SÄKERHET

Di

Sidorna 10–11

Experter varnar för manipulerad världsbild

FOTO: JACK MIKRUT

Forskaren Lisa Kaati.

Sidan 17

Hon sållar ut risker från tomma hot

Sidorna 2–3

FOTO: JOHAN NILSSON

Cyberhotet mot maten

Cyberattacker mot bönder är i dag en högst reell risk för landets livsmedelssäkerhet, hävdar Marcus Nohlberg, docent i cybersäkerhet.

Hans varning ska ses i ljuset av att Sveriges livsmedelsberedskap avvecklades under 1990-talet.

Så ska maten klaras

Att som svensk alltid ha mat på bordet och kylen full har länge setts som en självklarhet. Men kanske inte längre.

Inte minst den ökande omvärldsoron med Ukrainakriget i vår närhet och Natointrädet har åter aktualiserat frågan om svensk livsmedelsberedskap.

”Den mest extrema situationen som vi kanske ändå måste ta höjd för är att det ska bli krig i Sverige eller i vårt direkta närområde och att en antagonist av någon form då faktiskt försöker slå ut livsmedelsförsörjningen”, säger Camilla Eriksson, forskare på Totalförsvarets forskningsinstitut, FOI.

Camilla Eriksson, forskare på Totalförsvarets forskningsinstitut.

Sveriges livsmedelsberedskap, som den en gång såg ut, avvecklades under 1990-talet. De sista svenska beredskapslagren såldes ut i början av 2000-talet. Konserver med ärter, morötter, bönor och majs. Konserver med köttbullar, korv och makrill. Pasta och ris. Allt avvecklades.

Under flera decennier har det inte funnits någon nationell planering för livsmedelsberedskapen i Sverige. Det finns i dag ingen svensk myndighet med ansvar för livsmedelsförsörjningen i kris och krig.

Alla svenskar uppmanas att ha mat hemma för en veckas förbrukning. FOTO: J EKSTRÖMER

50

procent

Så hög bedöms Sveriges självförsörjningsgrad vara på livsmedel.

Källa: LRF

Den statliga utredningen ”En ny livsmedelsberedskap” som presenterades i februari i år vill råda bot på en del av bristerna i svensk livsmedelssäkerhet vid händelse av kris. Utredningen pekar på kommunerna som huvudsakligen ansvariga för den framtida livsmedelsberedskapen i landet, men också på den enskildes ansvar. Vi bör till exempel alla ha mat hemma för minst en veckas förbrukning.

Utredningen föreslår också en ny lag om livsmedelsberedskap där beredskapslagring och skydd av jordbruksmark ingår. Dessutom ska ett livsmedelsberedskapsråd inrättas, en nationell funktion för att tidigt upptäcka hot mot livsmedelsförsörjningen.

Nya beredskapslager ska också inrättas. Nu handlar det dock inte längre om konserver och torrvaror utan om insatsvaror för att kunna hålla jordbruket i gång, som mineralgödsel, växtskyddsmedel och utsäde.

”Det där är ett ganska vanligt missförstånd. Det lagrades en del färdiga livsmedel i det gamla systemet, men det man framför allt lagrade var insatsvaror för att hålla i gång produktionen. Det var diesel, handelsgödsel, utsäde och bekämpningsmedel. Det är egentligen ganska mycket samma tänk”, säger Camilla Eriksson.

Kostnaden för en ny svensk livsmedelsberedskap bedöms bli 2,3 miljarder kronor över tre år.

Historisk har den svenska livsmedelsberedskapen fokuserat både på beredskapslager av livsmedel och på att ha inhemskt produktion. Nu läggs allt fokus på det senare. Men det är långt ifrån okomplicerat, menar hon.

”Man tänker sig att i krig kommer vi att vara mer beroende av inhemsk produktion än vad vi är annars. Det kan bli stora handelsstörningar och då ska vi inte vara så beroende av import. Men inom livsmedel är det jättekomplicerat. Då handlar det både om färdiga livsmedel och om allt som behövs för att hålla i gång produktionen av livsmedel. Det är en mycket komplex kedja. Vilken produkt man än går in på så finns det en massa beroenden om man backar tillbaka i produktionskedjan. Oavsett om man tar mjölk eller spannmål så krävs det ganska mycket för att få till en produktion.”

Frågan om livsmedelsberedskap kommer idag också i ett lite annat ljus när vi är medlemmar i Nato.

”Ska vi göra den här planeringen fullt ut tillsammans med våra grannländer kanske? I det gamla totalförsvaret var det väldigt stort fokus på nationell förmåga, nationellt försvar. Vi var ju alliansfria och vi hade också den övergripande politiken för neutralitet i krig. Men planeringsförutsättningarna är ganska så annorlunda i dag.”

Samtidigt har vi coronapandemin i färskt minne, hur vi såg att nationella intressen seglade högst upp även då.

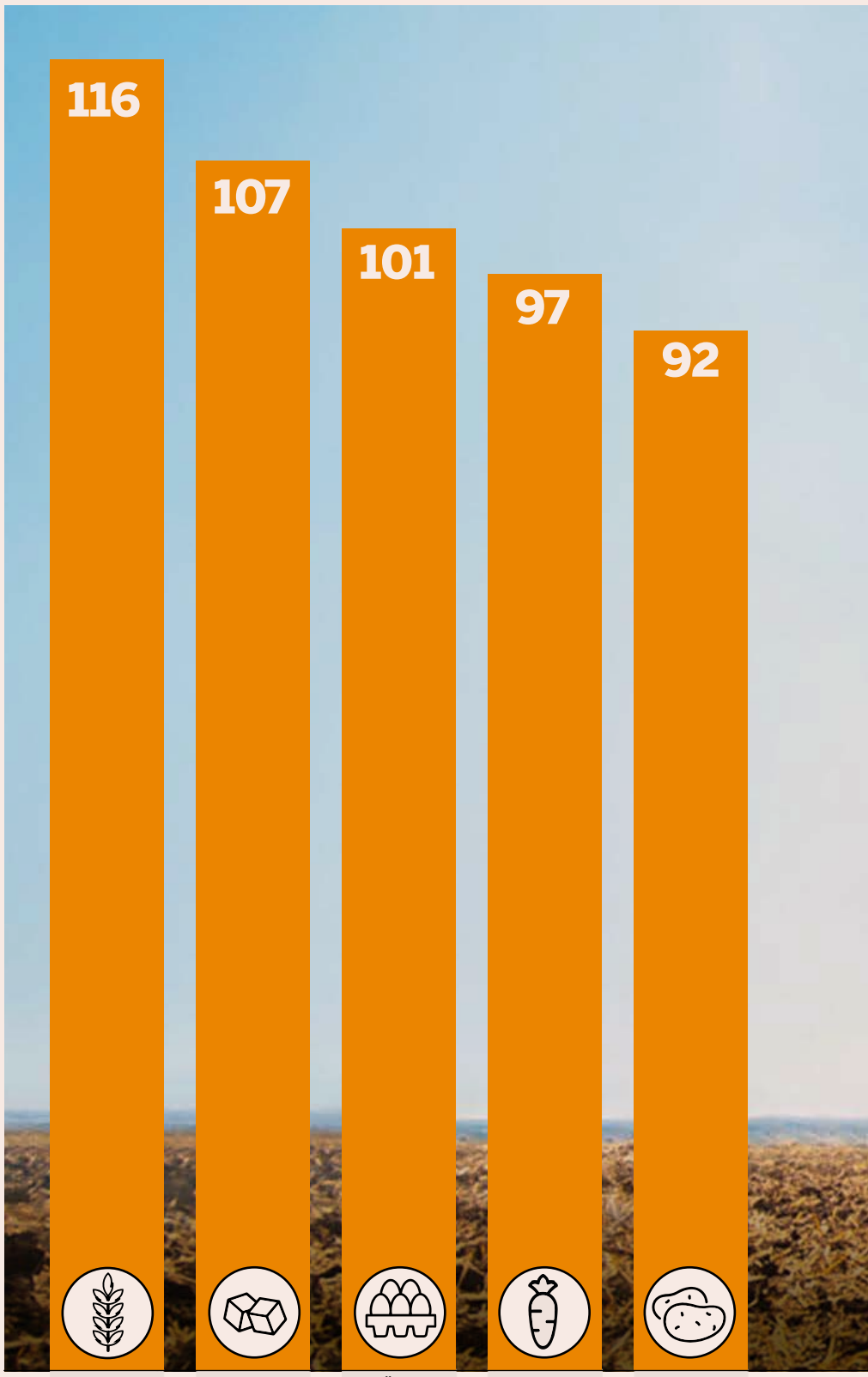
”Vid en allvarlig kris eller krig är det lätt att falla tillbaka i de tankarna. Vi har bara rådighet över det vi själva kan styra över nationellt. Vissa nationella intressen kommer nog alltid att finnas i de här frågorna trots att vi är Natomedlemmar”, säger Camilla Eriksson.

Nu är det inte heller bara den senaste tidens upptrappade oro kring geopolitik och krig som har fått upp frågan om behovet av en bättre svensk livsmedelsberedskap på bordet igen. En rad andra händelser i närtid som torkan 2018, pandemin 2020–2021 som sagt och cyberangrepp mot livsmedelsaktörer har likaså aktualiserat frågan. Andra hot mot en säker tillgång till mat för dagen är kommande effekter av klimatförändringarna, smittsamma sjukdomar och radioaktiva utsläpp som också kan få allvarliga konsekvenser för livsmedelsförsörjningen.

I dag är Sverige självförsörjande på åtminstone tre livsmedel, spannmål, ägg och socker. Svenska morötter finns det också gott om. I stort bedöms dock Sverige ha en självförsörjningsgrad av livsmedel på 50 procent, det vill säga att vi producerar här i landet bara ungefär hälften av de livsmedel som vi konsumerar.

Om det blir krig eller annan kris och vi måste ransonera livsmedel bör varje person tilldelas mat motsvarande 3 000 kilokalorier per dag, enligt en färsk rapport från Jordbruksverket och Livsmedelsverket. Det är långt ifrån någon kriskost eftersom ett rekommenderat kaloriintag ligger mellan 2 000 och 2500 kalorier per dag för vuxna svenska kvinnor och män.

PER OLOF LINDSTEN
per-olof.lindsten@di.se
08-573 650 00



Källa: Jordbruksverket, Från Sverige

Bönderna riskerar

Cyberattacker mot Sveriges bönder. Det är inte det första man tänker på, men det är i dag en högst reell risk för landets livsmedelssäkerhet, hävdar Marcus Nohlberg, docent i cybersäkerhet på Högskolan i Skövde.

”Man har inte riktigt tittat på livsmedelsbranschen ur ett cyberperspektiv. Den är ju numera också en högteknologisk bransch, men vi har inte riktigt hängt med och insett att den är det”, säger Marcus Nohlberg, docent i cybersäkerhet på Högskolan i Skövde.

”Dagens lantbrukare jobbar jättemycket med teknik och avancerad utrustning som AI, robotar och automatiseringssystem. Men de flesta som är i branschen är ju av helt rimliga skäl inte så engagerade i detta.”

Han menar att jordbruket är en bransch som är generellt jämförelsevis långt efter när det gäller it-säkerhet.

”Jag skulle säga att deras stora kompetens ligger inom något helt annat än säkerhet och teknik. De flesta i jordbrukssektorn är också små pytteföretag. Men de tvingas in i digitaliseringen för det går helt enkelt inte att driva den här verksamheten utan automatisering i dag.”

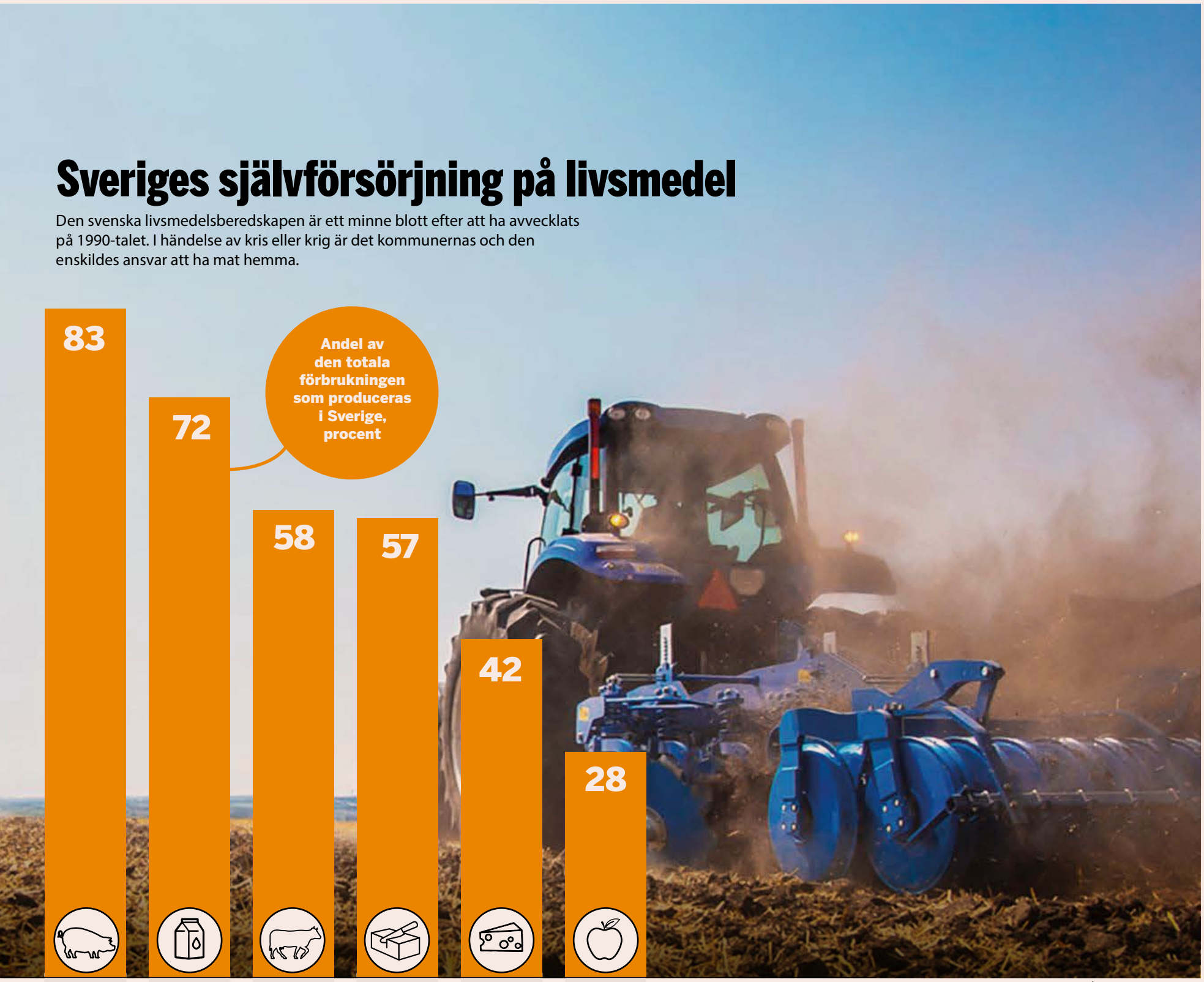
Många lantbrukare har en ansträngd ekonomisk situation, vilket är en del av förklaringen.

