Secify

Rapport

Säker framtidsutveckling

-Lägesbild industrisektorn

Hot, utmaningar och risker som berör industrisektorn.

Sammanfattning

Vikten av att beslutsfattare har en kontinuerlig lägesbild ökar allt mer. Vi hoppas att du ser ett värde av att Secify släpper denna rapport för att öka medvetenheten om området för flera inom industrisektorn och inte bara de som har möjlighet att ha egna underrättelsefunktioner.

Vi är inne i en tid där den tekniska utvecklingen och regleringen går väldigt fort samtidigt som flera konflikter fortsätter att påverka oss på kort och lång sikt. Industrisektorn har även under 2024 varit den näst mest utsatta sektorn för cyberangrepp globalt, och i Sverige den mest utsatta sektorn. Hur man ska navigera i denna omvärld och vilka delar som är viktigast att ta med sig ifrån rapporten summeras nedan.

Det finns stora och kända sårbarheter i den svenska industrin.

- Det generella gapet mellan digitaliseringsgraden och säkerhetsnivån i Sverige är stort. Myndigheten för samhällsskydd och beredskap pekar bland annat på i en bred undersökning att endast tre av tio organisationer i Sverige når upp till en ytterst basal nivå av informationssäkerhet och att den stora majoriteten inte ens når det.
- I vår egen undersökning ser vi att det för ett typiskt större industriföretag finns över 2500 läckta användaruppgifter och över 1500 loggar att köpa redo att användas för att attackera företaget. Motsvarande siffror för ett mindre företag är över 600 användaruppgifter och över 200 loggar redo att användas för angrepp.

Du behöver förstå ditt och dina leverantörers digitala fotavtryck. Ska du bedriva ett effektivt säkerhetsarbete behöver du förstå vad det är för aktörer som du framför allt måste skydda dig mot.

- På det geopolitiska planet är det vanligt att aktörer som inte har en aktiv del i konflikten drabbas av cyberangrepp på grund av förändringar i konflikterna.
- Genom att följa utvecklingen, modellera scenarion och indikatorer kan man vara lite bättre förberedd, och agera lite snabbare, om någonting skulle förändras. Beakta även stabilisering i konflikter som skulle kunna ge en hotaktör möjlighet att frigöra resurser för andra mål.
- Följ särskilt utvecklingen i Ukraina, Mellanöstern och motsättningar mellan väst och Kina.
- Hotet från de kriminella hotaktörerna är komplext och föränderligt över tid. Du hittar vår lista över de att hålla koll på just nu på sidan 18.

Leverantörshantering kommer att bli en allt viktigare komponent i säkerhetsarbetet.

- Allt fler incidenter sker i leveranskedjan och vi går mot fler kritiska beroenden till leverantörer där det inte finns något giltigt alternativ.
- Särskilt kinas försprång inom teknologi och komponenter gällande försvar, rymd, AI, kvantdatorer, cybersäkerhet, robotik och avancerade material är något som kan bli en stor utmaning att hantera.
- Effektiv leverantörshantering kräver att en del av bevisbördan och kontinuerlig uppföljning läggs på leverantören att bevisa.

Glöm inte att samarbete mellan de goda krafterna inom industrisektorn aldrig varit viktigare eller att informationssäkerhet och cybersäkerhet måste få ta plats i lednings och styrelserummet.

En investering i området får aldrig vara noll utan det gäller att som med allt annat hela tiden utveckla organisationen för att möta dagens och framtidens utmaningar.

Som verksamma inom säkerhetsbranschen är det lätt att säkerhet får ett egenvärde och blir ett oreflekterat mål. Säkerhetsnivån måste dock alltid vägas mot verksamhetsnyttan och vid införandet av en säkerhetsåtgärd för att hantera en risk måste detta alltid vägas mot den potentiella förlusten av att inte göra något som säkerhetsåtgärden begränsar en från att göra. Precis på samma sätt som att kostnaden för en säkerhetsåtgärd för de allra flesta privata bolag behöver vara i paritet med den potentiella kostnaden för en incident.

Innehåll:

Analys och textansvariga: (per område)

Martin Palmqvist
Huvudansvarig

Joakim Bernhardt
Ansvarig för Threat intelligence

Aida Rokni
Ansvarig för Juridik/regelverk

Kontaktpersoner:

Martin Palmqvist
martin.palmqvist@secify.com

Jonas Stewén / VD
jonas.stewen@secify.com

Form / design:
Henrik Pettersson / Secify

DEL 1

Omvärlden under slutet av 2024

När vi går mot slutet av 2024 kan vi konstatera att det säkerhetsläge vi gick in i året med i stort kvarstår eller har förvärrats. Pratar vi om säkerhetsdrivande händelser i omvärlden är såklart utvidgningen av konflikten i mellanöstern en drivande faktor.

De tidigare bedömningarna från såväl säkerhets-ochunderrättelsemyndigheter som säkerhetsföretag om en breddad och fördjupad hotbild kvarstår därmed. Många bedömare uttrycker sig i högre grad i termer av krig under en

ISRAELISK BOMB SLÅR NER I GAZA | **FOTO: MOHAMMED IBRAHIM**

överskådlig framtid i både mellanöstern och Ukraina. Jämfört med de initiala faserna i konflikterna är de å ena sidan därav mer beräkneliga men å andra sidan har vi tidigare sett hur snabbt en konflikt kan svänga.

På dessa konflikter finns det flera andra konflikter och oroshärdar i bland annat Sudan och Koreahalvön. Retoriken, regulatoriska hinder och handelssituationen mellan väst och Kina är ytterligare en situation vi sett förvärras under året. Likaså den mellan Natoländerna och Ryssland.

> “ Vi har valt att fokusera på de händelser med ett tydligt hotscenario och som vi bedömer som mest aktuella att ta hänsyn till i närtid

Med så många pågående konflikter – eller med andra ord uttryckt som risker – är behovet av att följa omvärldsutvecklingen stort. Oavsett om man pratar i generella termer, utifrån ett nationellt perspektiv, en sektor eller organisation är detta något vi anser att man bör ta höjd för i sitt hot- och riskarbete. Själva händelseutvecklingen i omvärlden är dock bortom de flesta organisationers kontroll att påverka MEN genom att följa utvecklingen kan man vara lite bättre förberedd, och agera lite snabbare, om någonting skulle förändras.

Att arbeta systematiskt med underrättelser för att stärka sitt säkerhetsarbete handlar bland annat om att arbeta med indikatorer. I ett sådant arbete tar man fram ett antal scenarion över mer eller mindre sannolika händelseutvecklingar. Till varje händelseutveckling så kopplar man ett antal indikatorer, och det är dessa man sedan följer. För varje scenario modellerar man troliga konsekvenser och gör kopplingar till vilka säkerhetsåtgärder som ska användas för att bemöta dessa. Genom att göra ett sådant arbete har man kortat startsträckan och kan gå från observation av en indikator till att styra sitt säkerhetsarbete mot åtgärderna man modellerat för det scenariot. Givetvis innehåller verkliga applikationer ett antal kontrollmekanismer för att inte springa för långt på osäkra kort. Poängen är dock att med så mycket tillgänglig information kan det vara lätt att missa det man inte aktivt tittar efter. I de här situationerna så är mottot att den förberedde överlever sant. Vår version handlar dock inte om liknelsen om att springa ifrån björnen i skogen utan i stället om samarbete. När vi samarbetar och delar information blir vi alla starkare och kan bättre stå emot de hot som väntar.

I vår omvärldsanalys har vi valt att lyfta ut de större händelser som skulle kunna få stor negativ påverkan på det geopolitiska säkerhetsläget och/eller leda till stora negativa konsekvenser för organisationer inom industrisektorn. Vi har valt att fokusera på de händelser med ett tydligt hotscenario och som vi bedömer som mest aktuella att ta hänsyn till i närtid. På grund av utrymmesskäl har vi valt att i den här rapporten inte ta upp AI-utvecklingen, kvantdatorer eller spänningarna på koreahalvön och de mellan Kina och Taiwan.

Utvecklingen av kriget i Ukraina

Vi har tidigare under året konstaterat att det som är mest drivande för säkerhetsläget i Europa är kriget i Ukraina. Tyvärr är det nog en situation som kommer att kvarstå under överskådlig framtid. Riskerna med detta för svenska organisationer handlar inte bara om vad som skulle

FÖRSTÖRD RYSK PANSARVAGN VISAS UPP I KIEV 2022 | **FOTO: SERHII TYAGLOVSKY**

hända om konflikten utvidgades geografiskt. Det finns även en stark koppling till leveranskedjeproblematik och de delar av den som går genom Ukraina, Ryssland eller angränsande länder.

Hantering av sin leveranskedja är för många en komplex uppgift och något som fångats av flera kommande lagstiftningar vi berör senare i rapporten. Hur många har exempelvis koll på vilka delar av sin leveranskedja som rör sig genom grannländer som konflikten skulle kunna utvidgas till? Vilken av er data skulle då kunna hamna i orätta händer eller vilka kritiska tjänster skulle kunna bli otillgängliga? Vår rekommendation är därför att börja arbeta systematiskt med att kartlägga och riskbedöma sina mest kritiska delar av leveranskedjan. Därtill bör man aktivt arbeta för att minska riskerna, genom alternativa lösningar, byta ut riskfyllda leverantörer eller vidta andra säkerhetsåtgärder.

Det är dock inte bara länderna som rent geografiskt omfattas av kriget som kan vara riskfyllda som leverantörer. Länder som tar ställning för Ryssland skulle kunna omfattas av sanktioner från väst vilket skulle påverka deras lämplighet som en del i en leveranskedja. Dessa förändringar i dynamiken i kriget blir alltmer viktiga att följa.

Ytterligare aspekter på det är att länder som tar ställning för Ukraina på olika sätt också skulle kunna komma att drabbas av cyberangrepp som svar från rysksympatiserande aktörer. Detta är något som hänt flera gånger under invasionen när länder offentliggjort större vapenleveranser till Ukraina eller när Sverige gick med i Nato. Historiskt har vi sett att de organisationer som i slutändan blivit angripna många gånger inte haft någon aktiv del i ställningstaganden mot Ryssland. Det är därför av vikt att följa handlingar av Sverige eller svenska aktörer som går emot Rysslands intressen och hur dessa skulle kunna leda till cyberangrepp mot svenska organisationer.

