nye angrep hver dag, og det gjør vi blant annet ved å bruke AI og maskinlæring til å finne uvanlig oppførsel, sier Rasmussen.

Han understreker at AI også gjør sikkerhetsløsningene lettere å bruke – med bedre grensesnitt og presentasjon av innsikt. Dermed blir det enklere for ledelsen å forstå og følge med på hvor risikoen ligger.

Helhetlig forsvar fremfor punktløsninger

En annen utfordring mange virksomheter står i, er at de har for mange sikkerhetsverktøy – som ikke snakker sammen.

– Du ender opp med at informasjonen ligger for mange steder. Skal du få oversikt og kunne reagere raskt, må du ha færre, meget integrerte løsninger. Det handler om «plattformisering» av sikkerhet, sier Rasmussen.
Han viser til at sikkerhetsbransjen fortsatt er umoden sammenlignet med mange andre områder av IT-disiplinen.

– Vi ser at det fortsatt finnes én sikkerhetsløsning for hvert problem, noe som skaper støy og tap av innsikt. Ved å sy sammen et samlet forsvar, får du bedre styring, lavere kostnader og bedre sikkerhet, sier han.

> **«Fra et sikkerhetsperspektiv har underleverandør-angrep vært en av de mest brukte metodene de siste årene.»**

Palo Alto Networks tilbyr en helhetlig sikkerhetsplattform med over 50 integrerte løsninger. Disse spenner fra datasenter-sikring til avanserte verktøy for innsikt og trusselhåndtering. Blant disse løsninger for angrepsflate-kartlegging (Attack Surface Management), som gir oversikt over alt du har eksponert mot internett. Altså de digitale inngangsportene som angripere kan utnytte.

Plattformen inkluderer også funksjoner for etablering av et sikkerhetssenter (SOC), som kontinuerlig overvåker IT-miljøet for å oppdage, analysere og håndtere trusler. Dermed kan risiko identifiseres, og du kan ta grep før det oppstår skade.

Hva må ledere gjøre nå?

Rasmussen er tydelig på at sikkerhet er blitt et lederansvar. Det er ikke lenger tilstrekkelig å lene seg på IT-avdelingen alene.

– Mange ledere har ikke tatt helt innover seg hvor mye risiko som følger med digitaliseringen. Internett er ikke et trygt sted. Og det er ledelsen som bærer ansvaret når noe skjer.

– Så hva bør ledere gjøre?

> **«Mange ledere har ikke tatt helt innover seg hvor mye risiko som følger med digitaliseringen.»**

– Start med å skaffe deg et bilde av hvordan det faktisk står til. Hva bruker du? Hva har du kontroll på? Mange ganger handler det ikke om å øke budsjettet, men om å rydde opp, konsolidere og prioritere riktig, sier han.

Han trekker frem at rådgivningstjenester som Atea leverer kan bidra til å identifisere både lavthengende frukter og mer langsiktige strategiske grep.

Kultur og metode er en del av svaret

Til sjuende og sist handler sikkerhet ikke bare om teknologi, men om kultur og metodikk.

– De som lykkes, er de som tar sikkerhet på alvor, forankrer det i ledelsen og bygger det inn i utviklings- og driftsprosesser. Å analysere kode kontinuerlig for å finne sårbarheter, før noe settes i produksjon, gjør utvikling både rimeligere og sikrere. Det handler om sunn skepsis og om å tenke sikkerhet fra starten av, sier Rasmussen.

> **«I mange tilfeller har virksomhetene gode løsninger på plass, men så skjer det noe på utsiden og risikoen sniker seg inn.»**

Sikkerhet i skyen:

Enklere, tryggere og alltid oppdatert

Lars Eidsten, sikkerhetsekspert i Fortinet

Slik kan en skybasert sikkerhetsløsning gjøre det lettere for deg å møte kravene i NIS2-direktivet.

Selv virksomheter som har investert i god sikkerhet, opplever alvorlige hendelser. Ikke fordi teknologien mangler – men fordi den brukes feil, ikke er riktig konfigurert eller har blitt svekket av tilleggsløsninger på siden.

I 85 prosent av tilfellene handler sikkerhetsbrudd om menneskelige valg, feil bruk og oppsett eller manglende oppfølging. Og det er nettopp dette NIS2-direktivet forsøker å gjøre noe med.

– I mange tilfeller har virksomhetene gode løsninger på plass, men så skjer det noe på utsiden, som at noen bestiller et kamera eller overvåkningsverktøy til et prosjekt, og det kobles til utenfor det etablerte systemet. Det er slik risikoen sniker seg inn, sier Lars Eidsten, sikkerhetsekspert i Fortinet.

Ifølge Eidsten er løsningen for mange virksomheter enkel: Flytt sikkerheten dit den er mest effektiv – nemlig til skyen.

> **«Når du konsumerer sikkerhet som en tjeneste, kan du også dokumentere sikkerhet som en tjeneste.»**

Hva er SASE – og hvorfor er det relevant nå?

SASE står for Secure Access Service Edge, og er i praksis en metode for å samle alle sikkerhetsfunksjonene dine på et sted, levert fra skyen. Der du tidligere kjøpte brannmur, trafikkontroll, overvåking og databeskyttelse som separate produkter – alle med hvert sitt grensesnitt og vedlikeholdsbehov – leverer en SASE-plattform alt dette som en helhetlig og oppdatert tjeneste.