”De har inte haft ekonomiskt utrymme att prioritera och köpa bra utrustning. Gårdarna drivs väldigt ofta på

vid kris eller krig

Sveriges självförsörjning på livsmedel

Den svenska livsmedelsberedskapen är ett minne blott efter att ha avvecklats på 1990-talet. I händelse av kris eller krig är det kommunernas och den enskildes ansvar att ha mat hemma.



GRAFIK: LINDA FRIES-ÅMAN. FOTO: MOSTPHOTOS

bli nästa måltavla för cyberattacker

vanliga hemmaroutrar och hemmadatorer. De har köpt billiga saker som fungerar, vilket jag absolut förstår. Men där behöver man ta höjd för att man faktiskt måste skaffa sig en bättre infrastruktur.”

Dagens jordbruk har också en hel del regleringar och krav på sig, både från Sverige och EU.

”Så vi får vara väldigt försiktiga om vi lägger till en jättestor pott med cybersäkerhetskrav också. De behöver den, men de har kanske inte utrymme att klara av det.”

”Faran med att lägga över ytterligare krav och kostnader på lantbrukarna är att många helt enkelt får lägga ned. Då har vi ett jätteproblem, om vi blir av med ännu fler producenter. Nyckeln till ökad livsmedelsberedskap är att vi ska ha så många producenter som möjligt.”

Det är dock inte bara livsmedelssektorns sårbarheter när det gäller cybersäkerhet som oroar Marcus Nohlberg.

”Vi har i Sverige också en

Marcus Nohlberg, docent i cybersäkerhet på Högskolan i Skövde. FOTO: PRESSBILD

massa administrativa sårbarheter. Vi har byggt upp lagar och regler kring att allt ska destrueras om någonting händer. Det där kan en angripare använda.”

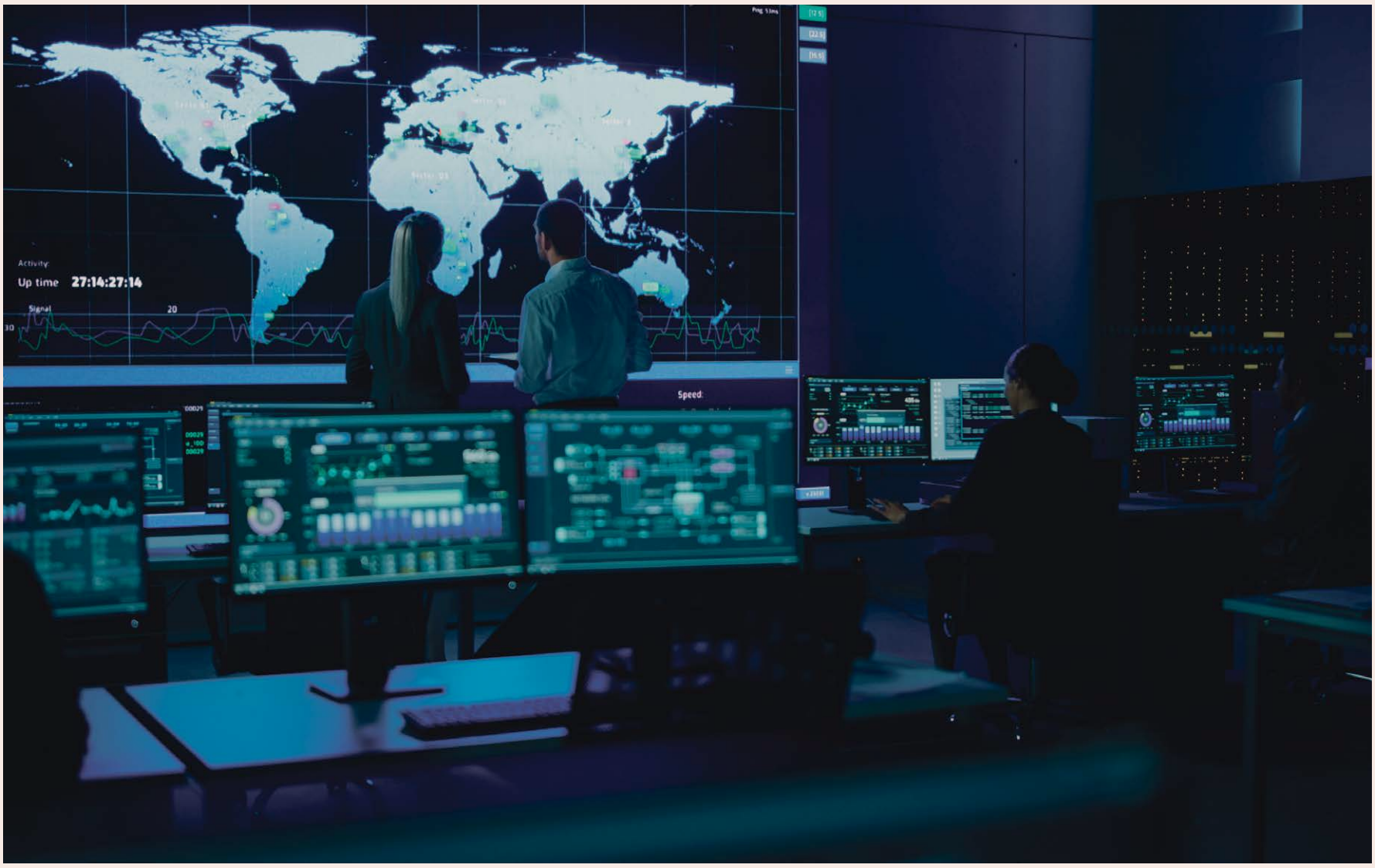
Ett kritiskt exempel han beskriver är att om ett testresultat indikerar att en kycklingbesättning har salmonella då säger reglerna att alla kycklingar i denna besättning måste destrueras, kanske tiotusentals.

”För vi tar det säkra för det osäkra i detta. Det är ju rimligt om vi får in två, tre sådana testresultat per år. Men om vi har en angripare som ger sig på den här databasen med testresultat så kanske vi gör oss av med 80 procent av våra svenska kycklingar på en vecka.”

”Vi har inte riktigt förutspått att vi även kan få processangrepp. Alltså att man lär sig hur våra flöden är med våra godkännanden och angriper dem. Så det handlar inte bara om cybersäkerhet utan det handlar också om att ha rimliga riktlinjer och regler”, säger Marcus Nohlberg.

”Om vi får antagonister som ger sig på att vilja att slå ut vårt samhälle så har vi en enorm sårbarhet i de här processerna. Det är klart att det är viktigt att folk har uppdaterad programvara och bra lösenord. Men som samhälle måste vi också titta över våra beslutsprocesser.”

PER OLOF LINDSTEN



Flexibel MDR-tjänst ger kunder ett starkt skydd – och får dem att växa

Sciber erbjuder en Managed Detection and Response-tjänst, MDR, som anpassas efter varje organisations unika behov – och premierar de som förbättrar det egna cyberskyddet.

– När kunden stärker sitt eget skydd, sänker vi priset på vår tjänst. Det driver utveckling för kunden och frigör resurser, säger Anders Stenwall, COO på Sciber.

Trots att organisationer lägger stora resurser på cybersäkerhetsprodukter, som brandväggar, intrångsskydd och endpointsäkerhet, sker återkommande IT-attacker och intrång med stora skador som följd.

En MDR-tjänst är en form av extern säkerhetstjänst som skapar ytterligare ett lager av skydd, och erbjuds av specialiserade leverantörer för att hjälpa organisationer att upptäcka, analysera och svara på cyberhot i realtid. Den inkluderar bland annat övervakning av organisationens nätverk, system och applikationer dygnet runt för att identifiera ovanliga aktiviteter eller avvikelser som kan indikera en säkerhetsincident.

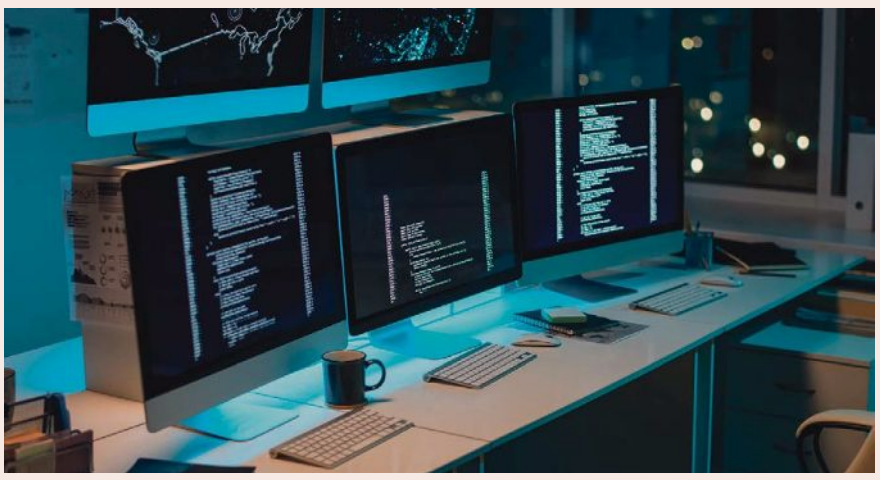
MDR från Sciber sticker ut

Sciber har lång erfarenhet av cybersäkerhetslösningar och erbjuder en MDR-plattform och tjänst som i flera avseenden särskiljer sig från andra lösningar på marknaden. Man arbetar med forskning och utveckling inom cybersäkerhet och kombinerar det med omfattande global hotinformation för att ge sina kunder ett starkt skydd, även mot framtida hot.

– De kunder som kommer till oss har ofta redan vissa grundläggande säkerhetslösningar på plats. Oavsett vad de har och vilka leverantörer de valt kan vi anpassa vår MDR-tjänst efter dem snarare än tvärt om. Det sänker också kostnaden för kunden, förklarar Anders Stenwall.

Väljer kunden att ytterligare stärka sitt cyberskydd kommer kostnaden för Scibers MDR-tjänst att minska efter hand.

– När kunden förbättrar sin egen grundsäkerhet betyder det att vår MDR-tjänst kommer att belastas mindre. Då är det också helt logiskt att priset går ner och resurser frigörs för mer strategiskt arbete. Det blir en väldigt bra motor för att göra förbättringar och jobba mer med strategin för att ytterligare stärka säkerheten, säger han.



Kunden äger Scibers MDR-anpassning

En viktig del av Scibers MDR-erbjudande är att de anpassningar som görs efter kundens existerande verksamhet stannar hos kunden, även efter att samarbetet avslutas.

– Alla anpassningar görs i kundens egen miljö, inte hos oss. Det gör att kunden kan dra nytta av dem i det långa loppet, även om de skulle byta tjänsteleverantör i framtiden, säger Anders Stenwall och avslutar:

– Vår MDR-tjänst är proaktiv och hjälper kunden att hela tiden förbättra och stärka sitt eget cyberförsvar. Det skapar en starkare verksamhet hos kunden vilket vi gärna bidrar till.

Anders Stenwall, COO på Sciber.

FAKTA

Sciber är en svensk aktör inom cybersäkerhet med ledande kompetens inom Managed Detection and Response-tjänster. Företaget stärker cybersäkerheten genom att integrera djup expertis med innovativ utveckling.

Läs mer och kontakta Sciber på:
www.sciber.io

sciber
DATA DRIVEN DECISIONS

netskope

SASE Summit 2024 Stockholm

Where Networking, Security, and Zero Trust Converge

Epicenter • May 14th

Join us for an immersive, educational in-person event. We will delve deep into understanding the benefits of a converged network and security as a service platform and how to begin or advance your journey to SASE and zero trust.

Scan the QR code to register.

netskope

EXCLUSIVE NETWORKS

sciber
DATA DRIVEN DECISIONS

Tryggt, effektivt och säkert med Heta Arbeten®

Med över 100 års kunskap av brandförebyggande arbete och drygt 2 miljoner utbildade hetarbetare är vi experter inom området. Med oss får du inte bara kunskap och certifikat Heta Arbeten®. Du får även tillgång till digitala verktyg som stöttar i ditt arbete, effektiviserar tillståndshanteringen och ökar brandsäkerheten för företaget.

Certifiering Heta Arbeten®

Boka din utbildning hos någon av våra drygt 300 arrangörer. De finns i hela landet så att du kan hitta en utbildning nära dig!

hetaarbeten.se/sv/hitta-utbildning

Effektivt och säkert med digitala vertyg för företag

Effektivisera tillståndsprocessen med Heta Arbeten® PREMIUM. Med PREMIUM sparar ni tid, får en unik överblick och ökar säkerheten.

hetaarbeten.se/sv/premium

Heta Arbeten®
BRANDSKYDDSFÖRENINGEN

DETTA ÄR EN ANNONS FRÅN AVOKI

AI som säkerhetsverktyg – hitta balansen mellan risk och nytta

Nu har Office Management, Xite och Bluecom samlats under varumärket Avoki. Med gemensamma krafter vill man hjälpa företag att stärka cybersäkerheten med AI.

