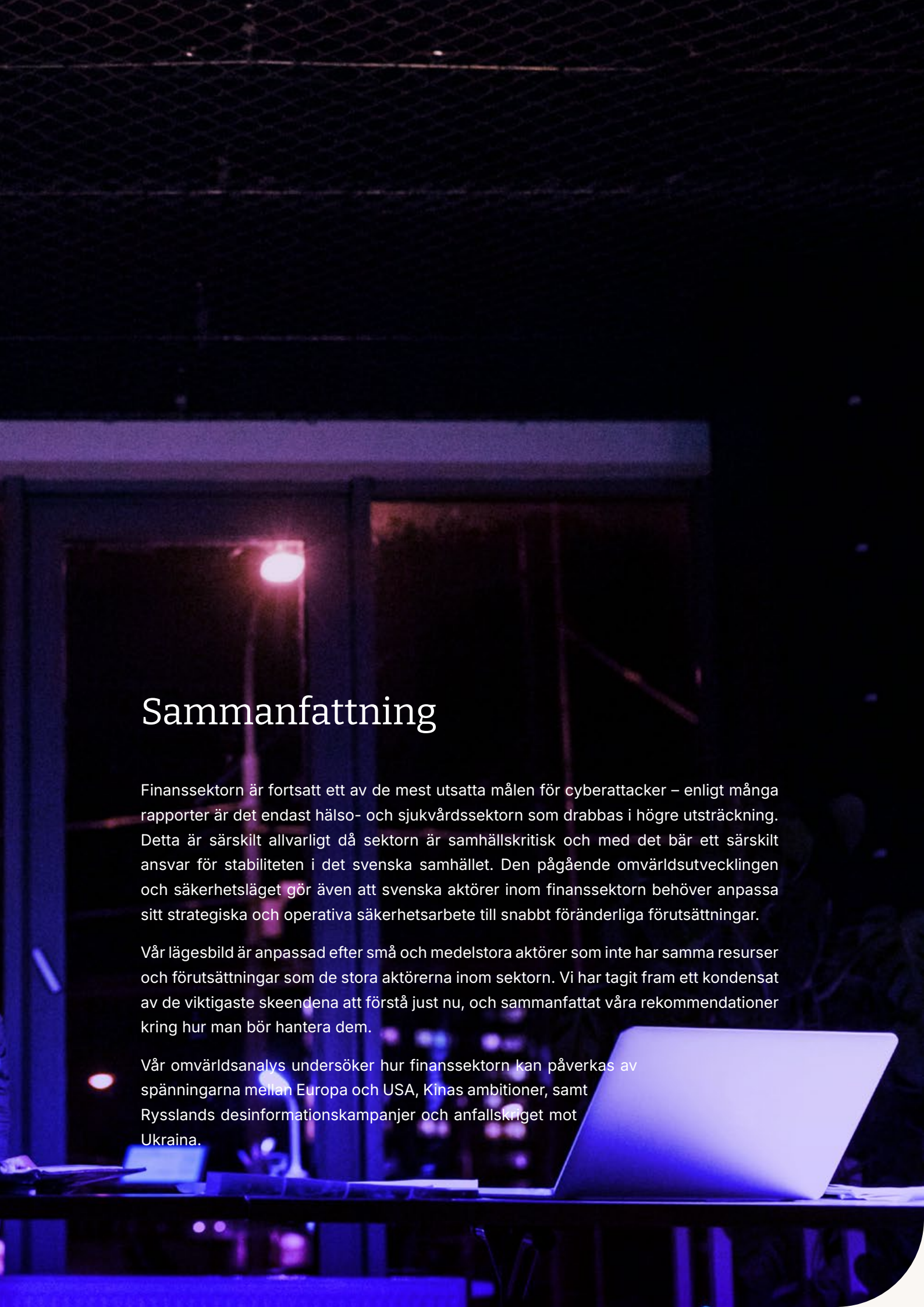
Secify

Rapport

Stannar sektorn, stannar samhället

- Lägesbild finanssektorn

Geopolitiska spänningar omformar förutsättningarna för finanssektorn. Vår lägesbild ger en samlad bild över risker, krav och möjliga vägval framåt.



Sammanfattning

Finanssektorn är fortsatt ett av de mest utsatta målen för cyberattacker – enligt många rapporter är det endast hälso- och sjukvårdssektorn som drabbas i högre utsträckning. Detta är särskilt allvarligt då sektorn är samhällskritisk och med det bär ett särskilt ansvar för stabiliteten i det svenska samhället. Den pågående omvärldsutvecklingen och säkerhetsläget gör även att svenska aktörer inom finanssektorn behöver anpassa sitt strategiska och operativa säkerhetsarbete till snabbt föränderliga förutsättningar.

Vår lägesbild är anpassad efter små och medelstora aktörer som inte har samma resurser och förutsättningar som de stora aktörerna inom sektorn. Vi har tagit fram ett kondensat av de viktigaste skeendena att förstå just nu, och sammanfattat våra rekommendationer kring hur man bör hantera dem.

Vår omvärldsanalys undersöker hur finanssektorn kan påverkas av spänningarna mellan Europa och USA, Kinas ambitioner, samt Rysslands desinformationskampanjer och anfallskriget mot Ukraina.

För finansaktörer med beroenden i omvärlden är det viktigt att:

- Anpassa det strategiska säkerhetsarbetet så att man skapar sig möjligheten att fånga upp och anpassa utefter snabbt förändrade förutsättningar. Man rekommenderas att ta sig tiden att modellera scenarios och bevaka indikatorer (skeenden som skulle kunna innebära att ett visst scenario kommer inträffa) för att kunna agera snabbare.
- Analysera och bedöm leverantörskedjan. Den nuvarande utvecklingen kommer sannolikt leda till fler europeiska leverantörer av nya produkter och tjänster inom IT och säkerhet, vilket kan vara positivt. Ett skifte till sådana kan bidra till ökad kontroll, minskad komplexitet kring dataskydd, förenkla problematiken kring tredjelandsöverföringar av personuppgifter och efterlevnad av informationssäkerhetslagstiftning, samt ge en stärkt robusthet i en alltmer osäker omvärld.
- Granska befintliga underleverantörer - särskilt de som hanterar kritisk information eller tjänster, såväl initialt som kontinuerligt för att upptäcka potentiella säkerhetsrisker så som dataläckor, ägarförhållanden eller överförd hotbild. Identifiera om er verksamhet är beroende av leverantörer utanför EU, särskilt USA. Bedöm konsekvenserna av om EU–U.S. Data Privacy Framework (DPF) skulle ogiltigförklaras. Förbered alternativa lösningar och stärk de legala och tekniska skyddsåtgärderna i era leverantörsavtal.
- Dimensionera säkerhetsarbetet efter att en sänkning av tempot i kriget i Ukraina kan leda till ökade mängder förstörelseangrepp och DDoS.
- Anpassa krisplaner och kommunikationsinsatser till att vid större negativa händelser kunna bemöta desinformationskampanjer

Vår analys visar att DDoS-attacker är den vanligaste attacktypen mot sektorn, ofta utförda av grupper som RipperSec, NoName05716 och RooTDos. Samtidigt fortsätter ransomwarehotet att växa, och infostealers används för att samla in inloggningsuppgifter som kan ligga till grund för framtida attacker.

Vår granskning visar på en variation mellan olika aktörer på marknaden:

Flera större och äldre banker påträffar vi med tusentals läckta uppgifter bara det senaste året, även om vi funnit en av dem med en ansenligt mindre mängd. Vi har samtidigt hos

mindre och nyare banker funnit en mindre mängd läckta uppgifter, runt 500 hos ett exempel.

Infostealerloggar är digitala spår från skadeprogram som samlat in användarnamn, lösenord och annan känslig information från infekterade enheter. I de fall vi har undersökt finner vi mellan 5 och 90 loggar som skulle kunna användas i en attack hos de större aktörerna, och motsvarande mellan 5-10 loggar hos mindre aktörer.

För gruppen försäkringsbolag ser vi att mängden läckta uppgifter är mellan 800 till 2000 under det senaste året och mängden infostealerloggar är mellan 20 och 50. Hos finanstjänster finns det en större mängd läckta uppgifter per anställd, vilket kan tyda på brister i utbildning och hygien gällande phishing, samt användning av arbetsmail i privata situationer.

Mot denna bakgrund är det avgörande att:

- Håll er uppdaterade om möjliga nya sårbarheter och metoder som säljs för att utnyttja dessa sårbarheter. På så sätt har ni möjligheten att tidigt upptäckta möjliga attacker.
- Threat-Led Penetration Testing (TLPT) är ett ramverk för säkerhetstestning och är ett kraftfullt verktyg för att testa både teknik och processer, samt personalens förmåga att upptäcka, hantera och återhämta sig från verkliga attacker. Utför den här typen av tester utifrån verkliga hotscenarios för att upptäcka sårbarheter, och efterleva ex. DORA.
- Lägg tid och kraft på att utbilda personalen i cybersäkerhetsfrågor för att höja den generella medvetenheten. Arbeta också enligt principen om att begränsa behörigheter, om olyckan skulle ske och en nyckelperson skulle bli lurad på sina uppgifter.

Vår bevakning av de just nu viktigaste regelverken visar på nya regelverk, förändringar i befintliga, samt vissa fall av osäkerhet. Finanssektorn har länge varit en regeltyngd bransch och med en EU-kommission som alltmer ser ekonomin som ett säkerhetspolitiskt verktyg, ser kraven inte ut att minska. Ny EU-lagstiftning, växande geopolitiska hot, regulatoriska strukturer för dataflöden och teknologiska hinder spär ytterligare på komplexiteten.

Med våra rekommendationer vill vi försöka ta ner kraven på jorden och förenkla genom att arbeta systematiskt och strukturerat:

Regelverket DORA innebär att styrelse och ledningsgrupp bär ett formellt ansvar för operativ motståndskraft. Se därför till att högsta ledningen har tillräcklig insikt i cyber-

säkerhetsrisker, tillsynskrav och verksamhetens förmåga att hantera störningar genom löpande utbildningar.

Etablera en integrerad strategi för informationssäkerhet och compliance för att säkerställa att efterlevnad av olika regelverk inte behandlas som separata initiativ. Bygg en samordnad och tvärfunktionell struktur där informationssäkerhet, juridik, IT och affärsstrategi samverkar.

AI utvecklas för fullt även inom finanssektorn, och för att tillse ett ansvarsfullt och säkert användande bör riskbedömningar genomföras, särskilt inom kreditprövning, automatiserat beslutsfattande och kundservice. Undvik att införa generativ AI i känsliga processer innan dokumentation, insyn och övervakning är fullt på plats i enlighet med kommande EU-krav.

Ett ledningssystem där man systematiskt samlar in information, dimensionerar sitt säkerhetsarbete och strategier, samt planerar, utför, kontrollerar och förbättrar i en kontinuerlig snurra, är ett sätt att omhänderta problematiken. Syftet är att ha just ett övergripande arbetssätt för att systematiskt samla in den information vi behöver och sedan anpassa det arbete vi har.

Analys och produktion:


Martin Palmqvist
HUVUDANSVARIG


Petra Jonsson
ANSVARIG FÖR ANALYS


Joakim Bernhardt
ANSVARIG FÖR THREAT INTELLIGENCE


Henrik Pettersson
FORM/DESIGN


Aida Rokni
ANSVARIG FÖR JURIDIK/REGELVERK

Kontakt

Växel: 020-66 99 00

Martin Palmqvist
martin.palmqvist@secify.com

Jonas Stewén
jonas.stewen@secify.com

Secify
www.secify.com

DEL 1

Omvärlden under början av 2025

Vi som arbetar inom säkerhetsbranschen har länge pratat i termer av att hoten ökar, omvärlden förändras och händelseutvecklingen går fortare. Till slut kan man fråga sig hur mycket mer läget kan förändras, utvecklas fortare eller om vi har nått taket. Inledningen av 2025 visade oss med all tydlighet att det fortfarande finns väldigt mycket som kan förändras väldigt fort.

Dynamiken mellan USA, EU och Ryssland har förändrats i grunden för en överskådlig framtid på ett sätt som kan få stor inverkan på säkerhetsläget i Europa. Exempelvis har handelspolitiska åtgärder och tullar haft en väldigt direkt inverkan på finanssektorn, men de har även påverkat indirekt genom det säkerhetspolitiska läget och förutsättningar för de säkerhetstjänster man använder sig av. Nästan 60% av organisationerna uppger i en ny undersökning av World Economic Forum, Global Cybersecurity Outlook 2025, att geopolitiska spänningar har påverkat deras cybersäkerhetsstrategi. Den geopolitiska oron har även påverkat synen på risker, där en av tre VD:ar anger cyberspionage och förlust

PRESIDENT DONALD J. TRUMP OCH MIKE PENCE | **FOTO: HISTORY IN HD**

av känslig information så som intellektuell egendom, som deras största oro. Vid en fokusgrupp under World Economic Forum's årliga möte om cybersäkerhet 2024 uttryckte dessutom 41% av deltagarna att ökad insyn i tredjepartsberoenden är den högsta prioriteten för att förbättra cybersäkerheten i leveranskedjan.

I vår föregående rapport poängterade vi att även om läget förefaller stabilt så kan det svänga snabbt och att det därför är viktigt att följa omvärldsutvecklingen. När svängningen är ett faktum och vi går mot delvis oprövad mark såväl säkerhetsmässigt som geopolitiskt, behöver vi bli ännu bättre på att upprätthålla en relevant lägesuppfattning för att kunna reagera snabbare. Nästa steg är att jobba med analyser och prediktioner för att kunna vara proaktiva snarare än reaktiva.

Det som kommer driva säkerhetsläget på makronivå i närtid är scenarion kopplade till relationen mellan USA, Ryssland och EU samt hur Kina kommer hantera dessa. Vi kommer i rapporten ge våra tankar och analyser kring detta kombinerat med det aktuella läget på hotaktörs- och sårbarhetssidan. Vi kommer även beskriva vad aktuella regelverk kräver och framför allt vad man som enskild aktör skulle kunna göra för att förbättra sin säkerhet.

Ett systematiskt underrättelsearbete innebär att strukturerat, efter ett informationsbehov, **samla in, bearbeta, analysera** och **presentera informationsläget** för att kunna ta beslut och stärka sitt säkerhetsarbete. Ett verktyg är indikatorer, det vill säga någonting som tyder på att ett visst händelseförlopp håller på att ske. I ett sådant arbete tar man fram **ett antal troliga scenarion.**

Till varje scenario kopplas ett antal indikatorer som skulle kunna peka på att de är på väg att ske, och det är dessa indikatorer som sedan bevakas. För varje scenario analyseras troliga konsekvenser och vilka säkerhetsåtgärder som ska användas för att bemöta dessa. Genom att göra detta har man kortat startsträckan och kan gå från observation av en indikator till att styra sitt säkerhetsarbete mot åtgärderna för det scenariot.

Ett yrvaket Europa försöker samlas

På den europeiska scenen pågår just nu en historisk utveckling där bland annat Tyskland, Frankrike och Storbritannien kan sägas vara centrala för utvecklingen. Storbritannien lämnade officiellt EU 2020 efter att det röstats igenom med knapp marginal ("Brexit"). Fem år senare anser nu endast 30% att det var rätt att lämna EU, vilket är den lägsta siffran sedan mätningen startade efter Brexit, jämfört med 55% som säger att det var fel. Med opinionsskiftet i åtanke vad gäller Brexit är det relevant att följa det som nu sker i London. Relationen med EU hade kunnat förbli relativt stilla i flera år till, men det är tydligt att den senaste tidens turbulens mellan Washington och EU har skakat om de planerna och flyttar Storbritannien och Europa allt närmare varandra.

Premiärminister Keir Starmer engagerar sig nu aktivt i Europas

försvars- och säkerhetsfrågor genom olika försvarsinitiativ och diplomatiska insatser. Det finns nu experter som tror att detta bara kan vara början på en mer långsiktig omorientering där Storbritannien närmar sig rollen som en geopolitisk stormakt. Även inrikespolitiskt i landet märks det att den rätta åsikten är att hålla en EU-vänlig linje.

Detta skapar möjligheter för fler former av europeiskt samarbete, inte bara inom försvar, utan även inom andra områden där ett mer flexibelt samspel mellan nationer och EU kan vara fördelaktigt. Valet i Tyskland kan ha stor betydelse i sammanhanget. Friedrich Merz, som efter en nagelbitare och en andra omröstning i det tyska parlamentet till slut blir ny tysk förbundskansler, har länge varit positiv till ett starkare tyskt försvar och, liksom Frankrikes Emmanuel Macron, förespråkat det som i EU-kretsar kallas ”variabel geometri” i samarbetet (flexibelt samarbete i olika konstellationer – inte alla i allt).