Något som också är värt att titta lite extra på är analyser av de angreppsmetoder som ryskstödda aktörer använder i Ukraina. Traditionellt har krig varit ett tillfälle att testa nya metoder. De metoder som används i Ukraina och de lärdomar dessa aktörer drar av detta är något de tar med sig och sannolikt inkluderar i sitt sätt att agera mot andra. Här kan nämnas angrepp mot kommunikationsinfrastruktur, ett stort fokus på kritisk infrastruktur genom överbelastningsattacker och förstörelsemjukvara samt tidigare i konflikten angreppet med kryptomasken NotPetya som fick global påverkan. Det är därför bra att notera nya typer av skadlig kod, sätt att agera eller målval och inkludera skyddsåtgärder i förhållande till detta i det egna säkerhetsarbetet.

Ett scenario att följa är vad som skulle hända om konflikten stabiliserade sig ytterligare över tid. En pågående konflikt men som bundits så att inga större framsteg görs från endera sida skulle potentiellt kunna vara en farligare situation för svenska organisationer än om konflikten pågår mer aktivt. Särskilt om en sådan stabilisering föranletts av stöd från västvärlden. Eftersom Rysslands resurser inte är oändliga skulle en sådan ”lugnare” period i kriget kunna innebära att fokus i större utsträckning riktas mot de som understött Ukraina. Som tidigare resonerats om skulle dessa resurser då också kunna vara beväpnade med nya lärdomar och metoder från krigsinsatsen. Vår bild är därför att det inte bara är händelseutveckling man bör hålla koll på utan även avsaknad av händelseutveckling. Detta är särskilt av vikt för de organisationer som producerat material som använts av Ukraina. Exempelvis rapporterades det tidigare under året om hur ett attentatsförsök avstyrdes mot VD:n för ett tyskt vapenföretag vars vapen använts i Ukraina. Som nämnts tidigare har vi dock kunnat se hur det ofta är företag som inte har någon aktiv del i konflikten som blivit mål för cyberangrepp vilket

> “Som nämnts tidigare har vi dock kunnat se hur det ofta är företag som inte har någon aktiv del i konflikten som blivit mål för cyberangrepp...

FÖRSTÖRT VÅNINGSHUS I KIEV PROVINSEN | **FOTO: ANDREW PETRISCHEV**

gör händelseutvecklingen av vikt att följa även för de utan direkt koppling.

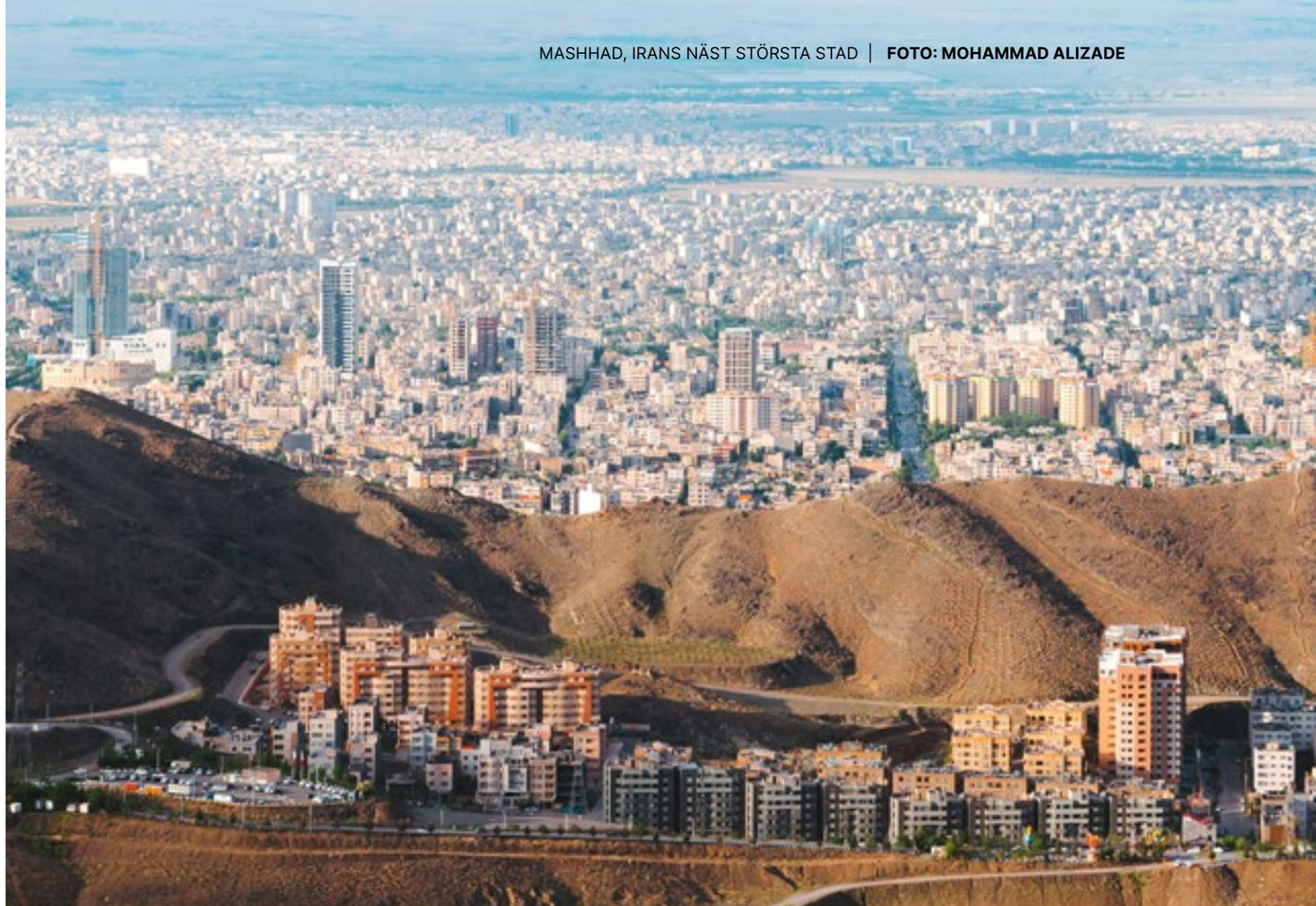
Slutligen är det svårt att bortse från hur det amerikanska presidentvalet kan påverka kriget. Seger för Demokraterna skulle troligen leda till en fortsättning på inslagen väg angående kriget i Ukraina. Fortsatt ekonomiskt stöd men en ovilja att rent fysiskt bli indragen i konflikten skulle troligtvis inte bidra till någon förändring jämfört med den utveckling vi ser i dagsläget. En republikansk seger skulle baserat på Donald Trumps tidigare uttalanden kunna påverka säkerhetsläget i Europa. Med Donald Trump på presidentposten är det troligt att det amerikanska fokuset kommer ligga mer på hemmaplan, det inhemska säkerhetsläget och stabiliteten snarare än konflikter i Europa. Däremot har Trump vid flera tillfällen visat sig ovillig att starta konflikter och uttryckt en vilja att avsluta kriget i Ukraina. Det sistnämnda är dock troligare att det sker om det är kopplat till någon tydlig vinning för USA och att se som ett relativt osäkert kort. Vid ett minskat monetärt och resursmässigt stöd till kriget i Ukraina och en kallare attityd till militära samarbeten skulle detta också kunna bidra till en gradvis urholkning av Natos ställning i Europa. Trump har gjort flera uttalanden som pekar på att det amerikanska stödet till Natoländer inte är lika orubbligt och självklart som det varit hittills även om mycket kan tillskrivas förhandlingstaktik och att mana på medlemsländerna att öka sin försvarsbudget. Dock är en bild av ett sviktande stöd, oaktat om den i praktiken skulle vara sann eller inte, något som skulle minska Natos avskräckande effekt och nedmontera tilliten till säkerhetsgarantier. Saker som givetvis skulle inverka negativt på säkerhetsläget i Sveriges närområde. Till detta kommer rapporter om att Putins underrättelseoperationer i Europa fortsätter att öka både kvalitativt och kvantitativt för att försvåra för Europa att hålla en enad front och för att underminera Natos ställning. Vid en utfrågning i det tyska parlamentet svarade landets två underrättelsechefer att Rysslands underrättelseoperationer i Europa nått en nivå vi inte sett förut där Ryssland kommer att fortsätta använda hybridkrigsföring och fysiskt våld för att testa gränser och eskalera konflikten.

> “..rapporter om att Putins underrättelseoperationer i Europa fortsätter att öka både kvalitativt och kvantitativt för att försvåra för Europa..

Ur ett företagsperspektiv så är det viktigt att inse att de potentiella negativa händelserna ovan bör betraktas som risker och att riskvärdet kan öka beroende på utfallet. Precis som att det på europeisk nivå börjar pratas om hur man ska kompensera för ett möjligt mindre engagerat USA så borde man som företag resonera på samma sätt, fast kopplat till den egna spenderingen på säkerhet, om säkerhetsläget i omvärlden försämras.

Konflikten i Mellanöstern förvärras

Situationen i Mellanöstern blir mer och mer spänd för varje dag, med ökande strider och en växande humanitär kris. Under året har konflikten eskalerat, särskilt i relation till Iran och dess allierade. Efter att Israel dödade Hizbollahs ledare Hassan Nasrallah i september, uppfattade Iran sannolikt detta som en direkt utmaning mot sin regionala inflytandesfär. Israel har även riktat attacker mot iranskstödda mål i Syrien, vilket förstärkt situationen och signalerat en vilja att försvaga Irans grepp över motståndsaxeln. Som svar avfyrade Iran den 1 oktober en storskalig missilattack mot Israel, en ovanlig direkt aktion från Teheran som markerar landets oro över att tappa kontroll över konflikten. Israels fortsatta markinvasion i Libanon har som en av flera faktorer bidragit till att öka risken för ett bredare regionalt krig, där Iran troligen kommer att agera för att bevara sitt inflytande och sin avskräckningsförmåga, vilket nu skulle kunna driva konflikten mot en farlig spiral av vedergällningar. Det är dock inte helt klart i vilken omfattning Hamas, Hizbollah eller även Iran kan fortsätta att eskalera konflikten.



MASHHAD, IRANS NÄST STÖRSTA STAD | **FOTO: MOHAMMAD ALIZADE**

Det är troligt att Iran kommer att skifta fokus med sina APT-grupper (Advanced Persistent Threat) mot mer direkta och strategiska mål i konflikten. Det innebär att Irans cyberattacker kan rikta sig främst mot Israel och dess allierade, särskilt militära och kritiska infrastrukturer, för att skada och störa deras förmåga i kriget. Detta fokus på direkta mål kan innebära en tillfällig minskning av cyberattacker mot länder som Sverige, som inte är direkt involverade i konflikten.