Avoki har gjort en ny trendspaning 2024, som fördjupar sig i den dynamiska utvecklingen och strategiska överväganden för att revolutionera sättet vi arbetar och samarbetar på. Trender som balanserad säkerhet och smart automation ses här som några av de viktigaste nyckelskiftena.

Avoki, som kan ses som ett svar på ovan nämnda trender, vill fungera som en rådgivande strategisk partner inom allt från den hybrida arbetsplatsen och mötesteknik till säkerhet, nätverk, cloud och AI. Inom AI-området bygger företaget lösningar tillsammans med kunderna.

– Vi hjälper dem att accelerera sina usp:ar många gånger om. Så sent som i dag fick vi en förfrågan från en kund som ville hyra in oss som AI-chefer, för att få till ett kontinuerligt strategiarbete med omvärldsbevakning. Vi kan alltså både bygga lösningar och hjälpa till att staka ut en plan för framtiden, säger Peter Uddfors, vd på Avoki.

Peter Uddfors, vd på Avoki.

Balansera risk mot nytta

Med en konkret AI-strategi kan företag värja sig mot cyberhot.

– Den geopolitiska situationen har resulterat i en acceleration av intrångsförsök och attacker mot företag. De kriminella börjar få riktigt kraftiga verktyg. Här har vi utvecklat skydd och säkerhetssystem baserade på AI som gör att vi nu kan ligga steget före, säger Peter Uddfors.

Att bromsa för att minska sårbarheten är inte ett alternativ – vinsterna med digitalisering är för stora. Det gäller att balansera risk mot nytta och hitta den gyllene medelvägen. Eftersom det handlar om företagets konkurrens- och motståndskraft bör frågan diskuteras på ledningsgruppsnivå, menar kollegorna på Avoki.

Fem punkter att diskutera i ledningsgruppen

1. **Regelbundna nulägesanalyser.** Var står vi i dag? Vilka säkerhetsåtgärder har vi gjort?
2. **Starka autentiseringsmetoder.** Användarnamn och lösenord är inte tillräckligt, var kan vi använda multifaktorautentisering?
3. **Angripare är dynamiska och påhittiga.** Använder vi dynamiska och proaktiva säkerhetssystem? Täcker vi molntjänster, ändpunkter, nätverk och kommunikationsvägar?
4. **Backuper.** Har vi säkerställt att våra säkerhetskopior fungerar och är skyddade?
5. **Utbildning.** Är våra användare utbildade i säkerhetsrutiner och potentiella hot?

Läs mer på:
www.avoki.com

Besök oss på Linkedin:
www.linkedin.com/company/avoki

AVOKI
IT that sparks your business

Genom att attackera fraktfartyg har huthirebellerna orsakat den största störningen i den globala handeln sedan covidpandemin. Oljetankern Marlin Luanda, som seglar under Marshallöarnas flagg, besköts tidigare i år i Adenviken av en missil som avfyrats av huthistyrkorna. I Sverige drabbar oron främst exporten av skogsprodukter. FOTO: INDISKA FLOTTAN VIA AP, HENRIK HOLMBERG

Attacker i Röda havet slår mot svensk skogsnäring

De jemenitiska huthirebellernas attacker på sjötrafiken i Röda havet, som står för 30 procent av containertransporterna, slår hårt mot världshandeln.

Extra hårt slår attackerna mot svensk export av skogsprodukter. Någon lösning finns inte i sikte.

”Vår väg till Kina är under attack.”

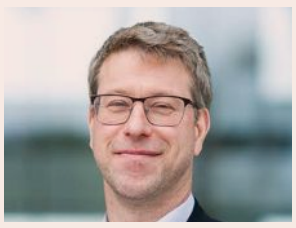
Det säger Anders Hermansson, vd för branschföreningen Svensk Sjöfart och syftar på attackerna från de Iranstödda jemenitiska huthirebellerna som har pågått sedan den 19 november i fjol.

”Vi ser löpande att det sker attacker eller incidenter i området. Att civila fartyg och besättningsmän attackeras är helt oacceptabelt.”

Huthirebellerna stöder Hamas i kriget i Gaza och gick tidigt ut med att rörelsen kommer att attackera alla fartyg som är på väg till eller från Israel. Men attackerna har utökats och ingen kan känna sig säker förutom möjligen fartyg med rysk eller kinesisk flagg efter att länderna nyligen, enligt nyhetsbyrån Bloomberg, har nått en överenskommelse med rebellerna i utbyte mot att stötta dem politiskt på den globala arenan.

Nyligen sjönk skeppet Rubymar, som seglade under belizisk flagg, med en last bestående av gödningsmedel. Olja har läckt ut från fartyget och riskerar att orsaka stora miljöskador. I början av mars fick också attackerna en dödlig utgång då tre besättningsmän ombord på ett grekisktägt fartyg, True Confidence, blev utsatt för rebellernas attacker.

Röda havet är en av världens viktigaste sjöleder, med 15 procent av den globala handelssjöfarten och 30 procent av containertrafiken. Den är också avgörande för exporten av olja och gas från Persiska viken till Europa, enligt Utrikespolitiska institutet.



Anders Hermansson, vd för branschföreningen Svensk Sjöfart. FOTO: CATHARINA FYRBERG

”Vi bedömer att vår bransch är den enskilt största svenska transportköparen av containerfrakter via Suezkanalen.”

CHRISTIAN NIELSEN, MARKNADSANALYTIKER PÅ SKOGSINDUSTRIERNA

Den svenska och europeiska handeln är väldigt beroende av sjötransporter genom Suezkanalen. När ett containerfartyg fastnade i Suezkanalen våren 2021 räknades de ekonomiska skadorna i miljarder.

”Den här gången fanns som tur var en viss ledig kapacitet som gjorde att störningar och förseningar kunde absorberas relativt väl. Men vi har ändå sett att situationen lett till såväl ökade transportkostnader som ökade koldioxidutsläpp”, säger Anders Hermansson, och syftar på att fraktbolagen har styrt om sina rutter och att många nu tar den längre vägen runt Afrika och Godahoppsudden.

”Beroende på typ av fartyg tar det mellan tio dagar och två veckor längre att gå den vägen vid trafik mellan Asien och Europa. I många europeiska länder är handeln med Asien stor och växande och detta är inte optimalt för ett handelsberoende land som Sverige.”

Framför allt drabbar oron i Röda havet svensk export av skogsprodukter. En tredjedel av den svenska exporten i volym som skeppas via Suezkanalen är skogsindustriprodukter. Det är nästan lika mycket som Sveriges samlade import genom kanalen, enligt branschorganisationen Skogsindustrierna.

”Vi bedömer att vår bransch är den enskilt största svenska transportköparen av containerfrakter via Suezkanalen, där kostnaderna nu oväntat har ökat med 100–200 procent, och därmed ser vi med viss oro på framtiden. Det finns risk för containerbrist, förseningar och begränsningar av fraktresurser”, säger Christian Nielsen, marknadsanalytiker på Skogsindustrierna, i ett pressmeddelande.

”I många fall har leverantörerna, särskilt på trävarusidan, lyckats komma överens med sina kunder om att dela på de ökade kostnader som har uppstått. Men självklart påverkas de. Vi befinner oss redan i en försämrad konjunktur med sjunkande färdigvarupriser, samtidigt som vi har ett generellt högt kostnadsläge. Men över tid, för nya kontrakt, bedömer vi att det i många fall är en kostnad som kunden i Asien kommer att behöva bära”, säger Christian Nielsen.

Den danska fraktjätten Maersk vill inte spekulera i hur länge det oroliga läget i Röda havet kan komma att bestå, men har liksom många andra fraktbolag dirigerat om sin trafik att ta vägen runt Afrika.

”Medan vi hoppas på en hållbar lösning i en nära framtid och gör vad vi kan för att bidra till detta, uppmanar vi våra kunder att förbereda sig för att störningarna kommer att fortsätta”, skriver bolaget i ett pressmeddelande.

JILL BEDEROFF
jill.bederoff@di.se
08-573 650 00

Dagens industri

- Ansvarig utgivare: Peter Fellman.
- Redaktör: Carl Björk.
- Tryck: Bold printing i Stockholm, Borås Tidning Tryckeri samt Daily print Umeå.
- Kontakt: Dagens industri AB, 100 26 Stockholm, 08-573 650 00, special@di.se
- Medföljer som bilaga i Dagens industri.

Cissi Nilsson, vd på Safety by Cilia.

Hennes armband ska stoppa överfall

Med ambitionen om att öka säkerheten för kvinnor och göra något åt den nattsvarta våldtäktsstatistiken, skapade Cissi Nilsson ett armband med inbyggt överfallslarm. Innovationen har tagits emot väl. Nu vill Safety by Cilia växa.

Framför starka studiolampor och fem drakar presenterade Cissi Nilsson sitt armband med inbyggt överfallslarm, en produkt som hon jobbat hårt för att realisera. Medverkan i tv-programmet ledde till att Safety by Cilia kunde påbörja sin tillväxtresa.

– Jag kom på idén för sex år sedan, men började jobba med den på riktigt under 2021. Sedan dess har jag och min CTO Suranjan Ram Ottikkutti utvecklat all vår teknik in-house, vilket tagit sjukt mycket tid och kostat mycket pengar. Men jag är glad att vi har gjort det, för nu har vi kunnat ansöka om patent, berättar vd:n Cissi Nilsson och fortsätter:

– I januari tog vi även in en större investering och kunde anställa mer folk. På mindre än ett år har vi nästan 20-dubblat vår bolagsvärdering, vilket är superkul.

Ett smycke som ska öka tryggheten

Historien bakom affärsidén är mörk. Efter ett våldtäktsförsök isolerade sig Cissi Nilsson i sitt hem i flera år, tills hon fick nog.

– Det hade varit lätt att känna sig uppgiven i den situationen, men det var som att något slog till. När jag upptäckte att min produkt inte fanns på marknaden kände jag ett driv. Det var jag som skulle göra något åt det.

Safety by Cilias första produkt är alltså ett smycke med inbyggt överfallslarm. Hjälp påkallas genom att trycka på knappen på armbandet. Då går det ut ett larm i form av ett avskräckande ljud, och GPS-positionen skickas till armbandsbärarens förvalda nödkontakter. För den som befinner sig i en otrygg situation i hemmet finns möjligheten att skicka ut ett tyst larm.

> ”När bäraren trycker på sitt armband startas en automatisk ljudupptagning genom vår app. Det inspelade ljudet, som inte kan raderas, kan fungera som bevismaterial. Jag hoppas att denna funktion ska göra något åt statistiken över fällande domar.”

Skapar bevismaterial

Samtidigt får ”räddare”, användare av Safety by Cilias app, notis om att någon i närheten är i nöd. Väljer räddaren i det läget att hjälpa till, godkänner hen att kontaktuppgifter delas med polisen för att underlätta vittnesförhör.

– När bäraren trycker på sitt armband startas en automatisk ljudupptagning genom vår app. Det inspelade ljudet, som inte kan raderas, kan fungera som bevismaterial. Jag hoppas att denna funktion ska göra något åt statistiken över fällande domar, säger Cissi Nilsson.

”Först i världen”

Det är armbandets funktioner som hon är mest stolt över, men designen är inte att förringa. Det är ett riktigt smycke, utformat för att kunna bäras i alla situationer.

– Min tanke var att det skulle vara naturligt att ha på sig ett överfallslarm, och då kändes det självklart att produkten skulle vara ett smycke. Vår plan är det ska bli en komplett kollektion framöver. Just nu sitter vi och skissar på örhängen, det blir vi först i världen med faktiskt, säger Cissi Nilsson.

FAKTA

Under 2022 anmäldes 9 635 våldtäkter i Sverige. Mörkertalet är stort – upp till 90 procent av fallen kommer inte till polisens kännedom. Bara 5 av 100 våldtäkter som går till rättegång leder till fällande dom. Studier har också visat att varannan kvinna är rädd för att bli utsatt för brott. Källa: Brottsförebyggande rådet, Brå.

Nyfiken på Safety by Cilias smycke? Läs mer här.
https://safetybycilia.se/

SAFETY BY CILIA

Expert: Därför behövs ett helhetstänk i säkerhetsarbetet

Att skapa en bra säkerhetsnivå i en verksamhet handlar lika mycket om fysiskt skydd som en kultur, men också god kännedom om personalen.

– Det behövs en systematik och ett helhetstänk i säkerhetsarbetet, och det kan vi hjälpa till med, säger Elias Tapper, VD på säkerhetsföretaget Fortify Security.

Det geopolitiska läget i Sveriges närhet har gjort att säkerhetsfrågor blivit allt mer aktuella. Samtidigt har säkerhetsskyddslagen skärpts, vilket ställer ökade krav på vissa verksamheter att stärka skyddet mot brott som spioneri, sabotage och terrorism.

Nu när Sverige blivit medlem i NATO kommer en hel del förändras för många inom totalförsvaret. Det är en omställning som man kan behöva hjälp med. Flera stora infrastrukturprojekt har redan påbörjats, och fler är på väg. Säkerhetsaspekter kring dessa är ofta en utmaning.

Fortify Security har lång erfarenhet av att hjälpa organisationer att hitta och bygga rätt säkerhetsnivå. Säkerhetsarbetet börjar med att man gör en analys. Utifrån den vidtar man sedan åtgärder.

– Det finns en uppsjö av olika perspektiv på säkerhet. Vi försöker skapa en helhet, och samarbetar med olika leverantörer för att skapa en komplett lösning anpassad för varje verksamhet, säger Tommy Stiernerlantz, säkerhetsskyddsrådgivare på företaget.

Arbetskulturen påverkar säkerheten

Ofta när man pratar om säkerhet tänker man på cybersäkerhet och fysisk säkerhet. Men lika viktigt är de människor som finns i organisationen – och att de vet vad som gäller.

