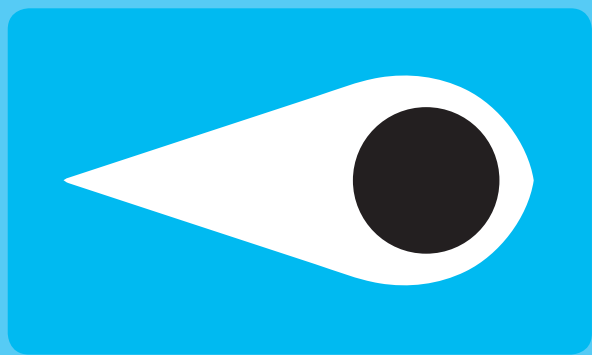




TRYGGARE samhälle

TIDNINGEN FÖR ETT SÄKRARE SVERIGE • UTGES AV SSF STÖLDSKYDDSFÖRENINGEN • NR 2 • 2021



Foto: Sören Andersson

Tema:

SÄKER IDENTITET

– vem kan man lita på och hur får vi reda på det?

Sid 8–12



Att förebygga vardagsbrott kräver ett helhetsgrepp

Thomas Brühl, vd,
SSF Stöldskyddsföreningen.

Sid 2



Staten bör kliva fram och säkra våra identiteter

Daniel Hjort,
affärsutvecklingschef, Nexus.

Sid 4



Tullverkets befogenheter ses över i ny utredning

Magdalena Andersson,
finansminister.

Sid 5

LEDARE



Thomas Brühl,
vd, Stöldskyddsforeningen

”Vårt engagemang för att förebygga vardagsbrott är större än någonsin – men står nu på två ben.”

Att förebygga vardagsbrott kräver ett helhetsgrepp

Vi har det senaste året satsat väldigt hårt på att bli en stark kraft när det gäller att förebygga digitala brott. Vår ambition är att koppla ett helhetsgrepp och kunna göra betydande skillnad i det förebyggande arbetet mot såväl fysiska som digitala vardagsbrott.

När det gäller fysisk säkerhet är vi starka och i fas med tiden. När det gäller den snabbt föränderliga digitala brottsligheten har vi en bit kvar, men vi gjorde en riktig kraftsamling under 2020 genom att exempelvis lansera sajten Säkerhetskollen.se och även skapa nya normer inom det digitala området. Vi har också bildat ett kunskapscenter med polisen och MSB. Vi har också investerat en hel del i marknadsföring för att säkerställa att våra digitala initiativ når ut och kan göra skillnad. Mest känd är kampanjen för för säkrare lösenord som har väckt mycket uppmärksamhet och haft stor positiv inverkan.

Finansieringen av vår satsning på informationsspridning och våra andra åtgärder mot digitala brott har inte tagits från den traditionella verksamheten och har sålunda inte haft någon påverkan på vårt arbete inom fysisk säkerhet. Vi har istället skjutit in egna medel för att jobba mot alla typer av vardagsbrott, där de digitala brotten står för en väldigt stor del. Arbetet mot digitala brott är också nödvändigt för att vi ska kunna utveckla normer och stärka skyddet för fysisk säkerhet.

Så rent generellt kan man säga att vi satsar lika mycket på fysisk säkerhet som tidigare. Under det senaste året har vi tagit fram och reviderat ett antal normer kopplat till lås, larm, certifieringsverksamhet, nyckelförvaringar och mycket annat. Vi fortsätter också bedriva en omfattande rådgivning och medieverksamhet där vi lyfter fram behov av förebyggande åtgärder mot inbrott, bilbrott, cykelstöld och andra fysiska brott. Dessutom har satsningen på Grannsamverkan varit mycket framgångsrik då konceptet nu täcker cirka 30 procent av hushållen i landet. Vårt engagemang för att förebygga vardags-

brott är större än någonsin – men står nu på två ben.

Det pågår ständigt olika försök till att lura av oss våra personuppgifter som sedan använts för att stjäla information, kapa datorer eller helt enkelt för att lura av oss våra pengar. Att vilseleda med identitet är också ett kraftfullt vapen om man försöker påverka opinioner eller val. Detta är inget nytt utan ett spel som pågått länge med både fysiska och digitala metoder, oftast i kombination med varandra. Hur kan man veta att den person som står i hemsjukvårdens kläder verkligen kommer därifrån eller att samtalet från banken är korrekt. Samma sak med mejlet eller sms:et man får från Postnord eller DHL där man ska klicka på en länk, är det verkligen rätt?

Tyvärr drabbas många av den här typen av brott och därför har vi på SSF sett som nödvändigt uppmärksamma detta i en stor pågående kampanj om olika typer av phishing, eller nätfiske på svenska. Kampanjen har gått på stortavlor, sociala medier och i radio. Vi vill verkligen att alla ska tänka till och ställa sig frågan ”Är jag säker?” innan de hamnar i en situation där de blir lurade. Teknikutvecklingen gör dock att det blir än mer komplicerat för människor att helt säkert veta vem som är vem. Vi också tagit fram en ny design till konsumenttjänsten säkerhetskollen.se och nästa steg är att utveckla och anpassa den så att den även riktar sig till företag.

En satsning som kommer att göra stor skillnad framöver är den nya normen ”SSF 1120 IoT Uppkopplade smarta enheter”. Den ska lyfta fram och verifiera säkerheten kring smarta produkter. Med produkter som har provats och märkts upp som certifierade blir det lättare för konsumenterna och brukarna att göra säkra produktval.

Nästa steg är att sätta in regelverket i ett ekosystem som exempelvis anger hur IoT-produkter fungerar ihop med digitala lås eller larm. På det här sättet får vi bra grund för att ta ett helhetsgrepp om vardagsbrotten och koppla ihop åtgärder för det fysiska och det digitala skyddet.

Vill du få nyheter, tips och information direkt i din inkorg? Registrera dig för vårt nyhetsbrev på www.stoldskyddsforeningen.se/nyhetsbrev

Chefredaktör Per Klingvall. **Annonser** Deniz Baykal tel 08-556 306 80.

Ansvarig utgivare Lennart Alexandrie. **Prenumeration** Tryggare Samhälle 4 nummer per år.

Pris 89 kr (exkl moms) per år. www.tryggaressamhalle.se **Tryck** V-TAB, Västerås 2021.

AR Media International AB

Västberga Allé 32, 126 30 Hägersten

Telefon 08-556 306 80

info@armedia.se, www.armedia.se

En produkt från

armedia

Officiellt media för

SSF
Stöldskyddsforeningen



Är ni säkert skyddade?

Utbilda er inom säkerhetsskydd

3 dagars utbildning
28 sep 2021
23 nov 2021

ssf.nu/utbildning

SSF
Stöldskyddsforeningen

A full-page background image of an astronaut in a white spacesuit floating in space. The Earth's horizon is visible in the upper left, with a bright blue and white light flare from the sun or a reflection on the planet's surface. The astronaut is positioned diagonally, with their head towards the upper right and legs towards the lower left. The suit is detailed with various straps, buckles, and a large black visor on the helmet.

MOBOTIX HUB

The **EXPANDABLE**
Video Management Platform



Experience the
MOBOTIX HUB

MOBOTIX
BeyondHumanVision

Daniel Hjort, Nexus Group:

Staten bör kliva fram för att säkra våra identiteter

En krigshandling mot Sverige skulle inte se ut som många av oss tror. Det finns idag mycket mer effektiva vapen än de traditionella. Nyckeln till försvar är därför säkra identiteter. Att överlåta identitetsfrågan till slumpen känns därför inte rättvist mot vare sig medborgare eller framtidens Sverige, menar Daniel Hjort, affärsutvecklingschef på Nexus Group.

Som land har vi sedan länge gått vår egen väg när det gäller godkända identitetshandlingar. Mycket faller under vår blåögd godtrogenhet, där vi som företagare inte alls tyckt att det varit konstigt att kunna utfärda godkända och officiella identitetskort till våra anställda utan någon större kontroll eller inblandning från stat eller myndighet. Att utfärda och underhålla pålitliga identiteter är ett utmanande och ansvarsfullt uppdrag, oavsett om det avser traditionella fysiska ID-kort eller elektroniska och mobila identiteter. Vad är det som gör att vi litar på dem?

Balansgång

Använder vi BankID för att det är säkert eller bara för att det är smidigt? När vi pratar om identiteter är det ofta en balansgång mellan integritet, kontroll och säkerhet. Men det måste också vara smidigt, människan kommer alltid att välja den lösning som är enklast att använda. Hur kontrollerar man att en identitet är säker, eller att den ens är giltig? Det är tillräckligt svårt när man pratar om fysiska ID-kort, men det blir ännu mer komplext med de elektroniska identiteterna.

Kan man lita på utfärdaren?