> “Om USA:s fokus skiftar mot Mellanöstern kan detta ge Ryssland mer spelrum i Europa [vilket] ...kan få långsiktiga konsekvenser för den svenska säkerheten.

Sett ur perspektivet för svenska företag så är det dock inte bara hotet från hotaktörer som är risker med konflikten. Det finns även här kopplingar till säkerhet i leveranskedjan. Som ett exempel har Israel ett väldigt omfattande värnpliktssystem och ju längre krigsinsatsen pågår, desto troligare är det att konsekvenser som försämrade leveranser kommer att börja märkas hos de israeliska säkerhets-, och It-företagen då en del av deras personal kommer att behöva användas för krigsinsatsen. En utbredning av kriget i regionen eller sanktioner mot inblandade nationer skulle också mycket väl kunna få påverkan på energikostnader och tillgång till råmaterial. Situationen skulle också om den eskalerade kunna riskera att påverka handelsflödet genom Suezkanalen som redan är hårt ansatt på grund av situationen vid Afrikas horn.

Även om det från amerikanskt håll uttryckts tvivel mot vissa av Israels aktioner är det troligt att USA kommer att fortsätta stötta Israel – oaktat vem som vinner presidentvalet. Dock skulle förmodligen stödet med Harris som president ske med en större hänsyn till Palestina och kringliggande länder. På grund av det utbredda stödet för kriget i Israel och med hänsyn till Israels agerande gentemot USA:s avrådan från vissa aktioner är det inte heller helt säkert i vilken utsträckning USA kan påverka Israels agerande. Det är därför mycket möjligt att USA återigen kan komma att intensifiera sin militära närvaro i Mellanöstern, i enlighet med sina allianser med Israel. Denna potentiella militära intervention, särskilt i en flerfrontskonflikt, kommer kräva betydande resurser. Det kan i sin tur påverka hur mycket USA kan investera i Ukraina. Om USA:s fokus skiftar mot Mellanöstern kan detta ge Ryssland mer spelrum i Europa, vilket kan leda till en förändring av den geopolitiska balansen i regionen. En sådan utveckling kan få långsiktiga konsekvenser för den svenska säkerheten.

Innovation, politik och kinesisk framfart på den europeiska marknaden

Det har länge sagts lite som en floskel i olika varianter att USA innoverar, Kina imiterar och EU reglerar. På det generella temat fick Mario Draghi nyligen i uppdrag av EU-kommissionen att skriva om EU:s framtida konkurrenskraft. I sin rapport framhäver han att den europeiska marknaden halkat långt efter den amerikanska och kinesiska och att särskilt industrin är fast i ”the middle technology trap”. Något som hindrar innovation och tillväxt. Många företag förblir inom traditionella sektorer utan att investera i högteknologi, vilket gör dem sårbara för konkurrens från länder som Kina. Denna bild delas av det australiska strategiska policyinstitutet som kvantifierar Kinas försprång inom teknologi gällande försvar, rymd, AI, kvantdatorer, cybersäkerhet, robotik och avancerade material till 89%. Till detta pekar de ut ett antal områden som riskerar att bli monopoliserade inom vilka Kina har en ledande ställning. Anledningar Draghi pekar på för situationen för den europeiska marknaden är att strikta konkurrensregler och begränsningar kring statligt stöd kan hämma industrins utveckling. Han föreslår att EU bör reformera dessa regler för att ge mer flexibilitet, särskilt i frågor om fusioner och investeringar i strategiska industrier.

Slutsatser från Draghis rapport som berör informations- och cybersäkerhet är att användandet av AI i verksamhetsprocesser halkat efter konkurrensen och att data måste göras tillgängliga för att kunna användas. Vidare menas att reglering, varav de rörande informationssäkerhet vi kommer beröra senare, begränsar innovationskraften.

Ytterligare en intressant slutsats är att riskaptiten bör öka för att tillåta innovation. Alla dessa slutsatser pekar

LASERSKÄRNING AV PLÅT

| FOTO: CLAYTON CARDINALLI

kanske inte på att slänga säkerheten genom fönstret men att hitta ramar för att arbeta med säkerhet som inte är för begränsande. Som verksamma inom säkerhetsbranschen är det lätt att säkerhet får ett egenvärde och blir ett oreflekterat mål. Säkerhetsnivån måste dock alltid vägas mot verksamhetsnyttan och vid införandet av en säkerhetsåtgärd för att hantera en risk måste detta alltid vägas mot den potentiella förlusten av att inte göra något som säkerhetsåtgärden begränsar en från att göra. Precis på samma sätt som att kostnaden för en säkerhetsåtgärd för de allra flesta privata bolag behöver vara i paritet med den potentiella kostnaden för en incident. Att helt enkelt ställa sig frågan ”om vi inför den här säkerhetsåtgärden, hur mycket kommer våra kostnader för incidenter att minska” men också ”om vi inför den här säkerhetsåtgärden, hur mycket kommer det påverka våra möjligheter till intäkter”.

Spolar vi tillbaka bandet till konkurrensfrågan på ett globalt plan målas särskilt Kina ut som ett stort hot där statssponsrade företag rent konkurrensmässigt är ett hot mot de europeiska företagen. Det är även så att europeiska företag är beroende av ett fåtal leverantörer av kritiska mineraler och tekniska komponenter från kinesiska leverantörer. Risken för fortsatt tillhandahållande av dessa är uppenbar vid geopolitiska förändringar. Ökad monopolisering av teknologier likt den beskriven ovan tvingar företag att i högre grad förlita sig på ett land. Detta kan skapa stora risker i leveranskedjan, för att inte tala om säkerhetsproblem om hårdvara tillverkad i Kina kompromitteras på något sätt. Historiskt har Kina, precis som de flesta länder, besvarat förändringar de upplever vara till deras nackdel med någon form av motaktion så som ekonomisk och politisk utpressning. Nyligen röstade EU igenom permanenta tullar på import av elbilar från Kina, där Sverige lade ner sin röst. Sverige har även nyligen för första gången antagit en försvarsstrategi för Asien som skulle kunna ge en öppning för svenskt militärt engagemang. Båda dessa beslut är exempel på något som skulle kunna få Peking att genomföra någon form av åtgärd.

Det har länge rapporterats om kinesiska företag och statsanknutna aktörer som bedrivit företagsspionage mot västerländska och svenska företag. Flera underrättelse- och säkerhetsorganisationer brukar göra den grova uppdelningen att gällande statssponsrade hackergrupper så där de ryska grupperna fokuserar på förstörelse och samhällsstörning så fokuserar de kinesiska grupperna i större utsträckning på företagsspionage och att komma över immateriella rättigheter. Kina har sällan respekterat immaterialrätten, till fördel för den inhemska produktionen, något som kan leda till uppenbara problem för företag på den svenska marknaden. En annan form av spionage, och som visar på kopplingen mellan kinesiska företag och kinesiska staten, rör den form av övervakning och informationsinhämtning som kinesiska hårdvaru- och mjukvaruföretag anklagats för att bygga in i sina produkter.

Situationen som beskrivs ovan är på intet sätt ny men har eskalerat i takt med teknologi- och omvärldsutvecklingen. Viktiga aktiviteter för att hantera dessa risker är att inventera och se över sina leveranskedjor på ett strategiskt plan. Vilka kritiska komponenter kommer jag att vara beroende av i framtiden? Vilka kan tillhandahålla dessa och finns det alternativa producenter som inte är lika geopolitiskt riskabla. En aspekt är också att inventera sina informationstillgångar, särskilt de kopplade till immateriella rättigheter och andra företagshemligheter, och vilket skydd de har. Det finns också en poäng att göra för att arbeta med hotunderrättelser. Vilka är de här grupperingarna som kan vilja komma över mina företagshemligheter och vilka metoder tenderar de att använda?

Något som ofta glöms bort i arbetet med att hantera risker här och nu är det långsiktiga perspektivet och vad man kan göra där. Som vi inledde är inte ensam stark och den kan vara värt att fundera kring vilka partners man vill utbyta information med, vilka sammanslutningar man vill vara del av och på vilket sätt man vill engagera sig i att utveckla politik, lagstiftning och standarder så att dessa anpassas till det klimat man själv vill verka i.

SHANGHAI, KINA | **FOTO: ADI CONSTANTIN**

DEL 2

Hur är bilden av den svenska industrisektorn?

Sverigebilden har påverkats av flera faktorer, inklusive koranbränningar, LVU-kampanjer samt nu senast den svenska regeringens satsning på återvandring. Regeringssatsningen för återvandringen har uppmärksammats medialt utomlands men även blivit viralt på utländska sociala medier-konton.

Därutöver har Palestinarörelsen som har ett relativt starkt fäste och stöd i Sverige, kontinuerligt spridit inlägg om Sveriges utrikespolitik som uppfattas som Israelvänlig.

Det finns flera exempel på när just Sverigebilden varit drivande i inträffade angrepp. När koranbränningarna fick stor medial uppmärksamhet under 2023 kunde vi notera en stark korrelation mellan när en koranbränning uppmärksammades i media och cyberangrepp mot svenska mål. I närtid har även Åklagarmyndigheten tillsammans med Säkerhetspolisen gått ut med att Irans säkerhetstjänst genomfört en operation under perioden. Genom dataintrång tog de över en svensk SMS-tjänst och skickade 15 000 meddelanden som uppmanade till hämnd mot koranbrännare. Liknande samband kunde vi se under perioden kring Sveriges Natoansökan där ett antal organisationer, både statliga och privata, blev mål för cyberangrepp. Många av de angripna saknade dessutom helt koppling till processen kring den svenska Natoansökan.

Närmare industrisektorn och i närtid har Elbit Systems, ett israeliskt vapenföretag, tecknade ett avtal med svenska Försvarsmakten värt 1,7 miljarder kronor. Företaget levererar vapen som används i konflikten, något som har lett till att flera finansinstitut och svenska pensionsfonder uteslutit dem på grund av inblandning i krigsförbrytelser. Amnesty International har bekräftat att Elbits vapen används mot civila i Gaza, vilket har väckt kritik på sociala medier om Sveriges samarbete med företaget och dess förenlighet med internationell rätt. På hemmaplan har det lett till upprepade angrepp i form av skottlossning utanför Elbit systems svenska dotterbolag i Göteborg.

Ett annat bolag inom sektorn som hamnat i blåsvädret i media är Northvolt, som förutom finansieringsproblem och problem med kinesiska underleverantörer, blivit kritiserade för sina arbetsförhållanden, arbetsplatssäkerhet, flera dödsfall och stora permitteringar.