– Ledningen måste förstå varför säkerheten är viktig. Först därefter kan man börja arbeta med frågan ute i organisationen. Det måste också finnas ett regelverk som alla kan förhålla sig till. Utan det här kommer man aldrig att lyckas med sitt säkerhetsarbete, förklarar Elias Tapper.

En viktig komponent är kulturen, och att få upp säkerhetsmedvetandet bland medarbetarna. Samtidigt vill man inte skapa en känsla av misstänksamhet, där de känner sig övervakade av ledning och kollegor.

Tommy Stiernerlantz, säkerhetsskyddsrådgivare, och Elias Tapper, VD, på Fortify Security.

– Man vill inte ha ett system med angiveri utan måste hitta en balans. En lösning är att införa en visselblåsarfunktion, där man kan påkalla uppmärksamhet om man sett eller hört något som inte är som det borde vara, säger Elias Tapper.

Infiltration ett allt större hot

En bra väg är också att inta en förlåtande attityd, där medarbetare utan risk för att förlora jobbet känner att de kan berätta för sin chef att man av misstag utsatt sin organisation för en risk.

En aktuell fråga är skydd mot infiltration. Sverige har nyligen haft flera fall där personal på olika myndigheter samarbetat med kriminella.

– Förutom säkerhetsprövning och bakgrundskontroller kan man motverka infiltration genom rätt ledarskap, tydliga rutiner, men också genom att bygga en vi-känsla bland personalen och få dem att förstå att man jobbar tillsammans. Det här kan vi på Fortify Security berätta mer om, avslutar Tommy Stiernerlantz.

FAKTA

Som kvalitetscertifierade enligt ISO 9001 är Fortify Security ett av få bolag i branschen som kan påvisa dokumenterad kvalité i de säkerhetstjänster som företaget erbjuder. Fortify Security erbjuder ett strukturerat och välbalanserat arbetssätt med kunden i fokus. Fortify Security är specialiserade på säkerhetsskydd, men kan erbjuda en helhetslösning vad gäller säkerhet.

Läs mer på:
www.fortify.se

FORTIFY SECURITY

När spekulationscirkusen runt brittiska prinsessan Kate till sist kulminerade i beskedet att hon behandlas för cancer var pressuppbådet stort. Både brittiska och utländska tv-team direktsände från utanför Windsor Castle.

FOTO: MAUREEN MCLEAN/SHUTTERSTOCK

Forskare: Hotbilden växer

Med de nya kraftfulla AI-verktygen är det lätt att fejka såväl bild som video för att sprida desinformation.

Plötsligt blir det lätt att avfärda en äkta bild för att den inte passar ens åsikter eller checka ut för att det ändå inte går att avgöra sanningshalten. Det menar två av Europas främsta experter på digital desinformation.

Det brittiska kungahuset är i gungning efter besked om två cancerdiagnoser inom loppet av en dryg månad. Först kung Charles i februari och förra veckan så även prinsessan Kate Middleton.

Det hade kunnat räcka kan man tycka, men i stället fick kungahuset även hantera den perfekta storm som uppstod efter att prinsessan hade försökt lugna allmänheten genom att lägga ut en bild på sig och sina tre barn på mors dag.

Det visade sig ganska snart att bilden var manipulerad och den togs därför snabbt ned från alla nyhetssajter. Detta i kombination med att prinsessan inte hade synts till sedan kungahuset i januari meddelade att hon skulle genomföra en magoperation lade grogrunden för ett viralt spinn som fullständigt saknade gränser.

”Detta är vad som händer när det finns ett stort informationsgap kring en fråga”, säger Eliot Higgins, grundare av den journalistiska grävargruppen Bellingcat.

”Det blir ett tomrum som fylls med konspirationsteorier och grupper som studerar varje liten detalj i bilder och skapar en massa teorier och idéer. Det plockas upp av andra och innan du vet ordet av så har det skapats en alternativ verklighet som folk tror är sanningen bara för att de har läst om det på nätet.”

Eftersom Kate Middleton också befinner sig i det mest granskade kungahuset i världen fanns det redan tidigare ett stort tryck.

”Vad det brittiska kungahuset säger och gör har en stor betydelse för hela samhället, inte bara för skvallerpressen”, säger Carl Heath, senior forskare och fokusledare för området digital resiliens på Rise samt doktorand vid institutionen för tillämpad it vid Göteborgs universitet.

Det dröjde inte länge förrän spekulationerna kring vad som hänt Kate Middleton landade i ryska medier där det spreds information om att kung Charles var död.

Eliot Higgins, grundare av den journalistiska grävargruppen Bellingcat. FOTO: PRESSBILD

Carl Heath, senior forskare och fokusledare på Rise samt doktorand vid institutionen för tillämpad it vid Göteborgs universitet. FOTO: PRESSBILD

”Det kom till och med falska dödsförklaringar i bilder som ryska aktörer spred. Det som började med ett folkligt spinn nyttjades sedan av en statsaktör för att driva sin politiska linje”, säger Carl Heath.

Att redigera bilder på kungafamiljer, kändisar eller andra är inget nytt. Men med explosionen av AI har den gångna tidens redigering nått en helt ny nivå.

Det finns allt fler verktyg för att skapa AI-genererade bilder i dag, Midjourney och Open AI:s Dalle-E är två exempel på tillgängliga verktyg som skapar väldigt realistiska bilder. Open AI har nyligen också lanserat Sora för AI-produktion av video.

”Den är inte tillgänglig för allmänheten ännu, de håller på att testa. Men det är en väldigt imponerande teknologi”, säger Eliot Higgins.

I spåren av detta har deepfakes, det vill säga datorframställd förfalskad information i form av bild eller film som framställs som äkta och trovärdig, fullkomligt exploderat. Inte minst i krigszoner som Gaza och Ukraina.

Efter terrorattacken i Moskva där IS Khorasan snabbt tog på sig skulden dök en fejkad video upp i ryska NTV där Oleksiy Danilov, nationell säkerhetschef, skämtade om attacken på ett sätt som antydde att Ukraina hade legat bakom.

”Den största utmaningen handlar inte om bilderna är AI-genererade eller inte, utan om att människor nu bara kan avfärda bilder som inte passar

Mors dags-bilden som skickades ut från det brittiska hovet fick stor exponering i pressen innan det avslöjades att den var manipulerad. Och draget som var tänkt att lugna spekulationerna om prinsessan Kates hälsa satte i stället i gång ett sällan skådat viralt spinn.

FOTO: RASID NECATI ASLIM

I slutet av januari fotograferades kung Charles III på väg ut från ett sjukhus. I kölvattnet av ryktesspridningen kring prinsessan Kate började information spridas i Ryssland om att kungen skulle vara död.

FOTO: ALBERTO PEZZALI

Under valet 2016 var Donald Trump i blåsväder med en läckt ljudfil. "Tänk om det hade hänt i dag. Då hade han bara kunnat säga att filen var AI-genererad och så hade saken varit ur världen", funderar experten Carl Heath.

FOTO: BRENDAN MCDERMID/POOL PHOTO VIA AP

Google vill vaccinera mot desinformation

"Vi måste vara modiga och ta vara på AI:s möjligheter, samtidigt som vi har ett ansvarsfullt och genomtänkt förhållningssätt till tekniken för att hantera utmaningar som deepfakes och desinformation", säger Sara Övreby, samhällspolitisk chef på Google Sverige.

Sara Övreby, samhällspolitisk chef på Google Sverige.

FOTO: PRESSBILD

från AI-verktyg

i deras världsbild genom att säga att de är AI-genererade", säger Eliot Higgins.

Carl Heath tar den läckta ljudfilen som spreds i det amerikanska valet 2016 där Donald Trump sa "Grab'em by the pussy" som ett intressant tankeexperiment.

"Tänk om det hade hänt i dag. Då hade han bara kunnat säga att filen var AI-genererad och så hade saken snabbt varit ur världen."

Att inte kunna skilja på vad som är sant och falskt kan också leda till att människor checkar ut och blir oengagerade samhällsmedborgare.

"För många blir det så tröttsamt att de helt enkelt lägger ned helt och hållet. De tomrum som vanligt folk lämnar efter sig fylls då med de mest extrema motpolerna och den balanserade dialogen försvinner", säger Eliot Higgins.

> "Den största utmaningen handlar inte om bilderna är AI-genererade eller inte, utan om att människor nu bara kan avfärda bilder som inte passar i deras världsbild genom att säga att de är AI-genererade."
>
> ELLIOT HIGGINS

En annan stor risk som Eliot Higgins ser med deepfakes är pornografi.

"Det skapar redan problem i skolor där unga placerar ett ansikte från en klasskompis på en porrbild. För några år sedan hade man behövt en rätt specifik mjukvara för att göra det, men i dag går det lätt och har blivit ett nytt sätt att kränka människor."

Samtidigt som utvecklingen av AI-verktygen går rekordsnabbt pågår många diskussioner såväl i forskarvärlden som i AI-företagen kring hur riskerna ska kunna hanteras, exempelvis genom vattenstämplar.

"Jag tror att det skulle vara mer värdeskapande att aktörer som medier, företag och organisationer som sänder information går samman för att kunna sätta en digital kod som knyts till avsändaren. En sådan typ av äkthetsinfrastruktur finns inte i dag", säger Carl Heath.

"Syftet skulle vara att man kan försäkra sig om att en tidning, ett företag eller myndighet som uttrycker något är den som den utger sig för att vara. Samtidigt är det jätteviktigt att det fortsatt är möjligt att vara anonym, och kunna till exempel läcka information."

JILL BEDEROFF
jill.bederoff@di.se
08-573 650 00

Google på val och du kommer till valmyndigheten eller googla på elections och du kommer till EU:s motsvarighet. Att styra i sökfunktionen är en av sökjätten Googles metoder för att bemöta den våg av desinformation som förväntas komma i spåren av detta historiska supervalår med val i totalt 76 länder runt om i världen, enligt en beräkning som The Economist gjort.

"Vi tittar på deepfakes i bild, video och ljud i många olika lager. Människor kommer till våra tjänster som Sök och Youtube varje dag, vilket innebär både fantastiska möjligheter för människor att ta del av ny kunskap och ett stort ansvar", säger Sara Övreby, samhällspolitisk chef på Google Sverige.

"Både på Youtube och Sök gäller svensk lag, men våra riktlinjer går längre än så som exempelvis kring hot och trakasserier eller att vissa grupper är mer värda än andra. Dessa riktlinjer är inte nya även om det har kommit ny teknik som vi måste hantera."

Lanseringarna av nya verktyg och policyuppdateringar har duggat tätt på Google under det senaste halvåret.

Nyligen uppdaterades bolagets policy för politiskt innehåll till att kräva att alla verifierade valannonsörer synligt måste informera om annonserna, med avseende på bild, video eller ljud, innehåller syntetiskt material där det ser ut som en person sagt något som de inte sagt eller där ett event manipulerats eller AI-genererats.

En färsk rapport från Google visar att sökjätten blockerade eller tog bort över 5,5 miljarder annonser under 2023, motsvarande 9 000 per minut, för att de bröt mot bolagets policyer. Fler än 12,7 miljoner annonsörkonton stängdes av för allvarliga policyöverträdelser, nästan dubbelt så många som 2022.

"Vi har 20 000 personer runt om i världen som jobbar med att granska och hantera innehåll, dygnet runt, året runt."

I slutet av augusti i fjol lanserade Google verktyget Synth ID som gör det möjligt att bädda in en unik digital vattenstämpel i AI-genererat innehåll, osynlig för ögat men som verktyget kan scanna av för att hjälpa användare förstå huruvida innehållet genererats av AI eller inte.

"Vi kan också använda AI för att hjälpa oss mer effektivt detektera exempelvis manipulerade media. Vi tränar så kallade klassificerare som lär sig att känna igen innehåll. Om du exempelvis är en rättighetsinnehavare och ditt verk dyker upp med en annan avsändare så upptäcks det."

About this image är ett annat verktyg från Google för att kunna hjälpa användaren att se om en bild dykt upp på nätet tidigare och på så sätt härleda bildens ursprung.

Jigsaw, en avdelning inom Google, driver bland annat projekt som syftar till att hjälpa människor att vaccinera sig mot desinformation, exempelvis i samband med Rysslands invasion i Ukraina.

"Det kan exempelvis handla om filmer som vi lägger ut på Youtube och som syftar till att lära ut hur desinformation fungerar, för att på så sätt göra människor mer motståndskraftiga. Nu utvidgar vi det arbetet till att omfatta alla europeiska språk", säger Sara Övreby.

JILL BEDEROFF

DETTA ÄR DEEPFAKES

- Deepfakes är samlingsnamnet för konstgjort framtagna bilder, videor och ljud som är så välgjorda att de kan uppfattas som äkta.
- Avsikten är att lura tittaren eller lyssnaren att personen som porträtteras har sagt eller gjort något som hen inte gjort. I regel används en känd persons utseende och röst.
- Bland personer som har blivit utsatta märks Donald Trump, Vladimir Putin, påven Franciskus, Morgan Freeman, Tom Cruise och Taylor Swift.

Cybersecurity Academys partnerföretag skickar sina medarbetare för att utbilda skolelever om cybersäkerhet.

Så kan företag bidra till barns säkerhet på nätet

Sårbara individer ligger i farozonen när cyberhoten tätnar. I den här gruppen finns barn och unga, som behöver mer kunskap om it-säkerhet. Här kan alla företag som jobbar aktivt med digitala säkerhetsfrågor göra stor skillnad, menar projektledarna bakom Cybersecurity Academy.

För barn och tonåringar är den digitala världen en stor del av livet. Närvaro på nätet och sociala medier möjliggör lärande och socialt utbyte med vänner. Baksidan är att det skapar en utsatthet. Mot den här bakgrunden och med stöd från Myndigheten för samhällsskydd och beredskap (MSB) startades Cybersecurity Academy, ett initiativ som ökar kunskaperna om nätsäkerhet hos skolelever.

