www.mediaplanet.com

Les hele kampanjen på **www.altomsamfunnssikkerhet.no**

Sikkerhet & beredskap

Et viktig redskap i kampen mot dødsulykker til havs:

Nytt sikkerhetssystem skal forhindre drukningsulykker

ANNONSE FRA DIMEQ

Cybersikkerhet
Tiden er avgjørende når det skjer en større hendelse

ANNONSE FRA DEFENDABLE

Er våre data trygge i skyen?
Truslene er reelle

ANNONSE FRA JOTNE

– Det er typisk norsk å være god ... på situasjonsbeskrivelse

I løpet av de siste to årene har Riksrevisjonen kommet med kraftig kritikk om hvordan offentlige etater og virksomheter som Helseforetakene, NVE. Politiet, Forsvaret og Justis- og beredskapsdepartementet sikrer både nasjonens og mine og dine data.

FOTO: LIV AABERG

Geir Olsen
Direktør for næringspolitikk og kommunikasjon, IKT-Norge

Gjennomgangstonen fra Riksrevisjonen er at det er betydelige mangler, liten oversikt, svak styring, kunnskapsmangel og lav fremdrift i informasjonssikkerhetsarbeidet. I tillegg peker Riksrevisjonen på svak samordning av roller, ansvar og krav og på utdaterte systemer, sier Geir Olsen i IKT-Norge.

Irrelevant om statlig eierskap

– Med dette alvorlige bakteppet skulle vi tro at regjeringens stortingsmelding om datasikkerhet inneholdt en ambisiøs strategi og konkrete tiltak. I stedet får vi en god situasjonsbeskrivelse, men hvor regjeringen går seg bort i irrelevante betraktninger om statlig eierskap når det kommer til konkrete virkemidler. Øvrige virkemidlene er langt på vei fraværende. Det meste konkrete er at regjeringen skal utrede og vurdere, påpeker Olsen.

– Det har vært en betydelig økning i cyberangrep mot norske bedrifter, myndigheter og enkeltpersoner, og behovet for å styrke digital sikkerhet og motstandskraft er større enn noen gang. Det underbygges også av den oppdaterte trusselvurderingen fra PST, Nasjonal Sikkerhetsmyndighet og E-tjenesten, sier Olsen.

Ny teknologi

Olsen peker dessuten på at ny teknologi som kvanteteknologi, kunstig intelligens (AI) og Internet of Things (IoT) vil bety mye for vår digitale sikkerhet og vår motstandskraft.

– Vi har ingen oppdatert strategi for bruk av AI, og vi er det eneste landet i Norden som ikke har en egen kvantedata-strategi. Hadde regjeringen brukt halvparten så mye energi og penger på disse områdene, som på å få oppløst sammenslåtte kommuner og fylkeskommuner, hadde vi kommet langt, mener Olsen.

Langtidsplan for digital infrastruktur

Olsen og IKT-Norge etterlyser en mer helhetlig tilnærming til digital sikkerhet.

– Norge trenger en mer omfattende og ambisiøs strategi for digital sikkerhet, med konkrete tiltak, klare målsettinger og tydelig rolle- og ansvarsavklaring. Dessuten er det nødvendig å styrke samarbeidet mellom offentlig og privat sektor blant annet når det gjelder utbygging av sikker digital infrastruktur og digital sikkerhet, styrke kunnskaps- og kompetansenivået i alle ledd og i alle sektorer, og utvikle innovative teknologiske løsninger for å beskytte oss mot nye trusler. Alt dette underbygger at vi har behov for en politisk forpliktende langtidsplan for digital infrastruktur, slik vi i IKT-Norge har foreslått, avslutter Olsen. ■

mediaplanet

Digital infrastruktur gir bedre mobilitet

Konsulentselskapet Knowit er sentral i Norges arbeid for å nå målet om nullutslipp innen 2030, med bidrag til å effektivisere og tilgjengeliggjøre kollektivtilbudet for norske brukere.

Tekst Jarle Petterson

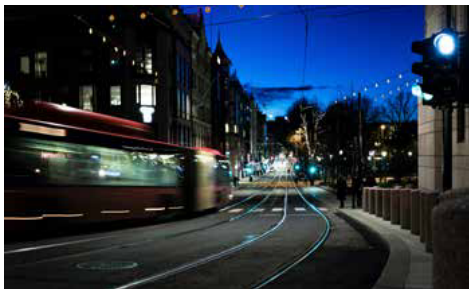


FOTO: BEN GARRATT/UNSPLASH

Et godt utbygget kollektivtilbud er ryggraden i et velfungerende samfunn.

Med 1000 ansatte i Norge, hvorav mange unge, brenner vi for bærekraft. På transport- og mobilitetsfeltet, så vel som andre områder, leverer vi digital infrastruktur, brukt i tjenester de fleste nordmenn kjenner godt, som Skatteetaten, Kartverket, Nav og, ikke minst, de store aktørene i transportsektor, sier Frode Kjos, Knowits direktør for forretningsutvikling mobilitet.

Altomfattende bærekraft

Knowits bidrag til bærekraftsmålene er spesielt uttalt innen god helse og livskvalitet, miljø, likestilling, ren energi, anstendig arbeid og økonomisk vekst.

– Reiser du kollektivt, har vi bidratt til å utvikle løsningene som gjør det enkelt å kjøpe billett, få sanntidsinformasjon og gir valg om fremkomstmiddel. Et godt utbygget kollektivtilbud er ryggraden i et velfungerende samfunn. Det kan ikke bli sånn at vi må bruke én eller to timer av arbeidsdagen til reise til jobb eller for å dekke reisekostnader, mener han.

Alle disse løsningene måler Knowit mot FNs 17 bærekraftsmål.

Alt må «snakke» med alt

Kjos forteller at Norge har forpliktet seg til EUs ITS-direktiv (Intelligente TransportSystemer), som frem mot 2030 og 2050 har prioriterte områder og tiltak for best mulig bruk av data i fremtidig transport. For at vi skal bli klimanøytrale i 2030, og ha et multimodalt transportnettverk i 2050, må vi begynne nå.

– Her jobber vi med aktører som Entur, kollektivselskaper og Statens vegvesen, som skal gi optimal bruk av vei, trafikk og reisedata, der IT-systemene og transportmidlene «snakker» sammen. Når vi legger ny asfalt i sør, bygger broer i vest og sikrer vinterdrift i nord, er vi avhengig av at biler «snakker» med biler, veiutstyr med biler, og så videre.

– Men smarte IT-løsninger er ikke hele svaret. Vi forfekter gulrot over pisk. Et forslag vi støtter, er at arbeidstager ikke beskattes om arbeidsgiver sponser kollektivbilletten, slik at vi får nok en grunn til å velge kollektivt. ■

FOTO: KNOWIT

Frode Kjos
Direktør for forretningsutvikling mobilitet i Knowit

> Reiser du kollektivt, har vi bidratt til å utvikle løsningene som gjør det enkelt å kjøpe billett, få sanntidsinformasjon og gir valg om fremkomstmiddel.

i

Knowit er et konsulentfirma som støtter bedrifter og organisasjoner i den digitale omstillingen. Med en unik kombinasjon av kompetanse innen IT, design, kommunikasjon og management, utvikler selskapet innovative og bærekraftige løsninger, som gir kundene høy forretningsverdi. Tjenestene utvikles og leveres av forretningsområdene Solutions, Experience, Connectivity og Insight.