Trovärdigheten av en identitet kommer från den kontrollerade utfärdandeprocessen och från den utfärdande organisationen. Enkelt förklarat: hur verifieras och kontrolleras det att du verkligen är du innan den nya, starka identiteten utfärdas. Och kan man lita på organisationen som tillverkar, kontrollerar och utfärdar den? Vågar vi bygga vår framtid på den gamla bankdosan eller på att spelombudets personal känner sitt ansvar?

Staten bör ta ansvar

Staten borde ta ett större ansvar för att säkra vår demokrati och framtid. Vi pratar, i stort, inte om bättre tekniska lösningar, utan om tydligt och oberoende ansvar.

Att alla i Sverige har tillgång till en digital ID-handling borde ses som ett samhällsansvar. Utmaningarna är stora

när det gäller svenskar med personnummer, men utmaningarna blir än större om vi pratar medborgare från andra stater som erhåller samordningsnummer hos oss. Om man vill gå i örlighetens spår finns här stora möjligheter att lura systemet. Samordningsnummer tilldelas av flera olika svenska myndigheter, med begränsad samkörning och kontroll.

Skapa en myndighet

Det hade känts tryggt om det från högsta nivå kunde beslutas om att en utvald myndighet får ansvar för att utfärda och underhålla digitala identiteter för svenskar, men även för andra som befinner sig i Sverige och har behov av att kommunicera med officiella instanser. Här skulle även utfärdande myndighet ta på sig ett större ansvar för att säkerställa att individen också får en möjlighet att verifiera vem man kommunicerar med på en myndighet och kanske framför allt känna sig trygg med att det är en "behörig" tjänsteman.

” Staten måste kliva in och ta initiativ för att säkra våra identiteter. Individens, företagets, den offentliga sektorns och till syvende och sist rikets säkerhet står på spel. Därför kan inte överlåta identitetsfrågan till slumpen.

Så kan identitet verifieras

Hur verifierar jag som enskild person att jag kommunicerar med en behörig tjänsteman? Här krävs ett tvåvägssystem som hjälper alla inblandade att verifiera både identitet och befattning. Vi ser även att det finns tydliga behov i samhället att säkert och kontrollerat kunna verifiera även annan typ av information. Ibland kanske utan att



Daniel Hjort, affärsutvecklingschef, Nexus Group.

avslöja personens identitet. Ett exempel på det kan vara vaccinationsinformation. Här kan man tänka sig att man med säkerhet vill kontrollera om någon är vaccinerad men nödvändigtvis inte vill avslöja identiteten på personen vid kontrollen.

Byggbranschen hårt utsatt

Vissa branscher är mer hårt utsatta än andra när det gäller falska identiteter. En av dem är byggbranschen med stor rörlighet av arbetskraften inom Europa. Här finns ett tydligt och starkt initiativ och ett faktiskt fungerande system för att motverka brottslig verksamhet i form av ID06. Tyvärr utmanas det av situationen med samordningsnummer och bristande kontroll och samverkan mellan myndigheter. Det leder fort till fusk och socialt utnyttjande, ökad kriminalitet samt osund konkurrens.

Allt uppkopplat är risk

Lägg därtill alla enheter som vi gladeligen kopplar mot Internet utan att försäkra oss om att de har någon form av stark identitet som kan kontrolleras. Det här berör alla, såväl privatpersoner och företag som kommuner och myndigheter. Särskilt viktigt är förstås att skydda vår kritiska infrastruktur. Vi måste exempelvis säkra vår el- och vattenförsörjning samt ha tillgång till livsmedel transporter och ha ett fungerande betalningssystem – annars blir vi väldigt sårbara.

erande betalningssystem – annars blir vi väldigt sårbara.

Utse en myndighet

Vi på Nexus välkomnar den välbehövliga nationella kraftsamling som nu görs kring cybersäkerhet för att accelerera forskning och innovation inom industri och offentlig sektor (för mer info om den, se www.cybernode.se)

När det gäller digitala identiteter för svenska medborgare och andra invånare bör en myndighet utses för att utfärda mobila identiteter som är enkla att använda. Det skulle stärka trovärdigheten om uppdraget också innefattar lösningar för att medborgare enkelt ska kunna verifiera statliga tjänstemäns rollbaserade identiteter.

Låt inte slumpen styra

Tekniska lösningar finns tillgängliga för att kunna genomföra allt detta, men det är ansvar och ägandeskap som efterfrågas. Staten måste kliva in och ta initiativ för att säkra våra identiteter. Individens, företagets, den offentliga sektorns – och i slutändan rikets säkerhet och framtid står på spel. Därför kan inte överlåta identitetsfrågan till slumpen.

Daniel Hjort
affärsutvecklingschef
Nexus Group

Tullverkets befogenheter ses över i ny utredning

Regeringen har tillsatt en utredning för att se över de regler som styr Tullverkets befogenheter att genomföra kontroller och arbeta brottsbekämpande.

Syftet är att modernisera och göra lagstiftningen mer enhetlig så att Tullverket får bättre förutsättningar att utföra sitt uppdrag.

Utredaren ska bland annat föreslå en ny sammanhållen författningsreglering för Tullverkets befogenheter gällande myndighetens kontrollverksamhet och den brottsbekämpande verksamheten. Syftet är att göra lagstiftningen mer enhetlig.

– Narkotika, sprängmedel och vapen är centrala verktyg för den organiserade brottsligheten. De ska stoppas vid gränsen. Därför har vi byggt ut Tullverket och nu tar vi ett helhetsgrepp om Tullverkets befogenheter, säger finansminister Magdalena Andersson.

Utredaren kommer även redogöra för och analysera Tullverkets befintliga befogenheter samt överväga om myndigheten behöver ges ytterligare

befogenheter och i så fall föreslå det. Det kan exempelvis handla om att möjliggöra för Tullverket att biträda Polismyndigheten i dess brottsbekämpande verksamhet i större utsträckning än i dag.

– Den organiserade brottsligheten utmanar vårt samhälle och utnyttjar samhällets svagheter. Men steg för steg tar nu samhället tillbaka initiativet. Ansvarsutkrävandet har ökat med allt fler rättegångar mot kriminella runt om i Sverige. För att skapa trygghet behöver kampen fortsätta med oförminskad styrka, säger Magdalena Andersson.

Utredare leds av före detta överåklagare Gunnel Lindberg. Uppdraget ska redovisas den 16 maj 2022.



Finansminister Magdalena Andersson.

Sms-bedrägerier mot företag ökar i västsverige

På tre månader har bedragare lurat av privatpersoner och företag i Västsverige 6,7 miljoner kronor genom sms-bedrägerier.

Det börjar med ett vanligt sms. Ofta ser det ut som att meddelandet kommer från en trovärdig avsändare, till exempel bankens spårservice eller ett inkassobolag. Den som får ett sms ombeds att klicka på en länk eller ringa upp ett nummer.

– I meddelandet, som ofta är kortfattat, vill man stressa mottagaren

genom att påstå att det till exempel skett bedräglig aktivitet på bankkontot eller att en räkning gått till inkasso, säger Elin Syberg Falguera, brottsförebyggare vid bedrägerisektionen i region Väst.

Om man ringer upp det angivna numret eller klickar på länken i meddelandet vill bedragaren att man ska använda sitt mobila BankID eller lämna ifrån sig kortuppgifter.

– Målet med sms:en är att lura av dig dina pengar genom att föra över dem till ett annat konto, köpa till exempel Bitcoins åt dem eller att skapa ett nytt BankID som de sedan kan förfoga över, säger Elin Syberg Falguera.

Över tid har antalet anmälningar

minskat – men polisen ser nu att brottsvinsterna ökar. Under januari-mars 2021 har bedragare lurat av västsvenskar 6,7 miljoner kronor. Enligt statistiken är brottsvinsterna också något högre i Västsverige jämfört med resten av Sverige.

– Vi ser en ny målgrupp för bedragarna som i högre utsträckning kontakter företag, troligen för att brottsvinsterna är större, flera hundra tusen kronor och uppåt. Vi ser även att bedragare förmår målsägare att genomföra köp av Bitcoin på olika handelsplatser.

Sms-bedrägerier underlättas också av att det är enkelt att skaffa virtuella telefonnummer samt att göra gratis massutskick av sms.



Under januari-mars 2021 har bedragare lurat av västsvenskar 6,7 miljoner kronor i sms-bedrägerier.

Så ska polisen förbättra hantering av bedrägeriärenden

Varje dag anmäls 600 bedrägeribrott och i dag är vart sjätte anmält brott ett bedrägeribrott.

Rikspolischef Anders Thornberg har beslutat om en rad åtgärder för att hantera det stora inflödet av bedrägerianmälningar. Detta efter att polisens internrevision pekade på en rad brister i handläggningen.

Bedrägeribrottslighet är ett växande samhällsproblem. Varje dag anmäls 600 bedrägeribrott och i dag är vart sjätte anmält brott ett bedrägeribrott. Många är svårutredda eftersom brotten ofta sker på distans via nätet och dessutom kan ha skett från ett annat land.