Även om vi inte kunnat se att kritiken mot Northvolt lett till cyberangrepp finns det gott om exempel på när missnöjda före detta anställda genomfört angrepp för att hämnas så som vid papperstillverkaren Georgia-Pacific och betalningslösningsföretaget Cash App. Ett av de största och mest kända exemplen på när en mediauppmärksammad händelse lett till cyberangrepp är kanske när Sony Pictures drabbades av massiva cyberangrepp efter att deras kontroversiella film The Interview annonserades.

Att ta med sig från dessa exempel är att omskrivningar, publicitet och den mediala bilden av den egna organisationen, sektorn och nationen mycket väl kan komma att påverka den egna säkerhetssituationen. Att ha förmågan att upptäcka sådan publicitet och rutiner för att kunna justera säkerhetsarbetet därefter bör därför vara en naturlig del av det förebyggande arbetet.

Ytterligare en bild som är värt att betänka är tillståndet för den generella säkerhetsnivån i Sverige. Det har länge pratats om det så kallade digitaliseringsgapet, det vill säga skillnaden mellan digitaliseringsnivån och säkerhetsnivån. Sverige placerar sig kontinuerligt på de högsta platserna när nivån av generell digitalisering i samhället mäts men också kontinuerligt på betydligt lägre placeringar vid mätningar av den generella informationssäkerhetsnivån i samhället. Gapet däremellan är känt och senast beskrev myndigheten för

FOTO: ANDREAS RASMUSSEN

samhällsskydd och beredskap hur sju av tio organisationer i Sverige inte ens når upp till nivå ett i deras modell där nivå tre motsvarar deras grundläggande krav i sina föreskrifter. Detta målar en skrämmande mörk bild av den generella nivån på säkerhetsarbetet i Sverige och för att återgå till liknelsen med att springa ifrån björnen i skogen så är det inte orimligt att, allt annat lika, att en hotaktör väljer att angripa ett svenskt företag i stället för ett från någon annan nation. Detta illustrerar, för att återgå till mediabild, vikten av att även tänka på positiva omskrivningar inom informationssäkerhet och hur man väljer att arbeta med och signalera status på sitt säkerhetsarbete.

> “Bara under 2024 har vi sett flertal läckta uppgifter från både större och mindre företag inom industrisektorn i Sverige.

Kända sårbarheter inom den svenska industrisektorn

De flesta företag läcker användaruppgifter. Oanvända kan man argumentera för att de inte är någon större sårbarhet och att med goda rutiner för byte av dessa uppgifter kan man minska sårbarheterna. Dock som vi kommer se nedan är just användaruppgifter ofta en vanlig ingångsväg för ett cyberangrepp. Förutom att uppgifterna i sig kan användas för att få tillgång till system och konton (på grund av dåliga rutiner för byte, snabbhet hos angripare eller system/konton som inte hanteras enligt ordinarie rutiner) så signalerar mängden läckta uppgifter något om säkerhetsnivån hos företaget i fråga. Det är också vanligt att vi ser att en ökning av läckta användaruppgifter från ett företag korresponderar mot ökade angreppsförsök, oaktat om det är gamla eller nya uppgifter som läckts. Det finns också en koppling till det mer personliga planet och risken för utpressningsförsök när det läckt att någons företagsmejl använts för att registrera sig på andra hemsidor. Detta fenomen är något vi ser frekvent där någons personliga företagsmejl använts för att registrera sig på sidor som det är troligt att personen i fråga inte vill ska komma ut att den registrerat sig på. Steget från en sådan läcka till att man har en ofrivillig insider i sitt företag är inte långt. Till detta kan man lägga till ytterligare att på grund av hur frekvent samma lösenord används på flera siter så om läckan gäller en privat tjänst så är steget inte heller långt till att få tillgång till personens jobbkonto.

Bara under 2024 har vi sett flertal läckta uppgifter från både större och mindre företag inom industrisektorn i Sverige. Vi ser läckta uppgifter från företagsdomäner, men också andra hemsidor där företagsmejl har använts och läckts. Ett tydligt samband gäller storleken på företaget och mängden läckta uppgifter, av naturliga skäl, även om det finns en viss variation.

Infostealer i tre steg:

1. Infostealers är mjukvara som installeras på ett offers dator, genom exempelvis phishing eller social engineering, för att sedan stjäla alla redan sparade inloggningsuppgifter, bankuppgifter, och annan intressant information, så som skärmdumpar, IP-adresser och installerad mjukvara. Mjukvaran stannar på datorn och fortsätter att hämta ny information, för att sedan skicka vidare informationen till en hotaktör.

2. Informationen som hotaktören får in genom infostealers sammanställs sedan i loggar som går att köpa på olika forum på deep- och darkweb och kan användas till att exempelvis logga in i ett offers miljö.

3. När en hotaktör får åtkomst till ett offers miljö, installeras ett så kallat implantat som underlättar för hotaktören att behålla åtkomst till de datorer som hotaktören tar över. Implantatet är en mjukvara som underlättar vid vanliga operationer, så som kartläggning och rörelse från dator till dator inom miljön. Mjukvaran fortsätter att kommunicera med en server under hotaktörens kontroll, där kommandon ges tillbaka till mjukvaran. Denna kommunikation kallas för Command and Control (C&C).

För de större företagen inom sektorn kan vi i dagsläget hitta flera tusentals läckta användaruppgifter medan det för de mindre företagen finns ett par tio- eller hundratal läckta uppgifter.

När vi granskade vilka uppgifter som finns tillgängliga för ett antal företag verksamma inom industrisektorn hade samtliga läckta användaruppgifter. Som vi resonerade om ovan är detta illa i sig, men vad som är än mer illa är att för mer än hälften av företagen fanns tillgängliga infostealerloggar på deep- och darkweb. Dessa loggar innehåller betydligt fler uppgifter än användarkonton och är därmed en större säkerhetsrisk. Informationen i dem skulle kunna användas för utpressning, bedrägerier eller för att få tillgång till företagets IT-miljö. Som ett exempel finns det för ett större industriföretag för närvarande över 2500 läckta användaruppgifter och över 1500 infostealerloggar medan motsvarande siffror för ett mindre företag är över 600 användaruppgifter och över 200 infostealerloggar.

Förutom det som ofta benämns som kontors-IT så präglas industrisektorn i hög grad av det som kallas för operational technology (OT). Det har länge problematiserats kring OT-utrustning ur en säkerhetssynvinkel. Dels hur den i många fall sitter samman med kontors-IT och därmed möjliggör för en angripare att komma in på ett ställe och sedan vandra vidare i nätverken, och dels problematiken kring säkerhetsuppdateringar. Många mjukvaror som driver OT är föråldrade och därmed byggda för inga, eller helt andra säkerhetsstandarder än vi har idag. De är i många fall mer komplicerade

att uppdatera än kontors-IT då det inte finns samma system och mekanismer för uppdateringar och framför allt den starka kopplingen till produktion och eventuellt produktionsbortfall om något skulle gå fel. Det är därför inte ovanligt att OT körs så länge det går och så hoppas man på det bästa.

Ett illustrerande exempel från året är sårbarheterna CVE-2024-37998 och CVE-2024-39601, som tillsammans ger en hotaktör möjligheten att installera en bakdörr i Siemens SICAM SCADA system. Hotaktören kan sedan med hjälp av förstnämnda sårbarheten återställa administratörslösenordet på systemet, och sedan med hjälp av den andra sårbarheten nedgradera systemets version och öppna upp systemet för flera äldre sårbarheter. Dessa sårbarheter illustrerar just att stor tyngd behöver läggas på att begränsa OT-teknologier och system från att nås av obehöriga. Både att externa kommunikationer mot systemet stryps ner, och att genom nätverkssegmentering utesluta systemen från normala användarmiljöer.

FOTO: WARREN WONG

DEL 3

Hotbilden

Innan vi går in på vår kartläggning av de mest relevanta hotaktörerna i dagsläget är det viktigt att bära med sig att det inte bara är de antagonistiska hoten som man behöver arbeta med. Rena systemfel och mänskliga misstag, som nu senast i fallet med CrowdStrike, samt påverkan från naturhändelser, som vid chipbristen under pandemin kan ge lika stora konsekvenser.

Faktum är att enligt de senaste sammanställningarna av inrapporterade incidenter till MSB så utgör de antagonistiska incidenterna endast en tredjedel medan systemfel, mänskliga misstag och naturhändelser står för majoriteten. Enligt deras sammanställningar förefaller det inte heller finnas något samband mellan konsekvenserna av en incident och vad som orsakade den. Många av de hot som realiseras, oaktat orsaken, sker i dagsläget också i leveranskedjan och inte hos den

drabbade aktören i sig. Vi kommer att problematisera detta ytterligare nedan.

Ser vi till de antagonistiska aktörerna finns det en mängd olika grupperingar som genomför angrepp med olika syften. Man brukar prata om att det finns statsaktörer, statssponsrade aktörer, rent kriminella grupperingar, hacktivister och ideologiskt motiverade aktörer. Dessa olika typer av aktörer tenderar att använda olika metoder för att åstadkomma olika syften. Statsaktörerna och de statssponsrade aktörerna tenderar att arbeta mer långsiktigt för att kunna komma åt information av nytta för den egna staten eller orsaka skada inom ramen för hybridkrigsföring eller som stöd till rent militära angrepp. De kriminella grupperingarna genomför ofta angrepp för ekonomisk vinning så som ransomware till skillnad mot hacktivister och andra ideologiskt motiverade aktörer som genomför angrepp som stöd för den egna övertygelsen och agendan.

I praktiken är gränsdragningarna dock inte så skarpa utan en och samma person kan tillhöra en statsaktör eller statssponsrad aktör på dagtid men agera i en kriminell gruppering på kvällarna samt att allianser med olika grupperingar och nationer kan skifta över tid. Det är också så att vissa nationer, även med de inhemska kriminella grupperingar de formellt inte samarbetar med, ändå ger grönt ljus att angripa mål i länder de anser som illvilliga. Det vill säga att angreppen sker med statens goda minne och i den egna nationen, i alla fall för stunden, med straffrihet i praktiken. Det är på grund av den beskrivna föränderligheten som det blir viktigt att kontinuerligt följa hotaktörernas agerande. Vet man vilka hotaktörer som är mest sannolika att angripa den egna verksamheten, vad deras syften är och vilka metoder de använder har man betydligt större chanser att kunna skydda sig mot dessa.