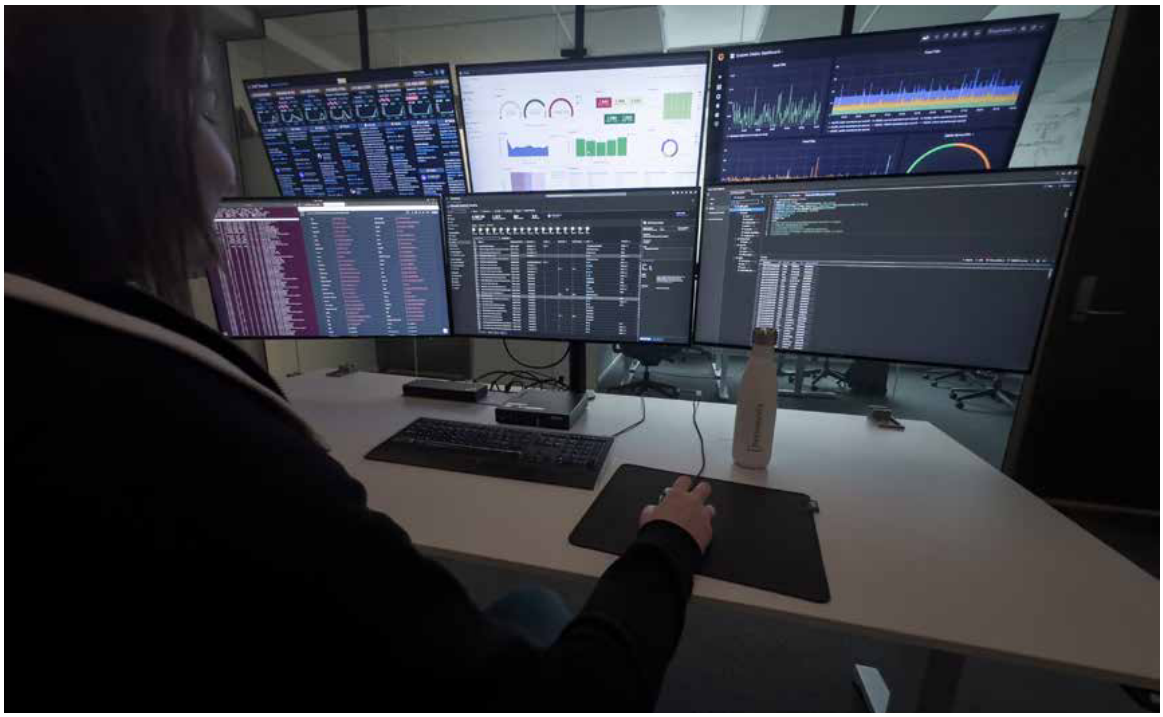
knowit.no

knowit

Prosjektleder: **Fabian Prøsch** (fabian.prosch@mediaplanet.com) Adm.dir.: **Petter Hjelvik Søberg** Produksjonsleder: **Emma Wirenhed** Forretningsutvikler: **Anniken Trollebø** Designer: **Sarah Casu** Distribusjon: **Aftenposten**, Mars 2023 Trykkeri: **Schibsted Trykk** Mediaplanet kontaktinformasjon: E-post: **no.prod@mediaplanet.com** Forsidebilde: **Dimeq**

Defendable

FOTO: DEFENDABLE



Defendable er totalleverandør av sikkerhetstjenester til flere offentlige og private virksomheter. Det innebærer at de også driver 24/7-overvåkning av nettverkene til flere av kundene.

– Det viktigste er å komme raskt opp igjen

Tiden er avgjørende når det skjer en større hendelse. – En time fra eller til kan faktisk være avgjørende for hvor alvorlige konsekvensene blir, sier ekspert.

FOTO: DEFENDABLE

Christer Berg Johannesen
Leder for teknisk sikkerhetsrådgivning Defendable

Christer Berg Johannesen er leder for teknisk sikkerhetsrådgivning i cybersikkerhetsselskapet Defendable og har vært involvert i håndtering og skadebegrensning etter flere store sikkerhetshendelser og angrep mot norske og utenlandske virksomheter.

Han sier at det aller viktigste når noe skjer, er å få et dedikert og erfarent team for hendelseshåndtering (IRT) på plass for å kunne bistå organisasjonen med å få oversikt og begrense skade. Disse er eksperter på å håndtere slike situasjoner, og har erfaring med å løse problemer raskt og effektivt.

– Det primære fokuset er alltid å få gjenopprettet normal drift så raskt som mulig, og samtidig sikre systemene slik at ikke disse forblir sårbare overfor nye angrep. Da handler det om å organisere og koordinere arbeidet med å motvirke angrepet og bygge opp systemene solid fra grunnen av. Når bedriften er oppe og står igjen, vil et team som dette i tillegg kunne hjelpe til med oppgaver som reduksjon av risiko, identifikasjon av hvorfor ting har skjedd, samt å forfatte rapport om hendelsene, sier han.

Med dagens avanserte digitale trusler, er det ikke til å komme fra at et angrep i verste fall kan true en bedrifts eksistens. Da hjelper det også å være forberedt.

– Det er klart at håndteringen kan være mer effektiv når vi allerede kjenner bedriftens systemer og infrastruktur. Da har vi på forhånd utarbeidet planer, rutiner og har oversikt over kontaktpersoner - og kan derfor reagere hurtig og optimalt når et angrep skjer.

Bedriften kan bli ansvarlig

Dagens trusselaktører er dessverre både dyktige og kreative. Det gjør at de stadig finner nye måter å utnytte data fra innbrudd på.

– Moderne angrep er delt i flere faser. Først handler det om å påføre skade og få utbetalt løsepenger. De siste årene har vi imidlertid også sett at de i stadig større grad også går etter kunder og persondata, som kan ende opp med å bli solgt på det mørke nettet, sier han.

Angriperne krypterer altså først offerets filer, ofte i så stor grad at maskinen blir ubrukelig. De stjeler også data, som deretter benyttes til utpressing av både offeret selv, men også offerets kunder, ansatte og øvrige kontaktnettverk.

Blir man utsatt for et dataangrep som fører til at kundedata, og særlig persondata, kommer på avveie, risikerer bedriften i verste fall store bøter fra myndighetene - i tillegg til de direkte konsekvensene av at systemene er nede og personopplysninger kan være eksponerte, sier Johannesen.

– Å investere i sikring før et angrep skjer blir dermed enda viktigere enn mange tror, sier senior sikkerhetsanalytiker i Defendable, Håkon Prestvik.

FOTO: DEFENDABLE

Håkon Prestvik
Senior sikkerhetsanalytiker Defendable

Han ser daglig eksempler på bedrifter som ikke tar sikkerheten på alvor, og mye handler om ganske enkle grep.

– Det kan være utstyr som ikke blir oppdatert, naive passordsystemer som er lette for kriminelle å finne ut av eller brukerkontoer som ikke blir slettet når ansatte slutter. Kriminelle bruker programvare som aktivt leter etter slike svakheter, for å velge seg ut mål og automatisk angripe systemene.

– Ingen hendelser med aktiv overvåkning

Defendable er totalleverandør av sikkerhetstjenester til flere offentlige og private virksomheter. Det innebærer at de også driver 24/7-overvåkning av nettverkene til flere av kundene. Såkalt Managed Detection and Response (MDR) handler om å alltid være i forkant av angrepene og oppdage dem før de utvikler seg til noe alvorlig.

– Vi har faktisk aldri hatt behov for å håndtere større hendelser i miljøer der vi har aktiv overvåkning. De store konsekvensene får man der sikkerheten er for dårlig. Det er mange detaljer som må på plass, men i hovedsak handler det om grundige forberedelser og testing, god sikkerhetshygiene i hele organisasjonen og aller helst kontinuerlig, aktiv overvåkning av alle systemer, avslutter han. ■

FAKTA OM DEFENDABLE

- Norsk sikkerhetsselskap som er en del av NSMs kvalitetsordning for hendelseshåndtering og medlem av NSMs nasjonale cybersikkerhetssenter.
- Hjelper bedrifter med å forsvare seg mot et stadig mer komplisert og økende digitalt trusselbilde.
- Tilbyr blant annet rådgivning og r isikovurdering, sikkerhets- og penetrasjonstesting, 24/7-overvåkning og hendelseshåndtering.

DataEquipment

FOTO: THOMAS B ECKHOFF

Det er ikke lenger mulig å stoppe datakriminelle uten dette

IT-systemer bør overvåkes 24 timer i døgnet. Bruker du fortsatt manuelle løsninger for IT-sikkerhet, er faren overhengende stor for at datakriminelle allerede er på plass.

Løsningen er å knytte seg til et automatisert Security Operations Center (SOC). Cyberkriminalitet var for få år siden noe bare store selskaper og virksomheter måtte bekymre seg nevneverdig for. Nå er situasjonen helt annerledes.