I syfte att granska polisens interna styrning och kontroll gav rikspolischef Anders Thornberg Internrevision i uppdrag att granska polisregionernas handläggning av bedrägeriärenden. Granskningen följer upp en redan tidigare genomförd granskning.

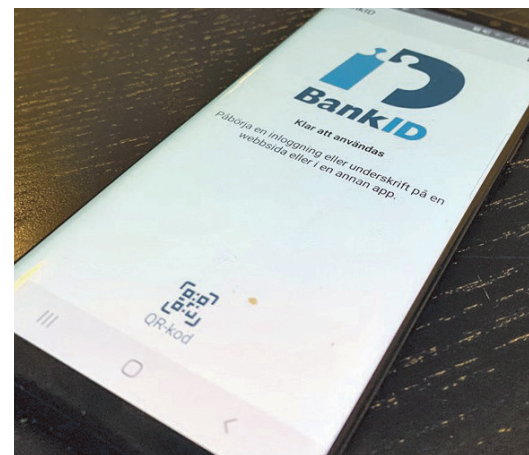
Rapporten visar brister på en rad punkter som omfattar bland annat anmälningsupptagning, utredningsåtgärder och dokumentation.

Sedan granskningen genomfördes har bedrägeriverksamheten utvecklats på flera plan menar polisen, bland annat flyttades processansvaret 2020 från Region Stockholm till Nationella operativa avdelningen (Noa) för att bedriva ett mer strategiskt och underlättat arbete mot bedrägeribrott samt utveckla samverkan mellan

regionerna.

– Polisen arbetar offensivt i flera delar för att komma åt bedragarna och minska risken för att bli utsatt för brott. Vi är medvetna om de brister som nämns i rapporten och flera åtgärder har redan satts in. Det stora inflödet gör att det inte är möjligt för polisen att utreda bort bedrägeribrotten, här krävs att flera aktörer tar större ansvar för att exempelvis skapa säkrare betalplattformar och tjänster för att försvåra för bedragarna, säger Jessica Nilsson, chef för Nationellt bedrägericenter.

I rekommendationerna till Polismyndigheten konstaterar Internrevisionen att tidigare lämnade rekommendationer fortfarande är relevanta.



Rapporten visar brister på en rad punkter som omfattar bland annat anmälningsupptagning, utredningsåtgärder och dokumentation.

Fler företagare utsätts för brott – färre anmäler

De senaste åren har andelen företagare som upplever otrygghet på grund av låg polisnärvaro ökat från 41 till 51 procent. Och sedan 2017 har andelen företagare som blivit utsatta för brott ökat från 30 till 36 procent. För företagare med anställda har vartannat företag blivit utsatt, enligt Företagarnas rapport *Brott mot företagare 2021*.

Brotten mot företag och företagare måste tas på största allvar. Det mänskliga lidandet och de ekonomiska kostnaderna är i slutändan ofta förödande, hävdar rapportförfattaren Pontus Lindström, brottsexpert på Företagarna.

Konsekvensen om företagaren till slut får nog av kriminaliteten och flyttar – alternativt lägger ner sin verksamhet – kan bli ytterst kostsam för samhället då arbetstillfällena försvinner,

menar Företagarna.

– Låt inte de högt smällande brotten förblinda för det faktum att mängdbrotten som inbrott, bedrägerier, skadegörelse och stölder är det absolut vanligaste brotten. Vi vill från politisk nivå se en nolltolerans mot den här typen av brott, säger Pontus Lindström.

Investeringar skjuts upp

Utsattheten för brott har framför allt ökat inom branscherna handel och tillverkning. De vanligaste brottskategorierna är bluffakturor, stölder, inbrott och skadegörelse.

Rapporten visar att 79 procent har fått ökade kostnader för brottsförebyggande åtgärder. 42 procent uppger att utsattheten för brott leder till att planerade investeringar har skjutits upp eller uteblivit. Andelen företagare som funderat på att lägga ner sin verksamhet på grund av brottsligheten har ökat från 13 till 19 procent.

– Att så många företagare övervägt att lägga ner sin verksamhet på grund av kriminaliteten är otroligt allvarligt. Att andelen dessutom har ökat med 6 procentenheter på bara ett år är också en dyster varningssignal, säger Pontus Lindström.

”För att företagare ska se det som meningsfullt och orka avsätta tid att anmäla mängdbrotten måste det vara tydligt att det ger resultat när man gör det.”

skatteintäkterna minskar och utanförskapet riskerar att spås på ytterligare. Därför är själva förekomsten och närvaron av lokala företag i sig både trygghetsskapande och brottsförebyggande,



Utsattheten för brott har framför allt ökat inom branscherna handel och tillverkning. De vanligaste brottskategorierna är bluffakturor, stölder, inbrott och skadegörelse.

Låg anmälningsbenägenhet

Undersökningen visar att endast var tredje företag som blivit utsatt för kriminalitet anmäler brotten till polisen och anmälningsbenägenheten har minskat.

Det innebär att delar av den offentliga statistik som presenteras regelbundet innehåller stora mörkertal. Det kan i sin tur få allvarliga konsekvenser när myndigheter och regeringsföreträdare planerar och allokera resurser utifrån underlag som ger en inkorrekt beskrivning av verkligheten, menar Företagarna som därför vill att regeringen ger brottsförebyggande rådet, Brå, i uppdrag att särskildovisa brott som drabbar företagare. Det gäller även i den Nationella trygghetsundersökningen (NTU) där det tydligare behöver framgå om

det är en näringsidkare som har blivit utsatt.

– För att företagare ska se det som meningsfullt och orka avsätta tid att anmäla mängdbrotten måste det vara tydligt att det ger resultat när man gör det, säger Pontus Lindström.

Minskad tilltro till rättsväsendet

Rapporten visar att 84 procent av de brottsutsatta företagarna upplever minskad tilltro till rättsväsendet.

– Vi identifierar en lång rad åtgärder på olika områden som vi vill se. Men på ett sätt det rätt enkelt: Fler poliser. I hela landet. Trygghet byggs över tid utifrån goda relationer mellan polisen och det lokala näringslivet, säger Pontus Lindström.

Colonial-hackarna har dragit in 750 miljoner

Hackergruppen Darkside, som misstänks för ransomwareattacken mot Colonial Pipeline, har dragit in runt 750 miljoner i bitcoin i lösensummor på sju månader.

FBI menar att hackarna bakom attacken mot amerikanska Colonial Pipeline har koppling till gruppen Darkside. Hackergruppen ska ha några dagar efter attacken meddelat att de avslutade sin verksamhet och att deras mål var att ”tjäna pengar och inte skapa problem för samhället”, skriver Computer Sweden.

Ransomware-attacken slog ut Colonial Pipelines verksamhet och det har kommit ut att företaget betalat motsvarande 42 miljoner kronor i bitcoin till hackergruppen. Darkside ska enligt Gizmodo ha fungerat som en ransomware-as-a-service-operatör som lånat ut sin skadliga mjukvara till andra.

Blockchain-analysföretaget Elliptic menar att hackare som använt sig av Darksides mjukvara har dragit in bitcoin till ett värde av sammantaget runt 750 miljoner kronor

Patientuppgifter läckta efter cyberattack

Nyligen tog sig hackare in i it-systemet för ett sjukvårdsdistrikt söder om Nya Zeelands största stad Auckland och spred patientuppgifter till bland annat mediebolag.

Flera inhemska mediebolag fick patientuppgifterna skickade till sig och skickade vidare uppgifterna till polisen. Dataintrånget har skapat problem för sjukhusen i distriktet Waikato, vilket har cirka 425 000 patienter. Bland annat har patienter fått sina behand-

lingar tillfälligt avbrutna och löneutbetalningarna har stött på problem, skriver TT.

Sjukhusen har fått övergå till manuell hantering av patienterna och journalerna och har uppmanat allmänheten att avvakta med att kontakta sjukvården vid ärenden som inte är akuta.

Myndigheterna kommenterar inte om hackarna har kommit med några krav. Regeringen har dock sagt sig våga betala någon form av lösensumma.

Överbelastningsattacker mot Region Gotlands webbsida kostade 1,6 miljoner kronor

Mellan den 27 januari till 21 mars utsattes Region Gotlands webbsida gotland.se för överbelastningsattacker. Kostnaden för skattebetalarna blev 1,6 miljoner kronor.

Kostnaderna täckte konsulter, teknisk utrustning och eget arbete enligt SVT. Digitaliseringsdirektör Anders

Granvald tycker inte att erfarenheterna är värda 1,6 miljoner kronor.

– Jag hade mycket hellre skaffat den här lärdomen för tio kronor, säger han till SVT.

Region Gotland har inte upplevt några mer attacker sedan 21 mars.