– Vi såg att det fanns en farlig kunskapslucka hos barn och unga i Sverige gällande it-säkerhet. Nu befinner vi oss dessutom i en geopolitisk situation som gör säkerhetsaspekten än viktigare. De flesta säkerhetshålen i de tekniska lösningarna är tilltäppta, så nu handlar det för kriminella om att hitta sårbara individer. Här är tyvärr barn och ungdomar en viktig målgrupp, säger Evelina Pärnerud, CSR Manager på IBM, som tillsammans med det ideella ungdomsförbundet Unga Forskare driver Cybersecurity Academy.

Partnerföretagen gör viktiga insatser

Judith Maiers, Unga Forskares projektledare för Cybersecurity Academy, berättar att många lärare inte känner sig trygga med att ta upp frågan eftersom de själva saknar kunskapen. Här kommer Cybersecurity Academy in i bilden. Genom lärarhandledningar med färdiga lektionsserier kan alla lärare, oavsett tidigare it- och teknikkunskaper, arbeta med it-säkerhet i klassrummet.

> ”Vi såg att det fanns en farlig kunskapslucka hos barn och unga i Sverige gällande it-säkerhet. Nu befinner vi oss dessutom i en geopolitisk situation som gör säkerhetsaspekten än viktigare.”
>
> – Evelina Pärnerud.

– Sedan har vi också våra partners som jackar i initiativet. Som partnerföretag skickar man medarbetare för att hålla i föreläsningar om it-säkerhet för skolklasser från mellanstadiet upp till gymnasiet. Samtidigt får företagen chans att visa upp sig och nå en målgrupp som de annars inte når. Tanken är att skapa intresse hos barn och ungdomar kring it och teknik, så att fler ska söka sig till relevanta utbildningar och på sikt även jobb inom området, säger Judith Maiers.

Unga Forskare tillhandahåller ett färdigt material för föreläsarna och förmedlar kontakten till skolorna. Mycket av Cybersecurity Academys material finns även på den kostnadsfria utbildningsplattformen IBM SkillsBuild. Detta material är också tillgängligt för föräldrar som vill lyfta sin kunskapsnivå tillsammans med sina barn.

Judith Maiers, projektledare på Unga Forskare.

Evelina Pärnerud, CSR Manager på IBM.

”Teknikbranschen har ett ansvar”

Evelina Pärnerud lyfter fram att föreläsningarna, som kan hållas på plats eller online, skapar engagemang inte bara hos skoleleverna, utan även bland företagens medarbetare.

– En av mina kollegor kom in till kontoret efter att han hållit en föreläsning och var helt uppfylld. Han berättade med sådan inlevelse för två äldre kollegor hur kul det hade varit och att eleverna ställt så intressanta frågor, säger hon och fortsätter:

– Vi i teknikbranschen har ett ansvar att utrusta samhället, inte minst våra unga, med verktygen som behövs för att använda teknik på ett säkert sätt. Här har alla företag en möjlighet att dela med sig av sin kunskap.

Läs mer på:
www.cybersecurityacademy.se och www.skillsbuild.org

Cybersecurity Academy

Gängens bakväg in i bolaget går via knark

Kriminaliteten äter sig in i näringslivet och företag behöver vara vaksamma för att inte drabbas av insiders. Men okunskapen om vad som utgör risker är stor, enligt flera experter.

”Även ett litet narkotikabruk kan vara ett problem”, säger Ola Liljendahl på Vesper Group.

Näringslivet har blivit de kriminellas nya guldkalv. Det slog en rapport från Handelskammaren fast tidigare i år.

”Kriminalitet har alltid haft samma drivkraft över tid. Där pengarna finns, där finns brottsligheten”, säger Martin Waern, affärsområdeschef på säkerhetsföretaget SRS Security.

Förr i tiden kunde kriminella råna en bank för att få pengar. Nu krävs mer avancerade upplägg. De behöver kunna regelverken, vara pålästa och bygga sina egna bolagsstrukturer. Genom att ta sikte på svagheterna i systemet kan de komma över betydande belopp och där har så kallade insiders en viktig roll.

”Systemen blir mer och mer robusta, de blir svårare att komma åt från utsidan. För att verkligen lyckas är det bra att ha någon på insidan som har tillgång till nätverk, lösenord, och kunskaper om hur pengar och varor flödar”, säger Martin Waern.

Men bland företagen är okunskapen om hur de ska skydda sig fortfarande stor. En insider behöver inte vara en ond person. Det kan lika gärna vara någon som blir manipulerad att utföra tjänster åt kriminella utan att själv förstå det.

Det kan också vara någon som blir pressad för att den har andra svagheter.

Bakgrundskontroller vid rekrytering är ett viktigt verktyg för att fånga upp sådana svagheter. Även om metoden blivit vanlig bland företag, brister de ofta i hur informationen ska hanteras, menar Ola Liljendahl, senior säkerhetskonsult på säkerhetsbolaget Vesper Group.

”Narkotika är ett klockrent exempel. Många gånger släpper företag igenom narkotikabruk i de större bakgrundskontrollerna. Man tror att det farliga med narkotika är att man inhalerar något i näsan eller röker på. Man förstår inte att man gör sig otroligt sårbar”, säger han.

Ola Liljendahl, senior säkerhetskonsult på Vesper Group. FOTO: PRESSBILD

Martin Waern, affärsområdeschef på SRS Security. FOTO: PRESSBILD

Han ger ett påhittat exempel om en medarbetare som har köpt kokain av en langare i sex år utan att det hänt något. Sedan sätter sig langaren i skuld till någon och försöker komma undan genom att fresta med kontakter inom bankväsendet som den andra parten kan få tillgång till.

Plötsligt får medarbetaren hot om att de kriminella till exempel ska berätta om drogerna för arbetsgivaren, om inte medarbetaren är behjälplig och utför några tjänster.

”De jobbar ofta med stress och press. Men de är också skickliga på att söka mer exakt information om en individ och därigenom manipulera dem till samarbete”, säger Ola Liljendahl.

Men narkotika har ju blivit ganska vanligt. Innebär det att man inte alls ska anställa personer med sådan historik?

”Ingenting är svart eller vitt, utan man behöver träna på att göra korrekta bedömningar. Man måste gå till botten med hur den här personen ser på det som har hänt och få fram relevant information om hur det faktiskt ligger till i dag.”

Förutom att säkerställa att rätt personer anställs kan det vara relevant att göra kontroller av konsulter, underleverantörer och affärskontakter.

Säkerhetsexperterna påminner också om att inte glömma alla de som redan är anställda.

Ett ofta underskattat verktyg för att förhindra infiltration är en god personalpolitik.

”Man ska inte förakta att ha ett gott arbetsklimat. Att försöka utveckla en företagskultur där man kan prata med varandra och fråga hur man mår. Att man också försöker hitta individer i organisationen som är på väg att falla ur det sociala mönstret, som är missnöjda och kanske kan utgöra riskfaktor”, säger Martin Waern.

”Det går att göra otroligt mycket med prevention. Kriminaliteten tar snabbaste till vägen till pengar, och stöter dem på motstånd genom strukturer och bra säkerhet, då tar de nästa objekt istället”, konstaterar Ola Liljendahl.

LOVISA TERNBY
lovisa.ternby@di.se
08-738 10 57

Narkotikaanvändande anställda kan användas av kriminella till att ta sig in i bolag, varnar experterna. FOTO: HELENA LANDSTEDT

DE KAN BLI INSIDERS

- Personer som blir manipulerade utan att förstå att de utför tjänster åt kriminella nätverk.
- Personer med svagheter, till exempel narkotikaproblem, som haft kontakt med kriminella och kan pressas att hjälpa dem.
- Personer som tar en kalkylerad risk för att tjäna pengar.
- Släktingar eller nära vänner till kriminella som är aktivt placerade på en viss position för att utföra tjänster.

Källa: Ola Liljendahl, Vesper Group

Vita huset och den brittiska regeringen förbereder anklagelser mot ett flertal kinesiska hackare. FOTO: C DHARAPAK

Kineser anklagas för företagsspionage

Vita huset och Storbritanniens regering står i färd med att på varsitt håll presentera anklagelser mot ett flertal kinesiska hackare för storskaligt cyberspionage mot amerikanska företag på uppdrag av kinesisk underrättelsetjänst, rapporterar CNN med hänvisning till källor.

Kinas underrättelsetjänst MSS, som sorterar under departementet för inrikes säkerhet, anklagas för att med kinesiska techbolag som front ligga bakom hackningsaktiviteten. Flera amerikanska departement kommer enligt uppgifterna att agera gemensamt.

Namn och fotografier på anklagade kommer att publiceras och flera miljoner dollar kommer annonseras i belöning till den som ger avgörande uppgifter.

Gruppen är sedan tidigare känd, och går under namnet APT31, eller Judgement Panda. Utredare har även tidigare sett spåren av hackargruppen, som konstaterats rikta in sig på alltifrån amerikanska juristfirmor till europeiska industribolag.

Inför det amerikanska presidentvalet 2020 försökte gruppen hacka mejlkonton i Bidenkampanjen, enligt information som delgivits av techkonglomeratet Microsoft.

Åtgärderna vidtas i en särskilt skör tidpunkt för de bilaterala relationerna mellan USA och Kina i fråga om cybersäkerhet. Frågan om den sociala medieappen Tiktok har hamnat högt på agendan sedan kongressens representanthus röstat igenom ett lagförslag som i praktiken förbjuder användning av appen så länge den ägs av det kinesiska moderbolaget Bytedance.

Dessutom vittnade FBI-chefen Christopher Wray nyligen i kongressen, och varnade då för att en helt annan grupp kinesiska hackare än de som nu avses förbereder sig för att ”orsaka förödelse och fysisk skadeverkan på amerikanska medborgare och samhällen när väl Kina beslutar sig för att det är dags att slå till”.

DIREKT

DETTA ÄR EN ANNONS FRÅN ASECOS

asecos: Brandklassat batteriskåp gör laddningen säkrare

Litiumjonbatterier finns överallt omkring oss – i mobiltelefoner, datorer, handverktyg och elcyklar.

– Även om batterierna möjliggör bra saker, är det viktigt att vara medveten om riskerna, menar Rickard Dahlstedt på asecos.

I dag finns inget regelverk för hur batterier ska förvaras, hanteras eller laddas, trots att de kan vara farliga för både människor och egendom om de går i termisk rusning. Det kan ske om batteriet exempelvis utsätts för stötar eller slag, överladdas eller kortsluts. När ett batteri går i termisk rusning kan de skapa en snabb och svårsläckt brand, explodera och även avge giftig rök*.

Elsäkerhetsverket har publicerat statistik som visar att bränder orsakade av laddningsbara produkter ökar, och står för en stor del av de bränder där människor skadats allvarligt.

– Tillverkarna anger att deras batterier ska laddas under uppsikt, vilket innebär att ansvaret för att batterierna övervakas vid laddning ligger på användaren. Men man kan inte ha en anställd som sitter och tittar på batterier hela dagarna, säger Rickard Dahlstedt, vd på asecos och fortsätter:

– Här har vi en lösning i form av ett brandklassat laddningsskåp testat och certifierat för invändig och utvändig brand i 90 minuter. Det innebär att man har tillräcklig tid på sig att utrymma och tillkalla räddningstjänst. Skåpen är även utrustade med ett larmsystem som varnar så fort det börjar ryka eller om temperaturen stiger över det normala. Larmet vidarebefordras till larmcentral eller skickas via GSM-nätet för snabb aktion.

Skyddar människor och egendom

asecos är experter på säker förvaring av farligt material. Företaget är en av världens största tillverkare av brandklassade kemikalieskåp och batteriskåp. Statistik som asecos tagit fram visar att ungefär 1 av 20 000 levererade kemikalieskåp utsätts för en riktig brand, medan 3 av 100 levererade batteriskåp redan utsatts för termisk rusning.

– Även om batterierna möjliggör bra saker, är det viktigt att vara medveten om riskerna som finns. Här ingår både risker med utrustningen som köps in för att användas i verksamheten, och batterier som anställda tar med sig till jobbet. Det kan vara batterier till elcyklar som man passar på att ladda i kapprummet under arbetsdagen, säger Rickard Dahlstedt.

Laddas batterierna i ett brandklassat batteriskåp med aktiv övervakning får man direkt en varning om något går fel, har tid att utrymma och vidta lämpliga åtgärder. Det kan vara skillnaden som gör att man undviker en katastrof, konstaterar Rickard Dahlstedt.

** Storstockholms brandförsvar.*

Läs mer på:
www.asecos.se

Besök oss på Linkedin:
linkedin.com/company/asecos-ab

Besök oss på Facebook:
facebook.com/asecos.gruendau

asecos®

DETTA ÄR EN ANNONS FRÅN ANCHOR LÅS

Svenska IP-klassade lås som skyddar kritisk infrastruktur

Behovet av att säkra kritisk infrastruktur har blivit allt mer aktuellt i takt med att medvetenheten om intrång ökar. Tomas Eriksson, vd för Anchor Lås, märker detta eftersom det är en större efterfrågan på deras lås.

– Våra lås, som tillverkas lokalt i Eskilstuna, är mycket tåliga och används på många håll i världen just för att säkra kritisk infrastruktur, säger han.

Anchor Lås har en lång historia med rötter ända från 1600-talet. Dagens ägare, Tomas Eriksson och Robert Fredriksson, köpte bolaget 2012 och sedan dess har både antalet anställda och omsättning ökat.Idag är företaget en av Skandinaviens största hänglåstillverkare

– Vi har egen tillverkning i Eskilstuna och använder svenskt råmaterial som stål och mässing i våra hänglås. Vi har bland annat en patenterad serie IP-klassade hänglås riktade mot kritisk infrastruktur, säger Tomas Eriksson.

En av funktionerna som han beskriver är tätningen vid hänglåsets lucka som förhindrar att damm eller vatten kommer in. Detta säkerställer att låset kan användas i såväl Nordens kalla klimat som i dammig miljö runt om i världen.

– De flesta av våra lås levereras till kritisk infrastruktur. Låsen säkrar inspektionsluckor för att skydda vattenförsörjning. Elbolag använder låsen för kraftnätet och telekombolag för att freda mobilmaster från intrång. Våra klass fem lås skyddar till exempel Londons vattenförsörjning, säger Tomas Eriksson stolt.