– Det handler om å konsumere sikkerhet på samme måte som vi konsumerer serverkapasitet eller programvare; som en tjeneste, forteller Eidsten.

I stedet for å kjøpe og drifte fysiske bokser, som eldes

Falsk trygghet: Lave forventninger til angrep

29 prosent av norske virksomheter vurderer angrepsrisikoen som liten eller svært liten.

Samtidig svarer 18 prosent at IT-nedetid gir umiddelbar driftsstans. Mange over-vurderer egen trygghet.

Kilde: Atea sikkerhetsrapport 2025

og må oppgraderes, abonnerer du på sikkerhet – per ansatt, per måned. Alt vedlikehold, alle oppdateringer og beste praksis er ivaretatt av leverandøren. Du vet at det fungerer, og at det dokumenteres.

En enklere vei til NIS2-samsvar

Der mange virksomheter nå bruker tid på å kartlegge hvilke sikkerhetsfunksjoner de har, og dokumentere hvordan de brukes, snur SASE dette perspektivet på hodet.

– Når du konsumerer sikkerhet som en tjeneste, kan du også dokumentere sikkerhet som en tjeneste. Du har et system hvor alt er konfigurert etter beste praksis, og du kan vise det i sanntid, sier Eidsten.

Dette løser en av utfordringene flest virksomheter vil møte på ved innføringen av NIS2. Nemlig kravet til at du hele tiden må kunne dokumentere hva du gjør og hvordan du tenker i sikkerhetsarbeidet.

Fortinets SASE-løsning har allerede vært gjennom flere samsvarsvurderinger knyttet til NIS2, og erfaringene er gode: Fordi Fortinet bygger egne datasentre og egne skytjenester, unngår de mange av utfordringene som oppstår når sikkerhetslagene legges på toppen av andres skyløsninger.

– Mange skybaserte sikkerhetsplattformer er bygget på tredjepartsinfrastruktur – med amerikanske kontrakter og uklar ansvarsdeling. Vi bygger våre egne og har kontroll hele veien. Det gjør det enklere å sikre, og enklere å dokumentere i samsvar med kravene i NIS2, sier han.

Ikke en magisk løsning på alt

SASE er særlig relevant for deg som har begrensede ressurser, men samtidig må oppfylle krav fra større kunder eller offentlige samarbeidspartnere.

– I disse verdikjedene vil det komme krav om dokumentert sikkerhet. Med en god SASE-løsning kan du raskt få på plass både teknologi og dokumentasjon, uten å måtte bygge alt selv. Det er ikke en magisk løsning på alt, men det er så tett på som det kommer, sier Eidsten.

En SASE-modell gir også fleksibilitet: Har du lokale systemer, som skrivere, kan de kobles til skyen via små, sikre komponenter. Har du en kombinasjon av lokal lagring og skytjenester, kan løsningen følge deg på reisen. Det handler ikke om å gjøre alt over natten, men om å komme i gang.

Enklere, tryggere og mer forutsigbar sikkerhet

– Sikkerhet er ikke et dokument. Det er ikke en brannmur. Det er summen av alt som er satt opp riktig, overvåket, oppdatert og dokumentert. Det er nettopp det vi tilbyr gjennom SASE, sier Eidsten.

For deg som leder betyr det mindre kompleksitet og mer forutsigbarhet. Og en konkret vei til å oppfylle et komplekst direktiv.

Ikke glem de industrielle komponentene

Fortinet er også en solid leverandør innen OT-sikkerhet, altså sikring av industrielle styringssystemer og fysiske anlegg. Det er en helt annen verden enn datasentre og skyløsninger, men like relevant i en NIS2-kontekst.

> **«Sikkerhet er summen av alt som er satt opp riktig, overvåket, oppdatert og dokumentert.»**

– OT-sikkerhet handler ofte om helt andre utfordringer. Som hvem som fysisk får tilgang til styringsskap eller hvordan informasjon sikres fra en sensor til et styringssystem, gjennom hele sin levetid. Her snakker vi ikke om sky, men om analyse av kommandoer som sendes, isolasjon og kontroll på det mest grunnleggende nivået, forklarer Eidsten.

Det er kjernen i Fortinets budskap: Du skal ikke presses inn i én løsning. En helhetlig sikkerhetsstrategi må ta høyde for både digitale og fysiske realiteter, og det er først når du forstår begge, at du virkelig kan oppfylle kravene i NIS2-direktivet.

Atea er Norges største IT-selskap

Med 1800 ansatte fordelt på 23 kontorer rundt i hele Norge står vi i Atea klare for å bistå virksomheten din. Våre rådgivere har solid teknologiforståelse og høy kompetanse, og vi støtter alt av teknologi.

Sammen med våre teknologipartnere tilbyr vi det du trenger for å sikre din virksomhet. Vi tilbyr sikkerhetstjenester som er skreddersydd for din virksomhet og ditt trusselbilde og er tilgjengelig 24/7.

Vil du vite mer?

Ta kontakt med:

Kato Kristiansen
IT-sikkerhetssjef, Atea Norge
Kato.Kristiansen@atea.no

atea.no/it-sikkerhet/

ATEA

Cisco Partner

Microsoft

DELL Technologies TITANIUM BLACK PARTNER

IBM Platinum Partner

paloalto NETWORKS

FORTINET