Hamntillsyn i skärgården ska minska båtstölderna

Båtstölder är ett växande samhällsproblem och varje år stjäls båtar och båtmotorer för över 300 miljoner kronor. Trots den negativa utvecklingen saknas tillräckligt med konkreta åtgärder för att komma till rätta med problematiken, menar Larmtjänst. Hamntillsyn är dock ett initiativ som syftar till att öka säkerheten i svenska småbåtshamnar.

Nu går ledande aktörer i försäkringsbranschen samman med Team Marin och lanserar Hamntillsyn för ökad trygghet i småbåtshamnar över hela landet.

Sverige är ett av de värst drabbade länderna i Europa när det gäller båtrelaterade stölderna. Stölderna genomförs nästa uteslutande av internationella stöldligor.

Pandemin bakom färre stölderna

Under 2020 polisanmälades 5 115 stölderna av båtar, båtmotorer och annan utrustning från båtar. Detta är visserligen en liten minskning jämfört med året innan, vilket sannolikt beror på att de internationella stöldligornas härjningar tillfälligt minskade när gränserna stängdes under pandemin. Risken är dock stor att stölderna tar fart igen när det blir lättare för ligorna att röra sig över gränserna igen, menar Larmtjänst. Kostnaderna för de båtrelaterade

stölderna uppgår till uppskattningsvis 300 miljoner kronor årligen.

Väktare på vattenskotrar

Hamntillsyn är ett brottsförebyggande initiativ som lanseras av If, Trygg-Hansa, Svenska Sjö, Atlantica, Team Marin och Securitas och genomförs i samarbete med Larmtjänst. Den branschgemensamma satsningen möjliggör bevakning med väktare på vattenskotrar i svenska småbåtshamnar under sommarhalvåret i syfte att minska förekomsten av båtrelaterade stölderna.

– De internationella stöldligornas härjningar skapar otrygghet och stora kostnader. Hamntillsyn är ett konkret initiativ för att bidra till ökad trygghet för båtägarna. Samtidigt vill vi uppmärksamma problemet med stölderna som drabbar båtägare. Vi önskar att regeringen och berörda myndigheter tillsätter mer resurser och vidtar åtgärder som kraftfullt och långsik-



Under 2020 polisanmälades 5 115 stölderna av båtar, båtmotorer och annan utrustning från båtar.

tigt motverkar problemet med internationella stöldligor. Den nya lagen som ger Tullen vissa befogenheter att ingripa vid utförelse av stöldgods från den 1 augusti är ett steg i rätt riktning men långt ifrån tillräckligt, säger Mats Galvenius, vd på Larmtjänst.

Drabbar samhället hårt

Stölderna av utomhusmotorer är ett stort problem och värdet på de stulna objekten ökar. En vanlig utombordsmotor kostar i dag runt 100 000 kronor och under sommarmånaderna stjäls båtmo-

torer för en miljon kronor om dagen.

– Stöldligornas härjningar får stora negativa konsekvenser i samhället. Många båtägare blir brottsoffer, vilket skapar otrygghet och bidrar till att tilliten i samhället minskar. Dessutom riskerar båtägare att långsiktigt drabbas av högre försäkringspremier. Försäkringsbranschen vill bidra till att motverka denna utveckling. Det krävs konkreta insatser och Hamntillsyn är ett bra komplement till Båtsamverkan för att öka tryggheten för fritidsbåtsägare ytterligare, fortsätter Mats Galvenius.

Lyckad internationell insats mot stöldligor

I en EU-insats som genomfördes synkroniserat i flera polisregioner mellan den 13 och 16 april i lyckades polisen frihetsberöva 22 personer.

Aktionen bestod av olika typer av insatser och kontroller. Polisen samverkade också med en rad andra svenska myndigheter – Tullverket, Kronofogden, Kustbevakningen, Skatteverket och Arbetsmiljöverket.

Insatsen skedde inom ramen för EMPACT-samarbetet och var inriktad mot gränsöverskridande organiserad stöldbrottslighet. Polis och andra samverkande myndigheter arbetade synkroniserat i flera länder.

200 personer frihetsberövades

Sammanlagt har över 200 personer frihetsberövats på olika platser i Europa, varav 22 i Sverige. De misstänks bland annat för olika typer av stölderna, till exempel stölderna av bildelar och båtmotorer samt inbrottsstölderna. Flera personer greps också misstänkta för narkotikabrott och penningtvätt.

– De som nu är gripna skulle annars sannolikt ha varit på fri fot och stöldgodset transporterat ur landet, säger Bengt Grönlund, som varit nationella operativa avdelningens (Noa) operativa ledare för insatsen. Att polisregionerna arbetar metodiskt och synkroniserat mot samma mål gör svensk polis mycket effektiv och försvarar för de kriminella.

Underrättelsebaserad insats

Polisarbetet bedrevs underrättelsebaserat och under insatsen genomfördes också kontroller av bland annat omkring 1 400 fordon. 14 av fordonen omhändertogs, bland annat eftersom förarna saknade körkort eller på grund av ägarnas skulder till Kronofogden.

Dessutom skedde flera riktade kontroller vid olika gränspassager, vilket resulterade i att flera personer också avvisades från Sverige.



Sammanlagt har över 200 personer frihetsberövats på olika platser i Europa, varav 22 i Sverige, i den samordnade insatsen.

– Att flera svenska myndigheter samverkar inom ramen för EMPACT och dessutom genomför insatser tillsammans med andra länder och Europol ger en styrka i brottsbekämpningen. Brottsligheten är internationell och svensk polis ser samma gränsöverskridande utmaningar som andra länder

inom EU och det är avgörande att vi har en internationell samverkan. Den insats som nu genomförs är ett bra exempel på att vi inom EU är starka tillsammans, säger Håkan Wall, chef Polismyndighetens internationella enhet vid Noa och Sveriges EMPACT-koordinator.

Vem kan man lita på? – hur får vi reda på det?

I en allt mer uppkopplad värld finns det inget som är mer viktigt än att kunna säkerställa identiteten. Därför kan man säga att säkerställd identitet är trygghetens hårdvaluta.

Varje dag begås en enorm mängd olika typer av IT-relaterade brott. Här inryms allt från bedrägerier till utpressning. En gemensam nämnare är att offret vanligen inte har kontrollerat identiteten på den som har ringt upp eller avsändaren bakom ett mejl eller en webbsida. Tilliten eller underlåtenheten att kontrollera avsändarens identitet möjliggör för kriminella att enkelt utföra en allt för lönsam brottslighet.

Tryggare Samhälle har talat med några experter och företrädare för IT-säkerhetsbranschen om hur dagens cyberbrottslingar agerar och vilka metoder som används samt hur företag och privatpersoner kan skyddas från att drabbas av brott som bygger på att offret lurats av en falsk identitet.

Social manipulation

– ett effektivt verktyg för att begå brott

Begreppet social manipulation används ofta som metod för digitala bedrägerier och är effektivt för att få människor att hantera sin data eller sina privata konton ovarsamt.

Tryggare Samhälle har pratat med Per Klingvall, rådgivningschef på SSF, om social manipulation och om bedrägerikategorier där denna teknik används samt om vad man ska tänka på för att undvika bli ett offer för den.

Text: Lennart Alexandrie

Social manipulation har genom historien även använts för att driva in skatter, i förhörsteknik inom brottsbekämpning samt inom journalistiken som ett sätt att få svar på känsliga frågor. Social manipulation bygger på forskning inom psykologi, och kunskap om mänskliga reaktioner och beteenden.

– Genom att utnyttja denna kunskap kan bedragare få oss att lämna ut information som vi egentligen vet att vi måste skydda. Hur säkra våra lösenord och säkerhetssystem än är kvarstår den mänskliga faktorn som en risk för att cyberbrottslingar kan komma åt känsliga uppgifter eller privata konton, säger Per Klingvall, rådgivningschef på SSF.

Det finns flera olika tillvägagångssätt och tekniker som används för att lura människor med hjälp av social manipulation, och bedrägerierna sker till största del via röstsamtal (vishing), men också via annat nätfiske (phishing), som till exempel e-postmeddelanden och sms.

Befogenhetsbedrägeri

Den allra vanligaste typen av social manipulation är att utge sig vara från en myndighet eller bank, och på så sätt utnyttja sin ställning som en auktoritet för att få personer att lämna ifrån sig viktig information eller privata uppgifter. Detta kallas mer specifikt för ett befogenhetsbedrägeri.

– Personen som ringer påstår sig ofta vilja hjälpa dig att skydda eller verifiera

dina konton. Du uppmanas därför att logga in på din internetbank eller BankID, där du i själva verket genomför överföringar eller betalningar till bedragarens konto, förklarar Per Klingvall.

– Med samma motiv kan bedragaren skapa falska e-postadresser och skicka ut meddelanden som ser ut att komma från en bank, ett företag eller annan myndighet. I dessa mejl uppmanas du att lämna ut uppgifter via länkar till falska sidor, eller ladda ned bilagor som i själva verket består av skadlig kod som infekterar din dator. Liknande utskick med falska länkar sker även via sms.