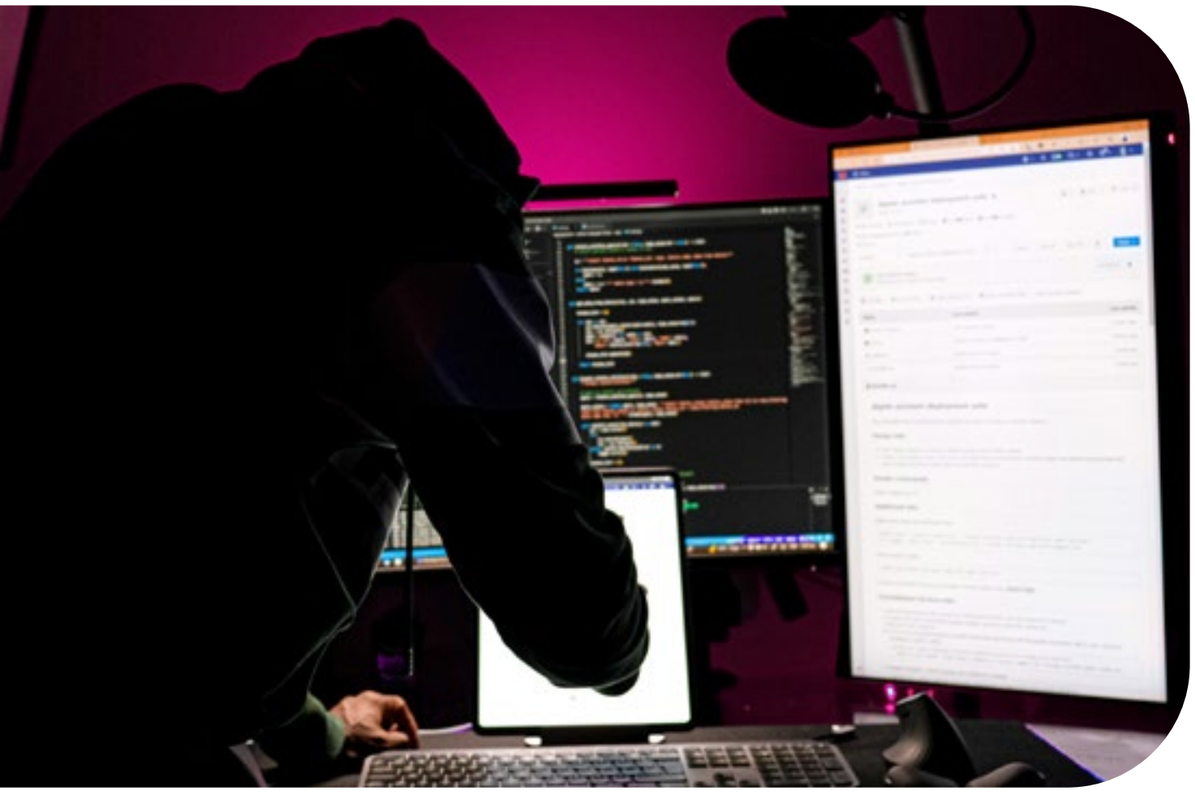


FOTO: PHETLA BOITUMELO

Affiliates:

En affiliate, eller en grupp affiliates kan använda sig av en ransomware-grupps tjänster för att utföra attacker och slutligen få betalt. Tjänster som oftast ingår i att vara en affiliate till en ransomwaregrupp inkluderar krypteringsmjukvara, utpressning på pengar (förhandlare via chatt), och till slut en mixerservice, som tvättar kryptovaluta (så som Bitcoin) för att sedan få betalt.

Genom att nyttja en ransomware-grupps tjänster, kan en affiliate fokusera på att fortsätta attackera företag, och inte behöva tänka på stegen därefter. Kostnaden för att använda dessa tjänster är oftast en procentdel av slutsumman som betalas ut, ofta 10–20%.

Aktuella hotaktörer 2024 och framåt

Industrisektorn har under 2024 varit den näst mest attackerade sektorn globalt, och i Sverige den mest attackerade sektorn när det gäller ransomwareattacker. Grupperna som genomför dessa attacker använder sig oftast av en RaaS-modell (Ransomware as a Service), där de förser hotaktörer med verktyg och tjänster som underlättar för hotaktörer att fortsätta utföra attacker på företag. Den vanligaste metoden för att få betalt från sina offer när det gäller ransomware är en dubbelutpressningsmetod. Vid en sådan metod stjäl de data från sina offer och lägger sedan upp den på sina läckagehemsidor för att slutligen kryptera datan och uppmana offer att betala för att få tillbaka den.

De kriminella grupperingar vi sett varit mest aktiva och störst hot globalt är:

Ransomhub

Storspelare under senare halvan av 2024 och innehar förstaplats i mängden offer per månad. Ransomhub som är en grupp som tillhandahåller ransomware som en tjänst, kallar sig själva “the next generation of ransomware”. De har utifrån erfarenheter från andra RaaS-tjänster, tagit fram en tjänst som lockar alla typer av samarbeten, och med det, en stor mängd offer. Hålet i marknaden som skapades när BlackCat/ALPHV tog emot en stor summa pengar från ett offer, och sedan la ner sina tjänster för att försvinna, i mars 2024 har gett Ransomhub möjligheten att rekrytera många högrankade affiliates, så som

de som nyttjat tjänster från BlackCat/ALPHV och LockBit, men även gruppen Scattered Spider.

LockBit

Efter åtalen mot den trodda ledaren av LockBit, Dmitry Khoroshev, även känd som ”LockBitSupp” på de större hackerforumen, har mängden offer utsatta för LockBits mjukvara minskat. Mängden offer har även påverkats av Operation Cronos, ett projekt startat av FBI som involverar flera brottsbekämpande myndigheter så som svenska Polisen. Projektet har lyckats ta ner större delar av LockBits infrastruktur, extraherat flertal dekrypteringsnycklar, flertal konton för kryptovaluta har blivit frysta, och ett par aktörer från LockBit har blivit åtalade och arresterade. Trots detta fortsätter offer att läggas upp på deras nya webbsida, och LockBit och deras affiliates är därför fortfarande en grupp att hålla koll på.

Play

En relativ ny grupp som startade 2022, har under åren gått över till den mer lukrativa RaaS-tjänsten. Med övergången till att agera som en RaaS-grupp har mängden offer ökat drastiskt under åren, och Play ses nu som ett av de största hoten när det gäller ransomware. Något som särskiljer Play och deras affiliates är att de generellt inte har några typer av offer som ses som “off limits”, utan de tar sig aktivt in i alla typer av organisationer. De använder sig av typisk phishing, men tar även hjälp av nya sårbarheter, så som Citrix Bleed (CVE-2023-4966). Play har via sin webbsida tagit på sig attacker mot svenska företag, och fortsätter under 2024 att angripa mål i Sverige.

Hunters Internationa

En RaaS-tjänst som under 2024 hållit ett högt tempo i antal drabbade offer, och som ser ut att behålla sin takt i mängden offer som läggs upp på deras webbsida. Hunters International sägs av vissa vara eftergångaren till gruppen Hive efter att deras infrastruktur blev nedtagen av brottsbekämpande myndigheter. Detta är dock endast baserat på att deras krypteringsmjukvara till del liknar den som användes av Hives. Hunters International har dock förklarat att de endast köpte källkoden för deras krypteringsmjukvara och delar av infrastrukturen. De valde att köpa källkoden då deras huvudsyfte inte alltid är att kryptera sina offers filer, utan de har vid flertal tillfällen endast stulit data, utan att kryptera i en så kallad dubbelutpressning.

FOTO: WARREN WONG

Akira

Gruppen som stod bakom attacken på en av TietoEvrys svenska serverhallar i januari, och med det skapat stora bekymmer för flertal svenska företag och myndigheter. Gruppen fortsätter att hålla sig i toppen över flest offer globalt, men har även setts attackera flera svenska företag och kommuner. Precis som alla grupper, används ofta phishing och spearphishing för att få åtkomst till offers nätverk, men Akira har lagt större fokus på att ta sig in genom osäkrade VPN-lösningar som inte använder sig av multifaktorsinloggning.

De grupper som vi sett varit särskilt aktiva i Sverige under 2024 är till del samma som de största aktörerna globalt men det finns även de aktörer som varit mindre globalt sett men väldigt aktiva i Sverige. Dessa är; Ransomhub, Play, Blacksuit, Akira och 8base. 8base som kallar sig själva för penetrationstestare sågs först under 2022 och är en ransomwaregrupp som både krypterar data och lägger upp på sin webbsida för att pressa sina offer på pengar. 8base använder sig även av skam, genom att säga att de endast attackerar företag som försummar säkerheten och inte lägger tillräcklig kraft på att hålla sina anställdas och företagets data skyddad. 8base har under 2024 setts lägga upp flest offer inom industrisektorn, med stort fokus på mindre företag (1–200 anställda). Det finns fortfarande inte mycket information om gruppen i sig, men deras metoder är väl dokumenterade. Utöver sin egen mjukvara, som liknar den mjukvara RansomHouse använder för att kryptera data, har gruppen även setts använda sig av en kombination av Phobos och Smokeloader.

> “8base har under 2024 setts lägga upp flest offer inom industrisektorn, med stort fokus på mindre företag (1–200 anställda).

Enbart sett till mängden aktivitet bör dessa vara några för svenska företag att hålla koll på. Vår sammanställning över vilka hotaktörer svenska organisationer inom industrisektorn bör ha lite extra koll på innehåller vissa av dessa men även några andra aktörer:

Blacksuit

Gruppen har enligt läckta uppgifter i forum och andra kontakter nyligen synts i angrepp

mot svenska aktörer inom industrisektorn även om det varken bekräftats av offer eller förövare. Vår bedömning är att det är troligt att kan komma att fortsätta inrikta sig mot svenska företag.

Lynx

Nyuppkommen grupp som började lägga upp offer på sin webbsida i juli där mängden offer har ökat stadigt sen dess. Gruppen har uttalat sig att de endast är ute efter ekonomisk vinning utan att göra onödig skada mot företag. De säger sig ha en strikt policy mot att attackera viktiga sektorer så som sjukhus, non-profitorganisationer och myndigheter. Lynx har senast synts attackera företag inom industrisektorn i Sverige och vår bedömning är att detta är något som kan komma att fortsätta.

Cicada3301

En till nyuppkommen RaaS-grupp som lade upp sitt första offer i juni 2024 och som har ett flertal offer inom industrisektorn. Större delen av offren är baserade i USA, men med ett antal i Europa. Vi ser att Cicada3301 skulle kunna se industriföretag i Sverige som nya potentiella offer. Gruppen rekryterar aktivt affiliates på ett känt hackerforum (RAMP), och sägs använda liknande BlackCat/ALPHVs crypter.