Ett samtalsämne som hörts runt många fikabord under slutet av första kvartalet är det om att ”Europa borde ha sett det komma”. Diskussionen handlar om hur man i årtionden har förlitat sig på framför allt amerikanskt stöd, och när det viker står man en aning handfallna. Man menar att Europa skulle ha varit mer förutseende och agerat långsiktigt på säkerhetsområdet redan efter annekteringen av Krim 2015 och under Donald Trumps första mandatperiod.

Allt fler forskare och experter uttalar sig nu om att Ryssland har varit mer eller mindre tydliga med att man kommer agera om man känner sig hotad – där Georgien och Ukraina varit tydliga röda linjer när det kommer till inträde i västliga allianser.

Historiskt finns det personer som varnat för det händelseförlopp vi nu ser. Under 90-talet gläntade dåvarande presidenten Bill Clinton alltmer på dörren till den västliga värmen för Ukrainas räkning. Från samma period finns det ett öppet brev från bland annat tidigare senatorer och utrikespolitiska experter som trycker på risken av att det kan ses som en aggression av Ryssland – att Nato helt enkelt kommer för nära.

Med facit i hand menar många alltså att varningssignalerna funnits där länge – vilket skulle innebära att frågan inte handlar om huruvida de har funnits, utan varför de inte tagits på allvar.

EU PARLAMENTET, STRASBOURG, FRANKRIKE | FOTO: LUKAS S

Merz har redan gått ut och tydligt deklarerat var han står i frågan om Europas försvar, enighet med Ukraina, och hur han ser på relationen med amerikanerna. I ett tal konstaterade han att USA framstår som likgiltigt inför Europas öde och ifrågasatte därmed Natos framtid och krävde att Europa snabbt stärker sitt eget försvar - en tonartsändring som hade varit otänkbar mellan de bägge allierade för bara ett par månader sedan.

Tyskland har varit frånvarande på den internationella scenen under en längre tid, och den förra regeringen blev alltmer försvagad. Tyska väljare har frustrerat krävt ett akut fokus på ekonomi och migration, och europeiska allierade har lika frustrerat efterfrågat stöd med åtgärder rörande säkerhet och försvar. Från Merz sida framstår det kristallklart att en av Tysklands högsta prioriteringar är att åter engagera sig internationellt. Verkligheten förblir dock en utmaning i detta – Tyskland dras med utdaterad infrastruktur, en släpande digitaliseringstakt, en omodern industrisektor, samt fortsatta utmaningar i inrikes frågor såsom migration och integration. När man nu slutligen tog ett historiskt steg genom att tillfälligt häva sin grundlagsfästa ”skuldbroms” för att möjliggöra en massiv satsning på försvaret, återstår det att se hur det tyska folket reagerar på prioriteringarna. Den tillträdande reger-

TYSKA RHEINMETALL KF51 PANTHER - SKA ENLIGT RHEINMETALL UTGÖRA GRUNDEN FÖR DEN NYA STRIDSVAGNEN I ITALIEN | **FOTO & KÄLLA: RHEINMETALL AG**

ingen har genom beslutet öppnat för ett flerårigt försvarsfokuserat investeringspaket på upp till 600 miljarder euro – ett markant paradigmskifte i tysk politik.

Tillsammans med Tyskland och Storbritannien kliver nu Frankrike fram för att ta på sig ledartröjan. President Emmanuel Macron gör sitt yttersta för att placera Frankrike i centrum för Europas upprustningsinitiativ. Frankrike har länge förespråkat ”strategisk autonomi” för EU, såväl militärt som ekonomiskt, med syfte att minska beroendet till bland annat USA.

Främst har detta berört försvarsindustrin där man drivit på ett ökat europeiskt samarbete inom försvarsmateriel, men Frankrike är även i allra högsta grad drivande för att skapa förutsättningar för en europeisk fintech-sektor. Enligt France Fintech samlade franska fintech-företag 2024 in totalt 1,3 miljarder euro, en ökning med nästan 30% jämfört med föregående år, vilket placerar Frankrike på andra plats i Europa efter Storbritannien. För banker och investerare skapar detta möjligheter att finansiera nya projekt, särskilt via EU:s försvarsfonder (EDF).

Utöver detta har Frankrike också drivit på frågor om privat-offentligt partnerskap för att finansiera gränsöverskridande projekt inom exempelvis cybersäkerhet och AI. Vi ser nu att vissa fonder och pensionsbolag har börjat revidera sina investeringspolicys och klassificerar försvar som en ”social nytta” inom ESG (Environmental, Social, Governance) – ett skifte som öppnar för nya kapitalinflöden.

Ekonomin som ett verktyg inom säkerhetspolitiken

EU-kommissionen presenterade den 19 mars en omfattande plan, ”Readiness 2030”, för att samla in 800 miljarder euro genom lån och skuldfinansiering för att stärka medlemsländernas möjligheter att köpa nödvändig försvarsutrustning. Satsningen har en tydlig preferens för EU-tillverkad materiel och syftar till att minska beroendet till bland annat amerikanska leverantörer.

> “ Readiness 2030 [...] syftar till att minska beroendet till bland annat amerikanska leverantörer.

Readiness 2030 beskriver EU:s långsiktiga försvarsstrategi där Kommissionen lägger fram fem förslag. Man uppmanar medlemsstaterna att aktivera den nationella undantagsklausulen i stabilitets- och tillväxtpakten, vilket ger extra budgetutrymme för att öka försvarsutgifter samtidigt som man följer finanspolitiska regler. För att säkerställa en hållbar ekonomi kommer avvikelsen begränsas till att gälla ökning av försvarsutgifter om maximalt 1,5 % av BNP per år, under maximalt fyra år.

Utöver detta vill EU-kommissionen styra europeiska medborgares uppskattade 10 biljoner euro i privata

besparingar mot investeringar inom bland annat försvarsindustrin. En viktig del av detta arbete sker genom Europeiska Investeringsbanken (EIB) som kommer fortsätta att diskutera lättnader i sin lånepolicy, samt möjligheten att öka investeringarna i försvarssektorn.

Parallellt pågår flera finansiella projekt inom EU där man arbetar intensivt för att nå en högre europeisk ekonomisk autonomi, exempelvis utvecklas en digital euro sedan drygt ett år tillbaka. Den typen av lösning skulle kunna öka den monetära självständigheten, autonomin och den inre säkerheten i Europa.

> “Sammanfattningsvis har EU börjat se ekonomin som ett verktyg för säkerhetspolitik – inte bara ett tillväxtområde.

EU:s finansiella system är i dagsläget starkt beroende av amerikanska system för betalning, vilket har visat sig vara en sårbarhet. Inom EU arbetar man därför på alternativet Wero, inom ramen för European Payments Initiative (EPI). Initiativet är backat av 16 europeiska banker och skulle innebära en europeisk betalningslösning.

Sammanfattningsvis har EU börjat se ekonomin som ett verktyg för säkerhetspolitik – inte bara ett tillväxtområde. Det innebär att flöden av kapital, teknik och varor regleras utifrån vem som står bakom dem och vad de kan användas till. Även om denna utvecklig i stort är positiv för europeisk självständighet och resiliens för den med sig ett par säkerhetsutmaningar. Som vi alla stora satsningar så kommer många nya företag, initiativ och sammanslutningar att bildas med tillhörande leverantörer av tjänster och varor. Det kommer föra med sig en underliggande komplexitet gällande flöden – det vill säga vart går pengarna, till vem och för vad – vem ligger bakom och hur blir det med transaktioner, uppköp och skydd av rättigheter? Många nya algoritmer kommer skapas och unika tillfällen för cyberspionage och infiltrationer, samt en högre risk för industrispionage. På det stora hela så påverkar det möjlighet att få tag på kompetens eftersom marknaden måste slåss om samma kompetens inom alla områden. Resultatet blir ett ökat behov av att skydda tillgångar – digitala som fysiska.

På andra sidan Atlanten är det ingen fråga om huruvida man redan ser ekonomin som en faktor i säkerhetspolitiken. Handelsutmaningarna växer i takt med tullarna, och amerikanska börser reagerar starkt på den förda politiken och de snabba svängningarna från Vita Huset. Om President Trump fortsätter införa höga tullar och annan typ av ekonomisk straffpolitik fortsätter, kommer recessionen som presidenten redan förvarnat för - vilket han medger kan innebära en tuff period för amerikanska företag och hushåll. Det finns bedömare som ser den förda politiken som en kraftfull återlan-

sering av Reaganomics – en omstridd politik under 80-talet med fokus på minskade offentliga utgifter, en stram penningpolitik, minskad statlig reglering och skattesänkningar. Kritiker har pekat på ökande statsskuld och att tillväxten inte "sipprade ner" till låginkomsttagare som utlovat – något som gör att man ifrågasätter samma bana igen.

De exakta skälen bakom beslutet att höja tullarna vet nog främst en person i världen om, men en diskussion som hörs i debatten är den om dollarns övervärdering. För ungefär ett halvår sedan publicerade Stephen Miran, en av president Trumps ekonomiska rådgivare, ett omfattande dokument som fokuserade på varför dollarns värde har blivit skevt och vad man bör göra åt det. Miran argumenterar för att dollarns historiskt dominerande roll i det internationella finanssystemet har ökat efterfrågan på valutan, vilket har drivit upp valutans värde. Den här övervärderingen menar man har lett till bland annat minskad exportkonkurrenskraft, handelsunderskott, och en urholkning av den amerikanska tillverkningsindustrin.

Mot bakgrund av detta presenterar Miran några, aningens okonventionella, förslag för att försvaga dollarn utan att förlora den globala dominansen. Bland annat nämner man ett "Mar-a-Lago"-avtal med landets handelspartners för att gemensamt agera mot dollarns värde, en "användaravgift" på utländskt innehav av amerikanska statsobligationer, samt även att pressa andra regeringar att förlänga löptiden på sina amerikanska obligationsinnehav. Dessutom kan nämnas att man blandar detta med säkerhetsgarantier, där man tänker sig att administrationen ska erbjuda amerikanska säkerhetsgarantier i gengäld mot hjälp att trycka ner dollarn.

Rekommendationer

- Anpassa ert strategiska- och säkerhetsarbete så att ni har möjlighet att fånga upp och anpassa utefter snabbt förändrade förutsättningar. Ta tiden att modellera scenarios och bevaka indikatorer.
- Utvecklingen kommer sannolikt leda till fler europeiska leverantörer av bland annat IT och säkerhetsprodukter och -tjänster. Ett byte till sådana leverantörer kan komma att inverka positivt på exempelvis rådighet och redundans - särskilt i en osäker framtid - förenkla problematiken kring tredjelandsöverföringar av personuppgifter och efterlevnad av informationssäkerhetslagstiftning.
- Se över behovet att skydda era digitala och fysiska tillgångar, såväl i er verksamhet som i era leveranskedjor. Säkerställ att ni har den kompetens som krävs för att hantera er säkerhetssituation, särskilt kopplat till upphandling, granskning och uppföljning av förändringar i er leveranskedja.

Kina som handelspartner och hotaktör

Med tanke på att Kina är världens näst största, eller enligt vissa analytiker världens största, ekonomi är det märkligt att vi inte pratar mer om stormakten i öst. Självfallet har det att göra med geografiskt och kulturellt avstånd, men det finns även en faktor i att landet är relativt stängt. Att det dessutom finns en parlamentarisk ”kuliss” uppsatt, men med all egentlig makt i toppskiktet i kommunistpartiet, gör det svårt att följa utvecklingen i landet på djupet.

Av det skälet är de få tillfällen som faktiskt finns kritiska att följa, exempelvis årets viktiga politiska sammankomst känd som de två sessionerna, eller ”lianghui”. Kinas högsta lagstiftande församling NPC (National People’s Congress) och Kinas högsta politiska rådgivande organ CPPCC (Chinese People’s Political Consultative Conference) samlades i Peking och i år var ekonomin, tech och det amerikanska handelskriget högt upp på agendan. Den största rubriken var regeringens löfte om att BNP-tillväxten under 2025 kommer att ligga kvar på samma nivå av runt 5%, som under 2024.

Kinas nuvarande tillväxt innebär för EU strategiska utmaningar ur ett säkerhetsperspektiv. Kina styrs på ett helt annat sätt än EU med ett auktoritärt system, och dessutom hänger utmaningen ihop med hur Kina använder handel, investeringar och teknik för att stärka sin makt och i vissa fall försöka bli den ledande globala makten.

Kina är alltjämt en viktig handelspartner för EU men samtidigt ökar landet nu kraftigt sina försvarsutgifter, med världens redan näst största militärbudget. Man intensifierar även vissa aktiviteter för att pressa Taiwan, samtidigt som landet undviker sådant som kan ses som direkt konfrontation. En eskalering av den konflikten skulle få djupgående ekonomiska och strategiska konsekvenser för inte bara Europa, utan för den globala stabiliteten i stort, bland annat när det kommer till Taiwans roll

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

som producent av kritiska produkter som till exempel mikrochip. Vi kan samtidigt se att Kina gör sig alltmer relevant i andra sammanhang, såsom i utvecklingen i Afrika, men även i konflikten i Kashmir, och för att fylla utrymmet USA lämnar efter sig när de förändrar sitt internationella engagemang.

De senaste 20–30 åren har det målats upp en bild av ett Kina som har nått sin topp. Det har spridits bilder av städer som har tömts på folk, fastighetsbolag som har gått i konkurs, medborgares bolån som ligger låsta i hopplösa räntelägen samt en generell tankebild om att auktoritära regimer inte kan skapa tillväxt i all evighet. Kombinerat med att populationen faller är det många som menar att Kina är en bubbla som, om inte redan har spruckit, definitivt är på god väg.

Samtidigt finns en annan tolkning som vissa gör. En nidbild är att Kina är duktiga på att kopiera, exempelvis bilar och telefoner – de skulle aldrig själva kunna bygga komponenterna till dem. Dagsbilden är att landet nu ligger i teknologisk framkant på många områden, inte minst inom AI. På en tidigare kongress la generalsekreteraren för kommunistpartiet, Xi Jinping, ut orden om den kinesiska drömmen där man mellan 2021 och 2035 skulle omvandla Kina till ett extraordinärt, modernt, socialistiskt land genom ekonomisk utveckling. Mellan 2035 till 2049 ska man fortsätta på stigen av nationell återuppståndelse för att bli vad som beskrivs som en global ledare när det kommer till nationell styrka och internationell påverkan.

Relationen mellan Kina och de två stormakterna USA och Ryssland är viktiga att bevaka noggrant. Efter en resolution från Ukraina i FN:s generalförsamling i februari röstade Ryssland emot förslaget, men något mer uppseendeväckande var att även USA röstade emot, och att Kina valde att lägga ner sin röst. Det är lätt att anta att USA och Ryssland ser vissa gemensamma intressen i att undvika en fullständig rysk kollaps. Sen ett tag tillbaka är USA:s primära säkerhetspolitiska fokus relationen till Kina, och en alltför svag rysk stat skulle kunna leda till ökat kinesiskt inflytande. Det innebär inte att man vill att Ryssland ska vinna kriget i Ukraina, utan snarare att man behöver dem som en motvikt för att gynna sina egna strategiska syften. Den diplomatiska utvecklingen sedan början av 2025 mellan USA och Ryssland kan också anses vara ett sätt för USA att separera Kina och Ryssland på ett geostrategiskt plan – ett grepp USA även försökte med under tiden för det kalla kriget.

> “ Dagsbilden är att landet nu ligger i teknologisk framkant på många områden, inte minst inom AI.

Att Kina avstod från att rösta emot den ukrainska resolutionen kan

tolkas som att landet vill värna sina ekonomiska intressen och relationer med västvärlden, inte minst den europeiska marknaden, vilket görs bäst genom att hålla en viss strategisk distans till Moskva. Samtidigt är det tydligt att Kina på kort sikt fortsatt är en helt kritisk partner för Ryssland, särskilt vad gäller energiexport och teknologi.