Alle virksomheter, uansett størrelse er i dag aktuelle mål for kriminelle aktører. Det dukker det stadig opp nye eksempler på. Økningen i antall sårbarheter og trusselaktører har vært eksponentiell. Det florerer av cyberkriminelle som er ute etter økonomisk gevinst av kriminell aktivitet på internett.

Derfor bør du bruke SOC

– Det var kanskje mulig å holde tritt med dataangriperne med en IT-ansvarlig som luket bort verstingene manuelt i arbeidstiden tidligere, men slik er det definitivt ikke lenger, konstaterer Thomas Lystad, Operations Manager i Data Equipment.

- Informasjon om alle aktiviteter i IT-systemet logges og undersøkes på et sted.
- Kunstig intelligens og maskinlæring sørger for kontinuerlig overvåking som identifiserer sårbarheter i IT-sikkerheten automatisk.
- Preventiv IT-sikkerhet sørger for at du kommer de datakriminelle i forkjøpet. Dermed kan du stenge dem ute før de har gjort noen skade.
- Du slipper å ha egen, kostbar døgnbemanning for å håndtere dataangrep og IT-trusler.

Datakriminelle bruker selvsagt også automasjon i sine dataangrep. Det er ikke mennesker som sitter aktivt bak en skjerm lenger.

– De bruker automatikken til å gå bredt ut i første angrepsbølge. Så brukes det mer manuelle angrepsmetoder i andre bølge, hvor de jobber seg innover for å komme dit de vil, forteller Lystad.

IT-sikkerhet i alle ledd

Som daglig leder eller sjef i offentlig sektor er det ditt ansvar å sørge for at IT-sikkerheten er ivaretatt 24 timer i døgnet, 7 dager i uka på alle helligdager og i ferier. De færreste har nok ansatte, kompetanse eller systemer til å håndtere dette internt. Så hva skal du gjøre nå som du vet at IT-sikkerheten i virksomheten din mest sannsynlig ikke er god nok?

Det du absolutt ikke bør gjøre, er å lukke øynene og håpe at det går bra allikevel. Du leser kanskje om de store hendelsene og tenker at det skjer ikke meg? Det kan fort bli deg. De datakriminelle tilpasser kravene sine etter størrelsen på virksomheten og bruker automatiske prosesser for å finne akkurat dine sårbarheter.

– Da har du ikke noe annet valg enn å svare med samme mynt, noe som innebærer å knytte seg til en automatisert SOC (et Security Operations Center) De cyberkriminelle kan være lenge inne i systemene før de oppdages. IT-sikkerhet i alle ledd må prioriteres høyere enn noen gang tidligere, sier Lystad.

Viktig å velge riktig SOC

Heldigvis har det heller aldri vært enklere å beskytte seg på riktig måte gjennom å kjøpe IT-sikkerhet som en tjeneste. Tidligere var datasikkerhet på dette nivået kun tilgjengelig for de største aktørene med råd til å investere i eget utstyr og kompetanse.

Nå kan du knytte deg til et automatisert Security Operations Center (SOC) som håndterer alle dataangrep døgnet rundt. Men det er viktig å velge riktig SOC. Du må forsikre deg om at den er tuftet på integrasjon og automasjon. Det betyr at SOAR benyttes, det vil si Security Orchestration, Automation and Response. I Data Equipment er det en selvfølge.

– I en nestegenerasjons SOC, kan du identifisere dataangripere allerede i rekognoseringsfasen, før de har fått tilgang til verdifull informasjon. I de eldre variantene av SOC-er er det mest fokus på reaktiv sikkerhet. Det vil si muligheten til å kunne identifisere hackere og datakriminelle etter at de har kommet seg inn og gjort skade, sier Lystad.

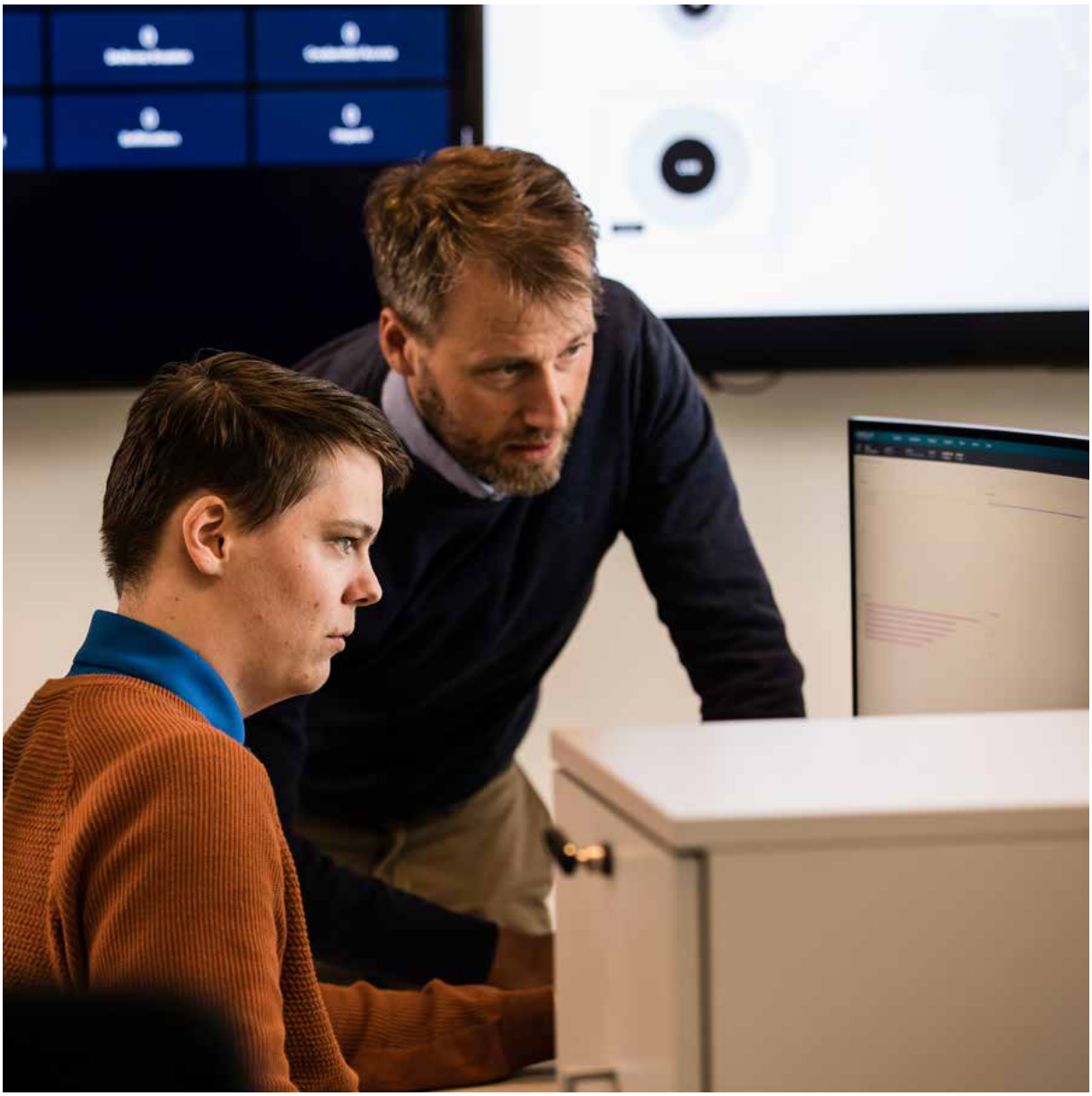
FOTO: THOMAS B ECKHOFF

Thomas Lystad
Operation Manager
Data Equipment

Nøkkelen til god IT-sikkerhet

Data Equipment har utviklet en sikkerhetsplattform som består av flere tjenester. Plattformen heter Intellisec, og en av tjenestene er Managed Detection & Response (MDR). 90 prosent av alle trusler mot IT-sikkerheten kan avverges allerede i rekognoseringsfasen. SOC-en kan håndtere ekstreme mengder data samtidig.

I SOC logges og avdekkes alle



Data Equipment er eksperter på IT-sikkerhet.

hendelser som skjer på maskiner, servere, nettverk og endepunkter. Ved å bruke kunstig intelligens og maskinlæring lukes alle falske positiver ut. Det utgjør over 90 prosent av sakene. Dermed fjernes støyen fra alt som rapporteres som ikke er kritisk. Rundt 10 prosent av tilfellene, gjennomgås manuelt av Data Equipments Incident Reponse-team bestående av IT-sikkerhetseksperter.