Play

Gruppen har setts utföra attacker och kryptera miljöer och data hos många svenska företag under 2024. Stora företag som DGC (nu Iver - driftleverantör till Visma recruit), och under senaste tiden InfraCom, är exempel på företag som Play listat som offer. Bara under 2024 har minst fem svenska företag blivit upplagda på Plays webbsida som offer.

Vilka är de vanligaste angreppsmetoderna att skydda sig mot?

Det finns givetvis mängder av olika metoder som hotaktörer använder för att genomföra cyberangrepp. Nedan listar vi de metoder vi ser som extra viktiga att skydda sig mot i dagsläget.

Initial access

Phishing (allmänt formulerade bluffmejl) och spearphishing (bluffmejl med innehåll skräddarsytt efter mottagaren) fortsätter att vara det vanligaste sättet för hotaktörer att få tillgång till ett offers nätverk. Hotaktörerna går i takt med att teknik och säkerhetsåtgärder utvecklas mer mot spearphishing för att få sina offers uppgifter vilket kan vara administratörer för system, högt uppsatta chefer, men även i vissa fall vanliga medarbetare. Eftersom hotaktörerna fortsätter att utveckla bluffmejlen och metoderna de använder för att lura sina offer krävs utbildning av personal och verktyg, som till exempel spamfilter, för att minska risken att uppgifter läcks och att hotaktörer tar sig in obehörigt. Det kan också kräva kontinuerlig monitorering av nyckelpersoners användaruppgifter och om de figurerat i någon läcka eller om de omnämns i vissa hackerforum.

FOTO: WARREN WONG

Flertal hotaktörer utnyttjar även offentligt exponerade VPN-lösningar som inte använder sig av MFA för inloggning. Här används både bruteforce (metod där man med särskilda mjukvarors hjälp testar samtliga möjliga lösenord för att hitta rätt) för att hitta inloggningsuppgifter i VPN-lösningen, läckta uppgifter online samt phishing för att få användaruppgifter med syfte att till slut ta sig in i offrets nätverk.

Många av de senaste läckorna börjar genom att uppgifter till en underleverantör till företaget blir överkomna av hotaktörer, antingen genom att leverantören har fått intrång eller genom läckta uppgifter. Inloggningsuppgifter och data till olika företag kan finnas i leverantörens miljö och kan leda till att uppgifterna sedan utnyttjas för att ta sig in i kundens miljö.

Det händer också att nya Zero days (tidigare okända sårbarheter) framkommer, vilket man kan anta alltid kommer att ske förr eller senare. Dessa situationer är mycket ovanligare än de tidigare nämnda metoderna för initial access. Något som hjälper mot sådana sårbarheter är att offentligt exponerade tillgångar är nätverkssegmenterade ifrån den vanliga arbetsmiljön i ett så kallat DMZ. Det är också viktigt att utgå från best practices när det gäller patchning av mjukvara så man undviker större delen av möjliga svagheter som kan utnyttjas för att få åtkomst till ett offers miljö.

SEO Poisoning och Malicious Ads

SEO Poisoning är en metod för att få illegitima kopior av hemsidor att synas högt

upp i listan av sökresultat när ett offer använder en sökmotor för att exempelvis söka efter en mjukvara. Beroende på om offret tillåter reklam i sina sökresultat, kan även kopior dyka upp där. När offret går till fejkhemsidan ser den ut precis som den vanliga hemsidan, med undantag för sidans URL. Den mjukvara som laddas ner kan även ha alla de önskade funktionerna, men innehålla en trojan som även kör skadlig kod för att exempelvis installera infostealers, eller koppla upp till en hotaktörs Command & Control server. Denna metod fortsätter att vara ett stort hot, speciellt för företag som inte har ordentliga säkerhetsåtgärder på plats. Ett sätt att undvika dessa händelser är att som regel blockera applikationer som inte är explicit tillåtna att köras. Exempel på mjukvaror som ofta kopierats med skadlig kod är gratis mjukvara så som 7Zip, Winrar och Advanced IP Scanner.

EDR Killers

Användandet av så kallade "EDR Killers" (Endpoint Detection & Response, säkerhetsprogramvaror) har ökat hos hotaktörer. EDR Killers gör som namnet antyder, de stänger av antivirus/EDR produkter för att ge hotaktören fri kontroll över servrar och datorer utan att behöva tänka på att säkerhetsåtgärder kan blockera deras framfart. EDR Killers består av legitima drivrutiner som har släppts med inbakade svagheter som kan utnyttjas för att få en behörighetsnivå som tillåter avstängning av säkerhetsfunktioner. I vissa fall sker det lite mer sofistikerat genom att ta bort hooks i ofta använda WinApi:er som används i skadlig kod. Det finns ett projekt, kallat loldrivers, som listar funna drivrutiner med svagheter som kan utnyttjas i dessa fall. Flera drivrutiner fortsätter att hittas, men att se över loldrivers lista och blockera är en start. Större vikt bör även ligga på behörighetsgränsning och kontroller för att blockera installation av drivrutiner då administratörsbehörigheter krävs.

FOTO: YUYA UZU

False claims

Något som är värt att lyfta i diskussioner kring hotaktörer och angreppsmetoder är det som går under benämningen false claims – när någon påstår sig gjort något de inte har gjort. Många ransomwaregrupper använder sig av false claims där företag kan läggas upp som offer på flera olika webbsidor, vilket gör att det blir svårt att bekräfta vilken specifik grupp som ligger bakom attacken.

False claims kan även uppstå när en affiliate är illojal mot en ransomwaregrupp på grund av att de tar för mycket betalt, eller att deras tjänster (exempelvis utpressningstadiet) inte håller den standard som affiliategruppen kräver. I vissa fall leder detta till att en affiliate tar sin stulna information och låta en annan grupp sälja informationen på sin hemsida.

Vissa grupper har också sett potentialen i att sälja vidare sin åtkomst till ett offers nätverk, speciellt de grupper som endast stjäl data från offer och undviker att kryptera material. Dessa grupper har möjligheten att ta in mer pengar genom att först stjäla informationen, och sedan sälja vidare sin access till ett nätverk för att tjäna pengar. Detta kan leda till att den första gruppen lägger upp ett företags data till försäljning och att sedan en annan grupp lägger upp samma företags data för att bli såld.

Slutligen finns det de som använder sig av false claims för att göra sig kända. Grupper kan exempelvis lägga ut fejkdata på sin utpressningssida och säga att datan kommer från ett större företag eller myndighet för att få flera ögon på sig och göra sig kända inom hackercommunityn. Ett problem för namngivna organisationer i sådana fall är att resurser kan behöva läggas på att hantera ett angrepp som faktiskt aldrig ägt rum!

Hur ska man hantera risker i leveranskedjan?

Att incidenter sker i leveranskedjan är inget nytt men det är något som uppmärksammats i media de senaste åren allt sedan angreppen mot SolarWinds och Kaseya, som drabbade bland annat butikskedjan Coop. Mer nyliga exempel rör TietoEvry och CrowdStrike som fick omfattande påverkan både i Sverige och globalt. Att dessa incidenter sker, och högst sannolikt bara kommer att bli mer frekventa, är en naturlig effekt av den digitaliseringsgrad samhället har tillsammans med den ökade specialiseringen

hos företag där man fokuserar på kärnverksamhet och lägger ut annat på underleverantörer.

Handlar det om misstag eller rena fel så som vid incidenten hos CrowdStrike är frekvensen av dessa i leveranskedjan en naturlig effekt av ovan nämnda specialisering och sammankopplingen mellan olika företag via leverantörer. Handlar det om antagonistiska angrepp så som vid incidenten hos TietoEvry är det en enkel logik att det är lättare att angripa en underleverantör och på så sätt få åtkomst till delar av, eller alla, dennes kunder i stället för att angripa var och en separat. Här är det även värt att poängtera att hantering av leveranskedjan, även avgränsat till det som rör informationssäkerhet, inte enbart handlar om mjukvara eller tjänster utan även hårdvara och komponenter. Situationen under pandemin lärde oss att flera samverkande naturhändelser kan bidra till en stor chipbrist – med naturlig koppling till IT och informationssäkerhet. Mer nutida, och dödliga, exempel på vikten av säkerhet även gällande hårdvara kunde vi bevittna gällande Israels attack med hjälp av personsökare. Attacken ger flera viktiga lärdomar kopplat till leveranskedjesäkerhet, bakgrundskontroller och kontroller av leveranser.

Ur riskhanteringssynvinkel är något av det farligaste när man har ett monoberoende, det vill säga en leverantör där det inte finns ett rimligt alternativ. Tyvärr ser vi fler och fler av dessa som en effekt av att stora företag tenderar att köpa upp eller konkurrera ut mindre företag. När det inte råder monoberoende är den vanligaste rekommendationen för de allra mest kritiska leveranserna att prata om redundanta leverantörer och att ha alternativ om något skulle uppstå – eller att bygga bort beroendet helt genom att ha flera alternativ som normalfallet. Som komplement till detta, eller som huvudlösning när monoberoende råder, kan man arbeta med monitorering, kravställning och säkerhetsåtgärder inom ramen för sin leverantörshantering. Det finns flera ramverk att ta hjälp av i ett sådant arbete, exempelvis SOC2 som är ett ramverk för rapportering av säkerhetsnivån hos leverantörer.

> “Ur riskhanteringssynvinkel är något av det farligaste när man har ett monoberoende, det vill säga en leverantör där det inte finns ett rimligt alternativ.

Även standarder som ISO 27001 och NIST CSF innehåller delar kopplat till att strukturera upp leverantörshanteringen. Även om ramverk och standarder är en god hjälp är de inte nödvändigtvis en magisk lösning utan det handlar också om att kunna verifiera en säkerhetsnivå. Men hur gör man då detta på ett effektivt sätt men så att det även lägger grunden för en god leverantörssäkerhet?

I september 2024 genomförde Israel en sofistikerad attack mot Hizbollah i Libanon, där tusentals handhållna personsökare och walkie-talkies riggades med sprängmedel. Den 17 september exploderade dessa enheter, vilket enligt öppna media resulterade i minst ett tiotal dödsfall och tusentals skadade. Det finns dock obekräftade uppgifter visar att dödsfallen var betydligt fler än så.