Hur säkra våra lösenord och säkerhetssystem än är kvarstår den mänskliga faktorn som en risk för att cyberbrottslingar kan komma åt känsliga uppgifter eller privata konton.

Romansbedrägeri

Romansbedrägerier är en välkänd kategori brott som baseras på social manipulation. Genom att skapa en falsk

profil – i regel på en dejtingsajt – försöker bedragare vinna andra medlemmars hjärtan för att lura till sig pengar i transaktioner. Dessa profiler brukar påstå sig arbeta med spännande och attraktiva yrken, ofta internationellt, och bedrägeriet kan pågå flera månader eller till och med år. Plötsligt dyker frågan om pengar upp i sammanhanget och du kan bli ombedd att genomföra transaktioner till utlandet för att hjälpa personen ur en knivig situation

– Offret manipuleras genom att utnyttja känslor av förtroende och kärlek. De kan vara oerhört skickliga manipulatorer som vet precis vilka strängar de ska spela på för att locka in människor i förälskelse. Ofta ligger organiserad brottslighet bakom dessa falska profiler, säger Per Klingvall.

Investeringsbedrägerier

Vid investeringsbedrägerier utnyttjas människors förhoppningar och drömmar om ekonomisk vinning. Investeringsbedrägerier sker både mot privatpersoner och mot företag.

– Du blir kontaktad av någon som uppmanar dig att investera i en kryptovaluta, råvara eller företag med helt otrolig avkastning. När du investerar försvinner pengarna spårlost. Även här kan bedrägeriet äga rum under en lång tid, med diverse manipulativa försök att övertala dig till att du måste investera direkt för att ta del av denna unika möjlighet, kommenterar Per Klingvall.

– Många investeringsbedrägerier fortsätter även efter att du har investerat, och du kan till och med hänvisas till en sida där du tror dig se hur pengarna växer.

Enkla riktlinjer för att skydda sig

Per Klingvall betonar att bedragarna kan vara oerhört skickliga manipulatorer och drabba såväl privatpersoner som företagare. Han menar dock att tydliga regler kring vilka uppgifter vi är beredda



Per Klingvall, rådgivningschef på SSF.

att ge ut till en annan part gör det enkelt att inte låta sig luras.

– Det spelar i själva verket ingen roll om det är banken eller polisen som kontaktar dig, du ska aldrig lämna ut privata uppgifter eller logga in på ditt BankID efter uppmaning från någon annan. Om du känner dig det minsta osäker kan du alltid kontakta banken eller myndigheten själv för att höra huruvida informationen verkligen stämmer eller inte, säger han.

För romans- och investeringsbedrägerier gäller ett ganska generellt råd.

– Om det verkar för bra för att vara sant är det förmodligen så det är. Genom att vara källkritisk och söka efter bilder, personer och uppgifter i ditt sökverktyg online, kan du skaffa dig en ärligare bild av vad det är som försiggår. Om du misstänker att någon försöker manipulera dig för att lura dig på pengar eller andra känsliga uppgifter ska du alltid polisanmäla händelsen, säger Per Klingvall avslutningsvis.

Experten: "Deepfake-bedrägerier är snart här"

Om personen i bild ser ut precis som ditt företags vd och låter precis som ditt företags vd, kommer du då tveka att göra den överföring av pengar som hen ber om?

Deepfake är precis i startblocken för att börja användas vid bedrägerier, menar säkerhetskonsulten och författaren Åsa Schwarz.

Text: Henrik Söderlund

Deepfake kommer från "deep" som syftar på deep learning (maskininlärning) och "fake" och innebär till exempel att ansiktet på en person i ett videoklipp byts ut en annan person. Dessutom kan maskininlärning som används för deepfake återskapa röster.

Senast i raden av virala deepfake-videos som fått mycket uppmärksamhet var ett klipp på "Tom Cruise" som utför ett trolleritrick. Det är ingen tvekan om att tekniken blivit bättre och bättre och det blir allt svårare att urskilja vad som är fejk och vad som är på riktigt. Redan för tre år sedan spreds ett klipp på "Barack Obama" som verkade autentiskt. I maj i år rapporterades om att parlamentsledamöter i flera länder i Europa deltagit i fejkade videomöten med vad de trodde var den fängslade ryske oppositionspolitikern Aleksej Navalnyjs stabschef. I själva verket utsattes de för deepfake.

Just nu finns det framförallt exempel på ljudbedrägerier, alltså att man låtsas vara någon annan och på så sätt får någon att auktorisera utbetalningar.

Nästa steg är bedrägerier

– Deepfake har använts mycket i propaganda men det har börjat övergå mer till bedrägeriverksamhet. Just nu finns det framförallt exempel på ljudbedrägerier, alltså att man låtsas vara någon annan och på så sätt får någon att auktorisera utbetalningar, säger Åsa Schwarz.

Hon menar att vi är på väg in i en tid då den här typen av bedrägerier kom-

mer att bli allt vanligare.

– Det första ljudbedrägeriet som jag känner till är två år gammalt. Det har nått nivån att man inte längre hör skillnaden om det är en människa eller maskin som ringer, säger Åsa Schwarz.

Och nästa steg är att även video kommer att användas.

– Jag ser framför mig att det ganska snart kommer att komma bedrägeriförsök med deepfake-video. Det är kanske något år bort. Jag tror att vi är på väg in i en situation där vi snart kommer bli uppringda på Teams och vi kommer att tro att det är en person vi känner men i själva verket är det någon annan, säger hon.

En deepfake behöver inte nödvändigtvis låtsas vara en väldigt känd person. Åsa Schwarz betonar att det finns bilder, ljudfiler och ofta video på till exempel olika börs-vd:ar. Tekniken kan få det att både se ut som och låta som vd:n.

Och det behöver inte ens vara en särskild person, det kan handla om support-bedrägerier där till exempel en server ringer upp utan att någon person medverkar men att maskinen låter som en människa och ställer frågor för att ta reda på till exempel känslig information eller företagshemligheter.

Dubbelkolla identiteten

Åsa Schwarz menar att det i nuläget krävs en viss IT-vana för att skapa deepfake men hon tror att det inom något år kommer att finnas applikationer för att skapa deepfake som vem som helst kan använda.

Hon tror att det är två kategorier av måltavlor som framför allt kommer att drabbas av deepfake-bedrägerier: specifika mål där bedragarna kan tjäna väldigt mycket pengar samt äldre och datorovana personer.

– De kommer tro att det är barnbarnen som ringer och ber dem om att göra en överföring när det inte är



Säkerhetskonsulten och författaren Åsa Schwarz.

barnbarnen säger hon.

Hennes tips till privatpersoner är att alltid dubbelkolla.

– Om ett barnbarn säger i chatten att du ska föra över pengar så kanske du ska ringa till barnbarnets telefon och dubbelkolla att det är rätt person du pratar med. Sedan kommer det säkert att vara svårt att vara misstänksam om det är ett videosamtal och ser ut och låter som en person som man vet vem det är. I dagsläget skulle nog de flesta gå på det, säger hon.

Måste inte handla om pengar

Företag å andra sidan behöver se till att ha bra rutiner så att det inte går att attestera och betala ut fakturor på ett osäkert sätt.

– Företag bör inte auktorisera saker bara genom telefonsamtal eller video utan de måste auktorisera på andra sätt. Ofta kan det vara så att någon ringer och påstår att den står på en flygplats någonstans och behöver göra en brådskande överföring och kringgå rutinerna. Men det ska inte gå att kringgå rutinerna på det sättet.

Hon betonar också att målet inte alltid är pengar utan syftet kan också

vara att lura till sig information eller lösenord för att få tillgång till organisationens IT-system.

Så kallade vd-bedrägerier har ofta gått till så att en medarbetare får ett mejl från en mejladress som ser ut som det egna bolagets vd, till exempel med en uppmaning om att göra en utbe-

Det första ljudbedrägeriet som jag känner till är två år gammalt. Det har nått nivån att man inte längre hör skillnaden om det är en människa eller maskin som ringer.

talning. När detta övergår till att vara ett telefonsamtal istället för ett mejl och personen låter precis som vd:n så kommer det att kännas mer trovärdigt, varnar Åsa Schwarz.

– Och nästa steg är videosamtal, avslutar hon.

David Jacoby, Deputy Director European Global Research and Analysis Team på Kaspersky:

"Automatiserade bedrägerier ett växande hot"

Nästan hela den digitala brottsligheten är numera mer eller mindre automatiserad, menar IT-experten David Jacoby, Deputy Director European Global Research and Analysis Team på Kaspersky och senior säkerhetsforskare.

– All form av ny teknik utnyttjas av kriminella, säger han apropå automatiserade bedrägerier.

Text: Henrik Söderlund

Än så länge används i regel inte robotar vid bedrägerier. Däremot script, eller program som kopplas upp till olika chattfunktioner och fungerar som chatbotar, menar David Jacoby.