Kundanpassning och klimatpåverkan

Det finns flera skäl till att Anchor Lås tillverkning sker i Sverige, som att ha kontroll över hela kedjan och att varken råmaterial eller partier med lås fastnar i Suezkanalen med långa transportledtider som följd. Något som blev påtagligt under pandemin och är högaktuellt nu i det geopolitiska läget. Korta transporter ger också en minskad klimatpåverkan. En annan anledning att tillverka lokalt är att kunna jobba i nära samarbete med bolagets kunder.

– Våra hänglås kan anpassas för såväl mekaniska som elektroniska cylindrar utifrån kundens specifikation. Om en kund vill ha ett speciallås kan vi göra små serier och jobba snabbt. Senaste gången vi fick ett sådant uppdrag hade vi en fungerande prototyp efter två veckor.

FAKTA

ANCHOR LÅS är ett privatägt låsföretag med rötter i svensk industrihistoria. Fokuserar på utveckling och tillverkning säkerhetsklassade hänglås av högsta kvalitet. Stordelen av volymen exporteras. Utöver tillverkning och försäljning av låsprodukter under eget varumärke utvecklar och tillverkar företaget hänglås till flertalet ledande, globala låstillverkare.

Läs mer på:
www.anchorlas.se

ANCHOR LÅS · MADE IN SWEDEN ·

MilDef rustar it för tuffa förhållanden

I utmanande miljöer krävs robust utrustning. Med skräddarsydda it-lösningar hjälper MilDef sina kunder att digitalisera viktiga informationsflöden. Målet: att skydda frihet och demokrati.

Daniel Ljunggren, vd MilDef Group.

Efter 27 år i branschen är MilDefs verksamhet mer relevant än någonsin tidigare. I en alltmer osäker omvärld förser de kunder med it-lösningar för tuffa miljöer. Det handlar om platser påverkade av värme, kyla, sand, vatten och damm, där utrustningen är monterad på plattformar som ska klara såväl skakningar som chock och vibration.

– MilDef tillhandahåller hårdvara, mjukvara och tjänster som hjälper till att digitalisera viktiga informationsflöden under de tuffaste förhållandena och i de mest utmanande miljöerna. Genom att leverera skalskyddet för digitalisering hjälper vi våra fredsbevarande krafter, som med tillgång till digital information i realtid kan fatta bättre underbyggda och snabbare beslut, säger Daniel Ljunggren, vd MilDef Group.

Kundanpassade lösningar

MilDefs ambition är att vara den mest innovativa och flexibla aktören i branschen. De jobbar därför mycket med innovation och teknikutveckling, och det görs i nära samarbete med kunder och partners. Tack vare sin mångåriga erfarenhet har de byggt upp en bank av kunskap och lösningar som hjälper dem att på ett snabbt och säkert sätt ta fram skräddarsydda lösningar.

– Det här är en förtroendebransch där det är viktigt att vara beprövade i fält. När allting står på spel måste vår utrustning leverera för att kunna skydda de mest kritiska informationsflödena och systemen. Vi har en lång historik med gott förtroende från våra kunder, och tittar hela tiden på hur vi kan säkerställa och driftsätta de bästa lösningarna för dem, säger Daniel Ljunggren.

– MilDef säkerställer inte bara motståndskraftig och tillförlitlig it, vi har också ett väldigt krävande hållbarhetstänk kring våra slutkunder och hur vi vill göra affärer. Den etiska kompassen är väldigt viktigt för oss: vår teknik får aldrig komma på villovägar.

FAKTA

MilDef Group förser en global marknad med taktiska it-lösningar som bärbara datorer, servrar, switchar, routrar, intelligenta diskar, programvara och integrationstjänster. De skräddarsyr it-produkter och system av militär kvalitet, gjorda för att fungera under tuffa förhållanden. Företaget startade 1997, har huvudkontor i Helsingborg och verksamhet i ytterligare nio länder.

Läs mer på:
https://mildef.com

Besök oss på Linkedin:
inkedin.com/company/mildef-group

MILDEF
WE ARMOR IT.

Molnets inverkan på företagens säkerhet

Företag förlitar sig alltmer på molnets smidighet och skalbarhet. Som 2023 och början av 2024 visade oss kommer det att vara avgörande att på ett säkert sätt integrera AI-funktioner i molnmiljöer.

Matilda Eriksson, Head of Nordics på Cloudflare.

Visste du att en blinkning tar ungefär 300 till 400 millisekunder? Cloudflare är endast 50 millisekunder från 95 procent av världens befolkning med sitt globala nätverk, som sträcker sig över 120 länder och 310 städer, där Stockholm och Göteborg ingår.

2023 skedde en dramatisk ökning av så kallade DDoS-attacker (distributed denial of service), både i frekvens och omfattning. Det resulterade i de mest massiva DDoS-attackerna som någonsin registrerats. Botnät, alltså infekterade datorer som fjärrstyrs av angriparen, utnyttjar dessutom i allt högre grad kraften i molninfrastrukturen.

Förebygga bättre än bota

Det största cyberhotet är att vara underutrustad och oförberedd. Frågan är inte om din organisation kommer att attackeras, utan när och hur. Förebyggande är bättre än botande. Cyberbrottslingar angriper ofta från flera håll – en DDoS-attack kan utföras för att dölja en annan. Medan säkerhetsteamen mobiliseras för att hantera DDoS-attacken sker den verkliga attacken, exempelvis via SQL-kodinjektion.

– Kunder som har infört vår Zero Trust-teknik (ZT) beskriver att aktionsradien för en framgångsrik attack blir mycket snävare, vilket möjliggör en snabbare återgång till det normala, säger Matilda Eriksson, Head of Nordics på Cloudflare, och fortsätter:

– ZT-arkitekturen bidrar till att ransomware inte sprids i nätverket. Dessutom bidrar ett e-postskydd integrerat med ZT-teknik och utökat med AI-tjänster till att skydda både anställda och organisationen.

Skapa holistiskt skydd

Matilda Eriksson uppmanar alla att etablera en skuldfri arbetskultur, där anställda vågar rapportera fel som kan leda till en attack eller ett intrång. Även om det är uppenbart att cyberattackerna kommer att fortsätta att spridas och bli alltmer sofistikerade, finns det medel för att motverka dem.

– Att drabbas av en attack är inte längre oundvikligt. Det vinnande mantrat för en säker molnstrategi är enkelt: skydda applikationer, nätverk och anställda på ett helt holistiskt sätt, helst i Connectivity Cloud, avslutar Matilda Eriksson.

FAKTA

Inför 2024 och framåt kommer teknikledare att behöva undersöka trenderna inom moln och säkerhet, som kommer att utgöra en dubbel utmaning för deras team: de alltmer sofistikerade säkerhetshoten och nödvändigheten av att behålla kontrollen över flera molnplattformar.

Läs mer på:
www.cloudflare.com

Besök oss på Linkedin:
linkedin.com/company/cloudflare

Besök oss på X:
www.twitter.com/Cloudflare

CLOUDFLARE

DETTA ÄR EN ANNONS FRÅN SRS SECURITY

Här finns stöd vid misstanke om insiders eller otillbörlig påverkan

Organisationer kan ovetandes dras in i eller drabbas av organiserad brottslighet, både inifrån och utifrån. SRS Security kan då hjälpa till med både operativa och rådgivande tjänster.

– Misstänker man något är det viktigt att agera snabbt och klokt, säger Fredrik Janse, VD på SRS Security.

BRÅ släppte nyligen sin rapport Möjliggörare i kriminella nätverk, som bland annat belyser hur kriminella nätverk kan placera möjliggörare inne i offentliga organisationer eller privata företag. Där kan de med en legitim fasad agera med kriminella syften, som att läcka känslig information, eller medverka till korruption eller penningtvätt.

Experter från SRS Security har bidragit till rapporten och finns citerade.

– Rapporten belyser på ett mycket tydligt sätt ett antal särskilt riskutsatta branscher och funktioner där organiserad brottslighet söker och placerar sina möjliggörare, säger Fredrik Janse.

För den som blir drabbad uppstår ofta en stor osäkerhet där man har svårt att orientera sig.

– Det är viktigt att förstå att möjliggörare i många fall är att likställa med medbrottsling och att det kommer med ett straffansvar som kan landa både på individer och företag.

”Rapporten belyser på ett mycket tydligt sätt ett antal särskilt riskutsatta branscher och funktioner där organiserad brottslighet söker och placerar sina möjliggörare.”

Här kan vi kliva in och erbjuda både trygghet i ärendet samt ett oberoende perspektiv, säger han.

SRS har en bred produktportfölj

SRS erbjuder tjänster för att hantera interna och externa angrepp, såväl reaktivt som proaktivt. De har specialtränad kompetens och gedigen erfarenhet inom kvalificerat utrednings- och spaningsarbete, men även experter inom rekrytering och mänskliga system.

– Vi vill komma in tidigt för att klarlägga avvikelsen, identifiera samband mellan individer, nätverk och företag samt bedöma aktuella risker kopplat till bolagets interna processer och affärer, förklarar Fredrik Janse.

SRS erbjuder också kunder en genomlysning av det interna antikorruptionsarbetet.

– Vill man som företag förstå hur en möjliggörare arbetar och påverkar företaget eller vilka brottsmodus man kan vara en del av så har SRS en expertgrupp inom antikorruption. Där är våra samlade erfarenheter en avgörande resurs för att skapa proaktivitet och trygghet, avslutar Fredrik Janse.

Fredrik Janse, VD på SRS Security.

FAKTA

SRS grundades 2004 och är i dag en ledande helhetsleverantör för kvalificerade säkerhetstjänster inom Security Risk Management. SRS och dess cirka 120 medarbetare kan hjälpa till med operativa, rådgivande och utbildande tjänster i Sverige och utomlands.

Läs mer på:
www.srsgroup.se

SRS

DETTA ÄR EN ANNONS FRÅN FRIENDS

Friends: Att förvandla ord till handling för en värld utan mobbning

Tre barn i varje klass. Det är den skrämmande siffran som visar att Sverige, trots ansträngningar, fortsätter att kämpa med att skapa säkra, inkluderande och trygga utbildningsmiljöer. För att möta denna utmaning uppmanar Friends näringslivet att engagera sig i kampen mot mobbning genom att bidra till utvecklingen av framtidens verktyg mot mobbning.

Friends, med över 25 års erfarenhet, vet att varje handling gör skillnad. Genom att erbjuda stöd och verktyg för både barn och vuxna skapar de tryggare skol- och idrottsmiljöer där alla barn kan komma till sin rätt.

Magnus Loftsson, Innovationsledare på Friends.

Nu vänder de sig till näringslivet för att tillsammans utveckla innovativa lösningar för att bekämpa mobbning i skolorna.

— Genom att utveckla framtidens verktyg mot mobbning kan vi tillsammans kartlägga och skapa en tryggare och mer inkluderande skolmiljö för alla barn. Vi behöver näringslivets engagemang och expertis för att göra detta till verklighet. Det är genom att gå från ord till handling som vi tillsammans kan stoppa mobbning. Det är ju Sveriges framtid det gäller, säger Magnus Loftsson, Innovationsledare på Friends.

Näringslivet kan göra skillnad Friends står inför en utmaning som kräver gemensamt ansvar och engagemang från hela näringslivet. Genom att agera för trygghet, inkludering och en säkrare skolgång kan näringslivet spela en avgörande roll i att göra verklig skillnad i kampen mot mobbning och ge alla barn en likvärdig chans att klara sin skolgång. Friends uppmanar företag att ta ställning och vara en del av lösningen. Då kan vi halvera mobbningen i Sverige på 10 år.

FAKTA

Friends tror på kraften i en enskild röst och hur den kan göra skillnad. Genom att sprida fungerande verktyg och skapa engagemang mot mobbning, sänker Friends trösklarna för alla att agera. Vi vill inspirera människor att gå från ord till handling. Så att vi tillsammans kan skapa en värld där inget barn utsätts för mobbning.

Läs mer på:
https://friends.se/foretag

Följ oss på Linkedin:
linkedin.com/company/stiftelsen-friends

friends

Hon hittar hoten i giftigt språk

Från Stockholms universitet till FBI:s skrivbord – Lisa Kaatis forskning avslöjar digitala varningssignaler som kan förebygga nästa stora våldsbrott.
"Jag är gärna med och gör världen säkrare", säger hon.

Omgiven av datorskärmarnas brus sitter Lisa Kaati och analyserar dataflöden från sociala medier. Varje inlägg kan ge viktiga ledtrådar till hur människor kommunicerar om hot och våld på nätet. Med en blandning av datavetenskap och skarpt analytiskt tänkande avslöjar hon komplexa mönster som de flesta missar. Hennes forskning har lett till ett samarbete med brottsbekämpande myndigheter runt om i världen – bland annat FBI.

"Vi kunde studera kommunikationen från både dem som utfört våldsdåd och dem som ansågs vara risker av FBI, men som inte agerat. Många våldsverkare uppvisar samma typer av varningsbeteenden, och visade tecken på att vilja utföra våldsdåd. Flera identifierar sig med tidigare våldsverkare eller våldsideologier. Andra ser sig själva som krigare och har därför ett stort intresse för vapen och använder militär terminologi."

Lisa Kaati är docent på Institutionen för data- och systemvetenskap vid Stockholms universitet och forskar om toxiskt språk på nätet, extremism och riskbedömningar.

Genom att granska inlägg på sociala medier kan hon ge tidiga varningar om riskbeteenden, vilket skulle kunna hjälpa polisen att förhindra exempelvis en skolskjutning.

"Nästan alla våldsverkare radikaliseras på nätet och många väljer att kommunicera sina avsikter på nätet", säger Lisa Kaati.

Hon forskar på metoder för att granska nätet – både för att hitta hotfulla meddelanden och bedöma om de som skriver dem kan tänkas agera på hoten.

"Man har märkt att personer som utför våldsdåd ofta visar vissa varningstecken i förväg. Det kan handla om allt från att frekvensen av hotfull kommunikation eskalerar till att det utvecklas en osund fixering vid en person eller en sakfråga."