– Noen få av de 10 prosentene må eskaleres og meldes fra til kunden, slik at endepunkter som er utsatt for datakriminalitet blir isolert. Teamet tar seg altså av de kritiske tilfellene, hvor det må ageres raskt. Her sitter det erfarne analytikere med den nødvendige kunnskapen om nettverkstrusler og sårbarheter. De vet hvordan de skal identifisere og velge ut de kritiske truslene, forteller Lystad.

Stadig smartere beskyttelse

Den kunstige intelligensen blir stadig smartere og lærer seg nye angrepsmetoder som raskt avverges. Dermed blir tjenesten videreforedlet over tid. Datakriminelle gjenbruker gjerne sårbarheter. Alle kjente måter å hacke på vil ikke bite på dette systemet, og automasjonen lærer hver gang den møter en ny teknikk. Målet er at en kunde skal slippe å håndtere samme type angrep to ganger.

– IT-sikkerhet som en tjeneste er noe de aller fleste virksomheter bør ha. Det viktigste argumentet er at vi håndterer all informasjonen som antageligvis ikke gås gjennom i dag, fordi den ligger spredt i ulike systemer. Det er et gedigent sjansespill av daglig leder å sitte og håpe på det beste. I morgen kan det være du som blir møtt av svarte skjermer og en beskjed om å betale 10 millioner i bitcoin til en ukjent angriper, sier Thomas Lystad, Operations Manager i Data Equipment.

Velger du MDR, plasseres det en agent eller sensor i alle IT-systemene dine som sender dine data inn i SOC-en. Det samles inn og logges så mye data som mulig. Jo mer tilgjengelig data, jo mer velinformerte valg. Logging kombinert med å ta i bruk et Security Operations Center betyr at all denne dataen ved hjelp av kunstig intelligens omgjøres til verdifull etterretningsinformasjon.

En røykvarsler for IT-sikkerhet

Det bør være like naturlig å investere i en SOC som det er å investere i en røykvarsler til huset ditt. Det er essensielt å ha en partner som ivaretar IT-sikkerheten i hele systemet. Da kan unormal brukeratferd oppdages så tidlig som mulig. Tradisjonelt har andre aktører gravd i aska etter at huset har brent ned. Vi vil forhindre at det tar fyr. Data Equipment har en SOC-løsning som ivaretar både dagens og fremtidens datasikkerhet.

Det vil ikke kreve masse ressurser eller spesialkunnskap fra deres side for å komme i gang. Det eneste vi trenger er at våre sensorer settes opp i systemene som skal overvåkes. I tillegg trenger vi en kontaktperson internt som vi kan varsle, dersom det må gjøres tiltak. Vi tar oss av resten. Du slipper å administrere eller utvikle noe selv. Du får en ferdig løsning som alltid er oppdatert til siste og beste versjon. ■

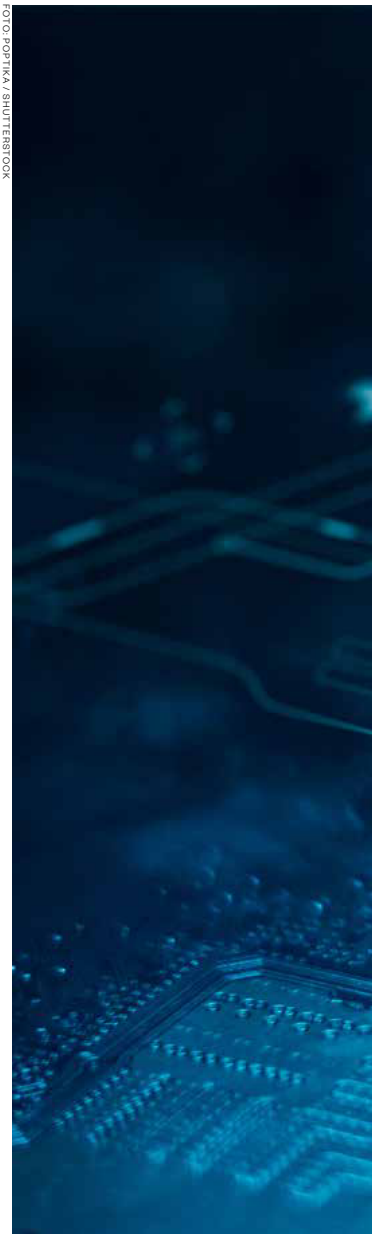
i

Data Equipment har lang erfaring og høy kompetanse innen design og implementering av avanserte sikkerhet- og nettverksløsninger. Les mer på:

dataequipment.no

Jotne

FOTO: POPTIKA / SHUTTERSTOCK



Er våre data trygge i skyen?

Hvorfor aksepterer noen objekteiere at deres data legges i skyen, mens det for andre er totalt uakseptabelt? Digitale tvillinger krever ekstra skjerming, men det ser ut til at også disse dataene legges ut i skyløsninger uten tilstrekkelig verdivurdering? En nasjonalt sikret skyløsning for kritisk infrastruktur er diskutert.
Før denne er realisert er vi svært sårbare – og enda verre, har de ansvarlige for lite kunnskap og fokus på problemstillingen?

Vi omfavner alle de digitale løsningene som omgir oss, i den grad at det har blitt utfordrende å klare seg uten smarttelefonen apper, som styrer vår hverdag og fritid. Siden sårbarhet selger dårlig, har vi liten kunnskap om truslene i vår digitale hverdag. Men truslene er reelle. Her er noen eksempler:

I Ukraina ble en stor gruppe russiske soldater drept fordi de ble avslørt av høy tetthet av russiske mobiltelefoner inne i en og samme bygning. Hadde befalet vært klar over sårbarheten som de utilsiktet ga den som kontrollerte digitale data og som hadde ressurser til å styre granater, hadde de nok forbudt bruken av mobiltelefon.

Andre eksempler er norske pasient-journaler som havnet i Ukraina, at data-operatører i India kunne stoppe lossing av olje på norsk sokkel, og stortings-representanter som tar med seg jobbtelefonen på feriereise og slik kan spores, avlyttes eller hackes.

Heldigvis har de fleste tilfeller av svikt i datasikkerhet ikke dødelig utgang. Men de kan medføre store tap av verdier eller omdømme som det har tatt år å bygge opp, både for selskaper, organisasjoner og individer.

Data samles via skyløsninger

Fremveksten av store dataselskaper som Microsoft, Google, Amazon, Meta, Twitter og TikTok viser hvilken enorm verdi som ligger i digital informasjon. Likevel gir vi disse selskapene full tilgang til dataene våre gjennom deres gratis eller sterkt subsidierte skyplattformer.

I flere av tjenestene samles dataene våre i enorme datasentre uten at eierskap, bruk, misbruk, analyser eller brukerrettigheter er avgjort og tydelige. Avanserte algoritmer (kunstig intelligens) sin tilgang til slike datasentre øker bare verdien for dataselskapene.

Dermed er det slik at de store data-selskapenes tjenester ser ut til å være gratis, men har likevel en kostnad for brukerne. Denne lunsjen er ikke gratis!

Data lagres utenfor vår lovgivning

For en vanlig bruker er det umulig å vite hvor «egne» data er lagret og hvor mye data som er lagret. De fleste skyløsninger håndteres av en lovgivning som ikke er tilpasset brukerens, men dataselskapenes behov.

Derfor har vi trolig heller ikke kontroll over hvilke land eller tidssoner dataene våre befinner seg i, eller hvem som tilgang til dem.

Det vil dermed være umulig å ivareta en verdivurdering, der de som lagrer dataene skal være sikkerhetsklarert eller signere taushetserklæringer.

Hvordan overføres data?

Skyløsningene er også ofte basert på en leverandørs egne formater og tjenestelag (silo). Men hva skjer når brukeren ønsker eller må bytte leverandør. Hvordan overføres data fra en silo til en annen? Hvordan vet vi at dataene våre, som dataselskapene har stor interesse av å eie og kontrollere, faktisk slettes?