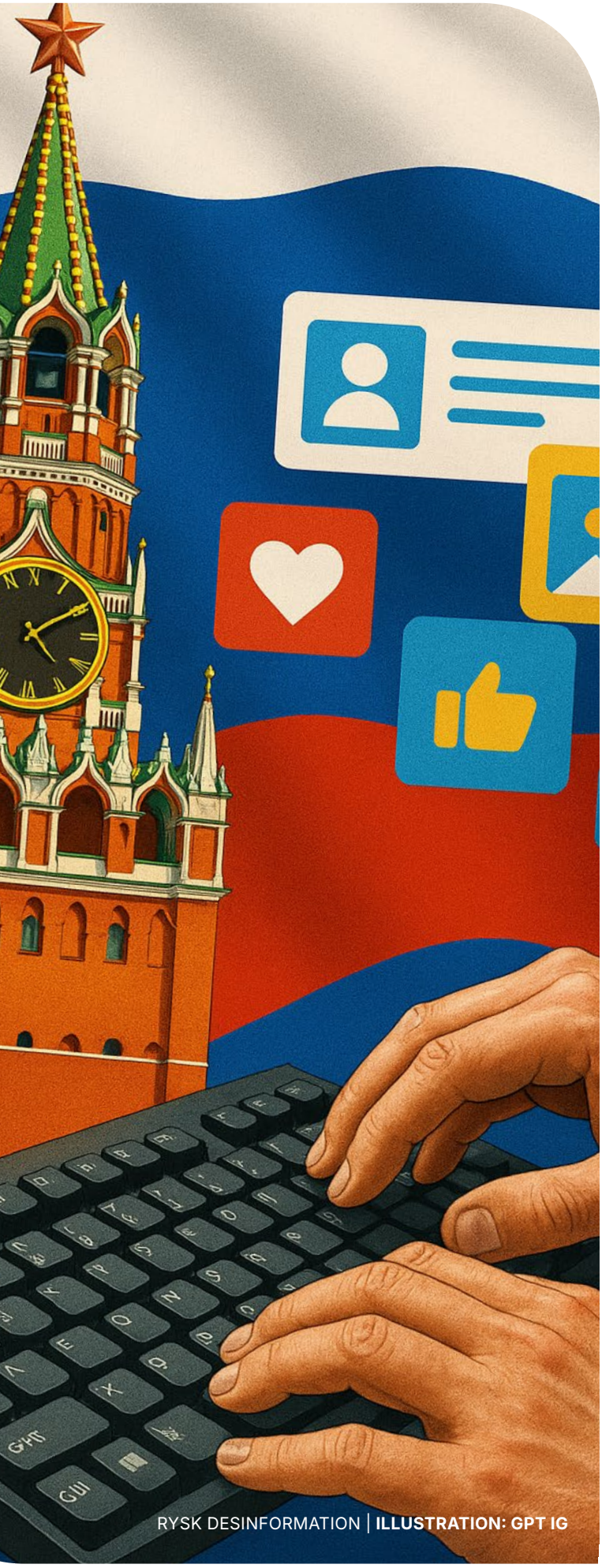
Kina organiserar sina relationer med andra stater i partnerskap snarare än västvärldens allianser, och just partnerskapet med Ryssland är sen många år relativt starkt, om än obalanserat till Rysslands nackdel. De intressen som sammanför stormakterna är många, men det kanske främsta strategiska är att motverka den västliga ordningen och anpassa den till något som låter dem dominera mer fritt i sina respektive intressesfärer.

> “Allteftersom Ryssland har blivit utsatt för allt tuffare sanktioner har därför också beroendet av Kina blivit alltmer påtagligt,

Allteftersom Ryssland har blivit utsatt för allt tuffare sanktioner har därför också beroendet av Kina blivit alltmer påtagligt, där man har tvingats att ställa om sin handel österut. Sedan kriget började har inte bara dollarn minskat i betydelse för Ryssland – utan kinesiska yuan har också ökat kraftigt, vilket märks i såväl handeln, nationella reserver, börs- och valutamarknader, samt i privat sparande. Detta har dock lett till ett ökat beroende av Kina, vilket i längden inte nödvändigtvis gynnar Ryssland, särskilt eftersom Kina behåller en hård kontroll över sin valuta och använder den till sin fördel.

Rekommendationer

- När den mest påtagliga konflikten är mellan väst och Ryssland är det viktigt att tolkningar av relationen samt handlingar dem sinsemellan även tolkas utifrån Kinas roll och att man inte ser dem som enskilda företeelser. Beakta även Pekings roll i relation till deras grannländer som ni kan ha beroenden till tjänster och produkter från.
- Utveckla metoder för att hantera beroenden till kinesiska produkter och beakta eventuella nuvarande och framtida teknologiska framsteg de kan stå för. Oavsett om vi pratar om ett svagare eller starkare Kina i framtiden, behövs metoder för att hantera det scenario vi kommer att stå inför.



RYSK DESINFORMATION | **ILLUSTRATION: GPT IG**

Ryskt hot och hybridkrigföring

Rysslands agerande har länge varit en drivande faktor för det säkerhetspolitiska läget i vårt närområde. Förutom regelrätt krigsföring har hybridkrigsföring varit ett stående inslag för att underminera och påverka länder i västvärlden. De senaste åren har vi sett allt från planer på att mörda företagsledare inom försvarsindustrin, GPS-störningar för flyg- och fartygstrafik, och sabotage av undervattenskablar till förstörande och störande cyberoperationer. Vanliga inslag har därtill varit uppköp av utländska bolag och ekonomiskt inflytande samt användande av desinformation för att påverka specifika individers eller allmänhetens uppfattning vid exempelvis val eller större samhällshändelser.

Desinformationskampanjerna kan grovt delas in i två kategorier: de som sprider information om inhemska förhållanden i syfte att missleda och framhålla en bild av ett starkt land och de som syftar till att påverka utländska förhållanden så som val eller försök till samhällsstörning vid särskilda händelser. Att destabilisera en samhällsviktig aktör inom finanssektorn är ett attraktivt mål för en motståndare och därmed får man räkna med att det finns incitament att använda desinformation för att skapa eller förstärka en negativ händelse. Vilseledning sker dock inte enbart genom desinformation utan ekonomisk påtryckning och uppköp av utländska bolag används för att kringgå sanktioner och inhämta underrättelser.

Svenska bolag med ägar-förhållanden

med direkta eller indirekta kopplingar till den ryska statsapparaten eller organiserad brottslighet har kartlagts först av Totalförsvarets forskningsinstitut 2022 och sedan av researchbolaget Acta Publica i samarbete med Försvarshögskolan. Undersökningarna visade på ett hundratal bolag med ryska kopplingar och var i många hänseenden de första i sitt slag. Huruvida dessa bolag har använts eller inte, och i så fall i vilka syften, fastslår inte utredningarna men omvärldsläget visar på en osäker situation och hur vi varken har råd att vara naiva eller underskatta bredden av potentiella säkerhetsrisker. Vi ska dock inte vara paranoida eller se allt som en säkerhetsrisk, utan det vi i stället behöver är metoder och information för att särskilja riskerna från möjligheterna så att vi kan vara resurseffektiva.

Resursmässigt har kriget i Ukraina varit förödande för den ryska militären och ekonomin där stora resurser gått förlorade eller bundits i konflikten. Att bedöma hur skadligt det varit för framför allt ekonomin har visat sig vara problematiskt på grund av avsaknaden av tillförlitliga datapunkter och integreringen av desinformation i rapporteringen. Av allt att döma förbrukas dock resurser och reserver hastigt och i en takt som inte kommer gå att upprätthålla och vissa experter spekulerar i en inte allt för avlägsen statsbankrutt om nuvarande läge kvarstår. Vi förefaller dock gå mot någon form av status quo i kriget i Ukraina under året oavsett om det nås via ett fredsavtal, brist på reella framsteg eller något däremellan. Ett sådant stille-

RYSKA STRIDSVAGNAR I BYN DMYTRIVKA, NÄRA KYIV. 2022.
| **FOTO: MYKHAILO VOLKOV**

stånd, om det skedde på Kremls villkor, skulle sannolikt vara negativt för säkerhetsläget i Europa på lång sikt då det ger Ryssland tillfälle att återhämta och återuppbygga förmågor. Det finns dock en annan potentiell negativ konsekvens av detta skeende mycket mer nära i tid.

Med färre resurser bundna i kriget i Ukraina är det troligt att en del av dessa kommer riktas mot annat håll. Ryssland har tidigare visat sig villig att hämnas på de man upplever gått emot deras intressen och det har sedan krigets utbrott kommit flera hot mot de länder och aktörer som stöttat Ukraina. Det är inte troligt att hämnd mot dessa kommer att ske genom regelrätt krig utan snarare genom hybridkrigsföring där ett troligt inslag skulle vara förstörelseangrepp från deras statsunderstödda APT-grupperingar. Förutom detta är det även troligt med händelsestyrda DDoS-angrepp likt de som utfördes i samband med Sveriges NATO-ansökan.

Framtidens krav på svensk finanssektor – Bankgirots CSO om cyberhot i förändring

Under mars månad 2025 satte sig Jonas Stewén ner med Christian Bengtsson, CSO och chef för Säkerhet på Bankgirot, för att prata om de ökandegeopolitiska riskerna, det förändrade hotlandskapet och hur Bankgirot arbetar strategiskt för att skydda Sveriges betalinfrastruktur. Samtalet gav en inblick i hur organisationen kombinerar teknisk motståndskraft med en stark säkerhetskultur, samtidigt som de rustar sig för regelverk såsom DORA och NIS2.

Bankgirots strategi för att bedöma och hantera de största geopolitiska riskerna idag

”De geopolitiska riskerna har inte bara intensifierats utan också blivit alltmer komplexa i en tid av internationella maktkamper, ekonomiska sanktioner och cyberkrigföring”, säger Christian. ”För Bankgirot, som bedriver en verksamhet som alltid måste fungera, jobbar vi ständigt med att hålla oss uppdaterade kring hotbild, risker, och vilka åtgärder vi tar för att mitigera dessa. Den senaste tiden har vi också sett att förändringarna på dessa områden kan gå väldigt fort och det är därför viktigt att arbeta med detta kontinuerligt och inte bara en gång om året”.

Bankgirot jobbar nära kollegorna i branschen och med berörda myndigheter för att hålla sig uppdaterade - det har hänt mycket på området sedan 2022, exempelvis genom etableringen av Nationellt Cybersäkerhetscenter (NCSC) och samverkan utvecklas hela tiden. Eftersom Bankgirot precis som samhället i stort hela tiden höjer ambitionerna på säkerhetsområdet, tittar man också på hur man som central aktör kan ta en större roll och i större utsträckning bidra till att

driva säkerhetsfrågorna i sektorn.

”Vi verkar enbart på den svenska marknaden, men även här så påverkas vi av geopolitiska förändringar”, förklarar Christian. ”Vi har under de senaste åren sett ett antal omvärldshändelser som gått emot vad vi i Sverige kanske naivt trodde skulle kunna hända, och vi behöver kunna förhålla oss till dessa ändringar och anpassa oss. Under ständigt föränderliga förutsättningar gäller det t.ex. alltid att fundera på vem man kan lita på.”

Christian menar att alla behöver göra egna bedömningar kring vilka hot som ens egen verksamhet är utsatt för och vilka incitament som kan finnas hos en hotaktör för att angripa verksamheten. Därefter vidtas åtgärder, både tekniska men även kring arbetssätt och motståndskraft och hur man bygger vidare på detta. Verksamheten behöver heller inte alltid vara det primära målet, utan är kanske endast en bricka i ett större spel.

Han avslutar: ”Vi tror på en öppen dialog och samarbete där vi regelbundet diskuterar aktuella risker med intressenter och myndigheter för att säkerställa att vi tillsammans är förberedda på att hantera de utmaningar vi ställs inför.”

De mest kritiska cyberrelaterade hoten mot den skandinaviska finanssektorn kräver en strategi

Som många andra aktörer i den finansiella sektorn ser Bankgirot fortsatt hot som överbelastningsattacker, skadlig kod, ransomware och leverantörskedjeattacker som de mest sannolika att ställas inför. Dessa hot utvecklas snabbt och kan få betydande påverkan såväl direkt som indirekt på många, beroende på vem som utsätts för angreppen.

”Koncentrationsrisken hos ett antal stora leverantörer ska inte underskattas – vi har sett flera exempel i samhället på hur många som kan bli påverkade av angrepp mot leverantörskedjan”, konstaterar Christian. ”Här måste vi som beställare också kräva mer av våra leverantörer, säkerhet måste prioriteras och inte bara vara något som finns i teorin.”

Han menar att flera aktörer i samhället behöver ta höjd för statsstödda hotaktörer och hybridangrepp – cyberattacker med en geopolitisk agenda som inte bara syftar till ekonomisk vinning utan också till att destabilisera samhället. Gråzons-problematiken där fysiska angrepp eller sabotage på viktiga samhällsfunktioner som kan påverkas, direkt eller indirekt, är också något som man bevakar och kontinuerligt bedömer.

Som erfaren CSO har Christian upplevt hur tekniken förändras – även på hotsidan.

”Tittar vi på evolutionen av mer klassiska hot så ser vi att alltmer sofistikerade phishing-kampanjer och identitetsbedrägerier genomförs med AI-stöd och deepfakes nu. Vi kan se exempel på även mycket säkerhetsmedvetna organisationer som drabbas, vilket visar på hur viktigt det är att bygga en stark säkerhetskultur som sitter i ryggmärgen hos alla medarbetare – man ska inte dra sig

för att rapportera när något verkar fel", betonar Christian med eftertryck." Han tillägger: "Den här säkerhetskulturen omfattar våra gemensamma attityder, beteenden och vanor kring säkerhet – både individuellt och som organisation".

Den nyligen presenterade nationella svenska cybersäkerhetsstrategin sätter tydligt fokus på att stärka Sveriges förmåga att hantera och förebygga cyberhot genom ökad samverkan mellan myndigheter, privata aktörer och andra intressenter. Strategin betonar vikten av att arbeta proaktivt tillsammans – något Christian och hans kollegor på Bankgirot välkomnar.

Kort och tydligt sammanfattar han: "Överlag är det viktigt att kunna möta hoten med en utvecklad threat intelligence (hotunderrättelse), teknisk motståndskraft och en inarbetad säkerhetskultur."

Finanssektorn är samhällsviktig och störningar för denna skulle kunna få stora konsekvenser för en nation, varför aktörer inom sektorn är särskilt utsatta. En nyligen publicerad sammanställning av Europas cybersäkerhetsbyrå ENISA visar på just detta och hur olika typer av cyberangrepp använts för att påverka sektorn. Pratar vi specifikt om Ryssland finns en historik av att inte enbart begränsa sig till cyberangrepp utan det framstår snarare som en del i en komplex väv av multipla aktioner inom ramen för hybridkrigföring. Dessa aktioner har på intet sätt begränsats till statsapparaten utan som vi exempelvis noterade vid Sveriges NATO-ansökan eller koran-bränningarna de senaste åren så är de som blivit angripna i många fall inte officiella representanter för staten Sverige. Det har i stället handlat om målval som haft gemensamt att de varit baserade i Sverige och i många fall burit upp en viktig funktion i samhället.

Rekommendationer

- Dimensionera säkerhetsarbetet efter att en sänkning av tempot i kriget i Ukraina kan leda till ökade mängder förstörelseangrepp och DDoS
- Anpassa krisplaner och kommunikationsinsatser till att vid större negativa händelser kunna bemöta desinformationskampanjer
- Granska era underleverantörer, särskilt de som hanterar kritisk information eller tjänster, såväl initialt som kontinuerligt för att upptäcka potentiella säkerhetsrisker så som dataläckor, ägarförhållanden eller överförd hotbild

DEL 2

Kända sårbarheter inom den svenska finanssektorn

Läckta uppgifter fortsätter att vara ett problem för företag, och ser vi till finanssektorn i Sverige kan vi se många tusentals läckta uppgifter där vissa företag når upp i tusentals uppgifter bara under det senaste året.

BILD: GPT IG

Dessa läckta uppgifter behöver inte leda till direkt åtkomst till ett företags miljö, utan kan även ge en hotaktör en möjlighet att förstärka sina attacker genom exempelvis spearphishing eller mer avancerad social engineering på sociala medier. Uppgifter kan i den här kontexten vara allt från mailadresser till telefonnummer och personnummer, samt mer kompletta paket för att utföra attacker som kan finnas i så kallade kombolistor, där listor läggs upp med samlingar av konton och tillhörande lösenord.

Det som är än värre än de läckta uppgifterna är att det finns möjlighet att köpa infostealerloggar för ett stort antal företag inom den svenska finanssektorn, vilka innehåller mer information som kan användas för att få åtkomst till information och system. Dessa uppgifter, särskilt infostealerloggar, kan användas för att utföra attacker mot dessa företag genom antingen direkt inloggning till tjänster som uppgifter har läckt för, eller indirekt genom utpressning då flera konton även är registrerade på mindre arbetsvänliga hemsidor.

Sammantaget kan vi kan se flera uppgifter för att logga in i tjänster hos dessa företag, som en hotaktör idag skulle kunna köpa för att utföra en attack utan större förberedelser.

De uppgifter vi har hittat har vi delat in i tre olika grupperingar inom sektorn: banker, försäkringsbolag, och finanstjänster. Inom dessa grupperingar har stora som små organisationer flertal läckta uppgifter, både i form av läckta uppgifter så som mailadresser och i form av större infostealerloggar vilket kan göra dessa företag till en större måltavla.

Phishing (nätfiske):

En metod som går ut på att angripare skickar massmeddelanden som ser ut att komma från en trovärdig part. Syftet är att få mottagaren att klicka på länkar eller lämna ut känsliga uppgifter.