> "Nästan alla våldsverkare radikaliseras på nätet och många väljer att kommunicera sina avsikter på nätet."
>
> LISA KAATI

Hon understryker att en av de största utmaningarna är att skilja mellan tomma hot och verkliga risker.

"Det gäller att samla på sig så mycket information som möjligt om individen som har uttryckt hotet. Genom att analysera individens tanke- och beteendemönster försöker vi avgöra om personen faktiskt utgör ett riktigt hot. Vid en hotbedömning av en person används flera metoder, men alla bygger på att identifiera riskindikatorer och varningssignaler."

Lisa Kaati använder AI för att förstå digital kommunikation i sin forskning. Men hon betonar att AI ska vara ett verktyg, inte den som tar besluten, i att hitta hot och risker i kampen mot brott.

"Det är viktigt att människor alltid avgör hur ett hot ska bedömas. AI kan hjälpa oss att snabbt sålla fram olika indikatorer ur stora mängder data som skulle vara nästan omöjliga att hitta med bara mänskliga resurser."

I sin yrkesroll vill Lisa Kaati att hennes forskning verkligen ska komma till användning. Tillsammans med forskarkolleger har hon grundat företaget Mind Intelligence Lab som omsätter resultaten till riktiga analysverktyg.

"Under hela min karriär har jag försökt få brottsbekämpande myndigheter att använda de tekniker vi utvecklar men det har varit svårt att ta in våra forskningsprototyper i riktiga verksamheter. Våra prototyper har i dag blivit riktiga verktyg som skolor använder för att stoppa skolskjutningar och som säkerhetsavdelningar använder för att förebygga våldsbrott. Det är häftigt!"

HENRIK LENNGREN
henrik.lenngren@di.se
070-891 98 06

Lisa Kaati forskar om toxiskt språk på nätet, extremism och riskbedömningar. FOTO: JACK MIKRUT

DECHEFR

■ Dechefr är ett AI-baserat verktyg för hotbedömningar som bygger på flera års forskning. Bakom Dechefr står bland andra Lisa Kaati, docent på Institutionen för data- och systemvetenskap, DSV, vid Stockholms universitet.

■ Syftet med Dechefr är att kunna upptäcka potentiella ensamagerande våldsverkare genom att identifiera olika typer av varningsbeteenden i olika typer av kommunikation exempelvis i mejl eller inlägg i sociala medier.

Översvämning av nätskräp – en osynlig utmaning för samhället

Det pågår en översvämning av elektroniskt skräp, som stör ledningsnätets infrastruktur. I värsta fall kan detta påverka kritiska branscher som sjukvården, industrin och försvaret. Kunskapen behöver bli större, menar Karlstadsföretaget KAMIC som delar med sig av samhällsviktig information om EMC.

Elektromagnetisk kompatibilitet, EMC, är förmågan hos elektroniska komponenter, anläggningar och system att fungera tillsammans utan att orsaka eller bli påverkade av elektromagnetiska störningar i deras normala miljö. Ett exempel – våra mobiltelefoner och smarta bilar måste fungera utan att störa radiokommunikationen på närliggande flygplatser eller den uppkopplade utrustningen på sjukhusen.

I dag innehåller många elektroniska produkter komponenter som kan orsaka störningar i ledningsnätet*. Det skapas nätskräp som påverkar allt från kablar till sensorer och styrsystem, vilket i sin tur kan äventyra ledningsnätets prestanda och pålitlighet. Torbjörn Jansson, sakkunnig inom EMC-frågor hos KAMIC, förklarar:

– Ledningsnätets infrastruktur får löpande fler anslutna anläggningar som påverkar både nätets kvalitet och effekt. Förändringar i spänning som spikar, dippar, transienter och övertoner förekommer allt oftare, och det beror inte sällan på nätets uppbyggnad, anslutna produkter samt ökade anslutningsgrad, totalt sett.

Förkortar elektronikens livslängd

Laddstolpar, solcellsanläggningar och liknande installationer som omvandlar likström till växelström samt frekvensstyrningar, orsakar det som kallas övertoner. Övertoner innebär att elnätet belastas med mer eller mindre än det normala, 50Hz. Detta kan, i sämsta fall, resultera i kortslutning eller brand.

– Forskning har visat att övertonsproblematiken även kan förkorta livslängden på elektronik mellan 25–30 procent, samt att kablar behöver överdimensioneras. Ett stort hållbarhetsproblem på sikt då elektronik måste bytas ut i förtid, menar Jörgen Persson, projektingenjör i skärmningsteknik.

Jobbar med skärmningsteknik

För att skydda samhällskritiska installationer här och nu krävs kunskap om EMC samt effektiv skärmningsteknik. Det kan till exempel handla om specialkonstruerade rum med avancerade filter som stänger ute nätstörningarna. KAMIC har lång erfarenhet och stor kunskap om tekniken.

– I dag används detta främst av Försvarsmakten och myndigheter, men vi ser att även företag som jobbar med känslig och kritisk information bör se över sitt skydd mot intrång och elektromagnetiska fält, säger Jonas Eriksson, affärsområdeschef, KAMIC Skärmningsteknik.

Det är förstås viktigt att också gå till botten med problemet – att minska översvämningen av elektroniskt skräp är helt nödvändigt. Tillverkare behöver utveckla produkter som är EMC-kompatibla.

– Genom att anamma hållbara EMC-lösningar kan vi tillsammans säkerställa att våra ledningsnät blir mer robusta och tillförlitliga så att vår elektronik blir mer hållbar, i en tid av ökad elektronisk konsumtion, avslutar Jonas Eriksson.

Jonas Eriksson, affärsområdeschef, KAMIC Skärmningsteknik.

”Forskning har visat att övertons-problematiken även kan förkorta livs-längden på elektronik mellan 25–30 procent, samt att kablar behöver över-dimensioneras. Ett stort hållbarhets-problem på sikt då elektronik måste bytas ut i förtid.”

** Elsäkerhetsverket.*

Läs mer på:
www.kamic.se

Besök oss på Linkedin:
linkedin.com/company/kamic-installation-ab

Följ oss på Instagram:
@kamicinstallation

Kontakta oss på:
emc@kamic.se

KAMIC

Cristian Klein, DPO och produktägare av Elastisys plattform, och Lars Larsson, Field CTO på Elastisys.

Elastisys skyddar din samhällskritiska app – återställd på timmar

I dag hjälper en mängd digitala verktyg till att hantera våra liv. För drift av samhällskritiska sådana är säkerhetskopior avgörande. Två cybersäkerhetsexperter reder ut varför backups hos flera molntjänstleverantörer ökar motståndskraften – och hur de säkrar driften, trots att molntjänstleverantörerna skiljer sig åt.

Många av oss synkar våra mobilbilder till molnet för att kunna återställa förevigade minnen på en ny telefon, om den gamla går sönder. De flesta organisationer gör detsamma. Det finns en backup i molnet för att säkra tillgången till data i händelse av en hackerattack eller ett it-haveri.

Men vad händer om molntjänstleverantören i sin tur blir hackad? De senaste åren har vi sett exempel på attacker mot it-bolag som resulterat i stora konsekvenser för deras kunder.

– Ditt primärdata kanske finns i Sverige och din backup i Finland. Det är lätt att tänka att de säkerhetskopierade filerna finns kvar i Finland om det svenska datacentret slås ut. Problemet är att molntjänstleverantören oftast kör samma mjukvara på alla sina datacenter. Hackare kan då påverka mjukvaran över regiongränser, förklarar Lars Larsson, Field CTO på Elastisys.

> ”Ditt primärdata kanske finns i Sverige och din backup i Finland. Det är lätt att tänka att de säkerhetskopierade filerna finns kvar i Finland om det svenska datacentret slås ut. Problemet är att molntjänstleverantören oftast kör samma mjukvara på alla sina datacenter. Hackare kan då påverka mjukvaran över regiongränser.”

Vikten av leverantörsöverskridande backups och återställning

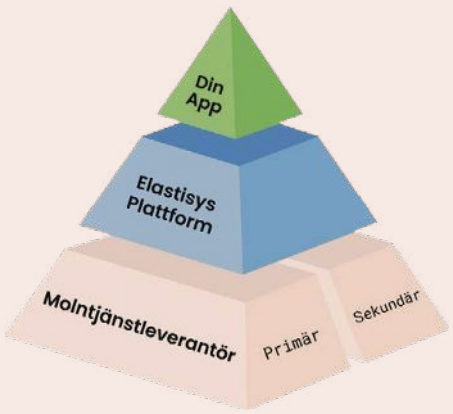
Elastisys, som utvecklar en säker plattform för mjukvara driftad i molnet, betonar vikten av leverantörsöverskridande backups. Enkelt förklarat handlar det om att inte lägga alla ägg i en och samma korg.

En leverantörsöverskridande backup behöver inte bara sparas hos flera molntjänstleverantörer, utan applikationen behöver även kunna sättas i drift hos dem. En utmaning är de stora skillnaderna mellan de olika molnleverantörerna som tekniskt är svåra att överbrygga. Man vill inte bara ha en kopia av sin backup, utan även kunna använda den. Här kommer Elastisys in i bilden. Cristian Klein, DPO och produktägare av Elastisys plattform, gör en liknelse:

– Som resenär behöver du inte bry dig om vilket flygplan du sätter dig i, utan piloterna hanterar komplexiteten som skiljer mellan olika flygplan. Vårt team är som piloterna. Precis som piloter går igenom omfattande checklistor före flygning, ser våra ingenjörer till att plattformen är säker, uppdaterad och uppfyller kraven. Därmed fungerar allt på samma sätt för din applikation, oavsett molntjänstleverantör

Uppe efter några timmar – i stället för veckor

Organisationer kan köra sin serverprogramvara, den som gör att en webbsida eller app fungerar, genom Elastisys plattform. Plattformen fungerar på många olika molnleverantörer, och du som kund väljer vilken som används i första och andra hand. Elastisys suddar ut de tekniska skillnaderna mellan molntjänstleverantörern. Om den första leverantören av någon anledning skulle falla bort, startar Elastisys upp plattformen hos den andra. Där finns en uppdaterad backup redo.



– På några timmar ser vi till att applikationen är uppe igen. Det känns mycket rimligare än ett leverantörsbortfall som påverkar i flera veckor. Vi har sett exempel på hur sårbart samhället blir när olika samhällskritiska tjänster ligger nere, säger Lars Larsson.

Läs mer på:
www.elastisys.com

Följ oss på Linkedin:
linkedin.com/company/elastisys

elastisys

HÅLLBAR SÄKERHET FÖR BIDRAGSGIVARE

Säkerhet, kontroll och integritet har kommit högt upp på allas agendor. Som bidragsgivare kan man idag också ställa högre krav på sina bidragstagare. Det underlättas med plattformen Digiplant SBS Manager®.

Läs mer på **sbsmanager.net/sakerhet**

Att vara bidragsgivare idag ställer stora krav på säkerhet, oavsett om du är en bidragsgivande stiftelse, ideell organisation, forskningsfinansiär, sponsor eller offentlig verksamhet. Omkring 400 organisationer använder redan **Digiplant SBS Manager®** för sömlös ärendehantering, säkra utbetalningar samt effektiva och spårbara processer.

digiPlant.

Kinesiska elbussar säkerhetsrisk i den svenska kollektivtrafiken

Det finns en oro för att kinesiska fordon kan vara en genväg till spionage i väst.

Nu är säkerhetsrisker en parameter i bland annat Region Stockholms upphandlingar, rapporterar Sveriges Radio.

EU-kommisionens ordförande Ursula von der Leyen.

FOTO: CORNELIA JÖNSSON

Kina dominerar världsmarknaden med sina elbilar. Att Europa på så vis gör sig beroende av den auktoritära regimen oroar inte minst beslutsfattarna i Bryssel. I höstas aviserade EU-kommissionens ordförande Ursula von der Leyen en utredning om att lägga strafftullar på kinesiska elbilar.

”Globala marknader översvämmas av billiga kinesiska elfordon, vars priser hålls nere på konstgjort sätt av statliga stöd”, sa hon i sitt årliga tal om läget i unionen.

Men det är inte bara beroendeförhållandet som oroar. Det finns också farhågor om att fordon från Kina kan användas för spionage.

”Oron består i att moderna bilar, särskilt autonoma elbilar med kameror och sensorer, genererar en stor mängd användardata som sedan kan användas av producenterna”, säger Ulla Lovcalic till Sveriges Radios podd ”Gräns”. Hon är Kinakännare på Utrikespolitiska institutet.

Även om en enskild användares information är ointressant kan den sammanlagda informationen från tiotusentals resor förse regimen med relevant information om hur man till exempel orsakar trafikkaos. Enligt kinesisk lag är nämligen alla bolag skyldiga att lämna information till staten om staten begär det.

I den svenska kollektivtrafiken rullar redan många kinesiska fordon. Elbussar av märket BYD, Build your dreams, finns till exempel i Stockholm, Eskilstuna, Piteå och på flera platser i Skåne, enligt SR.

SKR, som samlar Sveriges kommuner och regioner, har inte några rekommendationer eller föreskrifter om användningen av kinesiska elfordon i regionernas kollektivtrafik.

”Nej, det har vi inte. Ansvaret ligger hos den som upphandlar”, skriver presstjänsten per mejl till Di.