Dessuten flyter data mellom ulike virtuelle servere, sikkerhetskopieres til ulike datasentre og gjøres tilgjengelig i flere tidssoner. Dataselskapenes egne proprietære løsninger medfører ofte at det er krevende å flytte data fra en skyløsning til en annen - eller til en på-stedet (on premises) løsning.

Det er kanskje gjort med hensikt, fordi den som eier dataene, eier kunden.

FOTO: NICKI TWANG, PIXEL & CO

Jorulv Rangnes
Avdelingsleder
Jotne

Mangel på nasjonal myndighet

Dermed er det et paradoks at organisasjoner som er underlagt norsk sikkerhetslovgivning ekskluderer bruk av skyløsninger fordi det ikke forenlig med deres verdivurdering, mens andre organisasjoner som også er viktig inn-enfor samfunnssikkerhet og beredskap kommer til den motsatte konklusjonen.

Mest trolig har den sistnevnte gruppen ikke gjort en forsvarlig verdivurdering, men ensidig fokusert på leverandørens markedsføring om tilgjengelighet, skalerbarhet, sikkerhet og lav pris.

En mangel på nasjonal myndighet på området medfører også at stat og kommune i stor grad tar egne valg i kraft

> De fleste skyløsninger håndteres av en lovgivning som ikke er tilpasset brukerens, men dataselskapenes behov.

av prinsippet om sektorstyring. I private og offentlige selskaper er det styret som tar slike valg, og det skjer gjerne uten tilstrekkelig kunnskap, uten veiledning fra myndigheter og ofte basert på det som ser ut til å være laveste kostnad.

Noen virksomheter og andre lands myndigheter stiller krav til at deres data ikke skal behandles av tredjepartsaktører. Det innebærer at de ikke aksepter bruk av skytjenester for sine data.

– For eksempel benytter amerikanske myndigheter klassifiseringen Controlled Unclassified Information (CUI). Her er informasjonen ugradert, men det er krav til at oppbevaring og lagring av dataene skal være hos sluttbrukeren. Skytjenester er her en tredjepartsaktør og kan ikke benyttes for oppbevaring av slik informasjon, sier Karsten Kleven, sikkerhetsansvarlig ved Jotne (tidligere seksjonssjef ved Forsvarets sikkerhetsavdeling).

Igjen er det slik at det som ser ut til å være billig, kan komme til å koste dyrt.

Digitale tvillinger må vernes

En digital tvilling er en digital samling av prosesser for design, produksjon og bruk av produkter. Derfor er en digital tvilling mye mer verdifull enn det fysiske produktet som tilbys i markedet.

– I motsetning til de store dataselskapenes enorme datamengder, som krever avanserte algoritmer for å oppnå en tilsvarende informasjonsverdi, består digitale tvillinger av strukturert informasjon, sier Jorulv Rangnes, avdelingsleder ved Jotne.

Derfor kan tap av - eller uautorisert tilgang til - digitale tvillinger medføre store økonomiske tap og tap av materiell, personell og omdømme. En digital tvilling må dermed passes på og vernes minst like godt som andre typer data, eller bedre.

Hva er løsningen?

Jotne leverer systemer for sikker behandling av digitale tvillinger innen romfart, forsvar, fly og byggeindustri.

Med økende datavolum, behov for tilgjengelighet, skalerbarhet, redundans, lastbalansering og tilgangsstyring, har skyteknologien flere fordeler.

Men kanskje er det slik at disse fordelene overskygges av de mange og uoversiktlige farene som finnes ved å lagre data i skyen. I slike tilfeller er det nok mer riktig å oppbevare og behandle sine data «bak lås og slå» innenfor egne murer. ■

Med økende datavolum, behov for tilgjengelighet, skalerbarhet, redundans, lastbalansering og tilgangsstyring, har skyteknologien flere fordeler.

Jotne leverer systemer for sikker behandling av digitale tvillinger innen romfart, forsvar, fly og byggeindustri.
Les mer på:

jotne.com

mediaplanet

Digitale hendelser må det øves på!

Informasjon fra medlemmer og samarbeidspartnere tilsier at kommuner og fylkeskommuner øver for lite på håndtering av digitale hendelser og kriser. Det er en situasjon det er viktig å gjøre noe med.

I etterkant av det digitale angrepet på Østre Toten har NTNU ved forsker Grethe Østby, gitt ut en forskningsrapport som påpeker konkrete læringspunkter som offentlige og private organisasjoner bør ta lærdom av.

Punkt i krise- og beredskapsplaner

Der påpekes det blant annet at «Cyber-angrep» må være ett konkret punkt på organisasjonens risiko- og sårbarhetsliste. Å miste tilgangen til strøm, internett og telefon er ikke dekkende for et digitalt angrep der man på ulike måter kan miste alle sine data.

Som en konsekvens av et digitalt angrep på kommunen eller fylkeskommunen kan opplysninger om innbyggere, elever, pasienter og ansatte bli lagt ut til salg på det mørke nettet, og enkeltpersoner kan bli utsatt for personlig utpressing. Et annet læringspunkt er at det må stilles krav til trening og øving på cyber-angrep, på lik linje med andre kriserelaterte hendelser.

Det må øves!

KiNS vil gi Statsforvalterne honnør for å ha initiert øvelser i digitale kriser inn mot kommuner i sine fylker. Vi ser likevel behovet for en styrking av selve øvelsesmateriellet og behovet for å heve kvaliteten på gjennomføringen. I tillegg må hyppigheten og realismen i øvelsesgjennomføringen styrkes.

Vi heier på kommuner, fylkeskommuner, Statsforvalterne, DSB, Digdir, KS og andre, som gjennom sine program arbeider for å styrke evnen til digital hendelseshåndtering.

KiNS arbeider for å bidra til å styrke kommuner og fylkeskommuner sin digitale sikkerhet og beredskap, gjennom å tilby nye ressurser og kurs, samt invitere til konkrete møteplasser der tematikken kan belyses, debatteres og erfaringer deles.

Det er ikke et spørsmål om du blir angrepet, det er kun et spørsmål om hvor godt du greier å håndtere hendelsen når den skjer. ■