– De är ganska statiska och ger automatiserade svar, men kan knappast kallas för intelligenta.

Svaren är inte baserade på vad du skriver till den. Däremot tror jag att det är något som vi kommer att få se mer av framöver, säger han.

Flyttar kommunikationen

Ett exempel på när kriminella använder chatbotar är för att svara på Blocket-annonser. Ett vanligt förfarande är att personen som försöker sälja något får ett svar där motparten vill flytta

kommunikationen till Whatsapp,

”Det är organiserad brottslighet som håller på med det här. De bygger systemen och precis som med spam och phishing-mejl så kan de använda till exempel Google translate för att skapa databaser på olika språk

Telegram eller något annat chatprogram.

– Först görs någon typ av profilering på vem du är: man eller kvinna, om du har sålt något på Blocket tidigare och så vidare och sedan kan den kommunicera med dig, men det är ofta ganska statiska saker. Det fungerar ungefär som chatbotar som du ser på olika hemsidor

”Jag tror att det här är ett hot som kommer att öka i framtiden. Det blir mer och mer intelligenta chatbotar.

som kan identifiera att om du skriver någonting och avslutar med ett frågetecken så får du ett visst typ av svar, eller om du skriver till exempel ”kreditkort” eller Pay Pal – så vet den att när det ordet kommer så ska den svara på ett visst sätt, säger David Jacoby.

Blir smartare

Han menar att det är ganska enkelt att skapa den typen av script och att det ibland kan verka relativt trovärdigt: de är programmerade för att kunna ställa ”rätt” frågor och när vi köper saker online, till exempel via Blocket, så ställer de flesta personer liknande frågor. Exempel på det kan vara att få se varan på bild, priset, hur den ska levereras etc.

– Jag tror att det här är ett hot som kommer att öka i framtiden. Det blir mer och mer intelligenta chatbotar, säger David Jacoby.

Vill stjäla kortuppgifter

Syftet med denna typ av automatiserade bedrägerier kan vara att få en person att föra över pengar eller att tvätta pengar, men också att komma över kortuppgifter eller infektera personen med skadlig kod. Bedragaren kommunicerar till exempel att den ska betala frakten vid en Blocket-försäljning men några pengar förs inte över utan till en tredje part, till vilken säljaren får en länk för att hämta sina pengar. I själva verket stjälar bedragaren kortuppgifter genom att låta säljaren tro



IT-experten David Jacoby, Deputy Director European Global Research and Analysis Team på Kaspersky och senior säkerhetsforskare.

att den måste fylla i dem för att få ut sina pengar.

Även om den automatiserade konversationen sker på svenska så betyder det inte att det är svenskar som ligger bakom.

– Det är organiserad brottslighet som håller på med det här. De bygger systemen och precis som med spam och phishing-mejl så kan de använda till exempel Google translate för att skapa databaser på olika språk, säger David Jacoby.

I februari rapporterades om ett ökat antal Blocket-bedrägerier.

– Det är sofistikerat och uppenbart gjort av personer med stora resurser, sa Blockets kundsäkerhetschef Daniel Mars.

Genom att skriva att köparen (chatboten) befinner sig i en annan stad fick chatboten säljaren att tro att den är beredd att betala för frakten. När sedan kommunikationen flyttats till Whatsapp skickades en länk till fejkisidan blocket-pay.com där säljaren skulle fylla i sina kortuppgifter. De som gjorde det riskerade att få sitt bankkort kapat.

Utnyttjar tekniken

David Jacoby berättar att kriminella ser bedrägerier som en vilken annan affärsidé som helst och affärsidéer blir bättre om man effektiviserar och det görs genom automatisering.

– Det är automatiserade processer som skannar efter kända lösenord, det är automatiserade processer som skannar efter sårbarheter och det är automatiserade processer som skickar ut mejl. Det är ingen som sitter och gör det där manuellt utan de automatiserar så mycket som möjligt, säger han.

David Jacoby tror också att kommunikationen vid bedrägerier kommer att automatiseras inte bara i text utan även genom ljud – det vill säga att ”någon” pratar.

I övrigt ser han ingen tydlig trend vad gäller bedrägerier på nätet.

– Förutom att det aldrig tar slut. Den digitala brottsligheten kommer bara att fortsätta och det kommer bara att bli mer och mer. All form av ny teknik utnyttjas av kriminella, avslutar han.

SECTECH 20år

EXPO & SEMINARS

Event: Sectech

Plats: Stockholmsmässan

Tid: 27 – 28 oktober 2021

Profil: Utställning/seminarier med fokus på teknikbaserade säkerhetslösningar.

Monterbokning:
Deniz.Baykal@armedia.se

Visst finns det ett liv efter pandemin – välkommen till vårt 20-årsjubileum

Det första Sectech-eventet ägde rum i Stockholm 2001 och sedan dess har säkerhetsmässan arrangerats med två års intervall i alla de tre skandinaviska huvudstäderna – totalt blir det 28 gånger.

Den 27 – 28 oktober öppnar Sectech på nytt. För den 29:e gången inbjuds fackbesökare till en inblick i det allra senaste när det gäller teknikbaserade säkerhetslösningar. Med gjorda pandemi-anpassningar kommer representanter från säkerhetsmarknadens alla led äntligen kunna mötas för att nätverka och bli den mest väsentliga delen av eventets 20-årsjubileum.

Ett arrangemang av:

armedia
...we are security



Stockholmsmässan

Entréspanzor:

seriline

AR Media International AB, Västberga Allé 32, 126 30 Hägersten, tel 08-556 306 80, www.armedia.se, www.sectech.se

Identifiering åt båda håll ska minska bedrägerier

Privatpersoner kan identifiera sig mot myndigheter och företag genom BankID. Men omvänt: hur ska en någon kunna veta om det verkligen är läkaren, banken eller myndigheten som ringer?

– Det är en fläck på kartan, man har glömt bort det här med säkra samtal, säger Lisa Hasselgren, en av grundarna till SecurifiD.

Text: Henrik Söderlund

Lisa Hasselgren har en bakgrund som projektledare inom IT-branschen och fick idén till SecurifiD efter att ha varit vittne till ett slagsmål som hon filmade och fotade med sin telefon.

– När polisen kom till platsen så stack alla bråkstackarna åt varsitt håll och jag gick hemåt. När sedan en ung kille ringde från inget upprignings-id och sa att han var polis så blev jag misstänksam. Dels för att killarna hade gett mig fingret då de såg att jag fotade och filmade, dels för att de hade gått förbi mitt hus innan och visste var jag bodde, säger hon.

Vill skapa säkra samtal

Det visade sig till slut vara polisen som hade ringt, men tvekan födde en affärsidé.

– I dag är det inget konstigt alls i samhället att privatpersoner måste identifiera sig gentemot företag och myndigheter. Vi använder BankID nästan dagligen för olika syften och tjänster. Men åt andra hållet – att en person som är kopplad till en organisation också ska kunna identifiera sig i ett samtal, det fanns det faktiskt ingen

tjänst för, säger Lisa Hasselgren.

Tillsammans med Jens Björkander startade hon SecurifiD som är en identifieringsportal och app som möjliggör att två parter kan identifiera sig i ett och samma gränssnitt.

– Syftet med vår tjänst är att skapa

” Om någon ringer och säger att han eller hon är läkare, hur ska du veta att det verkligen stämmer? Eller en bank.

säkra samtal. Det kan vara när man pratar i telefon eller när man träffas fysiskt. Och man är oberoende av vilken metod man använder sig av för att styrka sin identitet, till exempel BankID, Microsoft 365 eller Freja, säger Lisa Hasselgren.

Identitetens betydelse har ökat

Identiteten och att kunna styrka den har blivit allt viktigare. Det som kallas fysisk och logisk säkerhet har flutit samman allt mer – alltså att till exempel passerkortet som du använder för att öppna en dörr också används när du ska logga in i företagets eller organisationens dator. Under pandemin har den pågående digitaliseringen accelererat och den digitala identiteten har fått allt större betydelse. Hemarbete och inloggnings på distans har gjort att verifiering av identiteten kanske blivit viktigare än någonsin tidigare.

BankID lanserades 2003 när bankerna insåg att det var avgörande att kunna identifiera sina privatkunder digitalt. E-legitimationstjänsten Freja lanserades ett par år senare men det är först nu som allt fler börjar inse att även företag och organisationer behöver kunna styrka sin identitet, menar Lisa Hasselgren.

Lätt att luras

Det finns en rad olika sätt för bedra-



Lisa Hasselgren och Jens Björkander, grundarna till SecurifiD.

gare att få ett telefonnummer, mejl, sms eller annat att se ut som om det kommer från ett seriöst företag eller en myndighet. Fenomenet kallas för spoofing och Lisa Hasselgren menar att det i dag är väldigt enkelt att utge sig för att vara någon annan än den man är.