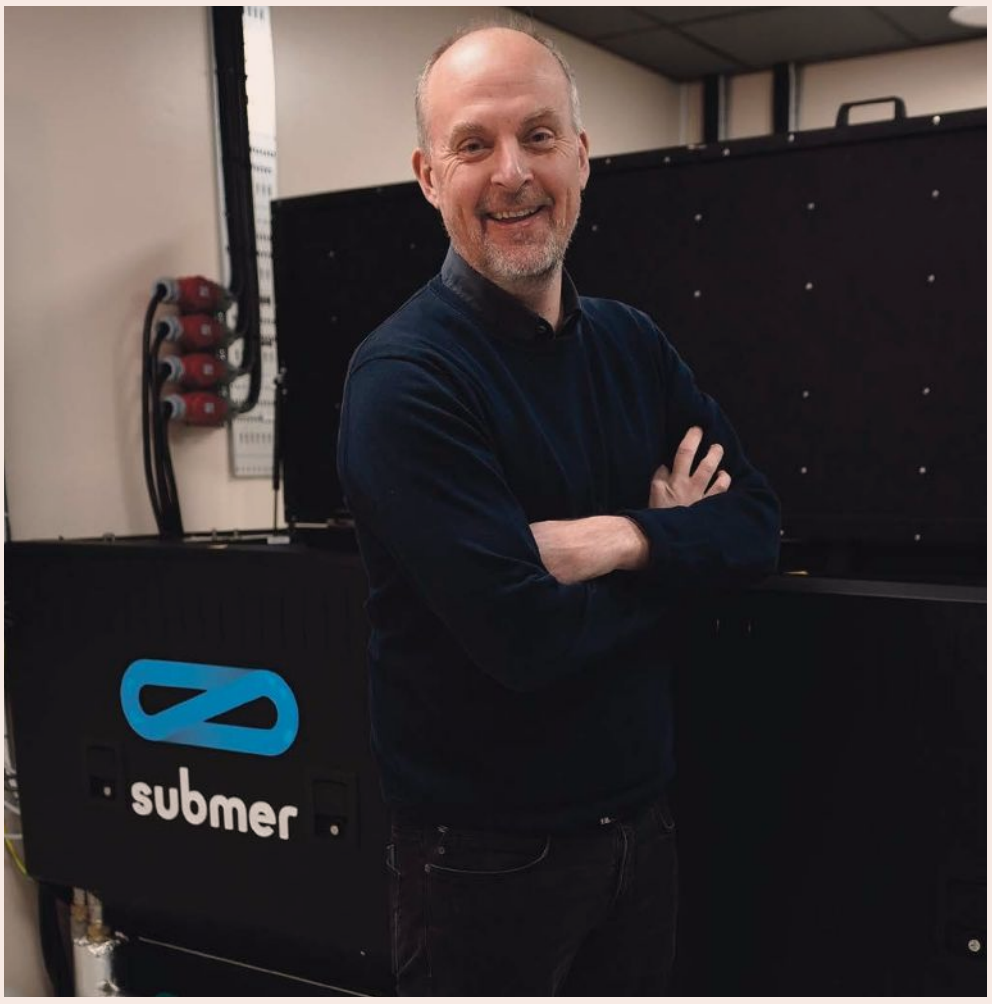
Region Stockholm uppger däremot till SR att man är medvetna om utmaningarna med säkerheten och jobbar aktivt med den faktorn i samband med bland annat upphandlingar. Faktum är att regionen inte längre godkänner bussar tillverkade i Kina, men av etiska skäl som arbetsvillkor.

Även i USA har frågan hamnat på agendan. Märket BYD har under flera års tid varit en av de största leverantörerna av elbussar till landet, enligt SR. Det har politikerna försökt sätta stopp för genom att stoppa det statliga stödet för bussköp om tillverkarna har för nära koppling till Kina.

LOVISA TERNBY
lovisa.ternby@di.se
08-738 10 57

En lastbil av det kinesiska märket BYD kör genom vad som ser ut som en europeisk stad. Märkets dominans oroar västvärlden.

FOTO: PRESSBILD



Cirkulära datacenter - ett fundament för IT-säkerhet

Datacenter står för större klimatpåverkan än flyget, vilket datacenteraktören T.Loop ändra på.

– Vi bygger datacenter i befintliga fastigheter och nyttjar restvärmen till att värma fastigheten och närliggande bebyggelse. Därmed minskar vi det totala CO2-utsläppet mer än vad själva datacenterdriften skapar, säger Staffan Stymne, VD T.Loop.

Digitala tjänster ses ofta som hållbara, men faktum är att IT-branschens klimatavtryck ökar kraftigt. I och med den snabba utvecklingen inom områden som AI, Internet of Things, VR, Blockchain så krävs det alltmer energi för att hantera all data och beräkningsmodeller. Enligt IEA (International Energy Agency) använde datacenter 460 TWh el år 2022. Med den extrema digitala utveckling som nu sker beräknar IEA vidare att elanvändningen hos datacenter kan fördubblas till ca 1000 TWh, motsvarande 4 procent av världens totala elanvändning. Som jämförelse är Sveriges totala elanvändning ca 140 TWh.

Ökad medvetenhet. EU:s nya krav på hållbarhetsrapportering har gjort allt fler företag medvetna om vikten av att köpa hållbara datacenterlösningar.

— Nordiska datacenter är de mest klimatsmarta och i samband med att det börjar uppstå brist på datacenterkapacitet på flera marknader ser vi att allt fler utländska aktörer säkrar upp sin kapacitet genom att etablera sig i Sverige, säger Cecilia Hjertzell, CSO & CMO på T.Loop.

Pionjär inom datalagring. I princip all energi som ett datacenter använder omvandlas till värme. Men idag byggs de flesta datacenter långt från annan bebyggelse. Det gör det svårt att skapa en effektiv värmeåtervinning eftersom det inte finns någon avsättning för värmen. Samtidigt finns det ett ökat behov av att lagra data nära användarna för att undvika fördröjning i dataöverföringen. T.Loop vill minska branschens enorma klimatavtryck genom att skapa stadsnära datacenter som även är nära användarna av data.

”Nordiska datacenter är de mest klimatsmarta och i samband med att det börjar uppstå brist på datacenterkapacitet på flera marknader ser vi att allt fler utländska aktörer säkrar upp sin kapacitet genom att etablera sig i Sverige”

Ett enkelt koncept.
T.Loops Data Energy Center®:

- installeras i befintliga byggnader där de samnyttjar fastighetens infrastruktur
- har effektiva kyllösningar såsom vätskekylning som kraftigt reducerar energianvändningen jämfört med konventionell luftkylning
- återanvänder restvärmen till att värma fastigheten, närliggande fastigheter eller fjärrvärmenätet
- använder datacentrets reservkapacitet till att stötta energinätet genom sk nätbalansering eller att jämna ut effekttoppar

Förutom hållbarhet är säkerhet och fysisk rådighet en viktig fråga för de som hyr datacenterkapacitet. Från EU införs nu ett stort antal lag- och regelkrav som handlar om cybersäkerhet, data, hantering av persondata och inte minst AI och bötesbeloppen för de som inte följer reglerna kan bli enorma.

— På T.Loop bygger vi datacenter som skapar rätt förutsättningar för att våra kunder ska kunna fortsatta utveckla sina digitala affärsförmågor och sin konkurrenskraft med full regelefterlevnad. Främst för att vi kan erbjuda lokala datacenterlösningar som en tjänst och att känslig data och kritiska affärsprocesser därmed kan hållas fysiskt separerat, fortsätter Cecilia.

Även beroendet av de stora amerikanska aktörerna är en stor fråga för EU. Europas möjlighet till fortsatt digitalisering är en viktig säkerhets- och suveränitetsfråga för EU.

Genom att vi bygger en plattform av många, decentraliserade datacenter så kan de backa upp för varandra och därmed minimera risken för avbrott eller dataförlust för våra kunder.

— Vår cirkulära affärsmodell tillsammans med vårt decentraliserade koncept gör att T.Loop bidrar till hållbarare städer, energiomställningen och inte minst ett säkrare och mer robust samhälle, avslutar Staffan.

FAKTA

T.Loop (Therma Loop AB) är en svensk datacenteroperatör, grundat 2020. T.Loop:s koncept för Data Energy Center® reducerar koldioxidutsläppen med 100% och energikostnaderna med 30%, jämfört med konventionella datacenter.
T.Loop var först i världen med att installera sk immersion cooling rack i en kommersiell fastighet. där servern sänks ner i en termisk vätska.

Läs mer på:
www.tloop.se

** Enligt Electricity Report från International Energy Agency, IEA, i januari 2024*

T·LOOP

DETTA ÄR EN ANNONS FRÅN SIMOVITS CONSULTING

Så kan OSINT leda till ett starkare cyberskydd

Open Source Intelligence – OSINT – är en metod för att samla in och analysera information från öppna källor för att generera underrättelser och insikter.
– Med OSINT kan man ligga steget före cyberkriminella för att bygga ett bättre skydd, säger Mikael Simovits, VD på Simovits Consulting.

Mikael Simovits, VD på Simovits Consulting.

Populära sökmotorer har stora begränsningar. Det finns kommersiella och geografiska hänsyn i sökresultaten, och information från delar av internet, som sociala medier, vissa diskussionsforum och det som kallas för deep- och darknet, presenteras ofta inte alls.

Simovits Consulting erbjuder kurser i att söka effektivare på internet, även inom dessa områden, men också lära sig värdera den information man får fram.
– Det kan även handla om att göra mer noggranna bakgrundskontroller på någon som söker jobb, eller bättre omvärldsbevakning utifrån ett affärs- eller konkurrensperspektiv, förklarar Mikael Simovits.

Använda öppen data till sin fördel
Det kan också handla om att lära sig avgöra om en bild är äkta eller AI-genererad, eller hur man kan utnyttja geotaggning och till exempel kontrollera att någon har varit på en plats som man uppgett, från data som personen frivilligt delat med sig av.
– Med OSINT får man ökad förståelse av en situation eller händelse från data som är tillgängligt för alla, säger han.

På kursen lär man sig också vilka spår man själv lämnar efter sig när man är ute på Internet, och vad man kan göra för att agera helt dolt.

Cyberkriminella är ofta aktiva i olika diskussionsforum på obskyra delar av internet. Även de som drabbats av cyberbrott kan vara aktiva i andra forum och aktivt dela med sig av sina erfarenheter. Genom effektiva sökningar kan man hitta dessa forum och där följa diskussionerna för att få en förståelse för hur de cyberkriminella arbetar, vilka mål de har och vilka brister de drabbade hade.
– Utifrån dessa diskussioner kan man anpassa sitt eget cyberskydd och hela tiden ligga ett steg före. Då kan man minska risken att drabbas av cyberbrott och möjlighet att återhämta sig snabbare, avslutar Mikael Simovits.

FAKTA
Simovits Consulting etablerades 1997, med grundidén att leverera informations- och IT-säkerhetstjänster med akademisk noggrannhet och pedagogik.
Simovits Consulting är en av marknadens främsta leverantörer av tjänster inom cybersäkerhet. Genom konstant utveckling kan vi möta en bred skara kundkrav och leverera väl uttänkta lösningar.

Läs mer på:
www.simovits.com

DETTA ÄR EN ANNONS FRÅN C2 VERTICAL SAFETY

Svenska företaget gör den vertikala världen säkrare

Jobb på svindlande höjder kräver hög precision och stort säkerhetstänk. Detta sitter i ryggmärgen hos entreprenörerna bakom C2 Vertical Safety. I över 20 år har de utbildat människor som arbetar på hög höjd och packat deras ryggsäckar med livsviktig kunskap och utrustning.

En härlig paus i solen under ett konsultationsuppdrag offshore.

Vad har militärer, vindkraftstekniker och brandmän gemensamt? De genomför riskfyllda arbeten på höga höjder, där felbedömningar och bristfällig utrustning kan få allvarliga, rent av livshotande konsekvenser. Dessa yrkesgrupper utbildar C2 Vertical Safety.
– Det har ändrats en del på senare år, men tidigare var det ofta så att kunder kom till oss efter ett tillbud eller när Arbetsmiljöverket kommit med synpunkter på arbetsmiljön. I dag är man lyckligtvis mer proaktiv i frågorna, säger Mikael Blixt, produkt- och marknadschef på C2 Vertical Safety.

Ett träningscenter som sticker ut
I Uppsala, i en byggnad som historiskt fungerat som ett forskningslaboratorium för högspänning, finns C2 Vertical Safetys träningscenter där experter på området håller fallskyddsutbildningar för räddningsinsatser och arbeten på höjd.
– Jag skulle säga att det här är norra Europas absolut vassaste träningscenter inom vårt fält, och det får vi ju också som feedback från kunder som har genomfört sådana här typer av kurser i andra länder. De säger att vi sticker ut, vilket vi är stolta över, säger Mikael Blixt.

Heltäckande koncept
Utbildning är C2 Vertical Safetys tyngsta område i dag, men det är bara en pusselbit i det så kallade C2 360-konceptet. De andra bitarna är konsultation, utrustning, repjobb, fallskyddssystem och periodiska kontroller. Konceptet fungerar som en helhetslösning för aktörer som arbetar på höjd.
– Vi eftersträvar att skapa partnerskap där vi kan lösa ett helt behov, i stället för att leverera enskilda tjänster eller prylar. Vi har ”know how” kring arbeten på hög höjd, men kan också leverera utrustningen som krävs, utifrån den metod som vi arbetar fram tillsammans med kunden. Eftersom vi är märkesoberoende har vi möjlighet att hitta den bästa lösningen för den specifika kunden och deras behov. Vi förstår deras vardag, eftersom vi också utbildar dem, säger Mikael Blixt.

Mikael Blixt, produkt- och marknadschef på C2 Vertical Safety.

FAKTA
C2 Vertical Safety AB grundades 2000. C2 står för Climbing Competence. Vertical Safety betyder vertikal säkerhet. Med fallskyddsutbildning, tekniker, metoder och kvalitativa produkter med lång livslängd vill företaget öka säkerheten för alla som arbetar i den vertikala världen.

Läs mer på:
www.c2safety.com

Besök oss på Linkedin:
linkedin.com/company/c2-vertical-safety-ab

Besök oss på Facebook: facebook.com/C2safety
Följ oss på Instagram: @c2verticalsafety

Trygghet i alla tider

Skyddsrumsspecialisten är godkända av MSB som skyddsrumsleverantör och har sedan 1970-talet verkat för ett tryggare civilsamhälle. Vårt uppdrag är att skydda fastighetsägare i fredstid och civilbefolkningen i krigstid, genom att designa, bygga, besikta, renovera och underhålla Sveriges skyddsrum.

Kontakt:
www.skyddsrumsspecialisten.se
info@skyddsrumsspecialisten.se
Tel: 010 207 01 22

Skyddsrums specialisten