Personsökarna som användes i attacken tillverkades av det taiwanesiska företaget Gold Apollo, medan distributionen hanterades av den ungerska licenstagaren BAC Consulting KFT – båda företagen har efter explosionerna avfärdat ansvar för tillverkningen. I samband med attacken har det framkommit att walkie-talkies, troligtvis tillverkade av Icom, också exploderade. Även Icom har avfärdat ansvar, då de slutade tillverka dessa radios för nästan ett decennium sedan. Denna komplexa struktur med leverantörer och underleverantörer visar hur svårt det kan vara att spåra ansvar och säkerställa produkternas integritet genom leveranskedjan.

Incidenten illustrerar tydligt hur bristande insyn i leveranskedjan kan leda till allvarliga säkerhetsrisker. Attacken understryker behovet för organisationer att ha tillräcklig kontroll över sina leverantörer, eftersom manipulation kan ske utan att slutkunden är medveten om det. Det blir alltmer uppenbart att även enklare teknologier, som personsökare, kan bli livsfarliga när de utnyttjas i konflikter, vilket ställer krav på ökad säkerhet och riskhantering.

Peter Bayer

Jonas Stewén

Experterna: Så ska du tänka kring dina leverantörer och leverantörskedja

Peter är Ciso på Stockholmsregionens Försäkring AB och Jonas är VD på Secify. Båda har en lång bakgrund inom säkerhetsbranschen och mångårig erfarenhet från leverantörshantering.

Hur brukar kravställning mot leverantörer se ut?

Peter: Kunder har historiskt sett varit bristfälliga när det kommer till kravställning inom informationssäkerhet, men alltid haft höga förväntningar på det som levererats. Det är en fråga om beställarkompetens och i avsaknad av sådan har leverantörerna av IT-system, webbtjänster och programvara inte behövt uppfylla dessa krav juridiskt sett. Om man ”undviker” att implementera grundläggande säkerhetsfunktioner, så kortas ju leveranstiden… Även om det är sant, så är det väldigt kortsiktigt tänkt. De flesta leverantörer har som avsikt att finnas länge på en marknad och då måste man inkludera alla delar. Många gånger är det dessutom leverantören som har en bättre beställarkompetens och det är därför viktigt att avsaknad av säkerhetskrav framförs till beställaren i ett tidigt skede.

Vilka frågor bör man ställa?

Peter: Internt hos beställaren behöver man fundera på vilka säkerhetskrav som måste uppfyllas och sen tydligt formulera dessa i text. När det gäller uppföljning av säkerhetskraven behöver man ställa sig frågor såsom; Räcker det att vi som beställare endast skickar ut en checklista med säkerhetsfrågor till leverantören för att styrka huruvida de efterlever lagar och specifika krav för systemet/tjänsten som erbjuds? Hur bör denna checklista vara utformad? Kommer leverantören att förstå frågorna och förstår vi som beställare de inkomna svaren? Vilka ”triggers” ska läggas in i frågebatteriet som innebär att svaren måste följas upp med ett samtal, stickprov eller ett platsbesök? Hur mycket ansvar kan läggas på leverantören att säkerställa regelefterlevnad även för sina eventuella underleverantörer, etc.?

Hur gör man då med kravställning och uppföljning?

Jonas: Först vill jag säga att jag tycker att det är positivt att denna diskussion landat i olika krav vilket innebär att det är något som måste göras och inte bara bra att ha. Det börjas tas med säkerhetskrav i olika inköpsprocesser på ett sätt som inte varit vanligt tidigare i vissa sektorer. Här ser jag också att mindre organisationer/leverantörer riskerar att tappa affärer då större kunder helt enkelt bara skickar vidare kraven rakt av. Detta tror jag inte är en vettig väg att gå eftersom det blir väldigt mycket krav som kanske inte är relevanta för just den tjänsten eller produkten som köps av kunden.

Sedan behöver det ju också följas upp och det är nästa steg i processen. Hur många leverantörer har man resurser att följa upp kontinuerligt? Och vad ska man fokusera på. Idag ser jag att de flesta uppföljningar är mer utifrån ett stickprov som en check i boxen aktivitet. Har ni ett ISO27001, check. Har ni en kontinuitetsplan, check. Har ni övat den senaste månaden, check. Här tycker jag också att den större frågan är vad detta ger. Det kostar också att genomföra detta kontinuerligt så det är viktigt att vi kan argumentera för dess nytta.

> “En vanlig missuppfattning är att alla produkter från en leverantör som har ett ISO 27000-certifikat automatiskt går att lita på.

Hur kan de här stickproven se ut?

Peter: Med stickprov menas att leverantören behöver ”bevisa” att kravet uppföljs på något sätt. Det kan till exempel göras genom att skicka in delar av de interna säkerhetsregelverken i form av policyer och riktlinjer, men det skulle i de mer tekniska frågorna även kunna efterfrågas konfigurationsfiler för specifika tredjepartsprodukter som används i systemlösningen alternativt loggdata från en driftsatt systemlösning, etcetera.

En vanlig missuppfattning är att alla produkter från en leverantör som har ett ISO 27000-certifikat automatiskt går att lita på. En del leverantörer använder felaktigt detta som det enda argumentet på assurans. Även om en certifiering av organisationens ledningssystem för informationssäkerhet är mycket positiv och ger goda förutsättningar för en bra leverans, så finns det ofta en historik att ta hänsyn till. De produkter som utvecklats och använts av kunder under flera år blir helt plötsligt inte säkra bara för att leverantören valt att certifiera sig.

Vad är problemen med att jobba med de här stickproven?

Jonas: Jag har själv jobbat med olika former av audits och evalueringar och en sak jag tycker att vi missar här är vad en uppföljning egentligen ger eller bör ge. Check i boxen kring exempelvis olika processer, ledningssystem, policys kan ge en bild av hur mogen organisationen är och vilken tilltro vi kan tillskriva organisationen. Detta brukar man benämna assurans och kan vara ett bra sätt att se hur strukturerad och medveten en organisation är. Jag skulle säga att de allra flesta uppföljningar utgår ifrån detta.

Det man missar i detta är hur de hanterar just er information eller hur de funktionellt skyddar densamma. Om man vill dra det lite längre så kan man säga att det innebär att leverantören skulle behöva bevisa att man verkligen skyddar informationen/systemet eller vad det nu är som innefattas över tid. Exempelvis, hur vet jag att min information inte blandas med era andra kunders, hur vet jag att om ni skulle bli drabbade av ett intrång från en annan av era kunder att det inte får negativa konsekvenser för mig.

Är det rimligt att man ber en leverantör att kontinuerligt visa hur de skyddar informationen?

Jonas: Jag skulle säga att det definitivt är rimligt och att det också kommer bli nödvändigt om inte alla som hanterar leverantörer ska öka sin budget kraftigt för all uppföljning. Värt att säga är att det också finns olika möjligheter att följa sina leverantörers digitala fotavtryck över tid och på så viss ligga steget före innan något händer. Vi har exempelvis sett olika fall där en leverantör kan ha många olika certifieringar och check i boxar där vi upptäckt ganska graverande brister i säkerhetsfunktionerna. Sådan information är viktig att förmedla till leverantörer så de kan bli bättre.

Men tillbaka till grundproblemet, kan vi skapa en säker leveranskedja enbart genom att titta på assuransen. Nej, är mitt svar. Vi måste börja kräva av leverantören att de kan bevisa hur de skyddar informationen över tid. Exempelvis kan ett rimligt krav vara att en gång i månaden bevisa hur man funktionellt skyddar denna. Kommer det att gå på en dag att lösa problemen? Såklart inte, men genom att börja att kräva funktionella bevis tillsammans med assurans så kommer vi att kunna skapa en betydligt mer robust försörjningskedja.

FOTO: TAYLOR VICK

DEL 4

Ökad kravställning mot industrisektorn

Europeiska kommissionen är på framfart och mängden reglering på informationssäkerhetsområdet som föreslås (och i många fall går igenom till gällande förordningar och direktiv) har de senaste åren ökat explosionsartat. Till detta kommer nationella lagar och sådana som härstammar från marknader utanför EU.

För organisationer är det i dagsläget en reell utmaning att hålla sig uppdaterad om alla eventuella regleringar som träffar dem. I den bästa av världar skulle man kanske också ha så pass god uppfattning att man visste vad som fanns kommande på horisonten så att man kan börja styra om sitt säkerhetsarbete i god tid. Vi har nedan gått igenom ett urval av de kommande regleringar som kommer att träffa den svenska industrisektorn.

FOTO: GETTY IMAGES

NIS2 & CER

EU har med erfarenheter från det första NIS-direktivet valt att anta direktivet om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen – det så kallade NIS2-direktivet.

Eftersom NIS2 kan ses som en uppdatering av det ursprungliga NIS-direktivet kommer många av kraven som ställs i NIS-direktivet att kvarstå – så som systematiskt och riskbaserat informationssäkerhetsarbete och incidentrapportering. Några av de ytterligare kraven som behöver uppfyllas enligt NIS2 är:

- Strategier för riskanalys
- Hantering av incidenter
- Planer för verksamhetskontinuitet
- Säkerhet vid anskaffning, utveckling och förvaltning
- Strategier och rutiner för att bedöma effektiviteten i riskhanteringsåtgärder
- Utbildning i informationssäkerhet
- Åtkomstkontroll och hantering av tillgångar
- Lösningar för multifaktorsautentisering
- Strategier och rutiner för kryptografi
- Säkerhet i leveranskedjan

I NIS2 har omfattningen av de sektorer som berörs av direktivet ökat avsevärt och viss förändring har även skett inom de tidigare existerande sektorerna. Bland annat gäller direktivet bara för de som betecknas som medelstora företag eller större. Gränsvärdena för vad som anses vara medelstora företag är 50 personer och en årsomsättning eller balansomslutning på 10 miljoner euro. Det finns dock flera undantag från storlekskraven som gör att organisationer som inte uppnår dessa ändå kan omfattas. Värt att notera är att det finns flera breda kategorier för de som tillhandahåller olika typer av digital infrastruktur så som bland annat leverantörer av molntjänster, datacentraltjänster och betrodda tjänster samt en lika bred kategori av olika former av tillverkningsindustri så som kemikalier, medicintekniska produkter och elektronikprodukter.

På grund av att NIS2 innehåller krav på säkerhet i leveranskedjan, i förslaget till ny svensk lag avgränsat till första linjens leverantörer, är det dock inte bara de verksamheter som omfattas som kommer att påverkas utan även deras leverantörer och underleverantörer. På så sätt kommer NIS2 att få betydligt vidare påverkan än enbart på de sektorer som explicit anges i direktivet.

CER-direktivet (Critical Entities Resilience) kompletterar NIS2 genom att fokusera på den fysiska säkerheten och kontinuiteten för kritiska infrastrukturer. Syftet är ett allriskperspektiv till kritiska entiteters motståndskraft mot störningar på deras funktionalitet där NIS2 hanterar informationssäkerhetsaspekterna och CER övriga risker. Kraven i CER-direktivet rör riskbedömningar och införandet av säkerhetsåtgärder för att motverka, begränsa och hantera incidenter. Det ställs även krav på ett antal säkerhetsåtgärder kopplat till fysiskt skydd och personalsäkerhet.

De entiteter som träffas av regleringarna är i stort överlappande. Av denna anledning har Sverige valt att utreda de båda direktiven samtidigt. Status för tillfället är att utredningen har presenterat sitt slutbetänkande med trolig tidsram för beslut av ny föreslagen cybersäkerhetslag och lag om motståndskraft hos kritiska verksamhetsutövare under första halvan av 2025 och att de sedan ska börja gälla 1 augusti samma år.

Cyber resilience act

Cyber Resilience Act (CRA) är en kommande förordning som syftar till att förbättra säkerheten för alla digitala produkter och tjänster som säljs på den europeiska marknaden. Den ställer krav på att produkter med digitala komponenter, som IoT-enheter, mjukvara och uppkopplade system, ska ha inbyggda säkerhetsfunktioner redan från designfasen. Tillverkare måste också erbjuda säkerhetsuppdateringar och rapportera incidenter och sårbarheter under produktens livslängd. Produkterna som uppfyller kraven ska inneha en märkning för att få säljas och information ska ges till slutanvändaren gällande produktens säkerhet så att denne kan ta ett informerat beslut vid köp. Förordningen kommer att vara ett viktigt steg i att stärka EU:s cybersäkerhet och skydda konsumenter och företag från cyberhot. CRA antogs slutligen den 10 oktober med publicering några veckor senare träder i kraft 20 dagar senare. De flesta kraven har en övergångsperiod på 3 år medan vissa krav börjar gälla tidigare.

För industrisektorn innebär detta:

1 Nya produktkrav

Alla uppkopplade produkter och system som industrin tillverkar eller använder måste uppfylla EU:s krav på cybersäkerhet. Produkterna måste designas med inbyggd säkerhet för att förhindra och skydda mot cyberattacker.

2 Säkerhetsuppdateringar

Företag måste tillhandahålla säkerhetsuppdateringar under produkternas hela livslängd, vilket kan innebära ökade kostnader och resurser för att hålla produkter säkra även efter försäljning.

3 Leverantörsansvar

Industriföretag måste säkerställa att alla tredjepartsleverantörer, som tillhandahåller komponenter eller tjänster, också uppfyller de nya cybersäkerhetskraven, vilket kan kräva tätare granskning och uppdaterade avtal.

4 Risk för böter

Om industriföretag inte följer reglerna riskerar de böter på upp till 15 miljoner euro eller 2,5 % av deras globala årsomsättning, vilket gör det avgörande att följa lagens krav noggrant.

FOTO: GETTY IMAGES

Data Act

Dataakten är en EU-förordning som antogs i december 2023 och ska börja tillämpas från 12 september 2025. Förordningen syftar till att skapa en rättvis datamarknad, där uppkopplade produkter och tjänster som genererar stora mängder data kan användas och delas för att stimulera innovation och ekonomisk tillväxt. Data som genereras av industriella IoT-enheter, såsom maskiner och produktionssystem, får central betydelse. Syftet med akten är att göra denna data mer tillgänglig och skapa tydliga regler för hur den delas och används.
För industrisektorn innebär akten framför allt:

1 Ökad tillgång till data från uppkopplade produkter: Industrisektorn, som använder ett stort antal uppkopplade maskiner och IoT-enheter, kommer nu att kunna utnyttja de data som genereras av dessa system i större utsträckning. Dataakten ger företag som använder dessa produkter rätt att få tillgång till och vidareutnyttja den data de skapar, till exempel för att optimera underhåll, förbättra produktionseffektiviteten eller utveckla nya tjänster. Detta skapar stora möjligheter för innovation och effektivisering, särskilt inom tillverkningsindustrin, där maskinernas prestanda och effektivitet kan förbättras med hjälp av dataanalys.

2 Datadelning mellan företag: Dataakten tvingar företag att dela vissa data med andra företag under rättvisa och icke-diskriminerande villkor. Detta minskar dominansen av större aktörer

som tidigare kunnat kontrollera marknaden genom att begränsa tillgången till värdefulla industridata. Små och medelstora företag kan nu delta mer jämlikt på marknaden genom att få tillgång till samma data som stora företag, vilket stärker deras konkurrenskraft.

3 Skydd mot oskäliga avtalsvillkor

Mindre industriföretag skyddas bättre mot oskäliga avtalsvillkor genom Dataakten. Större företag kommer inte längre att kunna påtvinga små aktörer ofördelaktiga avtal kring datadelning eller dataanvändning. Detta skapar en mer transparent marknad där alla aktörer har tydliga rättigheter och skyldigheter gällande datahantering.

4 Interoperabilitet och molntjänster

För att undvika leverantörslåsning och för att säkerställa att data enkelt kan flyttas mellan olika system och tjänsteleverantörer, inför Dataakten strikta krav på interoperabilitet mellan molntjänster. Industriföretag kan därmed byta leverantörer utan risk för dataförlust eller kostsamma systemomläggningar. Detta ger företag större frihet att välja de tjänster som bäst passar deras behov utan att begränsas av tekniska hinder.

Trots goda intentioner för Dataakten med sig några potentiella risker att begrunda:

1 Ökad attackyta och sårbarheter

Den ökade mängden delade data och de fler aktörer som nu får tillgång till denna innebär att attackytan för cyberhot utvidgas då det finns fler ytor för att komma åt den. Industriföretag, som ofta är beroende av IoT-system och uppkopplad produktion, riskerar att bli måltavlor för cyberattacker. Angripare kan utnyttja svagheter i uppkopplade system för att störa produktionen eller stjäla värdefull information, vilket ställer högre krav på säkerhetsåtgärder.

2 Leverantörskedjans säkerhet

Krav på datadelning mellan olika aktörer kan öka risken för leveranskedjeangrepp, där en angripare utnyttjar svagheter i en leverantör för att få tillgång till data längre upp i kedjan. Som företag behöver man därför stärka samarbetet med sina leverantörer för att säkerställa att alla led har tillräckligt robusta säkerhetssystem.

CSA

Cybersecurity Act (CSA) trädde i kraft den 27 juni 2019 och syftar förutom inrättandet av ENISA och etablerandet av en del av EU:s cybersäkerhetsstrategi till att skapa en säkerhetsram för certifiering av IT-produkter, tjänster och processer inom hela EU. Genom denna förordning vill EU säkerställa hög cybersäkerhet och förhindra fragmentering av säkerhetsstandarder på den digitala inre marknaden. Under 2024 har lagstiftningen uppdaterats för att skärpa efterlevnadskraven, särskilt för produkter med hög säkerhetsrisk. Full implementering och krav på efterlevnad förväntas vara på plats senast 2027. Trots att certifiering enligt CSA generellt är frivillig är det flera av de övriga kommande EU-regleringarna som innehåller eller ger möjligheter att påtvinga certifiering enligt CSA så som NIS2 och CRA.

Vad CSA och de regleringar som pekar mot användning av CSA innebär för den svenska industrisektorn:

1 Strängare säkerhetskrav

Svenska industriföretag måste nu se till att alla digitala och uppkopplade produkter är certifierade enligt de nya EU-standarderna. Detta påverkar främst företag inom industriell automation, maskintillverkning och IoT-sektorer, som måste inbygga cybersäkerhet redan i designfasen.

2 Certifieringskrav

För att kunna sälja produkter inom EU måste svenska företag genomgå certifiering på olika säkerhetsnivåer (bas, betydande eller hög). Detta kan kräva omarbetning av befintliga produkter och implementering av nya säkerhetsrutiner.

Ändringar av lagar

Nätkoder för cybersäkerhet (Riktlinje för sektorsspecifika regler för cybersäkerhetsaspekter av gränsöverskridande elflöden)

EU-kommissionen har antagit en ny delegerad EU-förordning som behandlar cybersäkerhetsaspekter av gränsöverskridande elflöden inom EU:s energisektor. Denna nätkod är ett tillägg till den tidigare förordningen (EU) 2019/943 om den inre elmarknaden och syftar till att förbättra cybersäkerheten i elsektorn, med specifikt fokus på gränsöverskridande elflöden.

Syftet med den nya förordningen är att stärka cybersäkerheten för kritisk energi-infrastruktur, vilket innebär nya regler och krav på elbolag och andra aktörer involverade i elöverföring, distribution och marknadsoperationer. Nätföreskriften innehåller bland annat:

- **Minimikrav för cybersäkerhet:**
  Både grundläggande och avancerade säkerhetskontroller jämfört med internationella standarder.
- **Riskhantering:**
  En gränsöverskridande process för identifiering och hantering av cybersäkerhetsrisker.
- **Informationsdelning och krisberedskap:**
  Regler för hur information om hot ska delas snabbt och effektivt mellan aktörer för att säkerställa samordnade insatser.
- **Cybersäkerhetsövningar:**
  Regelbundna övningar för att stärka sektorns förmåga att hantera cyberangrepp.
- **Klassificering av entiteter:**
  Identifiering av aktörer med stor eller kritisk påverkan på gränsöverskridande elflöden.

Stort tack för ditt intresse av vår rapport!

Vår förhoppning är att du har fått med dig viktiga insikter och idéer, som du kan omsätta i konkreta åtgärder i ditt företag – med syfte att öka ditt företags motståndskraft och skydda er information.

Vi på Secify arbetar holistiskt inom informationssäkerhet, vilket innebär att vi alltid tittar på hur allt hänger samman. Informationssäkerhetsstandarder, dataskyddsfrågor, IT-säkerhetsutmaningar och underrättelsebehov är alla länkade tillsammans.

För att arbetet inte ska kännas alltför betungande arbetar vi alltid efter vår filosofi, ”No nonsense security”. Den föddes ur vår övertygelse om att säkerhetsarbete som aldrig blir ”klart” kan skapa en känsla av hopplöshet. Vi vill förenkla, effektivisera och hjälpa våra kunder att fokusera på det absolut viktigaste genom att avgränsa sina projekt.

Vi tror dessutom på kraften i mänskliga relationer. Vi vill lära känna våra kunder och skapa starka team som har kul och mår bra tillsammans.

Kontakta oss om du har kommentarer, frågor, eller tillägg på det du nyss läst i rapporten?

Du når oss via kontaktformuläret på https://www.secify.com eller på 020-66 99 00!