– Om någon ringer och säger att han eller hon är läkare, hur ska du veta att det verkligen stämmer? Eller en bank. Vi såg även tidigt att det finns ett behov av identifiering för business to business. Socialtjänsten och polisen är ett exempel, de delar information med varandra dagligen utan att säkert veta att personen de kommunicerar med verkligen är den som den utger sig för att vara, säger Lisa Hasselgren.

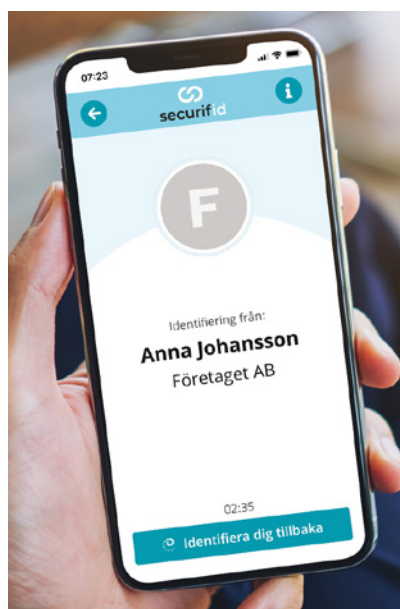
Ett annat exempel är att någon ringer och utger sig för att vara från IT-avdelningen på den egna myndigheten eller företaget och behöver access till personens inloggning i IT-systemet för att lösa ett problem som uppstått eller liknande. Ett annat är

att ”vd:n” på bolaget hör av sig till någon på ekonomiavdelningen och behöver hjälp med en skyndsam överföring av pengar.

” Syftet med vår tjänst är att skapa säkra samtal. Det kan vara när man pratar i telefon eller när man träffas fysiskt.

Lisa Hasselgren är helt övertygad om att det framöver kommer ses som en självklarhet att myndigheter och företag ska kunna identifiera sig både i kontakt med privatpersoner och med varandra och på så sätt visa att de inte är någon bedragare.

– Det blir en konkurrensfördel att som företag kunna styrka sin identitet. Jag tror att allt fler inser att det är viktigt att deras kunder ska känna sig trygga med att veta vem de pratar med, avslutar Lisa Hasselgren.



En person som är kopplad till en organisation också ska kunna identifiera sig i ett samtal.



Enabling
trusted
identities



Lisa
Andersson



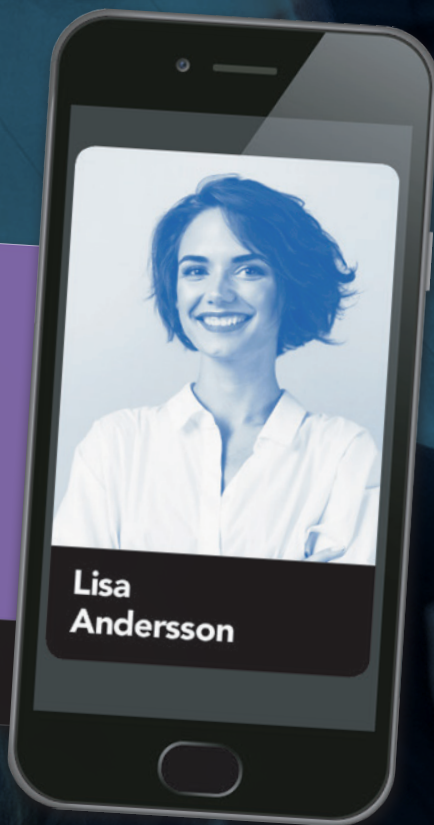
Johan
Eriksson



VISITOR



SECURITY



Lisa
Andersson

Automatisera hanteringen av ID-kort och mobila IDn!

Nexus GO Cards – en onlinetjänst för att snabbt och enkelt beställa och hantera ID-kort, mobila IDn, nyckelbrickor och tillbehör.

Aktivera tjänsten och få alla produkter skräddarsydda med företagets färger och logotyp, kodade och klara att användas!

customerservice@nexusgroup.com
Tel: 010 33 33 707

nexusgroup.com

SSF rekryterar ny utbildningschef

Säkerhetsbranschen upplever de största förändringarna på decennier. Nya tekniker, nya sätt att begå brott och stölder, samt en ström av information från aktörer som påverkar framtidens affärer ställer nya krav på ökad transformation och utveckling.

SSF tar nu steget för att möta omvärldens krav på kompetensutveckling kring detta och rekryterar ny utbildningschef.

Ulrica Heinrich tillträdde som ny utbildningschef i början på maj. Hon kommer närmast från Swedbank där hon har arbetat som utbildningsexpert. Dessförinnan har Ulrica arbetat som utbildningschef och utbildningsansvarig inom IT-säkerhet och utbildning. Dessa erfarenheter tror hon kommer att komma Stöldskyddsforeningen till nytta, då det gäller öka medvetenheten kring utbildningar och öka försäljningen av kompetensutveckling.

Kunskap allt viktigare

Nu när hoten ökar mot organisationer och privatpersoner i form av brott både på nätet såväl som fysiskt, så är kunskap ett viktigt led och därför stärka företaget utbildningsutbud och kompetensutveckling mot dessa områden.

– Jag ser verkligen fram emot att börja på Stöldskyddsforeningen och att

få jobba försäljningsinriktat och kundstyrt. Det skall bli spännande att få lära mig mer om kundernas behov och perspektiv och driva fortbildning mot deras kompetenskrav, säger Ulrica Heinrich.

Skräddarsydd utbildning

SSF är mitt uppe i en stor digital förändring, vilket innebär att utbildningsutbudet blir ännu mer flexibelt och styrt av kundbehov. Alla utbildningar i kurskatalogen går att få skräddarsytt efter organisationens behov. Det ger en stor variation och kunden kan vara med och utforma innehållet, lärandesätt och pedagogisk nivå direkt i kommunikation med utbildningsenheten.

– Målet är ju att vår utbildningsverksamhet ska vara en kunskapskälla och en mötesplats för företag och organisationer inom SSF:s områden. Utbildningsverksamheten innefattar distans, digitala och öppna kursutbildningar, så det är ett brett och intressant utbildningsutbud att välja ifrån, säger den nyrekryterade utbildningschefen.



Ulrica Heinrich tillträdde som ny utbildningschef i början på maj.

Rapport från säkerhetskollen.se

Hälften av e-postadresserna har varit exponerade i olika läckor

SSF driver tjänsten säkerhetskollen.se där man får råd och tips om hur man kan förebygga digitala brott

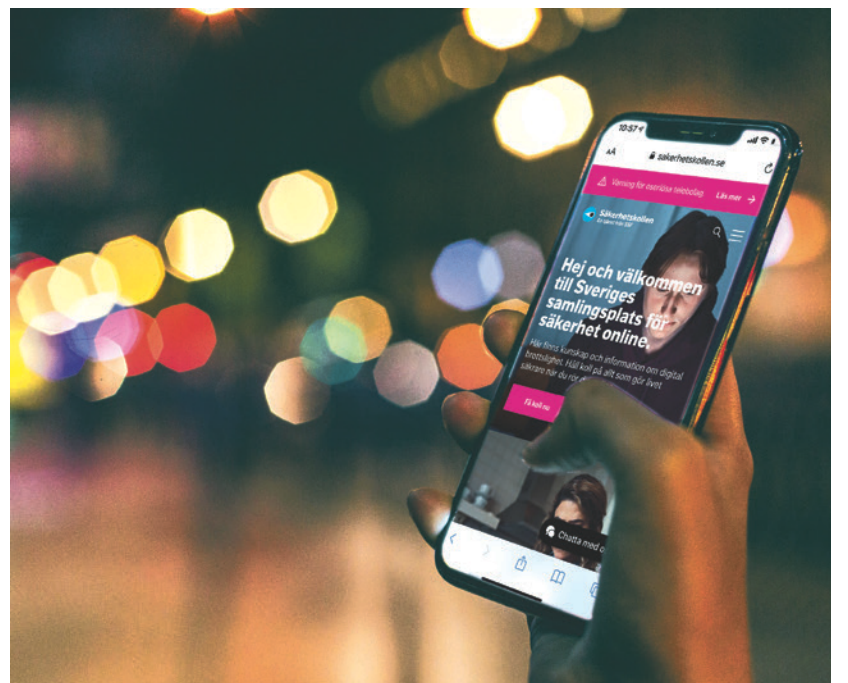
På webbsidan kan man också testa om en e-postadress varit exponerad i någon dataläcka. Av de 45 000 adresser som testats har 22 500 varit exponerade i någon läcka vilket är hälften av alla som testats.