Spearphishing:

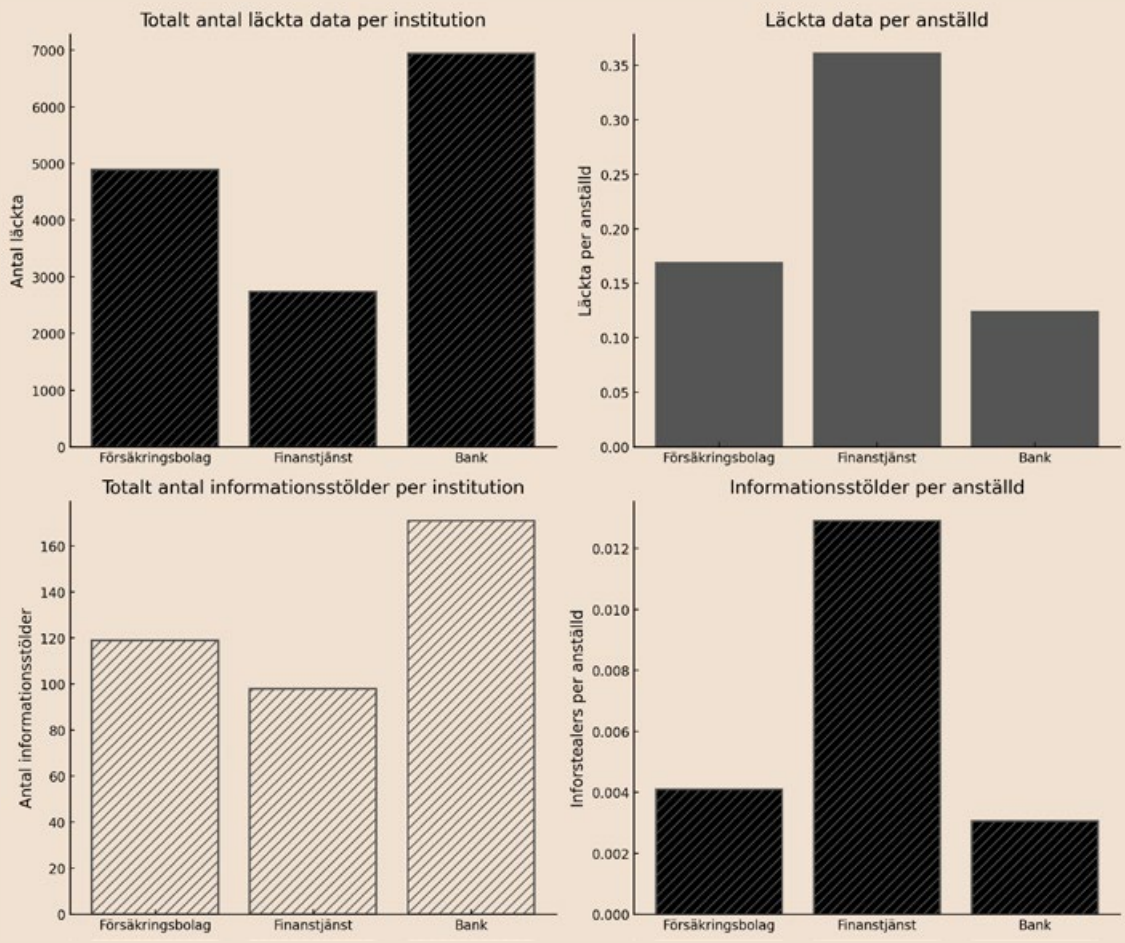
Phishing som genom informationsinhämtning är anpassat efter en specifik mottagare. När meddelandet är anpassat med en specifik mottagare i åtanke är de ofta svårare att upptäcka och har därmed högre chans att lyckas.
Social engineering: Metod att genom manipulation och vilseledning av en person, skaffa sig åtkomst till information eller tillgångar.

Infostealer:

Mjukvara som installeras på ett offers dator eller telefon, 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 och skicka ny information till en hotaktör.

Infostealerloggar:

Informationen som hotaktören får in genom infostealers sammanställs i loggar som går att köpa på olika forum på deep- och darkweb. Dessa loggar kan leda till direkt åtkomst till offers miljöer om de är externt exponerade, men loggarna kan även ge en hotaktör en bild av hur ett offers miljö ser ut inifrån.



Inom bankgruppen ser vi större och äldre banker med tusentals läckta uppgifter under det senaste året, men även en bank som sticker ut med endast 800 läckta uppgifter. Ser vi till infostealerloggar för samma banker ser vi en mindre mängd, mellan 5 och 90 loggar som skulle kunna användas i en attack. För de mindre och nyare bankerna hittar vi en mindre mängd läckta uppgifter, runt 500, och mellan 5 och 10 infostealerlog-

> “
> Skillnaderna i antalet läckta uppgifter kan såklart ha med storleken på banken, och därmed personalstyrkan, att göra..

gar. Skillnaderna i antalet läckta uppgifter kan såklart ha med storleken på banken, och därmed personalstyrkan, att göra men det kan även vara så att de nyare bankerna byggt sitt säkerhetsarbete annorlunda.

För gruppen försäkringsbolag ser vi att mängden läckta uppgifter är mellan 800 till 2000 under det senaste året och mängden infostealerloggar är mellan 20 och 50. Något som är i linje med bankerna vad gäller mängden läckta uppgifter och generell storlek på verksamheten. Hos finanstjänster finns det en större mängd läckta uppgifter per anställd, vilket kan tyda på brister i utbildning och hygien gällande phishing, samt. Vi ser mellan 200 och 500 läckta uppgifter, och 0 till 20 infostealerloggar. Jämför vi dessa mängder läckta uppgifter och infostealerloggar med mängden vi hittat inom andra sektorer, så som vård och industri, så är det en liknande omfattning både för större och mindre företag. Primärt är det storleken på organisationen som av naturliga skäl driver mängden läckta uppgifter. Men om vi ser till vilka typer av uppgifter det är, speciellt på infostealerloggar för finanssektorn, så ser vi en jämförelsevis större mängd jobbmailadresser som används för privat bruk vilket tyder på dålig hantering och utbildning gällande uppgifter tillhörande arbetet. Att separera det privata från det professionella är viktigt för att en organisation ska minska sina angreppsytor. Exempelvis ska hotaktörer inte ha möjlighet att utnyttja sårbarheter som att samma lösenord används i privat och professionellt bruk.

Rekommendationer

- Utbilda personal, speciellt gällande phishing och hur deras användning av jobbuppgifter i privat bruk kan leda till skada för företaget.
- Implementera ordentligt mailfilter, för att till större del blockera phishingförsök.
- Uppdatera tillämpliga styrdokument så att de reflekterar att skilja på konton och lösenord som används i arbetssyfte med de som används för privat bruk.
- Bevaka hur mycket användaruppgifter som läcker från er organisation och koppla det till mätvärden och indikatorer på hur väl ert arbete med säkerhetsmedvetenhet fungerar.

DEL 3

Hotbilden

Det finns ett antal hotaktörer som står ut i form av mängden offer, varav många inom finanssektorn.

De viktigaste globala hotaktörerna att hålla koll på

Cl0p

Den mest aktiva gruppen under första kvartalet av 2025, Cl0p, även känd som Clop, är en ryskspråkig ransomware-grupp som först upptäcktes i februari 2019. Gruppen är känd för sina sofistikerade cyberattacker och har riktat in sig på en mängd olika

FOTO: WARREN WONG

branscher globalt, inklusive detaljhandel, transport, utbildning, tillverkning, fordonsindustri, energi, finans, telekommunikation och hälso- och sjukvård. De är mest kända för sina attacker på hundratals företag under 2023 genom den välkända sårbarheten i MOVEit Transfer CVE-2023-34362, som tillät gruppen att stjäla data utan att offren fick kännedom om det.

Gruppen hade störst fokus på phishingkampanjer för att infektera offers miljöer i början, men har på senare tid prioriterat om till att huvudsakligen infektera sina offer genom användande av sårbarheter. Gruppen verkar för närvarande fokusera på programvara för filöverföring, så som sårbarheter i Cleos MFT (Managed File Transfer) programvara.

Akira

En ransomwaregrupp som fortsätter att samla på sig offer globalt, och har varit ett större namn bland ransomwaregrupper sen de först upptäcktes i mars 2023. Gruppen har offer inom flera olika sektorer, varav flera återfinns inom finanssektorn.

Gruppens intrång i miljöer börjar oftast genom inloggning i offers VPN-lösningar, genom antingen läckta uppgifter eller brute force. Gruppen har även setts utnyttja ett fåtal sårbarheter för att få sitt första fotfäste i offers miljöer, så som CVE-2022-40684 och CVE-2019-6693 som är sårbarheter i Fortinet FortiOS.

Play

Play, även känt som PlayCrypt är en

Ransomware:

Ett ransomware är en form av skadlig kod som krypterar filer på en dator eller i ett system och gör dem oläsbara utan en särskild dekrypteringsnyckel. Efter att ett system infekterats kräver angriparen vanligtvis en lösensumma för dekrypteringsnyckeln. Både företag och privatpersoner mål för denna typ av angrepp men när det rör sig om företag så är oftast attackerna mer riktade och sofistikerade.

Brute force:

Metod där man genom upprepade gissningar går igenom möjliga lösenord tills man finner det rätta.

False claims:

Företeelse där en grupp anger att de har utfört en attack på ett offer utan att det finns bevis på att detta har skett och/eller att även en annan grupp tar på sig ansvaret för angreppet så att det råder oklarhet kring vem som utfört aktionen.

grupp som upptäcktes i juni 2022, och är ett av de större namnen när man talar om aktiva ransomwaregrupper. Gruppen har fortsatt att lägga upp offer på sin leaksite, men har under 2025 inte haft lika många offer som tidigare. Gruppen har dock flertal offer inom finanssektorn och är en av grupperna med flest offer inom denna sektor, vilket gör att vi på Secify ser dem som ett större hot.

Gruppen använder sig av flera olika metoder för att göra intrång i sina offers miljöer. Flertal sårbarheter i publikt exponerade tjänster har exploaterats för att ta sig in i miljöer, speciellt i Fortinet produkter och Microsoft Exchange. Gruppen använder sig även av både phishing och spearphishing för att få ett fotfäste i miljöer där phishingen kan stärkas av läckta uppgifter och kartläggning av nyckelpersoner inom företag. De har setts använda sig av läckta uppgifter för att direkt kunna logga in i offers miljöer genom exempelvis Outlook-portaler eller publikt exponerade RDP-tjänster.

De viktigaste hotaktörerna att hålla koll på i Sverige

Nedan följer hotaktörer som publicerat flera offer inom finanssektorn på sina webbsidor och som vi på Secify ser som prioriterade hot för finanssektorn i Sverige.

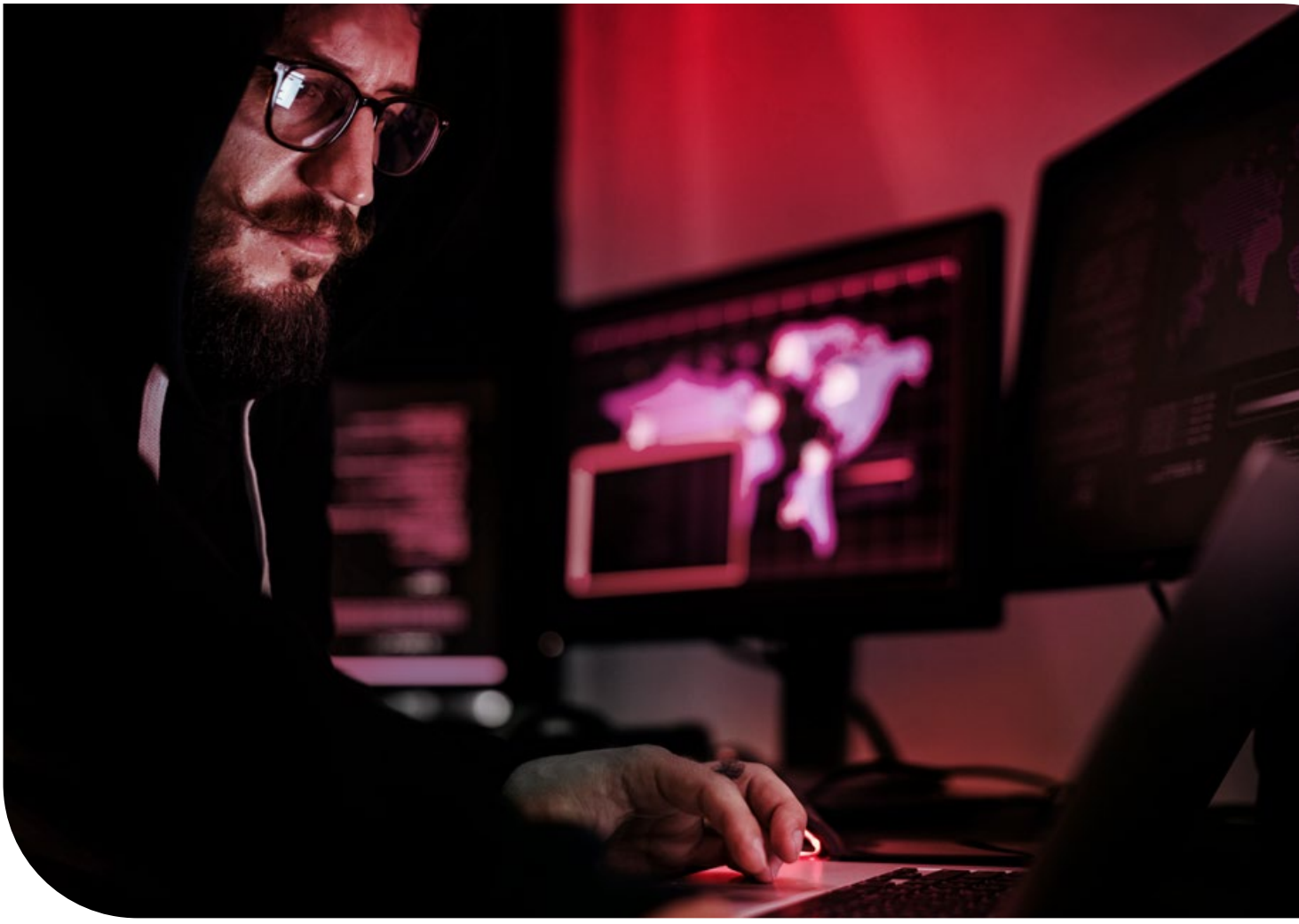
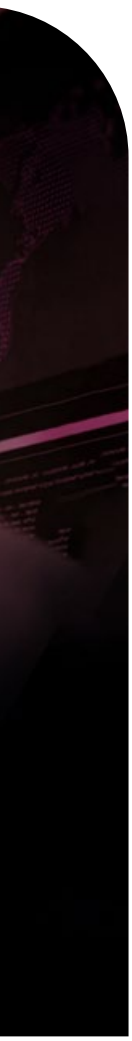


FOTO: UNSPLASH+

Akira

Gruppen har varit väldigt aktiv under en längre tid, och fortsätter att lägga upp offer inom finanssektorn. Gruppen har även lagt upp en mängd svenska företag som offer på sin webbsida, och vi ser därför Akira som ett stort hot för just finanssektorn inom Sverige.

> “Om man ser på deras tidigare offer och vilka sektorer som gruppen lagt upp flest offer inom ser vi att gruppens fokus ligger på finans, industri och fastighet.



Play

En till grupp som varit väldigt aktiv inom Sverige, och som har flera offer inom finanssektorn.

Lynx

En grupp som har exploderat i mängden offer sen deras upptäckt juni 2024, och som är en av de grupper som på senaste har lagt upp flest svenska företag som offer under 2025. Om man ser på deras tidigare offer och vilka sektorer som gruppen lagt upp flest offer inom ser vi att gruppens fokus ligger på finans, industri och fastighet. Vi på Secify ser Lynx som ett stort hot, då de verkar se ett stort intresse i svenska företag och gruppen fortsätter att öka angreppen från månad till månad.

Inte mycket är känt om hur gruppen tar sig in i offers miljöer, men det har rapporterats att flera attacker har startat via phishing.

Babuk2

En grupp även känd som Babuk-Bjorka och Babuk 2.0, är en nyupptäckt grupp som verkar imitera den tidigare stora och kända gruppen Babuk. Gruppen upptäcktes i januari 2025. Det är ännu okänt om detta är en återkomst av Babuk eller om de endast imiterar dem, då offer som läggs upp på deras webbsida skulle kunna vara så kallade false claims. Även fast gruppen har lagt upp flera offer sen deras upptäckt finns det ännu inga fastställda nya offer som har blivit attackerade av gruppen. Gruppen kan därför vara ute efter att skapa oro för tidigare angripna företag, och försöka bli kända inom hackercommunityn. Gruppen kan orsaka skada mot företags rykte och oro för kunder om företaget anges ha attackerats, utan att de egentligen har blivit attackerade.

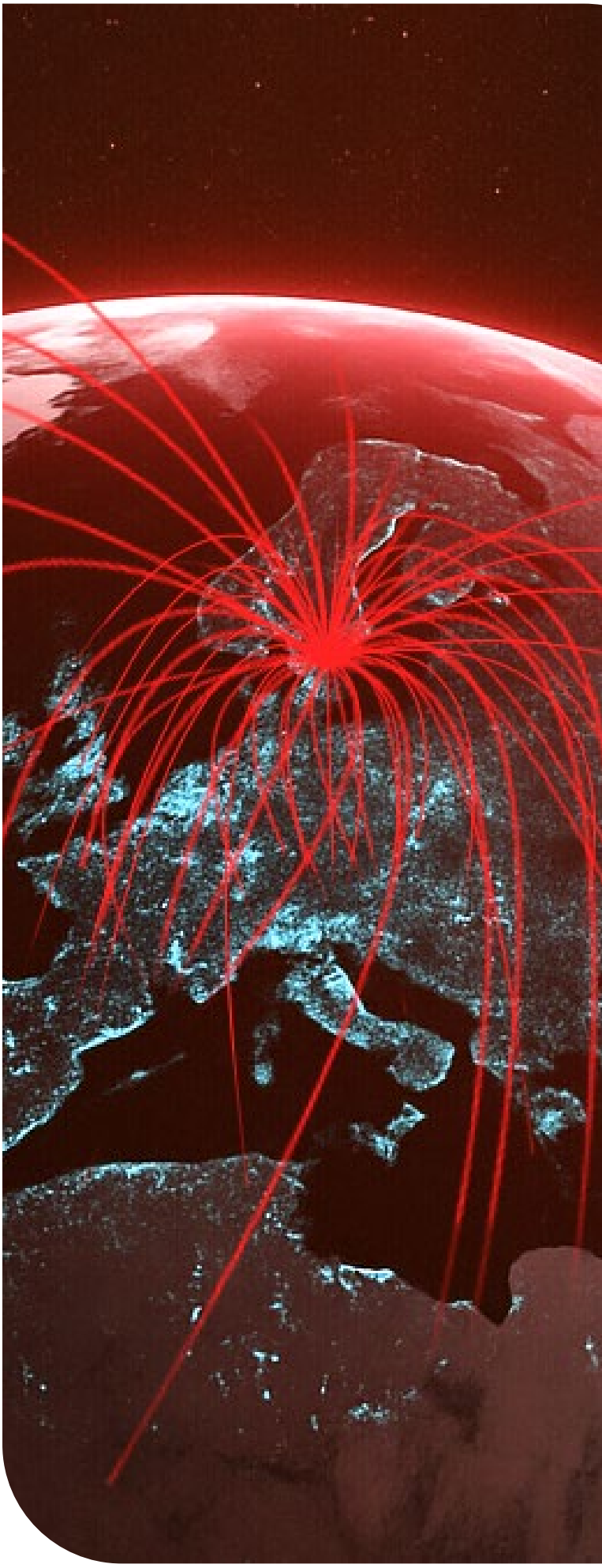
Vilka är de vanligaste angreppsmetoderna att skydda sig mot?

Ransomware

Ransomware fortsätter att vara ett problem för alla företag och antalet offer under första kvartalet 2025 är fler än motsvarande period under både 2023 och 2024. Trenden fortsätter peka mot att

mängden ransomware kommer att fortsätta öka. Den för närvarande vanligaste metoden som används av ransomwaregrupper är så kallad Double Extortion där de pressar offer på pengar genom kryptering av deras filer och miljöer, samt att de ändå publicerar informationen för folk att köpa och genom detta uppmana offer att betala.

De mer populära grupperna just nu agerar som en RaaS-tjänst (Ransomware as a Service), där gruppen förser affiliates (hotaktörer som samarbetar med eller tillhör en grupp) med allt ifrån mjukvara för kryptering till infrastruktur för att utföra phishing och servrar för kommunikation mellan hotaktören och offrets dator. Kostnaden för dessa tjänster är ofta en del av slutsumman som betalas ut av offren och ligger vanligtvis på tio till tjugo procent.



DDoS

DDos (Distributed Denial of Service) utförs till största delen av så kallade hacktivistgrupper, och är den mest frekventa typen av attack som vi ser mot finanssektorn. DDoS utförs oftast genom att en grupp sprider skadlig kod som gör att datorer och produkter blir en del av ett nätverk som sedan attackerar de måltavlor som gruppen bestämmer. Angreppen består av upprepade anropsförsök som leder till att tjänsten som angrips blir så hårt belastad att den slutar fungera.

På senaste tiden har vi sett både pro-palestinska grupper som angriper de som de upplever som

fientligt inställda och pro-ryska grupper som ofta attackerar NATO-länder. Inom just finanssektorn har vi sett grupperna RipperSec, NoName05716 och RooTDos utföra attacker på flera olika företag.

Då nätverken som används vid DDoS kan bestå av enheter från flera länder globalt är det svårt att geografiskt blockera alla IP-addresser för att undvika attacker. Att använda sig av geografisk blockering för att blockera trafik från länder som ej bör använda hemsidan kan dock ge ett starkt skydd mot större distribuerade attacker.

Phishing

Phishing är fortfarande en återkommande metod för att skapa ett fotfäste i ett offers miljö oavsett om det är genom skadlig kod som körs genom att övertyga användaren eller om medarbetare läcker sina inloggningsuppgifter genom social engineering. När en hotaktör vill köra kod för att skapa ett fotfäste i ett offers miljö går det oftast till så att ett mejl skickas till en eller flera medarbetare beroende på hotaktörens ambition och kartläggning av potentiella måltavlor. När offret tar emot mejlet är det oftast något meddelande som skapar intresse och engagemang hos användaren. Redan i mejlet kan det finnas en fil bifogad som meddelandet uppmanar användaren att öppna, eller i olika former av filarkiv eller virtuella hårddiskar som behöver extraheras. Meddelandet kan även leda till en hemsida där mjukvara laddas ner.

En trend är också att hotaktörer gått mer och mer åt angrepp utan skadlig kod där offret i stället uppmanas att ladda ner legitima mjukvaror så som RMM-verktyg (Remote Monitoring and Managing) som exempelvis AnyDesk, Atera eller TeamViewer. Dessa mjukvaror ger hotaktören direkt kontroll över datorn på samma sätt som en administratör för företaget skulle kunna använda dessa för att förse en användare med support.

> “ Fler och fler sårbarheter släpps kontinuerligt i exponerade tjänster, så som webbapplikationer, brandväggar och VPN-lösningar.

Sårbarheter i exponerade tjänster

En annan metod som återkommer är utnyttjandet av sårbarheter i externt exponerade tjänster. Fler och fler sårbarheter släpps kontinuerligt i exponerade tjänster, så som webbapplikationer, brandväggar och VPN-lösningar. Hotaktörerna använder denna metod då det kan ge direkt åtkomst till ett offers miljö, eller ge administratörsbehörigheter i tjänsten, vilket kan leda till att hotaktören kan ta sig vidare i miljön. Flera grupper söker aktivt efter möjligheter att använda

sårbarheter i tjänster, och köper aktivt kod för att utföra attacker eller använder utvecklare som själva kan skriva denna kod.

Vishing

En metod som har existerat ett bra tag, men som har haft stor framgång på senaste tiden är vishing. Vishing är precis som phishing på det sättet att hotaktören försöker övertala eller lura en användare att ge ut sina uppgifter som sedan används för att få åtkomst till ett offers miljö. Skillnaden är att där phishing är social engineering över mejl, så är vishing social engineering genom telefonsamtal. Ett exempel på hur denna attack kan se ut är att en hotaktör aktivt undersöker vilka uppgifter som finns tillgängliga för den tilltänkta måltavlan, vad de exponerar utåt, och vilka möjliga ingångar som finns till företagets miljö.

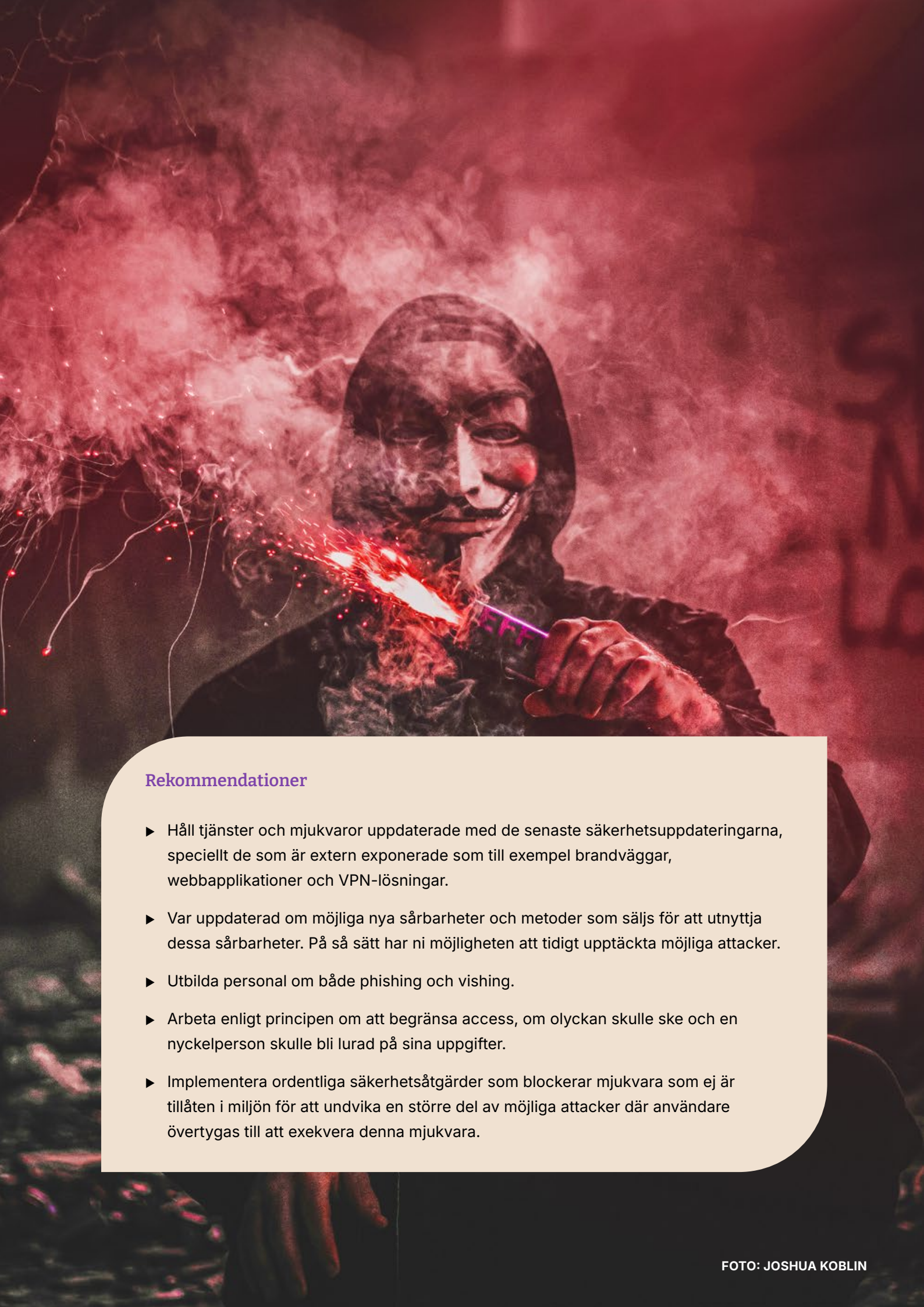
> “
> I vissa fall kan hotaktören även erbjuda pengar för att nyckelperson ska ge hotaktör åtkomst eller inloggningsuppgifter.

Hotaktören är specifikt ute efter nyckelpersoner och utifrån läckta uppgifter söker de igenom sociala medier samt går igenom personernas digitala fotavtryck för att till slut hitta en person av intresse. Hotaktören har genom läckta uppgifter fått denna persons telefonnummer och genomför ett samtal för att försöka övertyga dem om att till exempel installera en viss mjukvara, som ger åtkomst till deras dator. I vissa fall kan hotaktören även erbjuda pengar för att nyckelperson ska ge hotaktör åtkomst eller inloggningsuppgifter.

SEO poisoning

En till återkommande och populär metod är SEO poisoning och Malvertising. 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 adress.

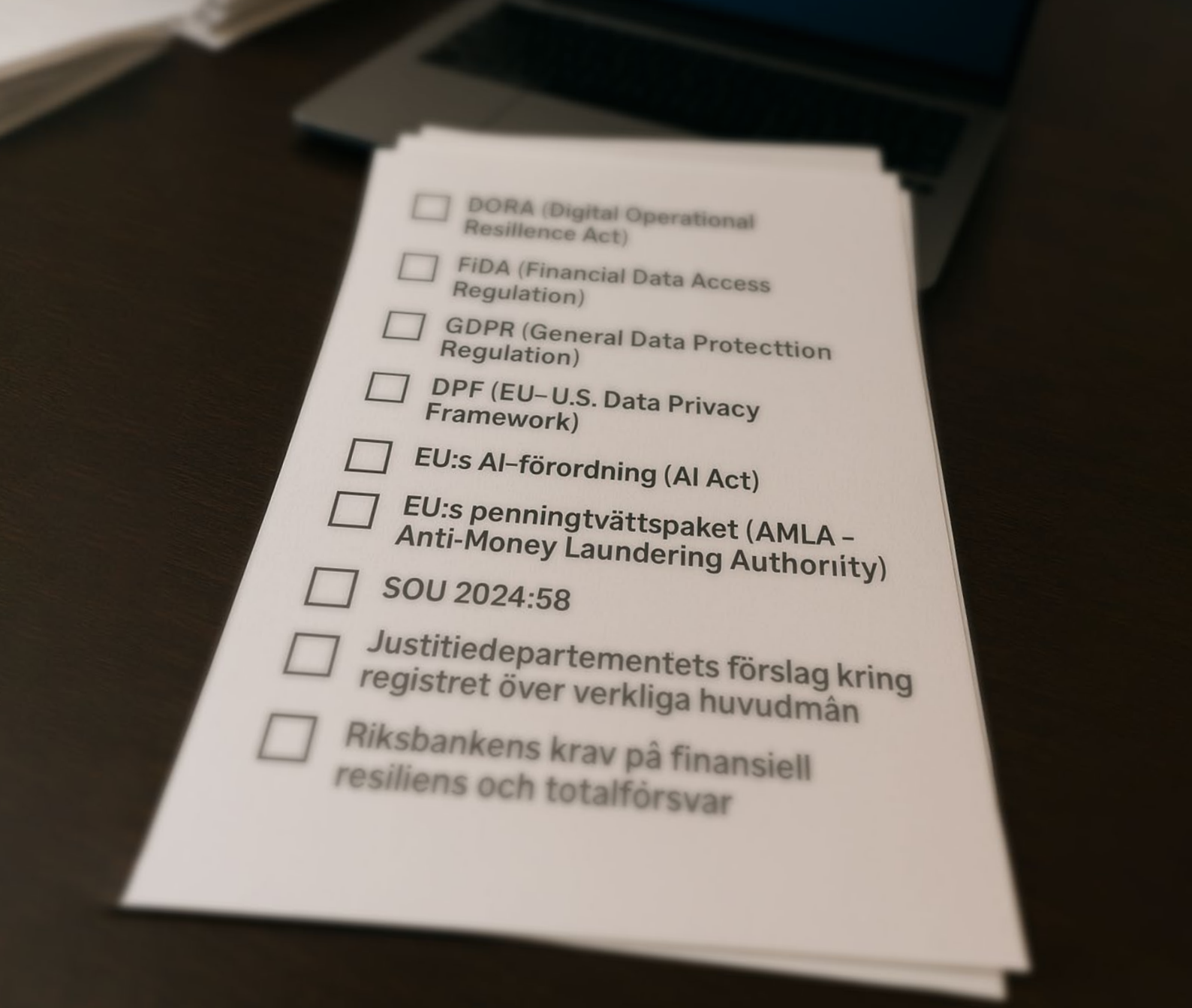
Den mjukvara som laddas ner kan även ha alla de önskade funktionerna men innehålla en trojan som även kör skadlig kod för att exempelvis installera infostealers, eller koppla upp till en hotaktörs server. Denna metod fortsätter att vara ett stort hot, speciellt för företag som inte har ordentliga säkerhetsåtgärder 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.



Rekommendationer

- Håll tjänster och mjukvaror uppdaterade med de senaste säkerhetsuppdateringarna, speciellt de som är extern exponerade som till exempel brandväggar, webbapplikationer och VPN-lösningar.
- Var uppdaterad om möjliga nya sårbarheter och metoder som säljs för att utnyttja dessa sårbarheter. På så sätt har ni möjligheten att tidigt upptäckta möjliga attacker.
- Utbilda personal om både phishing och vishing.
- Arbeta enligt principen om att begränsa access, om olyckan skulle ske och en nyckelperson skulle bli lurad på sina uppgifter.
- Implementera ordentliga säkerhetsåtgärder som blockerar mjukvara som ej är tillåten i miljön för att undvika en större del av möjliga attacker där användare övertygas till att exekvera denna mjukvara.

FOTO: JOSHUA KOBLIN



Ökad kravställning mot finanssektorn

2025 markerar en brytpunkt för den svenska finanssektorn. Det som tidigare kunde betraktas som compliancefrågor – isolerade till juridik, IT-säkerhet eller internrevision – har nu smält samman till ett nytt strategiskt landskap där cybersäkerhet, operativ resiliens och informationshantering blivit avgörande för affärsmodellens hållbarhet. Flera parallella krafter verkar tillsammans: ny EU-lagstiftning, växande geopolitiska hot, regulatoriska strukturer för dataflöden och teknologiska hinder.

Finanssektorn står idag i centrum för en alltmer komplex och krävande regulatorisk miljö. Nya regelverk inom EU och Sverige, i kombination med ökade säker-

BILD: **GPT IG**

hetshot och digitalisering, ställer högre krav på aktörerna än någonsin tidigare. Informationssäkerhet och digital resiliens har blivit grundförutsättningar för att upprätthålla stabilitet, förtroende och affärskontinuitet. Särskilt centralt är samspelet mellan dataflöden över gränser, nya EU-förordningar som DORA, FiDA och fördjupade krav på AI-ansvar, penningtvättstillsyn samt totalförsvarsförmåga. Dessa delar är inte fristående utan förstärker och påverkar varandra, vilket ställer höga krav på integrerad efterlevnad och strategisk helhetssyn.

En vision och en målbild kring hur man vill jobba med säkerhet, intervju med Christian Bengtsson.

Den svenska betalinfrastrukturen moderniseras och framtidssäkras och i det arbetet spelar Bankgirot en viktig roll – det är organisationens uppgift att se till att dagens betalsystem fortsätter att fungera som det ska, samtidigt som man fortsätter att utveckla morgondagens stabila och säkra system som följer internationella standarder och svenska regelverk.

Christian konstaterar att säkerhetsarbetet är avgörande i varje del av utvecklingen. ”Vårt mål är att erbjuda ett motståndskraftigt betalsystem som möjliggör innovation, regelefterlevnad och utveckling för våra kunder, och i alla delar av det här spelar säkerhetsarbetet en avgörande roll.” Han vidareutvecklar: ”Vårt mål är att tillsammans med bankerna skapa ett robust och framtidssäkrat ekosystem. Tillvägagångssättet kan låta enkelt – genom att arbeta proaktivt och ligga i framkant med avancerade tekniska säkerhetslösningar, nyttja ny teknik som effektiviserar vårt arbetssätt och förankra en säkerhetskultur i alla delar av verksamhet möter vi dagens och morgondagens utmaningar.”

Som chef för Säkerhet har Christian ett tydligt uppdrag; att säkerställa att säkerhet inte är ett sidospår, utan en integrerad och drivande kraft i hela verksamheten. ”Genom att arbeta målmedvetet och proaktivt bygger vi inte bara en säkerhetslösning – vi skapar en trygg och hållbar miljö där innovativa teknologiska lösningar möter ett robust försvar. Vår ambition om att vara en ledande aktör i sektorn inom säkerhetsområdet innebär att vi ständigt strävar efter förbättring och innovation, med ett helhjärtat engagemang för att skydda och främja en säker framtid för hela den finansiella sektorn.”

Organisation och stöd från ledningen – nyckeln till en hållbar säkerhetsstrategi

Christian poängterar vikten av att det finns en koppling till ledningen och att ledningsgruppen förstår förutsättningarna och varför vi alla behöver tänka och jobba med säkerhet. En del i Bankgirots arbete med Säkerhet har därför varit att se över hur man är organiserade.

”Den 1 januari i år etablerades ett nytt affärsområde som rapporterar till VD, ’Säkerhet & Beredskap’, med vilket Bankgirot vill ge dessa områden ett större fokus”, säger Christian. Han vidareutvecklar: ”Vi behöver belysa vikten av hur centrala dessa frågor är och ge dem mer utrymme för diskussion i Bankgirots ledningsgrupp, där vi är representerade av affärsområdeschefen för Säkerhet & Beredskap, Mikael Nyman, som anslöt till Bankgirot i början av året. Som företag anser vi att det är viktigt att hålla samman beredskapsarbetet med Säkerhet för att uppnå en hög motståndskraft i allt vi gör och kunna hantera allt från en vanlig incident till ett läge i samhället med höjd beredskap ”.

> “Vi är hårt reglerade och påverkas av många regelverk på flera områden, bland annat vad gäller säkerhet.

Efter att under en längre tid ha arbetat målmedvetet med att skapa en kultur där säkerhet är en affärskritisk fråga, vill Bankgirot fortsätta utveckla vad detta innebär och hur man agerar.

Han förklarar organisationsförändringen såhär: ”Vi har redan sen många år tillbaka ett stort engagemang för säkerhet, säkerhetsskydd, civilt försvar och beredskap i organisationen, men med utvecklingen i omvärlden behöver vi fortsätta arbeta in detta i ryggraden hos medarbetare och leverantörer. Alla inblandade vet att de produkter vi levererar är en viktig pusselbit för att betal-Sverige ska kunna fungera och detta ska genomsyra beslut och agerande, från styrelse ner till enskilda medarbetare.”

Regelefterlevnad i praktiken: förberedelser inför EU:s nya cybersäkerhetslagar

Nya regelverk som DORA och NIS2 ställer allt högre krav på operativ motståndskraft, rapportering och transparens. Bankgirot regleras under annat regelverk men behöver ändå som leverantör säkra sin efterlevnad liksom alla andra som träffas av regelverken, och tar samtidigt generell inspiration från de nya regelverken för att höja sin egen standard och bygga ett ännu starkare försvar.

”Vi är hårt reglerade och påverkas av många regelverk på flera områden, bland annat vad gäller säkerhet”, förklarar Christian. ”För oss innebär detta ett kontinuerligt arbete med att anpassa våra processer i takt med att regelverken utvecklas”. Han menar att en proaktiv och fokuserad ansats är avgörande för att identifiera de områden som behöver hanteras, eftersom regelverken oftast endast sätter en lägsta nivå; det är genom en gedigen risk- och hotbedömning som man kan fastställa vilka säkerhetsåtgärder som verkligen behövs i verksamheten. Det kan vara annat än vad som uttryckligen står i regelverken

och dessutom förändras verkligheten snabbare än vad regelverken hinner uppdateras.

Organisationer som träffas av många regelverk kan dra nytta av att hitta flexibla och anpassningsbara arbetssätt med fokus på de högsta riskerna. Man behöver helt enkelt förstå sin verksamhet och dess processer för att kunna implementera regelverk och säkerhet på ett smart och effektivt sätt.

> “Något vi arbetar med är att integrera de nya kraven tillsammans i hela verksamheten – med det tror vi att vi snabbare kan anpassa oss till de allt högre krav som ställs.

Christian beskriver utmaningen: ”Liksom många andra utmanas även vi av ständiga förändringar i regelverken, som ibland även kan upplevas vara motstridiga, såväl som i verkligheten runt om oss. Men jag tror att de som lyckas med detta kommer bygga en mer dynamisk och motståndskraftig verksamhet, som bättre möter kommande utmaningar.”

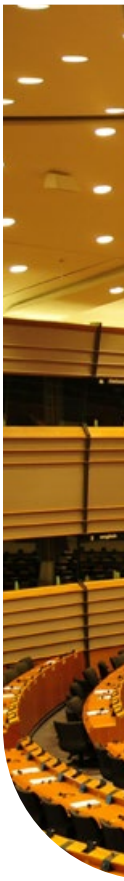
Han resonerar vidare: ”Något vi arbetar med är att integrera de nya kraven tillsammans i hela verksamheten – med det tror vi att vi snabbare kan anpassa oss till de allt högre krav som ställs. Genom att ha en ambition långt över miniminivån och arbeta strategiskt med riskbedömning, har vi bättre förutsättningar att på ett affärsmässigt och ansvarsfullt sätt möta de utmaningar vi alla står inför.”

Hotunderrättelser för att hjälpa organisationen att fatta rätt beslut

Threat Intelligence, eller hotunderrättelse, är en central del av Bankgirots säkerhetsarbete, något som Christian menar borde utföras i många verksamheter.

”Vi arbetar med att kontinuerligt samla in och analysera data från både interna och externa källor samt i samverkan med andra aktörer, för att proaktivt identifiera förändringar i hotlandskapet. Det här omvandlar vi sen till affärsrelevant information för att möjliggöra snabba, välgrundade beslut på strategisk nivå. Genom att arbeta på det sättet kan vi adressera och prioritera inriktningen på åtgärder och resurser till de områden där riskerna och hoten är som högst.”

Christian uppmanar organisationer att inte se threat intelligence som enbart en teknisk funktion inom säkerhetsarbetet, utan väva ihop detta med annan omvärlds- och marknadsinformation, och se det som en strategisk resurs som kan omvandlas till konkreta konkurrensfördelar och möjliggöra för organisationen att ligga steget före.



Han tipsar organisationer som vill arbeta mer med hotunderrättelser: ”Om du vill få värde ur att arbeta med threat intelligence så behöver du först förstå vad det är för informationsbehov du har och hur du vill använda det underlag du får ut. Du behöver också identifiera vilka målgrupperna för informationsinhämtningen är internt och vad dessa faktiskt har för behov. Målgruppernas behov kan variera i allt från operationellt i det dagliga arbetet i SOC och CISRT, till din verksamhets strategiska styrning.”

Realistiska scenarion med threat-led penetration testing

Threat-Led Penetration Testing (förkortas TLPT) förekommer som krav i regelverk såsom DORA och genom ramverk som TIBER. Dessa går längre än traditionella penetrationstester genom att utgå från verkliga hot och simulera realistiska attackscenarier. Testen kan även inkludera social engineering och fysiska intrång. Genom detta utmanas system och processer på ett sätt som speglar hela attackkedjan – från initial åtkomst till dataexfiltration – vilket ger organisationen en holistisk bild av sin motståndskraft. Vidare får man också möjlighet att verifiera att de beslut och åtgärder man har tagit faktiskt fungerar som tänkt - och om inte, justera och förbättra dessa.

Christian beskriver arbetet på Bankgirot: ”Vi skapar scenarion utifrån vår hotunderrättelseprocess för att förankra testningen så nära verkligheten som möjligt. Här är det viktigt att förstå sin motståndare, vilka tekniker och förmågor de faktiskt har, och utifrån detta bygga scenarierna som genomförs och på så sätt maximera värdet, då det är omöjligt att testa allt.” Här betonar Christian att det förstås är tätt sammankopplat med samma val du behöver göra när du väljer säkerhetsåtgärder, men menar att den som testar med förutsättningarna att angriparen har en för låg nivå av sofistikering kanske faktiskt inte kan upptäcka de mest relevanta svagheterna och bristerna i sina åtgärder.

”Jag menar att tester måste vara en integrerad del av vår förbättringscykel. Här jobbar Bankgirot på ett eget koncept som vi kallar ”Testdriven Säkerhet” - baserat på våra lärdomar och erfarenheter på området.”

Att skapa ett säkert och motståndskraftigt finansiellt ekosystem kräver mer än tekniska lösningar och regelefterlevnad – det kräver långsiktigt engagemang, samverkan och en djup förståelse för det föränderliga hotlandskapet.

På Bankgirot är säkerhet inte bara en teknisk fråga, utan en strategisk grundpelare som genomsyrar hela organisationen. Genom att kombinera proaktivt arbete med hög ambitionsnivå, en stark säkerhetskultur och avancerade metoder för hotanalys och testning, tar man ett tydligt ansvar för både sin egen roll och genom att bidra i det större ekosystemet. Med blicken framåt och fötterna stadigt i verkligheten fortsätter Christian Bengtsson och hans kollegor att stärka Sveriges digitala betalningsinfrastruktur.

EU PARLAMENTET, BRYSSEL | **FOTO: THOMAS LOHMANN**

Dataöverföring till USA: osäkerhet kring DPF och regulatoriska följdeffekter

Dataflöden över nationsgränser är en central nerv i dagens finansiella infrastruktur. Men regleringen av dessa flöden är direkt kopplad till frågor om suveränitet, säkerhet och rättssäkerhet. Här spelar DPF en nyckelroll. men utgör också en potentiell systemrisk i sig.

Den 10 juli 2023 antog EU-kommissionen ett beslut om adekvat skyddsnivå för överföring av personuppgifter till USA genom det nya EU–U.S. Data Privacy Framework (DPF). Det innebar att personuppgifter återigen kunde överföras till amerikanska organisationer som är certifierade under DPF utan att ytterligare skyddsåtgärder krävdes. Men denna trygghet är bräcklig då politiska förändringar i USA har väckt farhågor om ramverkets hållbarhet när flera medlemmar i den centrala tillsynsmyndigheten PCLOB avskedats. Därutöver har även de norska samt danska tillsynsmyndigheterna nyligen uppmanat organisationer att ta fram exitstrategier för amerikanska leverantörer, då DPF hänger på en skör tråd. Eftersom DORA och GDPR ställer krav på att finansiella aktörer har full kontroll över var och hur deras data hanteras, blir osäkerheten kring DPF särskilt problematisk. Om DPF skulle ogiltigförklaras tvingas svenska aktörer omförhandla avtal med molntjänsteleverantörer, genomföra dyra omstruktureringar och implementera alternativa skyddsmekanismer. Detta skulle medföra betydande juridiska, tekniska och operativa konsekvenser, vilket visar på den strategiska känsligheten i att vara beroende av tredjelandsbaserade molnaktörer.

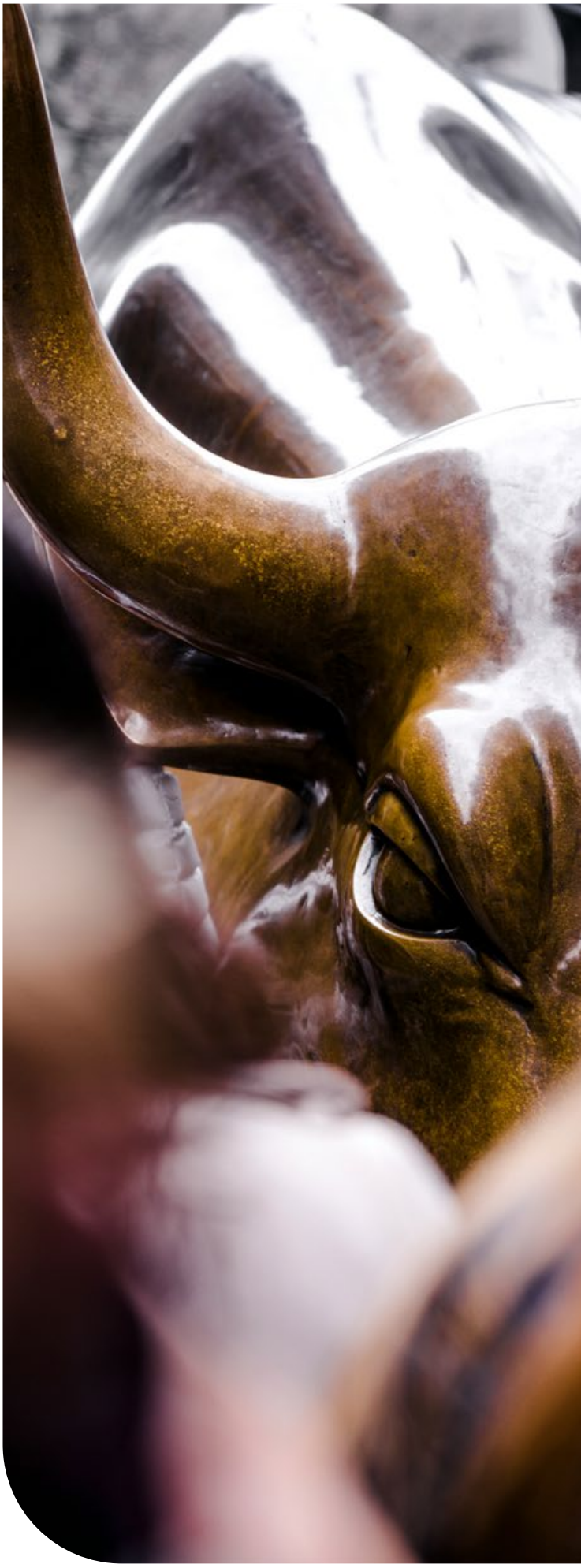
DORA: regulatoriskt skifte och nya säkerhetskrav

Som en direkt förlängning av problematiken kring DPF och i linje med EU:s bredare ambitioner att minska systemberoenden så är DORA en av de mest betydande regleringarna hittills. Den är också ett direkt svar på ökade cyberhot, digitalisering och riskhantering inom sektorn. DORA:s koppling till dataskyddsregler och dess beroende av tydlig styrning över tredjepartsleverantörer skapar ett ramverk där informationssäkerhet och affärsstrategi sammanvävs.

DORA (Digital Operational Resilience Act), som nu är i kraft, innebär ett grundläggande skifte i hur operativ risk hanteras i finanssektorn. Regelverket ställer krav på kontinuerlig riskhantering, incidentrapportering, säkerhetstestning av verktyg samt system, kontroll över tredjeparts-leverantörer inklusive

DORA innebär bland annat:

- Obligatorisk incidentrapportering inom snäva tidsramar
- Ökad granskning från Finansinspektionen och andra tillsynsmyndigheter
- Obligatoriska penetrationstester och red team-övningar
- Formellt ansvar på styrelse- och ledningsnivå



CHARGING BULL - NEW YORK | **FOTO: REDD FRANCISCO**

molntjänster, samt styrelseansvar för cybersäkerhetsstrategi och efterlevnad.

Den ökade regulatoriska komplexiteten kan särskilt påverka fintech-sektorn negativt. Högre säkerhetskrav riskerar att skapa inträdesbarriärer och leda till att mindre aktörer tvingas in i beroenderelationer eller slås ut. Dock kan de aktörer som tidigt investerar i resiliens och compliance vinna långsiktiga konkurrensfördelar.

> “Det råder för närvarande betydande osäkerhet kring framtiden för FiDA.

FiDA: reglerad datadelning

Financial Data Access Regulation (FiDA) är ett nytt EU-regelverk som syftar till att skapa en harmoniserad ram för tillgång och delning av finansiella data inom unionen. Förordningen bygger vidare på principerna i PSD2-direktivet men sträcker sig bortom betalningsdata och omfattar en bredare uppsättning finansiella data, inklusive lån, försäkringar, pensionssparande och investeringar.

FiDA samverkar med DORA och GDPR genom att föra in ett nytt kravkomplex som kombinerar öppenhet med säkerhet. Där DORA stärker den interna motståndskraften, skapar FiDA ett nytt system av kontrollerad datadelning – vilket ytterligare förhöjer betydelsen av starka ramverk för informationssäkerhet.

FiDA innebär att informationssäkerhet inte bara är ett internt systemansvar, utan ett ansvar för hela ekosystemet där delning och transparens måste balanseras mot kontroll och riskhantering.

Det råder för närvarande

Nyckelkrav i FiDA:

- Ökad kundkontroll över finansiella data: Kunder får möjlighet att bevilja och återkalla åtkomst till sina data.
- Tvingande dataåtkomst för finanssektorn: Banker och försäkringsbolag måste dela data med auktoriserade tredjepartsaktörer på begäran.
- Tekniska krav på API:er: Institutioner måste tillhandahålla högkvalitativa och säkra API:er.
- Dataskydd och cybersäkerhet: Delade data måste skyddas enligt GDPR och med robusta säkerhetsåtgärder.
- Reglering av ”gatekeepers”: Företag med dominerande marknadsställning omfattas av särskilda skyldigheter.
- Tydliga ansvarsförhållanden vid datadelning: Klara kontraktsvillkor och ansvarsutkrävande vid incidenter krävs.

betydande osäkerhet kring framtiden för FiDA. Enligt ett utkast till kommissionens arbetsprogram, planerar EU-kommissionen att dra tillbaka förslaget. Kritiken har bland annat handlat om att FiDA skulle medföra en oproportionerligt stor administrativ och teknisk börda för finanssektorn särskilt i ett läge där flera andra stora regelverk, som DORA och AI-förordningen, redan är på väg att implementeras.

Liknande uppgifter har rapporterats av POLITICO, som hänvisar till interna källor i kommissionen. Enligt dessa källor var avsikten att dra tillbaka FiDA inom sex månader, eftersom det inte längre bedömdes ligga i linje med kommissionens prioriteringar. Informationen sägs ha läckt ut från ett internt arbetsmaterial och EU-kommissionen har hittills avstått från officiella kommentarer, vilket ytterligare har eldat på spekulationerna om vad som faktiskt gäller.

AI och cybersäkerhet: behovet av samordnad styrning i ett nytt risklandskap

I takt med att DORA och FiDA skapar ramverk för teknisk och operationell motståndskraft inom finanssektorn, växer en ny och delvis oreglerad riskzon fram: artificiell intelligens. AI-verktyg har snabbt etablerat sig som en viktig del i effektivisering och innovation medan det regulatoriska skyddsnätet släpar efter. Detta skapar ett glapp, där cybersäkerhet måste utgöra en bärande spelare, mellan teknisk kapacitet och styrbarhet.

Finansinspektionens rapport visar att AI, särskilt generativ AI, används i allt högre grad inom den svenska finanssektorn för kundsupport, processautomatisering och riskhantering. Men många företag saknar tydliga styrningsmodeller och säkerhetsrutiner, vilket skapar betydande risker kopplade till datakvalitet, insyn, ansvar och regelefterlevnad.

EU:s AI-förordning som börjar tillämpas 2026 innebär:

- Riskbedömning och transparenskrav vid användning av AI i högriskfunktioner som kreditprövning
- Krav på förklarbarhet och tillsyn av AI-beslut
- Koppling till befintlig regulatorisk infrastruktur, exempelvis DORA och GDPR

Sammantaget krävs att AI-integrering sker i samklang med informationssäkerhetsstrategin. Det handlar inte bara om teknik utan även om styrning och etik.

EU:s penningtvättspaket och AMLA

Den regulatoriska utvecklingen inom finanssektorn handlar inte enbart om tekniska hot utan även om att förhindra systemmissbruk. Bekämpning av penningtvätt och terrorismfinansiering har blivit en central del av EU:s strategi för

EU:s nya regelpaket mot penningtvätt innebär:

- Inrättandet av den europeiska myndigheten AMLA, som får direkt tillsyn över högriskinstitut
- Harmoniserade krav på kundkännedom, transaktionsgranskning och transparens om verkliga huvudmän
- En ny mekanism för samarbete mellan nationella FIU:er, med förbättrad datadelning och analyskapacitet

finansiell integritet. Här är informationssäkerhet och dataspårbarhet nyckelkomponenter.

Sverige förbereder implementeringen genom SOU 2024:58, där den nationella anpassningen konkretiseras. Här blir informationssäkerhet inte bara skydd utan även ett verktyg för att identifiera, kartlägga och stoppa illegitima finansiella flöden. En säker digital miljö är en förutsättning för att den nya regleringen ska få effekt. Lagstiftningspaketet innehåller också en rad harmoniserade krav för alla medlemsstater, såsom standardiserade processer för kundkännedom (KYC), rapportering av misstänkta transaktioner, och transparens kring verkliga huvudmän. Implementeringen kommer dock att ske successivt. Enligt

FOTO: BEHNAM NOROUZI

det svenska Justitiedepartementet ska vissa delar av regelverket börja tillämpas redan från den 10 juli 2025, medan andra delar får längre övergångsperioder med slutdatum senast i juli 2027. Detta innebär att både finansiella aktörer och nationella myndigheter nu går in i en intensiv fas av anpassning och förberedelse.

I Sverige pågår en särskild utredning för att anpassa nationell lagstiftning till de nya EU-kraven. Ett delbetänkande med förslag kring registret över verkliga huvudmän publicerades i mars 2025, medan ett mer omfattande lagförslag väntas senare under året.

Riksbanken och det civila försvaret: finansiell resiliens som en del av totalförsvaret

Den svenska finanssektorn betraktas inte längre enbart som ett nav för kapitalflöden utan också som en samhällskritisk funktion. I takt med att geopolitiken hårdnar och hybridhoten ökar, har finanssektorns roll i totalförsvaret blivit mer uttalad.

- Riksbankens rapport från februari 2025 tydliggör detta genom att ställa följande krav på aktörer med en central funktion i betalningssystemet:
- Förmåga att upprätthålla verksamhet även vid störningar och krig
- Tillgång till redundanta tekniska lösningar och alternativa betalsystem (offline, backupdrift)
- Aktivt deltagande i sektorsgemensamma övningar och incidenthantering

Kopplingen mellan cybersäkerhet och samhällsberedskap är nu formell. Finanssektorns robusthet har blivit ett nationellt säkerhetsintresse och därmed ett strategiskt ansvar för varje aktör.

Nytt ansvarsparadigm för svensk finans

Den svenska finanssektorn befinner sig i ett omfattande systemskifte. Regelverk som DORA, FiDA, AI Act och AMLA utgör tillsammans en ny regulatorisk infrastruktur där informationssäkerhet, dataansvar och resiliens är centrala fundament.

Samtidigt har beroendet av globala molntjänster, AI-system och komplexa leverantörsnätverk skapat nya sårbarheter. Osäkerheten kring DPF visar hur snabbt förutsättningarna kan förändras, medan AI-utvecklingen belyser svårigheten att reglera teknik som växer exponentiellt.

De företag som klarar av att se sammanhanget, integrera regelverkens krav i sin strategi och bygga upp både teknisk och organisatorisk motståndskraft kommer att ha ett försprång inte bara i efterlevnad, utan även i affärsvärde. De som däremot fortsätter att hantera informationssäkerhet som en sidofråga riskerar sanktioner, förlorat kundförtroende och i värsta fall exkludering från ekosystemet.

Informationssäkerhet är nu inte enbart en skyldighet utan en strategisk möjlighet att bygga framtidens finansiella infrastruktur på tillit, transparens och kontroll.

Rekommendationer

- **Etablera en integrerad strategi för informationssäkerhet och compliance**
  Säkerställ att efterlevnad av DORA, GDPR, AI-förordningen och framtida AMLA-tillsyn inte behandlas som separata initiativ. Bygg en samordnad och tvärfunktionell struktur där informationssäkerhet, juridik, IT och affärsstrategi samverkar.
- **Kartlägg beroenden till tredjepartsleverantörer och molntjänster**
  Identifiera om er verksamhet är beroende av leverantörer i tredjeländer, särskilt USA. Bedöm konsekvenserna av att EU–U.S. Data Privacy Framework (DPF) ogiltigförklaras. Förbered alternativa lösningar och stärk de legala och tekniska skyddsåtgärderna i era leverantörsavtal.
- **Utbilda styrelse och ledning i digital resiliens**
  DORA innebär att styrelse och ledningsgrupp bär ett formellt ansvar för operativ motståndskraft. Se till att högsta ledningen har tillräcklig insikt i cybersäkerhetsrisker, tillsynskrav och verksamhetens förmåga att hantera störningar.
- **Upprätta interna riktlinjer för AI-användning**
  Genomför riskbedömningar för samtliga AI-tillämpningar, särskilt inom kreditprövning, automatiserat beslutsfattande och kundservice. Undvik att införa generativ AI i känsliga processer innan dokumentation, insyn och övervakning är fullt på plats i enlighet med kommande EU-krav.
- **Följ utvecklingen kring FiDA**
  Trots att det finns motstridiga uppgifter om FiDA:s framtid, bör arbetet med API-lösningar, dataintegritet och säker tredjepartsåtkomst fortsätta. Dessa funktioner blir avgörande även i andra regelverk och kundlösningar.
- **Förbered er inför penningtvättsregelverkets implementering**
  Se över era processer för kundkännedom, transaktionsövervakning och rapportering. Den nya EU-myndigheten AMLA kommer att få direkt tillsyn över vissa högriskaktörer, men alla större finansiella institut förväntas anpassa sina interna system för ökad spårbarhet, automatisering och analyskapacitet.
- **Systemviktiga aktörer bör stärka sin beredskap för samhällsstörningar**
  För aktörer med central roll i betalningssystemet eller i annan samhällsviktig finansiell infrastruktur är det avgörande att uppfylla kraven från Riksbanken och det civila försvaret. Det inkluderar redundanta tekniska lösningar, alternativa betalsystem samt deltagande i krisövningar och samverkansstrukturer.

Hur man kan omhänderta en komplex verklighet

När mycket händer i omvärlden och vi står inför flera olika områden som vi behöver ha koll på och anpassa vårt säkerhetsarbete utefter är det lätt att bli överväldigad och splittrad. Hur ser vi till att vi har koll på helheten, får de uppdateringar vi behöver och en överblick så att vi kan ta strategiska och operationellt kloka beslut?

FOTO: RYOJI IWATA

Cybersäkerhetsläget för svensk finanssektor - Intervju med Teresia Willstedt.

MedMera Bank verkar i en bransch som präglas av ökade regulatoriska krav, fler cyberhot och snabbt skiftande teknologier. Teresia Willstedt, ansvarig för informationssäkerhet och kontinuitet, delar med sig av hur en mindre nischbank arbetar med att skapa säkerhet, resiliens och medvetenhet – trots begränsade resurser och ett komplext omvärldsläge.

Hoten och kraven driver utvecklingen framåt

Bankväsendet befinner sig i ett stort skifte där kravbilden har förändrats över tid. Branschen är vana vid regulatoriska krav, men med ökande cyberhot, höga krav från bankkunder, och stora teknologiska genombrott befinner man sig i en annan miljö nu än för bara några år sedan. Teresia ser regelverken som en nödvändig struktur mitt i allt detta:

- Vår kravbild har förändrats en hel del, och jag tillhör de som faktiskt ser positivt på vissa regelverk. Med dem i ryggen får säkerhetsansvariga ett annat gehör från ledningen, särskilt när det gäller kostnader för nödvändiga åtgärder.

Teresia förklarar att man tidigare kunde behöva försvara varenda krona vid en investering, och vrida och vända på värdet det skulle ge.

- För några år sedan, om man ville införa exempelvis en sårbarhetsskanning, såg man kanske mest på kostnaden, men om det finns en compliance-risk blir investeringen mycket viktigare. När verksamheten redan har gjort sin riskanalys är det enklare att peka på den för att besluta om rätt vägval, så jag upplever helt enkelt att säkerhetsfrågor har kommit väldigt högt upp på agendan.

> “Titta bara på händelser som Nordea som blev utsatta före jul - det är ju ingen hemlighet att det händer mycket.

På frågan vad som driver utvecklingen svarar Teresia med ett skratt och utan att tveka:

- Hotbilden, helt klart! Titta bara på händelser som Nordea som blev utsatta före jul - det är ju ingen hemlighet att det händer mycket. Dessutom har vi, liksom många andra, fler tredjepartsleverantörer som även de har blivit utsatta för incidenter eller avbrott i tjänster vi är beroende av för att verksamheten ska fungera.

När även regelverken ställer andra

krav på ledning och styrelse är Teresia återigen inne på att det blir ett helt annat gehör jämfört med för bara några år sedan. Dora och andra regelverk lägger ett större ansvar på styrelsens kompetens och förståelse för verksamhetens risker.

- Tidigare pratade vi säkerhetsansvariga mycket om att vi vill få vara med i ledningsgrupper och påverka, men nu är det snarare ett måste.

Ett nära partnerskap som svaret på hanteringen av leverantörsrelationer

I många branscher är tredjepartsfrågan en högaktuell snackis – flera är de diskussioner som finns om hur man bäst hanterar tredjepartsledet för att säkra informationssäkerheten i flera led. Teresia applicerar samma princip som tidigare när det kommer till att identifiera det som är mest kritiskt för banken. Alla kan inte hanteras med samma prioritet, utan man får identifiera de viktigaste.

- Det är inte rimligt eller görbart att gå lika djupt med alla med tanke på hur noggrant och grundligt det behöver göras för att det ska ge ett värde – det finns i alla fall inte på min karta, resonerar Teresia. Men om du ser att en viss tjänst är affärskritisk, att om den skulle gå ner så får man stora problem – ja då måste du göra en mycket grundligare analys av hur de själva arbetar med säkerhet.

En annan utmaning är att få leverantören att inse att de behöver dela med sig av information som de kanske inte gjort tidigare. Efter att ha identifierat de mest kritiska leverantörerna kanske man gör stickprov på övriga, men det gäller att veta hur man ställer krav i avtalet och hur man verifierar att de talar sanning och har rätt rutiner.

För MedMera Bank har det skett ett skifte där man nu ställer andra krav på leverantören från början. Teresia igen:

- I och med Dora har vi gått igenom alla våra viktiga avtal och ställer nu andra krav på våra leverantörer. Sen har vi inte riktigt sett hur det kommer utveckla sig – vissa leverantörer kommer vi nog få mer information från, andra kanske inte. Men jag tror att grundtanken är bra, för det är verkligen en helt annan värld vi lever i nu.

> “I och med Dora har vi gått igenom alla våra viktiga avtal och ställer nu andra krav på våra leverantörer. [...] jag tror att grundtanken är bra, för det är verkligen en helt annan värld vi lever i nu.

Teresia menar att även köparen av en tjänst har ett helt annat ansvar idag när det kommer till att leverantörsrelationerna. Skiftet vi befinner oss i innebär att

många gör bedömningen att den bästa lösningen är att sätta sig på leverantörens sida av bordet och jobba tillsammans, snarare än bara ställa krav via avtal.

- Även som köpare har vi ett annat ansvar idag, att se till att vi inte bara får bekräftelser, utan på något sätt faktiskt se till att det är så på riktigt. Det är en utmaning.

Teresias tips för bättre leverantörshantering handlar om kommunikation – oavsett om det är en större eller mindre aktör. De stora leverantörerna kommer med sina bekymmer, men de mindre kan likväl ha problem med bland annat kompetens, tid eller resurser.

- Vår upplevelse är att det viktigaste är kommunikation så man inte bara hörs via en mailväxling utan verkligen pratar med dem. För de allra viktigaste försöker vi alltid få till ett partnerskap snarare än att bara köpa en tjänst. Då har man ett gemensamt ansvar, vilket underlättar när vi skickar frågebatterier om deras säkerhetsarbete.

Frågebatterierna förekommer i de allra flesta leverantöresrelationerna. Kunden vill veta hur leverantören arbetar, vilka policies som finns, hur de implementerar säkerhetsarbetet i företaget, osv. För MedMera Bank har man länge ställt sådana krav, med syfte att försöka förbereda sig för framtida krav.

- Vi vill undvika att bara fokusera på vad som krävs här och nu, och i stället lyfta blicken mot vad som kan komma sen. Om vi på något vis kan förbereda oss på morgondagens krav så blir det lättare att ta sig an det.

Hur man än vrider och vänder på det behöver hanteringen av leveranskedjan i ett mindre bolag med begränsade resurser vara effektiv och smart. Teresia och hennes kollegor har strategin klar för sig:

- Jag är tillbaka till det jag sa tidigare – det handlar om att identifiera vad som är mest väsentligt och att lägga fokus där. Är det en leverantör som är extra viktig, då måste vi få information om deras leverantörer också, alltså deras leveranskedja. Om en tredjepartsleverantör, även om den inte är den allra viktigaste, råkar ut för något så gör vi direkt en analys. Vi tittar på vad som skulle kunna påverkas, och om vi missat något vi borde ha tänkt på.

Teknologin, cyberhoten, och bankernas framtid

En utmaning som allmänheten ständigt blir medvetandegjord om i såväl det stora som det lilla är bekvämligheten och användarvänligheten i banklösningar - en bank behöver balansera kunders önskemål mot rimliga åtgärder. Den här frågan har vi sett aktualiseras i samband med äldrebedrägerier, där de flesta förmodligen är överens om att åtgärder krävs – men inte så att det påverkar den egna vardagen.

För Teresia är användarvänligheten balanserat mot säkerheten en viktig faktor när hon blickar mot framtiden, men för henne är det ändå främst regel-

verken snarare än teknologin som sätter agendan för framtiden.

- Regelverken får ju en väldigt stor betydelse eftersom du helt enkelt inte får driva banken om du inte följer dem. Compliance blir därför väldigt betungande för hela verksamheten. Självklart är det dock alltid vad kunderna vill ha och behöver som får styra. Vi kan ju implementera massa säkerhetsfunktioner, men allt måste vara användarvänligt och ge en smidig banktjänst – inget får vara för svårt.

MedMera Banks arbete med informationssäkerhet visar att även mindre aktörer i finanssektorn kan skapa robusta och hållbara säkerhetslösningar genom rätt prioriteringar, tydliga processer och ett nära samarbete både internt och med leverantörer. Teresia Willstedt påminner om att nyckeln till framgång ligger i att arbeta proaktivt, att ha vara närvarande och kommunikativ internt för att bygga en säkerhetskultur, och att ständigt omvärdera sin riskbild. Med blicken mot framtiden ser banken både regelverk och teknologiska framsteg som drivkrafter för att fortsatt stärka sitt skydd och möta nya hot – utan att förlora fokus på användarvänlighet och affärsnytta.

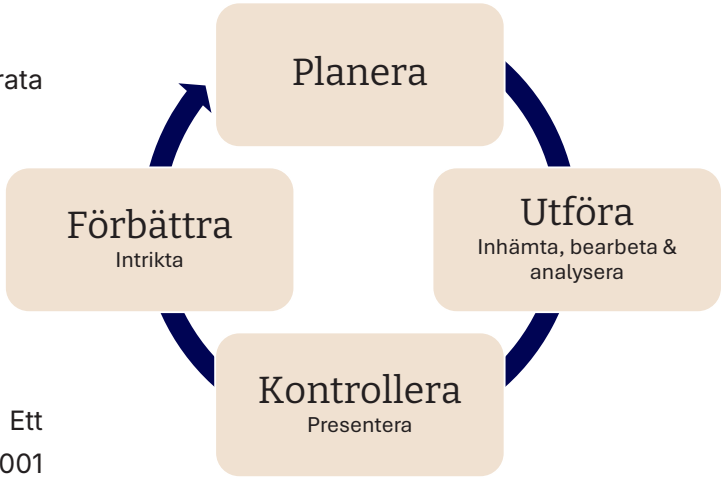
Systematiskt arbete

Ett ledningssystem där vi systematiskt samlar in information, dimensionerar vårt säkerhetsarbete och våra strategier, planerar, utför, kontrollerar och förbättrar i en kontinuerlig snurra, skulle kunna vara ett sätt att omhänderta problematiken. Det vill säga ett systematiskt underrättelsearbete som föder ett systematiskt informationssäkerhetsarbete. Syftet är att skapa ett övergripande lednings- och säkerhetsarbete där vi har arbetssätt för att systematiskt samla in den information vi behöver och sedan anpassa det arbete vi har. Alternativet kan annars bli att exempelvis efterlevnad av DORA, kundkrav, översyn av leveranskedjan och insamling av teknisk infor-

FOTO: KELLY SIKKEMA

mation om hotaktörer alla blir separata spår utan samspel vilket skapar onödigt mycket arbete för ledningen och viktiga intressenter. Följden av detta blir att ledning och säkerhet slängs än hit och än dit.

Ett ledningssystem kan man bygga upp på många olika sätt. Ett sätt skulle kunna vara enligt ISO 27001 som dessutom enligt den senast uppdaterade versionen innehåller säkerhetskontroll och best practice för att arbeta med just hotunderrättelser. Till ett sådant ledningssystem kan man sedan knyta många olika delar som har nytta av eller samspelar med hotunderrättelser eller informationsinsamling så som systematiskt riskarbete med grunden i en aktuell och organisationsspecifik hotbild. Kris och kontinuitetsövningar kan testa förmågan att stå emot om väl hotet blir verklighet, och säkerhetsarbetet blir än mer relevant om det anpassas efter organisationens specifika hot- och sårbarhetsläge.



PDCA-CYKELN (PUCK) ÄR EN METOD FÖR KONTINUERLIG FÖRBÄTTRING. VI PLANERAR VAD SOM SKA GÖRAS, UTFÖR ARBETET, KONTROLLERAR RESULTATET OCH FÖRBÄTTRAR PROCESSEN. CYKELN UPPREPAS FÖR STÄNDIG UTVECKLING.

Om vi bygger vår planering på en nykter bild av vår nuvarande säkerhetssituation, våra sårbarheter och våra hot kan vi omsätta denna i planer för att anpassa vår nuvarande säkerhetssituation efter sårbarheterna och hoten. När vi har utfört våra planer behöver vi effektiva sätt för att testa om vårt säkerhetsarbete är så bra som vi tror att det är. Ett relevant sätt för aktörer inom finanssektorn att testa detta är det som benämns som Threat Lead Penetration Testing (TLPT), vilket även är ett krav enligt DORA-förordningen.

Säkerhetstestning

TLPT är ett hotbildsstyrt penetrationstest, vilket innebär ett utförligt och längre test av kritiska och viktiga funktioner. Liknande ett Red Team-test utförs testning på flera olika funktioner i företaget beroende på testets omfattning. Inom TLPT måste dock kritiska och viktiga funktioner vara en del av omfattningen. TLPT består av fem olika faser: Preparation, Threat Intelligence, Red Team Test, Stängningsfas och Åtgärdsplanering.

Under preparationsfasen, ska kommunikation med en så kallad TLPT authority hanteras, dokumentation och omfattning ska tas fram tillsammans med de grupper som ska utföra både Threat Intelligence och Red Teaming. När allt är fastställt, kan företaget gå vidare till den första testfasen som är Threat Intelligence.

En TLPT Authority är en utsedd offentlig myndighet inom finanssektorn som ansvarar för kontroll av följsamheten av alla krav som ställs i artikel 26 i DORA. Myndigheten ska tillhandahålla ett så kallat TLPT Cyberteam, vilket är personal som ansvarar för TLPT-relaterade frågor. Det är upp till den myndigheten att meddela en finansiell entitet om ett hotbildsstyrt penetrationstest (TLPT) krävs.

Under testfasen för Threat Intelligence ska information som är relevant för företaget i form av relevanta hotaktörer, deras metoder och tekniker samt information som ska föda testningen i Red Team i efterföljande fas tas fram. Då det inte finns något krav på hur lång tidsperiod som ska läggas

FOTO: GPT IG

på denna testfas kan perioden variera beroende på företagets storlek. Ett riktvärde är att en period på åtminstone 6 veckor bör läggas för att kunna ta fram relevant och djupgående analyser om företaget för att simulera den mängd tid som en möjlig hotaktör skulle lägga för att ta fram möjliga ingångar och attack-

> “Red Team-test är nästa fas, där information som tagits fram i Threat Intelligence-fasen ska användas för att direkt simulera relevanta hotaktörer och deras metoder och tekniker.

metoder. Informationen som tas fram här ska leda till flera möjliga scenarion som ska simuleras i testfasen i Red Team och utifrån dessa scenarion ska åtminstone tre scenarion väljas ut av företaget för att användas och simuleras.

Red Team-test är nästa fas, där information som tagits fram i Threat Intelligence-fasen ska användas för att direkt simulera relevanta hotaktörer och deras metoder och tekniker. Red Team-testningen har som krav att det ska utföras under åtminstone 12 veckor för att kunna simulera aktörer som håller sig mer under radarn och spionerar och samlar information under en längre tid, precis som kända hotaktörer gör. Under denna testfas tas material fram på vad som har funkat, vilka metoder som har varit användbara och de åtgärder som behöver vidtas av företaget för att säkra upp sin miljö.

Under stängningsfasen ska företagets egna säkerhetsteam (Blue Team) informeras om att ett TLPT har skett och en rapport för Red Team-testningen ska förses till företaget. Blue Team ska, när de väl är informerade, ta fram en egen rapport av det som de har upptäckt under testningen och var det finns säkerhetsbrister. Efter att båda parterna har tagit fram rapporter ska Purple Teaming utföras, där både Red Team och Blue Team samarbetar för att ta fram larm och detekteringsmetoder för de attacker och metoder som användes under TLPT.

I den sista fasen, åtgärdsplanering, ska en åtgärdsplan tas fram. I planen ska det finnas information om alla de sårbarheter som hittades under TLPT med tillhörande rotorsaksanalys. Till dessa sårbarheter ska medarbetare och grupper utses för att åtgärda dem. Till alla sårbarheter ska även en risk dokumenteras, i fallet av att sårbarheten ej åtgärdas.

Leverantörshantering

Verkligheten vi står inför idag är att det finns ett ökat beroende till leverantörer på grund av globalisering, digitalisering och den form av specialisering som de flesta företag arbetar med. Att detta utgör en säkerhetsrisk är inte något nytt.

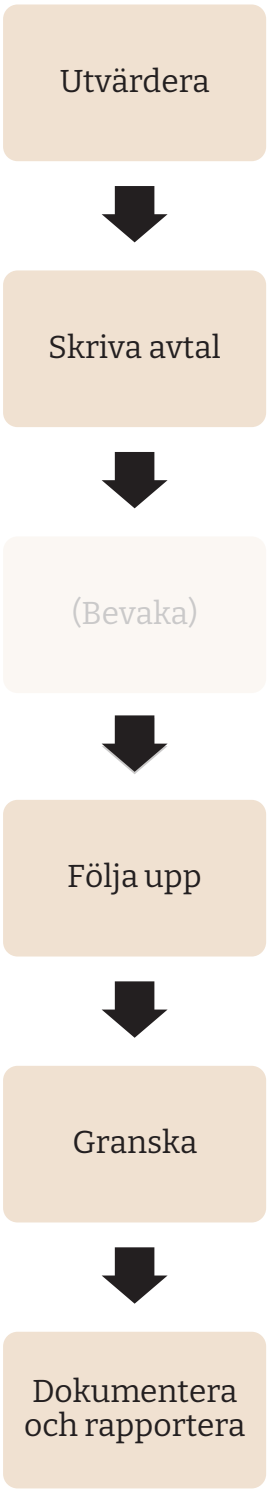
Angrepp via leveranskedjan är vanliga och kan drabba en organisation både via dennes leveranskedja och via organisationens roll i någon annans leveranskedja. Det kan helt enkelt vara så att säkerheten är mer bristande på annat håll än i den organisation som hotaktören vill åt, eller att hotaktören vill angripa en leverantör för att på så sätt kunna slå fler flugor i en smäll genom att påverka flera av leverantörens kunder.

Dilemmat som uppkommer är att leveranskedjan både är komplex och svår att överblicka för en vanlig organisation. Bara första ledets leverantörer kan uppgå till flera hundra aktörer och lägger vi till våra leverantörers leverantörer och deras respektive leverantörer blir det snabbt ett alltför stort antal aktörer med tillhörande risker att överblicka. Det är helt enkelt så att vi har fler leverantörer och potentiella säkerhetsrisker som vi behöver hantera, på grund av säkerhetssituationen och regleringar som exempelvis DORA och NIS2, än vad de flesta verksamheter har förmåga att hantera. Det är även så att vi, för att ha en effektiv leverantörshantering, behöver ha förmågan att följa upp de krav som vi ställt under avtalsprocessen kontinuerligt över tid

Ett första steg kan låta trivialt, dock är det för många ett reellt problem, men det är att få koll på vilka leverantörer som vi har i alla delar av organisationen. Nästa steg är att bedöma och sortera ut de mest kritiska leverantörerna, vilka leverantörer hanterar vår mest kritiska information eller tillhandahåller de tjänster som vi är beroende av för vår mest kritiska verksamhet? Det är förmodligen inte enbart de mest kritiska leverantörerna som kan orsaka problem för oss om något hände med dem, utan även andra. Vill ni därför ta säkerhetsnivån lite

högre kan ni av den anledningen bedöma och kategorisera samtliga leverantörer i exempelvis tre kategorier beroende på hur kritiska de är för er verksamhet. I en sådan bedömning behöver vi inte bara se till tjänsten eller informationen som leverantören tillhandahåller, utan även till leverantörens säkerhetsnivå utifrån deras interna säkerhetsarbete och den hotbild som finns mot dem.

När vi har placerat in leveran-



törerna i tre kategorier kan vi tillsätta säkerhetsåtgärder beroende på kategori. På så sätt behöver vi inte göra allt för alla eller inget för ingen. Kanske vill vi genomföra revisioner tillsammans med våra allra mest kritiska leverantörer och bevaka deras säkerhetssituation medan det för de mindre kritiska räcker med att vi skickar ut ett formulär vartannat år?

Vi får inte heller glömma bort att hur stora risker vi har i vår leveranskedja även beror på vår förmåga att hantera dem. Ett första steg här är att etablera en process för leverantörshantering utifrån den ambitionsnivå som ni väljer.

Pratar vi om uppföljning av leverantörer är det även värt att betänka hur ansvarsfördelningen ser ut och på vem det ligger att påvisa en god säkerhetssituation. Ska vi ställa våra frågor utifrån en checklista och sedan följa upp med jämna mellanrum, eller ligger det på vår leverantör att kontinuerligt bevisa att de uppfyller de krav vi ställt i avtalen? Denna svårighet har vi belyst i tidigare rapporter.

För att säkerställa robust leverantörshantering behöver vi kontinuerligt övervaka och följa upp leverantörernas säkerhetsarbete, anpassa våra krav vid förändrade hotbilder och tydligt definiera roller och ansvar. Leverantörshantering är en kontinuerlig process där proaktivt arbete och systematisk uppföljning minskar riskerna för angrepp via leveranskedjan och stärker organisationens motståndskraft.

Stort tack för ditt intresse av vår lägesbild!

Vårt syfte med rapporten är att samla ett kondensat av de viktigaste säkerhetsdrivande händelserna, hoten och regelverken just nu. Vi vill ge läsaren en överblick som ska hjälpa till att styra riktningen när det kommer till det interna informationssäkerhetsarbetet, men avser inte vara heltäckande vare sig vad gäller alla de hot som finns, eller alla möjliga lösningar. Vårt intelligence-team vill med sin lägesbild helt enkelt visa på vilka analyser som kan göras av de viktigaste skeendena, och hur du kan använda den informationen för att skaffa er ett försprång.

Vi tror att lägesbilden passar dig som lite mindre eller medelstor aktör inom finanssektorn, som har ett pågående informationssäkerhetsarbete men kanske inte samma typ av resurser som de stora aktörerna.

Vi hoppas att du har fått med dig viktiga insikter som du kan omsätta i konkreta åtgärder i din roll – 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


Secify