FOTO: UNSPLASH

FOTO: KINS

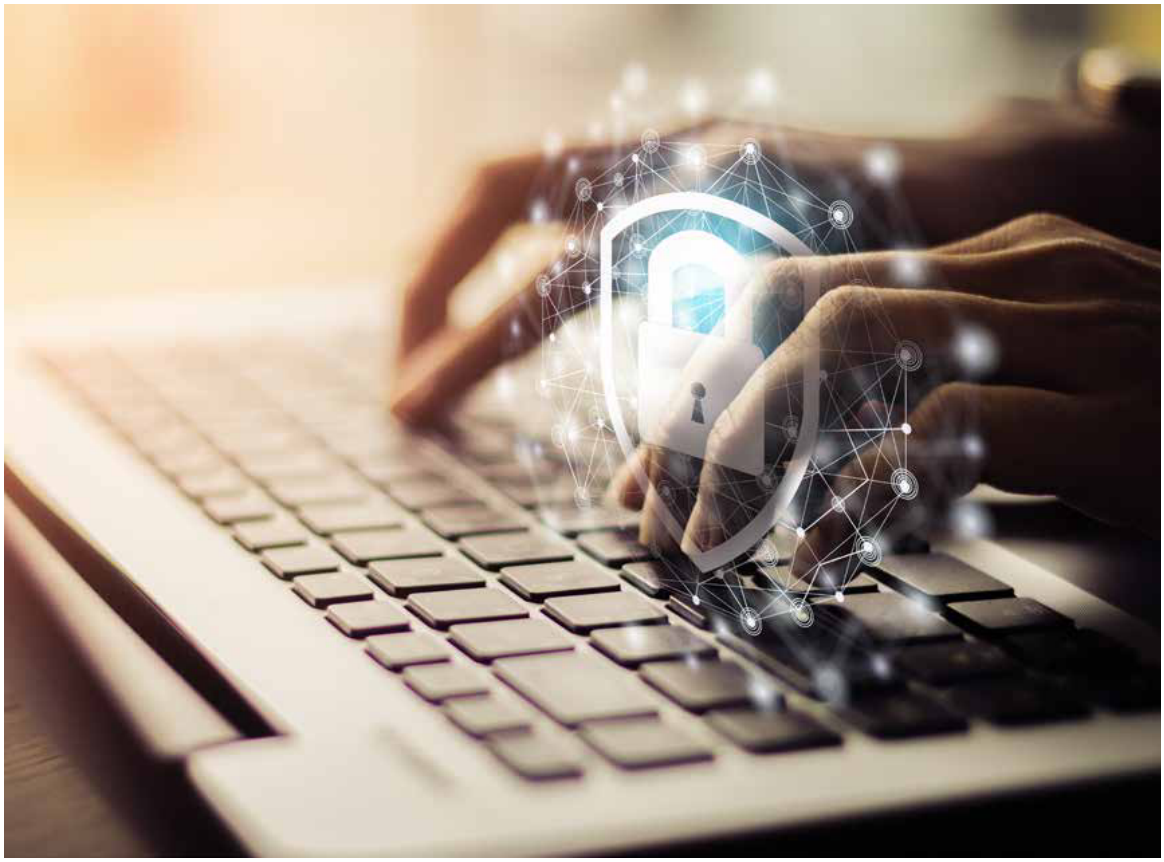
Navn Etternavn
Daglig leder
KINS

> Det er ikke et spørsmål om du blir angrepet, det er kun et spørsmål om hvor godt du greier å håndtere hendelsen når den skjer.

i

KiNS arrangerer en stor årlig konferanse der medlemmer møtes for «networking» og faglig påfyll. Les mer ved å skanne QR-koden:

FOTO: GETTY IMAGES



Operasjonell teknologi kan være vanskelig å sikre ettersom det ofte mangler integrerte sikkerhetsløsninger.

Palo Alto Networks **styrker den operasjonelle (OT) sikkerheten**

Bruk av operasjonell teknologi vokser raskt. Det samme gjør angrepene på denne type teknologi. Derfor lanserer nå Palo Alto Networks en ny løsning for økt operasjonell sikkerhet.

Angrep på operasjonell teknologi kan i tillegg til å forstyrre driften bidra til tap av både inntekter og omdømme. For å hjelpe bedrifter med å holde den operasjonelle teknologien lanserer Palo Alto Networks løsningen Zero Trust OT Security Solution.

– En nøkkelkomponent i løsningen er den nye skydistribuerte tjenesten Industrial OT Security Service. En tjeneste som enkelt kan aktiviseres uten behov for installasjon av flere sensorer. Takket være AI og enkel distribusjon, kan bedrifter enkelt sikre miljøer bestående av operasjonell teknologi, sier Cato Evensen som er daglig leder for Palo Alto Networks i Norge og Island.

Vanskelig teknologi å sikre

Operasjonell teknologi kan være vanskelig å sikre ettersom det ofte mangler integrerte sikkerhetsløsninger. I tillegg begrenser høye krav til oppetid muligheten for regelmessig vedlikehold. I tillegg gjør teknologi som 5G denne type miljøer sårbare da det åpner opp for ekstern tilkobling og tilgang.

– De fleste sikkerhetsløsninger for operasjonell teknologi kommer til kort.

> En viktig del av tjenesten er at den hjelper sikkerhetsteam med proaktivt å forstå risiko.

FOTO: PRIVAT

Cato Evensen
Daglig leder
Palo Alto Networks

Rett og slett fordi de ikke er i stand til å identifisere alle ressurser og eiendeler, og derfor bare kan varsle og ikke forhindre trusler. Noe som fører til sikkerhetshull, sier Cato Evensen.

– Løsningen vi nå lanserer er utviklet for å hjelpe bedrifter med å holde seg trygge gjennom detaljert synlighet, samt via effektiv og integrert sikkerhet. Det samtidig som kravene til tilgjengelighet og oppetid ivaretas, legger han til.

Oppdager uregelmessigheter raskt

Takket være bransjens første maskinlæringsbaserte synlighetsmotor for operasjonell teknologi, gjenkjenner tjenesten hundrevis av enhetsprofiler og over 1000 OT/Industrial Control System-applikasjoner. I tillegg har løsningen hundrevis av OT-trusselsignaturer.

– En viktig del av tjenesten er at den hjelper sikkerhetsteam med proaktivt å forstå risiko. Den observerer og visualiserer adferd kontinuerlig. Uregelmessigheter oppdages umiddelbart og adresseres via brannmuren, sier Cato Evensen.

Produksjon i skuddlinjen

Når industrielle systemer for operasjonell teknologi kobles sammen med IT-systemer, blir angrepsoverflaten mer tilgjengelig for angrep. Forsvar mot stadig mer sofistikerte trusler krever utvidede sikkerhetsstrategier.

– Produksjon er i skuddlinjen for mange nyere nettangrep. Palo Alto Networks Industrial OT Security er avgjørende for å sikre beste praksis for at sikkerheten ivaretas, avslutter Cato Evensen. ■

DIMEQ


FOTO: DIMEQ

Et nytt, smart sikkerhetssystem skal forhindre drukningsulykker

Det nye EyeD systemet som er utviklet av det norske selskapet Dimeq, kan bli et viktig redskap i kampen mot dødsulykker til havs.


FOTO: DIMEQ

Audun Bakke
Medeier, styremedlem og HSE Manager i Dimeq

Yrkesfiskerne har Norges farligste yrke. Ikke noe annet yrke registrerer flere årlige dødsfall. Dette ønsker Dimeq å gjøre noe med. Med det nyutviklede EyeD systemet ønsker de å redusere dødsstatistikken på havet.

– I årene 2000-2019 ble det i fiskeflåten registrert 143 personer som falt over bord, og 94 av de er omkommet. Så sannsynligheten for å overleve om man faller over bord, den er liten. Hadde det skjedd i en industri på land hadde bedriften blitt nedstengt på dagen, sier Audun Bakke, medeier, styremedlem og HSE Manager i Dimeq.

Et armbånd som redder liv

Dimeq sikkerhetssystem er basert på et armbånd med ulike sensorer som lokaliserer mannskapet om bord på skip eller oljeplattformer.

– EyeD har realtids-posisjonering, automatisert realtids-deteksjon av mann over bord og automatiserer alle registreringsprosesser som mønstring av mannskap om bord, sier administrerende direktør i Dimeq, Ronny Bakke.

Dersom en person skulle falle over bord, vil det utløse en alarm. Dermed vil man kunne sette i gang redningsaksjon med en gang. Dette vil øke sjansen for å redde liv.

– Det er ikke lenge siden vi hadde to tilfeller med mann over bord i Barentshavet, men hvor ingen visste at noen hadde falt over bord før det hadde gått flere timer. I slike tilfeller hadde de fått alarm med det samme noen falt over bord, dersom de hadde benyttet EyeD systemet, og muligheten for å bli reddet ville vært atskillig større, sier Audun Bakke.

Realtidsposisjonering av personell er knyttet til nødsituasjoner som brann eller grunnstøting der systemet aktiveres ved en nødalarm. Under en evakuering må kapteinen ha realtids-oversikt over mannskap og gjester dersom dette lar seg gjøre, men utenom det er systemet ikke et overvåkingssystem.

Panikknapp

På armbåndet finnes det også en panikknapp. Knappen gjør det mulig for mannskapet selv å utløse en nødalarm dersom en farlig situasjon skulle oppstå og man trenger å varsle noen.

– Armbåndet har toveiskommunikasjon, så det er også mulig å sende et vibrasjons og lyssignal fra broen ut til armbåndet. Når mannskapet mottar signalet, skal de kontakte broen umiddelbart. Dette vil gjøre det enklere og raskere å kontakte mannskapet spesielt på store fartøy.

Nullvisjon til havs

Timingen for dette produktet kunne ikke vært bedre.

– Det er nettopp gjort et stortingsvedtak om nullvisjon, og etter hva vi forstår er den ballen nå spilt over til Sjøfartsdirektoratet. De skal utarbeide tiltak som skal innføres for å oppnå nullvisjonen, sier Audun Bakke.

Han mener at armbåndet basert på EyeD-systemet har flere funksjoner som kan være gode tiltak for å imøtekomme denne nullvisjonen.

Unik kommunikasjonsplattform

Da Dimeq først begynte å jobbe med sikkerheten til havs, skjønte de fort hvorfor det ikke var blitt utviklet tilsvarende systemer tidligere. Problemet var kommunikasjonen internt ombord i et stålmiljø som vanskeliggjør trådløs kommunikasjon.

– Så begynte vi å forske på hvordan vi skulle gjøre dette, og fant en helt unik måte å gjøre det på. Vi bruker det elektriske nettverket ombord i skipet til å sende data på, og da unngår vi å installere ekstra kabling, sier Ronny Bakke.

Dette kombinerer de med en


FOTO: DIMEQ

Ronny Bakke
Administrerende direktør i Dimeq

Dimeq har nettopp signert «Acceptance Test» med PGS som aksepterer systemet og funksjonaliteten.

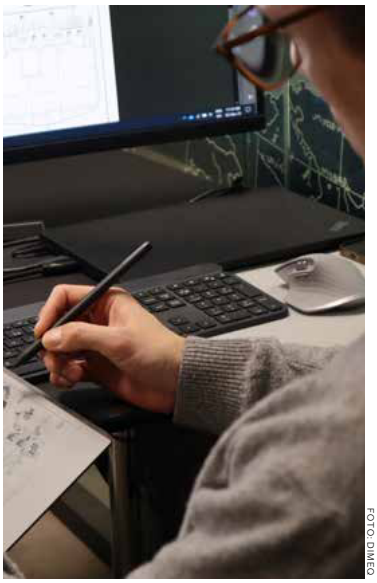


FOTO: DIMEQ

Ronny Bakke jobber med maskinvaren til sikkerhetssystemet.

Wi-Fi-Mesh radioteknologi, og dermed er det mulig å ha kommunikasjon i hele båten, uten store installasjoner.

– Vi har utviklet en unik kommunikasjonsplattform nesten uten kabling og med høy hastighet, sier Ronny Bakke.

Digitalisering åpner for nye muligheter

– Så vidt vi vet så er vi de første til å bruke det elektriske nettverket ombord på et fartøy til å sende data på denne måten, sier Ronny Bakke.

Den nye teknologien vil gjøre det mulig å utvikle smarte fartøy og smart sikkerhet. Dermed vil det bli mulig å analysere og bruke kunstig intelligens til å designe bedre båter i fremtiden og forstå hvordan mannskapet beveger seg.

– Digitalisering av smarte båter åpner opp for enorme muligheter: fjernstyrte medisinske operasjoner om bord, holde styr på lasten, forebygge brann og holde kontroll på farlig gods. Dette kan gjøre det mindre risikabelt og mer effektivt. Man sparer penger på å ha full kontroll på ting, sier Lars Johan Frigstad, arbeidende styreformann i Dimeq.

Selskapet opplever nå økt oppmerksomhet fra media og fra ulike kunder og samarbeidspartnere. Spesielt ser vi interesse fra fiskerifartøy, oppdrettsnæringen, vindmøller og offshore.

– PGS har vært en svært god samarbeidspartner i utviklingen av systemet vårt, og første installasjon på et stort seismikkskip er ventet i løpet av året. Kongsberg Innovasjon er en av våre eiere og har vært nyttig underveis i samtaler med mulige partnere.

Henter inn seks millioner kroner

Akkurat nå skal de starte en emisjon som skal bidra til å finansiere sertifiseringen av produktet slik at de første kommersielle kontraktene kan begynne.

– Vi vil nå gå ut og hente seks millioner kroner, og det er for å ta oss til kommersialisering stadiet med de første kontraktene. Produktet vårt er installert, det er ferdig utviklet på det første skipet, og siden 1. desember har vi vært operasjonelle. Men produktet er ikke produktgodkjent, sånn at de pengene vi nå skal reise, vil gå til å få et endelig produkt som er sertifisert og i kommersiell drift, avslutter Frigstad. ■

i

Dimeq AS er et norsk selskap, basert i Bremanger, som er spesialisert innen sikkerhet til sjøs. Bedriften har blant annet utviklet et personlig verneutstyr, samt sikkerhets-system med realtidsposisjonering for den maritime industrien.
Du kan lese mer om Dimeq her:

dimeq.no

Kommunene jobber for trygge og sikre lokalsamfunn

Alle norske kommuner kartlegger risiko og sårbarhet for å forebygge uønskede hendelser og bygger opp beredskap og evne til å håndtere kriser. Vi vet aldri når en situasjon kan oppstå. Det er kommunen som sørger for at innbyggerne kan leve trygt.

Flom, skred, branner, klimaendringer med mer ekstremvær, er noen av de mange krisene kommunen skal være forberedt på. Langvarig strømstans, pandemi og digitale angrep er eksempler på andre trusler vi må planlegge for å håndtere.

Utviklingen med blant annet økte påkjenninger fra naturhendelser, gjør at det kreves mer av kommunen enn tidligere. Uønskede hendelser forventes å skje hyppigere fremover, og hendelsene forholder seg ikke nødvendigvis til kommunegrensene. Innbyggerne må sikres at de viktigste tjenestene opprettholdes når det oppstår noe ekstraordinært og uforutsett, for eksempel ved langvarig bortfall av strøm og elektronisk kommunikasjon. Å redusere frykt og skape trygghet gjennom god informasjon til innbyggerne er en sentral oppgave for kommunen når noe skjer.

Vi kan aldri planlegge for alt som kan skje, men kommunen har beredskapsplaner som kan tilpasses ulike hendelser. Det er viktig at kommunen øver både på det som står i planene og at de kan improvisere når det utenkelige skjer. Vi kan forebygge og forberede oss så godt vi kan.

Samarbeid styrker aksjonsevnen

KS, kommunesektorens organisasjon, mener det er behov for å styrke samarbeidet mellom kommunen og andre som driver beredskapsarbeid lokalt, både sivile og militære. Vi må sikre at ressursene kjenner hverandre og finner hverandre raskt og effektivt når det gjelder. Kommunen, sammen med brann- og redningsvesen, må trene og samarbeide med politi, sykehus, bedrifter, sivilforsvar, Heimevernet og frivillige organisasjoner.

I dag har de fleste kommuner begrensede ressurser til beredskapsarbeid, og det er store forskjeller både i risikobilde og i hvilken grad de kan være forberedt. Kommunene har fått mange krav og plikter fra statlige myndigheter uten at det følger ressurser med. Mer samarbeid, klare ansvarslinjer og felles øvelser kan likevel bidra til at samfunnet som helhet blir bedre rustet til å håndtere kriser.

Bedre å forebygge enn å reparere

Skred, flom og stormflo kan få store konsekvenser for liv, helse, eiendom, infrastruktur og miljø. Risikoen for naturhendelser ser ut til å øke med klimaendringene. Det er viktig at kommunestyret tar hensyn til naturfare når de skal bestemme bruken av kommunens areal. Dermed kan de hindre utbygging i risikofylte områder og sørge for at utbygging skjer på en betryggende måte. Imidlertid er det allerede eksisterende bebyggelse som ligger i utsatte områder. NVE (Norges vassdrags- og energidirektorat) har anslått at 210 000 bygninger har et sikringsbehov. Alt kan ikke sikres, men KS jobber for at bevilgningene til sikringsarbeidet økes. ■

FOTO: SHUTTERSTOCK

FOTO: PRIVAT

Torill Neset
Spesialrådgiver samfunnssikkerhet og beredskap i KS

Det er viktig at kommunestyret tar hensyn til naturfare når de skal bestemme bruken av kommunens areal.

mediaplanet

NORSK FORENING FOR FJELLSPRENGNINGSTEKNIKK

Sprengstoff er en del av løsningen!

God samfunnssikkerhet og beredskap er avhengig av riktig og velfungerende infrastruktur. Norge er generelt godt rustet, men vi kan fortsatt sørge for at viktig infrastruktur blir enda bedre sikret.

Norsk forening for fjellsprengningsteknikk har mottoet: Utfordringer i dagen – løsninger i grunnen. Vi mener at vi kan utnytte bergmassen til å forbedre både sammfunnsikkerhet og beredskap.

Bergmassen som IT-hvelv
Store deler av samfunnet er etter hvert avhengig av digitale løsninger. Og når vi snakker om at dataene våre ligger i «skya», kan det godt være at vi egentlig mener nedi fjellet. Datasenteret i Lefdal gruver er et glimrende eksempel på god bruk av berget. Det byr på stabile temperatur- og fuktforhold, godt beskyttet for eksterne forhold av alle slag. Kjølesystemet er basert på bruk av sjøvann, og den elektrisiteten som trengs for å drifte anlegget, er hentet fra ren vannkraft.

Energiproduksjon og -lagring
Nesten all elektrisk kraft i Norge produseres i flere hundrede kraftstasjoner som ligger trygt og godt dypt inne i bergmassen. Når vi i tillegg har flere olje- og gass lagre plassert trygt inni fjellet og at flere av ilandførings-ledningene fra Nordsjøen også er lagt i tunneler under strandsonen, så er også dette en viktig beskyttelse av landets kritiske infrastruktur.

Vannforsyning under bakken
Et annet godt eksempel er den nye vann-forsyningen til hovedstaden. Råvannet fra Holsfjorden vil ledes inn til rensing gjennom en nesten to mil lang tunnel. Rensingen av vannet vil foregå i store fjellhaller under Huseby. Deretter vil det rene drikkevannet spres rundt til byens befolkning gjennom et nett av tunneler. Når anlegget står ferdig i 2028, vil bare noen tunnelportaler og et driftsbygg vises. Rensingen av vannet vil forgå trygt og godt inni fjellet uten unødvendig bruk av areal i et ellers tettbefolket område. Kanskje ikke like viktig for beredskapen i samfunnet, men vi kan nevne at også renseanleggene og store deler av transportsystemet for avløpsvannet i hovedstaden også ligger i bergrom og tunneler.

Tilfluktsrom i fjellet
Tilfluktsrom er vel noe de fleste assosierer med beredskap, og igjen er bergrom gode å ha. Flere steder i landet finnes idretts- og svømmehaller i fjell som ved behov kan brukes som tilflukts-rom. På Svalbard har vi også brukt berget til lagring av hele verdens frøbank, så også på den siden er vi med på å opprettholde muligheten til å gjenskape planter og vekster som ellers risikerer å bli utryddet.

90 prosent er tatt ut ved hjelp av sprengstoff
I tillegg til de nevnte eksemplene er det tatt ut mye bergmasse også for å få til et veg- og jernbanenett som støtter opp om samfunnssikkerheten. De siste ti årene er det bygd over 800 kilometer med tunnel i Norge. Over 90 prosent av dette fjellet er tatt ut ved bruk av sprengstoff.

Takk til landets bergsprengere som har gjort dette mulig! ■

FOTO: VEGARD SKOGHEIM

Vi kan sprenge ut store fjellhaller til mange formål under bakken.

> De siste ti årene er det bygd over 800 kilometer med tunnel i Norge. Over 90 prosent av dette fjellet er tatt ut ved bruk av sprengstoff.

FOTO: NFF

Tone Nakstad
Generalsekretær
Norsk forening for fjellsprengnings-teknikk (NFF)

i

Norsk forening for fjellsprengning-steknikk ble startet i 1963 for å samle og styrke fagmiljøene som jobber med teknologi for bergarbeid.
Les mer på:

nff.no

ARCTIC CLOUD SOLUTIONS AS
CLOUD GUIDES

Løsningen «Cloud Center of Excellence» fra Arctic Cloud Solutions vil sikre en trygg reise for din bedrift, hvor alle jobber mot samme mål.

FOTO: GETTY IMAGES

En trygg skyreise for hele bedriften

Digitaliseringen har for lengst gjort sitt inntog i norske bedrifter, men har bedriften din egentlig nok kompetanse om selve skyreisen?

Det er ingen tvil om at sky-tjenester er fremtiden, og den eneste riktige teknologien for å både møte morgendagens krav, holde seg konkurransedyktige og samtidig utvikle bedriften for å nå deres fremtidige mål.

– For å legge gode strategier er man nødt til å inkludere teknologi, men man er da også nødt til å forstå hva teknologien kan gjøre med effektivisering for din bedrift, sier administrerende direktør i Arctic Cloud Solutions, Joakim Brynestad Grøtvedt.

Mange selskaper undervurderer behovet for kompetanse i digitaliseringen, og her kommer Arctic Cloud Solutions inn i bildet.

– Dette landskapet er nytt, og det krever teknologikompetanse utover den tradisjonelle IT-avdelingen. At man har en bevisst strategi på bruk av teknologi i hele organisasjonen er viktigere enn noen gang, sier Grøtvedt.

Høyere sikkerhet

Løsningen «Cloud Center of Excellence» fra Arctic Cloud Solutions vil sikre en trygg reise for din bedrift, hvor alle jobber mot samme mål.

– Ved å forankre dette i ledelsen og nedover, sikrer man en stabilitet og kan samtidig effektivisere driften og levere høyere kvalitet, sier Grøtvedt.

For høyere sikkerhet, mer stabilitet og større fleksibilitet er blant gevinstene ved et velfungerende skykonsept, og Grøtvedt forteller at Arctic Cloud Solutions er ekstra fokusert på det førstnevnte.

– Sikkerhet er øverste prioritet hos oss, og vår kompetanse på teknologi bruker vi for å sikre kunden en sikker skyreise i fremtiden, avslutter Grøtvedt.

Med en bred erfaring fra skyarkitektur i mange forskjellige bransjer, sitter Grøtvedt på en unik kompetanse for å skreddersy optimale løsninger for din bedrift.

– Vi vet hva som fungerer for de forskjellige bransjene og tilbyr alle løsninger innen skyteknologi - tilpasset til hver enkelt kunde, sier Grøtvedt.

> Sikkerhet er øverste prioritet hos oss, og vår kompetanse på teknologi bruker vi for å sikre kunden en sikker skyreise i fremtiden.

En samlet strategi

Arctic Cloud Solutions anbefaler blant annet at det opprettes en styringsgruppe som lager en god og samlet strategi man sammen jobber etter. Ved å benytte seg av «Cloud Center of Excellence»-løsnigen, vil organisasjonen klare å skape endringer på flere områder, som blant annet strategi, teknologi, organisasjons-struktur, kultur og budsjettering.

– Først og fremst er det viktig å bevisstgjøre bedriften på hva man faktisk trenger å ta med seg på veien videre. Vår rolle er å veilede og å heve kompetansen på skyløsninger, og opprette de løsningene som er ønskelig og nødvendig å ta med seg i skyen, avslutter Grøtvedt. ■

Vi gjør kunnskap og ideer til et effektivt forsvar

Foto: Lars Magne Hovtun

FFI driver anvendt forskning og utvikling for at Norge skal ha et effektiv og relevant forsvar og et styrket totalforsvar. Følg med på forskningen vår på ffi.no

FFI Forsvarets forskningsinstitutt

PRODUSERT I NORGE

Massivtre – lagrer CO2 i enorme mengder

Treet suger til seg CO2 når det vokser og lagres som karbon i trestrukturen.

Splitkon leverer komplette byggesystemer i massivtre og limtre.

Moderne og miljøvennlige trebygg er fremtiden. Fra en av verdens største massivtrefabrikker, forsyner vi den norske byggebransjen med bærekraftigeløsninger.

Massivtre fra Splitkon lages kun med PEFC-sertifisert trelast fra norsk skog. Dette gir den høyeste kvaliteten – tilpasset nordiske forhold.

Avansert CNC-teknologi gir oss uendelige muligheter, og en presisjon på millimeternivå, selv på elementer som er opptil 3,5 x 16 m.

Tre er både sterkt, lett i forhold til styrke og kan formes i alle fasonger. Tre er det mest miljøvennlige byggematerialet vi har.

Fakta: Miljøgevinsten/ besparelsen ved bruk av massivtre vs betong er 1 tonn CO2 per m³.

Les mer på **splitkon.no**

Se video om massivtre

Spor X - et av verdens mest miljøvennlige kontorbygg

Spor X i Drammen er et tietasjers kontorbygg med kortreist massivtre fra Splitkon. Prosjektet består av over 200 tilpassede limtrebjelker og 2500 m3 massivtre. Helt uten betong og stål fra grunnmur og opp.

ILLUSTRASJON: DARK ARKITEKTER

SPLITKON