Det förekommer ett stort antal intrång i olika databaser runt om i världen för att få tag på personliga uppgifter som kan användas i kriminellt syfte. Det kan vara kortuppgifter som sen används för att handla på olika e-handelssajter eller användarnamn och log in till olika konton som sen används för exempelvis dataintrång. Enligt den välrenommerade sidan haveibeenpwned.com hade fram till slutet på maj mer än 11 miljarder konton blivit exponerade i någon läcka. Av dem hade mer än 200 miljoner blivit postade på exempelvis Darknet där kriminella kan komma åt

dem. Idag är ofta kontouppgifter krypterade med olika krypton men det gäller tyvärr inte alla. Har e-postadressen blivit exponerad finns det också en risk att man kommer åt andra uppgifter eftersom e-postadressen oftast används som användarnamn.

– Gå in och testa era e-postadresser på säkerhetskollen.se för att se om den blivit exponerad. Har den det så se till att byta lösenord på det exponerade kontot, och på alla andra konton också där man eventuellt flernämnt lösenordet, säger Per Klingvall, rådgivningschef på SSF.

Testar man sitt lösenord på säkerhetskollen.se så får man omedelbart reda på om den funnits i någon läcka och vilket konto som blivit exponerat. Där får man även förslag på åtgärder som man ska vidta för att undvika att någon kan använda kontot.



Testar man sitt lösenord på säkerhetskollen.se så får man omedelbart reda på om den funnits i någon läcka och vilket konto som blivit exponerat.

www.säkerhetskollen.se



Illustration: Tumisu / Pixabay

Norm för IoT-produkter klar

Nu finns en norm/standard för att kunna integrera IoT-krav i befintliga och kommande SSF Normer, exempelvis SSF 3523 Digitala Låsenheter.

Med "SSF 1120 IoT uppkopplade enheter – Krav och provning" har SSF introducerat en svensk norm avsedd för klassning, krav och provning av uppkopplade enheter och datainsamlade sensorer.

Det har under en längre tid funnits ett stort behov av att kunna erbjuda konsumenter, försäkringsbolag med flera ett sätt att enkelt kvalitetsbedöma IoT-produkter.

Målet med normprojektet var att publicera en norm med relevanta krav på IoT produkter som via provning onormch certifiering bidrar till en ökad säkerhet och kunskap, samt möjlighet

till märkning av certifierade produkter för att underlätta val av IoT produkt för konsument och brukare.

– Viktigt i arbetet med normen var att en uppfyllnad av kraven i normen skulle innebära att man också uppfyller de certifieringsbara kraven "Provisions" i ETSI EN 303 645, säger Mats Moberg, normchef vid SSF.

Normens ursprung är ett samprojekt mellan SSF Stöldskyddsforeningen, och F-Secure AB. Fakta, underlag och diskussioner för att få till kravtexter i normen har bland annat inhämtats från ETSI European Telecommunications Standards Institute, NCSC UK National Cyber Security Centre, NIST, National Institute of Standards and Technology i USA samt olika testlaboratorier, penetrationstestare med flera.

– I arbetsgruppen för denna norm har det deltagit en rad mycket kompetenta experter inom området. Flera av dessa med en lång expertkunskap inom kravskrivande, provning, provningskriterier och internationellt samarbete inom området, säger Thomas Brühl, vd på SSF.

Ny SSF-norm definierar krav på certifieringsorgan

Allt fler certifieringsorgan utfärdar eller önskar utfärda certifikat mot krav i SSF:s normer. För att uppnå kvalitet och lika villkor har normen "SSF 1130 Certifieringsorgan – Krav" tagits fram.

Arbetsgruppen som tagit fram normen har bland andra innefattat representanter från – förutom SSF – Svensk Försäkring samt olika försäkringsbolag, myndigheter, organisationer och företag.

Normen "SSF 1130 Certifieringsorgan – Krav" visar vilka krav som anses nödvändiga på ett certifieringsorgan för att säkerställa att utfärdade certifi-

kat ska vara utfärdade på ett så lika och kvalitetssäkrat sätt som möjligt. Detta för att kunder och aktörer på marknaden inte ska behöva tvivla på certifikats innehåll och seriositet.

Normen innehåller krav på certifieringsorgan som i sin verksamhet utfärdar certifikat baserade på SSF:s normer. Normen innehåller komplettering eller förtydligande till kraven i SS-EN ISO/IEC 17021 (Ledningssystem), SS-EN ISO/IEC 17024 (Personcertifiering) samt SS- EN ISO/IEC 17065 (Produktcertifiering) som är grunden för certifieringsorgans ackreditering.

Normerna finns inom kort på: <https://www.stoldskyddsforeningen.se/produkter/foretag/ssf-normer/>

Är du en säker chef?

Bli diplomerad
Säkerhetschef
12 oktober 2021

ssf.nu/utbildning

 **SSF**
Stöldskyddsforeningen

TRYGGARE SAMHÄLLE 2-2021

www.stoldskyddsforeningen.se

Kraftsamling mot digitala brott

SSF har tagit initiativet till att bilda Varningsgruppen mot digitala brott med målet att samla samhällets viktigaste aktörer för att varna för digitala brott.

Digitala brott som bedrägerier och IT-brott är ett samhällsproblem som påverkar både individer och företag och som kan leda till stora kostnader och bristande tillit till varumärken och institutioner. Flera stora företags varumärken utnyttjas vid exempelvis phishingförsök där kriminella vill komma åt personuppgifter för ekonomisk vinning. Bedragare utnyttjar även ofta stora händelser som exempelvis den pågående pandemin för att lura människor att uppge sina personuppgifter.

Nätverk ska varna allmänheten

För att främja insamling och delning av varningar kring pågående digitala brott och brottsförsök har SSF därför tagit initiativet till att skapa ett nätverk av aktörer som samarbetar kring de här frågorna. Syftet är att snabbt kunna varna allmänheten på bred front, samt ge råd och information, om exempelvis social

manipulation, identitetsstöld, kortbedrägerier och spridning av skadlig kod, för att på så sätt minska risken för att fler privatpersoner eller mindre företag drabbas av brott med digital koppling.

– Tillsammans med polisen och Internetstiftelsen bjöd vi in de viktigaste företagen och aktörerna inom området i slutet av förra året för att skapa ett nätverk kring frågorna, berättar Thomas Brühl, vd på SSF.

Säkerhetskollen varnar

Nu finns gruppen etablerad och består idag av ett trettiotal större aktörer inom både myndigheter, branschorganisationer, företag inom bank, telekom, handel, och teknikföretag som Facebook och Microsoft, kommenterar han vidare.

Varningarna som genereras presenteras idag på säkerhetskollen.se men ska även kunna publiceras genom andra kanaler.

Stort engagemang

Elin Elkehad vid Rådgivningsavdelningen på SSF är projektledare för Digitala Varningsgruppen och den som jobbat med att få med de olika deltagarna i samarbetet.

– Det har varit oerhört inspirerande att se vilket engagemang det finns ifrån både myndigheter, företag och organisa-

tioner ifrån hela samhället när det gäller dessa frågor. Något som är extra roligt är att se alla de diskussioner och det kunskapsutbyte som sker över organisationsgränser i syfte att stärka det svenska samhället mot digital brottslighet, säger hon.

Varningar redan utskickade

Hittills har det skickats ut ett trettiotal varningar till allmänheten som genererats av varningsgruppen. Det är varningar där exempelvis bedragare utnyttjat varumärken från banker eller dagligvaruhandel men även sådant som berör vaccination av Covid och försäljning på Blocket.

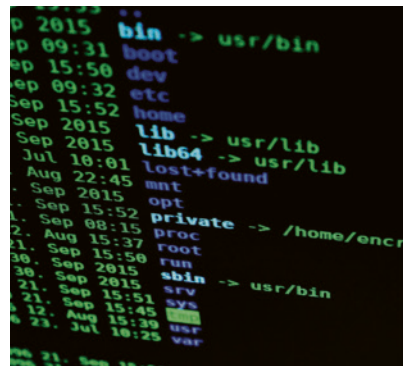


Foto: Joffi / Pixabay

– Utöver varningarna är syftet att medlemmarna i Digitala Varningsgruppen ska kunna stärka sin egen organisations förmåga inom digital säkerhet genom en aktiv community, fokuserad på kunskapsutbyte, omvärldsbevakning, föreläsningar och samarbete, säger Elin Elkehad avslutningsvis.



Aktörer som idag samverkar kring digitala brott. Utöver polisen stöds samarbetet också av MSB, Bolagsverket och Skatteverket.

SkyddGolfen
DETEKTOR Open

31 augusti

på Golf South Sthlm
Vidbyns i Nykvarn



Vi ses den 31 augusti

SkyddGolfen Detektor Open

– äger rum för 15:e året i rad den 31 augusti på Vidbyns GC i Nykvarn.

Eventet är inte bara världens största golf-tävling för säkerhetsproffs, utan också en mötesplats för alla som vill nätverka i vacker och säker utomhusmiljö.

Vi önskar er alla välkomna!

Anmälan görs enklast på www.detektor.com/golf/anmalan.asp

Arrangörer:



AR Media International, Tel +46 8-556 306 80, www.detektor.com

SPONSORER:

