TRYGGARE samhälle

TIDNINGEN FÖR ETT SÄKRARE SVERIGE • UTGES AV SSF STÖLDSKYDDSFÖRENINGEN • NR 3 • 2021







Tema:

SÄKERHETSSKYDD

– i företag och offentlig verksamhet

Sid 6–8

Samverkan är nyckeln till cybersäkrare liv

Thomas Brühl, vd, SSF Stöldskyddsföreningen.

Sid 2

Om kommunerna och säkerhetsskyddet

Richard Buske, säkerhetskonsult, Kronan Säkerhet.

Sid 4

Säkra din mobil mot QR-kod-bedrägerier

Paul Pintér, rådgivare digitala brott vid SSF.

Sid 16

LEDARE

”Jag tror starkt på att den här tjänsten kommer att vara ett viktigt verktyg i den brottsförebyggande verksamheten.”

Thomas Brühl,
vd, Stöldskyddsföreningen

Samverkan är nyckeln till cybersäkrare liv och företag

I vårt arbete för att förebygga digitala brott har det gångna året varit fantastiskt. Lanseringen av tjänsten säkerhetskollen.se är ett exempel på initiativ som tagit oss framåt. En annan milstolpe är etableringen av den Digitala varningsgruppen, där närmare 40 viktiga organisationer – både företag och myndigheter – samverkar. Därutöver har vi introducerat SSF Kunskapscenter och en ny norm för IoT. Det är därför med stolthet jag ser tillbaka på resultatet av den rapport vi på SSF tog fram i samband med att jag började som vd.

Rapporten syftade till att redogöra för hur kunskapen och samordningen i samhället såg ut i frågor som berör preventiva åtgärder för att minska risken för digitala brott. Det entydiga svaret, efter intervjuer med ett stort antal experter och beslutsfattare, var att det pågick en del arbete i de här frågorna men att samordning och synergieffekter.

Några av slutsatserna var:
- De statliga aktörerna räcker inte med.
- Ingen annan aktör arbetar idag strukturerat med detta.
- Som neutral part kan SSF bli den ledande aktören och driva på för att höja medvetandegraden hos allmänhet och företag via informationskampanjer.

För att motverka digital brottslighet krävs alltså ett omfattande samarbete mellan det privata och det offentliga. Vi behöver gemensamt samla våra resurser, både till tid och innehåll. Den slutsatsen var startskottet för vårt arbete för att förebygga digitala brott.

Vi har nått en bra bit på väg men det finns väldigt mycket mer att göra där vi ser möjligheter till samarbeten med ännu fler aktörer än vad vi har. Ska vi exempelvis nå full effekt av vår nyligen lanserade IoT-norm krävs att vi bygger relationer med både producenter, konsumentorganisationer och konsumenter för att nå ut med kunskap om behovet av säkra produkter. Nästa steg inom det området är att bygga kunskap för att inte bara göra hemmet utan även andra typer av fastigheter säkrare.

Ett samarbete som vi redan nu kommer att göra är att stödja och lyfta fram identifieringstjänsten som erbjuder ett sätt att drastiskt minska risken för telefonbedrägerier (whising).
Med tjänsten kan företag, myndigheter och andra organisationer ringa upp allmänheten och identifiera sig. Tjänsten kommer att vara ett viktigt verktyg i den brottsförebyggande verksamheten.

Vi bryter nu ny mark genom att lansera digitala äkthetsbevis, True cert, som ett sätt att verifiera sin utbildning. Syftet är att öka säkerheten och värdet i arbetsdokument som kan användas vid kontroll av nytillsättning och rekryteringar vid arbetstillfällen. Papperskopior och betyg är lätta att förfalska inför en tillsättning av en arbetsroll och därför är det enklare att kontrollera dessa digitalt via en säker källa som bygger på block chain-teknik.

Förra året lanserade SSF Säkerhetskollen som en heltäckande tjänst för information om digitala brott. Lanseringen riktade sig till allmänheten med funktioner som rådgivning, varningar om pågående brottsförsök och möjlighet att ge tips.

Nu lanserar SSF även en företagsdel på Säkerhetskollen. Företagsdelen har både inriktning mot att minska risken för intrång i IT-systemen och att ta fram information om företagsbrott och hur du som företagare kan förebygga dessa. Erfarenheterna och innehållet kommer förutom SSF vanliga rådgivningsarbete även från SSF samarbete med MSB kring cybersäkerhetsnormen SSF 110 som avhandlar åtgärder för att förebygga intrång i IT-system.

Jag ser fram emot en spännande höst där jag hoppas få chansen att möta många er fysiskt och där vi kan tala om hur vi kan samarbeta för att minska risken för digital brottslighet och öka cybersäkerheten i samhället.

Samverkan är trots allt nyckeln till cybersäkrare liv och företag.

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.tryggaresamhalle.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 Stöldskyddsföreningen
MILJÖMÄRKT 341069

MOBOTIX HUB

The **EXPANDABLE**
Video Management Platform

Experience the
MOBOTIX HUB

MOBOTIX
BeyondHumanVision

Richard Buske, säkerhetskonsult, om kommunerna och säkerhetsskyddet:

”Vi behöver ett forum där gemensamma säkerhetsfrågor kan knådas”

Vilka krav ska ställas på kommunens teknikleverantörer i en tid där man i alla led måste se över cybersäkerheten? Hur vet man att leverantörerna lever upp till kraven? Kan kravinnehållet i Säkerhetsskyddslagen användas vid upphandling? Det här är exempel på frågeställningar som säkerhetskonsulten Richard Buske från Kronan Säkerhet ger sin syn på på utifrån ett kommunalt säkerhetsperspektiv.

Artikelförfattaren Richard Buske har många års erfarenhet av kommunalt säkerhetsarbete. Han har exempelvis varit säkerhetschef i Sollentuna kommun. Numera är Richard säkerhetskonsult på Kronan Säkerhet.

Då tekniken blivit allt mer komplicerad samtidigt som vi ser ständigt förändrade hotbilderna så har upphandling blivit den kanske svåraste disciplinen inom säkerhetsarbetet. Gränssnittet mellan cybersäkerhet och den fysiska säkerheten är flytande. Molnbaserade tjänster och mobiler i var mans hand ställer krav på bekväma och användarvänliga lösningar. Kraven från försäkringsbolag och myndigheter är å andra sidan att man ska i högre grad tillämpa komplexa och komplicerade lösningar som cyberkriminella förhoppningsvis inte kan knäcka.

> ***Många säger ju att de kriminella alltid ligger ett par steg före säkerhetsbranschen. Det är kanske dags att ändra på det.***

Ett upphandlingsunderlag måste balansera bägge dessa sidor. En upphandling bör lämna öppningar för kreativa lösningar, men den måste också se till att skyddet bli så bra att det förhindrar brott. Vid en upphandling av säkerhetsteknik, oavsett om den orsakas av till exempel krav till följd av Säkerhetsskyddslagen, krävs ett sunt ekonomiskt perspektiv. Detta är knepigt men nog så viktigt. Det är inte alltid som en säkerhetsinvestering kan balanseras mot en intäkt (K/I-analys), men det går att visa på de ekonomiska nackdelarna om säkerhetsinvesteringen inte genomförs. Detta har även en direkt koppling till den riskanalys som förhoppningsvis ligger till grund för beslutet om en investering.

Kompetensen hos säkerhetsbranschens leverantörer varierar, dessutom finns det också många med bristande kunskap på beställarsidan. Mixen av dessa kan naturligtvis leda till konsekvenser som resulterar i allvarliga skador och onödiga kostnader.

Säkerhetsskyddslagstiftningen har i avseendet som mall för upphandling inte någon större roll, annat än ur rubriksynpunkt. Riskerna som kravställs handlar om person, egendom och information, och där kan en säkerhetsleverantör säkert hämta en del när det gäller metodik och logistik. Tekniken och utvecklingen är däremot något som säkerhetsbranschen själva får stå för.

Generellt kan man säga att det är svårt att vara annat än övergripande i resonemangen kring hur kommuner fungerar när det gäller upphandling av säkerhet. Det är stor variation på hur kommunerna ser ut när det gäller storlek och hotbild, detsamma gäller givetvis också för företag och organisationer.

> ***Det är inte alltid en säkerhetsinvestering kan balanseras mot en intäkt men det går att visa på de ekonomiska nackdelarna om säkerhetsinvesteringen inte genomförs.***

Det är heller inte särskilt mycket samarbete eller utbyte mellan kravställarna (försäkringbolagen och myndigheter) och säkerhetsbranschen. Man har varandra som remissinstans i bästa fall.

Vi behöver ett forum där gemensamma säkerhetsfrågor kan knådas till kundernas och alla andra skadelidande organisationers bästa. Det skulle sannolikt leda till en ökad kompetens och snabbare utveckling av det fysiska skyddet och cybersäkerheten. Erfarenheterna från skador hos försäkringsbolagen skulle exempelvis kunna trigga säkerhetstekniker att komma på nya lösningar.

Många säger ju att de kriminella alltid ligger ett par steg före säkerhetsbranschen.

Det är kanske dags att ändra på det.

Richard Buske,
Säkerhetskonsult,
Kronan Säkerhet,

SECTECH 20år
EXPO & SEMINARS

Event: Sectech

Plats: Stockholmsmässan

Tid: 27 – 28 oktober 2021

Profil: Utställning/seminarier med fokus på teknikbaserade säkerhetslösningar.

Fri entré – boka här:
www.sectech.se

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

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

Huvudsponsor: AXIS COMMUNICATIONS

Entrésponsor: seriline

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

Nya krav på säkerhetskänslig verksamhet

Regeringen har beslutat att genomföra en lagrådsremiss med förslag på ändringar i säkerhetsskyddslagen, för att stärka skyddet av Sveriges säkerhet. Lagändringen träder i kraft den 1 december 2021.

Text: Lennart Alexandrie

Säkerhetsskydd innebär förebyggande åtgärder för att skydda Sveriges säkerhet mot spionerі, sabotage, terroristbrott och andra brott. Dessutom bör även allmänna och enskilda verksamheter ingå inom ramen för säkerhetsskyddet. Den som bedriver säkerhetskänslig verksamhet kan hindras att ingå avtal och andra samarbeten som kan skada Sveriges säkerhet.

Verksamhetsutövarens ansvar

I remissen framkommer att det är verksamhetsutövarens ansvar att utreda om det man bedriver är säkerhetskänsligt och att dokumentera verksamhetens behov av säkerhetsskydd. Varje enskilt företag i en organisation ses som en separat verksamhetsutövare oavsett om företagen ingår i samma koncern.

Alla verksamhetsutövare ska göra en bedömning av säkerhetsskyddet och pröva lämpligheten av kontrakt som kräver säkerhetsskyddsavtal. I vissa fall måste verksamhetsutövare samråda med tillsynsmyndigheten om handlingen är lämplig att genomföra. Om tillsynsmyndigheten anser att avtalet är olämpligt ur säkerhetsskyddssynpunkt kan myndigheten göra nedslag och även utdela böter.

Ökat behov av utbildning

I lagförslaget får säkerhetsskyddschefen får en mer framträdande och drivande roll i säkerhetsskyddsarbetet.

Det innebär det att kompetensen inom säkerhetsområdet hela tiden måste vara aktuell mot kraven på kunskap inom säkerhetsskydd, något som SSF Stöldskyddsföreningen tagit höjd för.

– För att förstå och korrekt hantera de förstärkta kraven gällande säkerhetsskydd behövs utbildning och kompetensutveckling, säger Stöldskyddsföreningen vd Thomas Brühl.

Stöldskyddsföreningen vd Thomas Brühl.

– Just dessa fördjupningar inom området får man genom att delta på Stöldskyddsföreningens utbildningsserie inom säkerhetsskydd avslutar Thomas Brühl.

Tomas Devenyi, säkerhetskonsult:

”Bli bättre på säkerhetsskydd, det gynnar alla”

Tryggare Samhälle har tagit kontakt med Tomas Devenyi, säkerhetskonsult och grundare av Ancoris Security. Som expert på Säkerhetsskyddslagen har han ombetts att reda ut vad det nya lagförslaget betyder för företag och andra organisationer och hur dess innehåll även kan tillämpas av företag som inte omfattas av lagen

Text: Hans-Erik Nilsson

Vilka nya utmaningar får verksamhetsutövare i och med att lagändringarna träder i kraft?

– Förslaget innebär i huvudsak förändringar inom tre områden. Det första området handlar om att generellt få säkerhetsskyddsfrågor mer prioriterade och stärka säkerhetsskyddschefens roll. Regeringen föreslår därför att säkerhetsskyddschefen placeras direkt under den högsta ledningen.

Och det andra och tredje området?

– Det handlar om ett stärkt skydd av säkerhetskänsliga verksamheter. Förslaget innefattar ett större krav på verksamhetsutövaren att bedöma lämpligheten i utkontrakteringar. Tillsynsmyndigheterna ska även få möjlighet att ingripa i eller helt förbjuda olämpliga avtal. Slutligen ska en mer effektiv tillsyn säkerställas genom att myndigheterna får undersökningsbefogenheter och möjlighet att besluta om vitesföreläggande mot den som inte följer säkerhetsskyddslagen.

Var uppstår de största bristerna när det gäller efterlevnaden av säkerhetsskyddslagen?

– Säkerhetspolisen har vid upprepade tillfällen påtalat att det finns stora brister i säkerhetsskyddsarbetet. Enligt Säkerhetspolisen beror bristerna på otillräckliga resurser, andra prioriteringar, avsaknad av styrdokument samt att frågan inte når den högsta ledningen.

– En mycket viktig faktor är otillräcklig utbildning. Bristerna handlar dock inte enbart om tekniska frågor. Säkerhetsprövning är ett område där det tyvärr ofta råder bristande kunskap om vad det är och hur det ska genomföras. I dagens lagstiftning nämns bara att utbildning ska genomföras utan att beskriva innehåll eller omfattning. Det saknas förtydligande krav om utbildning.

Hur kan företag och organisationer tillämpa hela eller delar av lagändringarna för att öka sin driftsäkerhet?

– Säkerhetsarbete, oavsett om det handlar om skydd av hela Sveriges eller det enskilda företagets säkerhet, handlar om en systematik och en kombination av åtgärder. Områden som fysisk-, informations- och personalsäkerhet är frågor som berör alla organisationer i någon mån.

Kan du ge specifika exempel?

– En skyddsprincip som exempelvis sektionering är relevant oavsett om det rör sig om en av Försvarsmaktens ledningscentraler eller ett vanligt civilt kontor i Nässjö. I båda fallen behövs olika nivåer och lösningar på skyddsåtgärder i olika delar av lokalen. Kunskap om sektionering och andra säkerhetsskyddsåtgärder gällande fysisk säkerhet kommer att vara till stor nytta även för Nässjökontorets säkerhetsarbete.

Något mer exempel?

– Informationssäkerhet. Även om man inte jobbar med säkerhetsskyddsklassificerade uppgifter har alla verksamheter någon form av känslig eller skyddsvärd information. Frågor om tillgänglighet, riktighet och konfidentialitet måste hanteras utifrån de risker som verksamheten identifierar. Hotet är då kanske inte främmande makt utan en konkurrent eller en bedragare. System, behörigheter, rutiner och regler måste anpassas därefter.

Är skärpningarna nog, eller kan det behövas ökade kravställningar på sikt?

– Att riskera vite om 50 miljoner kronor, vilket är maxbeloppet för enskilda verksamhetsutövare, kommer att öka motivationen till att göra rätt. De stärkta kraven är därför något mycket positivt på många sätt. Den ökande förståelsen för att säkerhetsskydd är viktigt får också positiva konsekvenser generellt. Regelverket skapar nämligen en systematik som samtliga aktörer kan dra nytta av.

Tomas Devenyi, säkerhetskonsult och grundare av Ancoris Security.

Har du något kort råd till de som vet med sig att deras verksamheter omfattas av lagändringarna?

– Tycker du det är viktigt med säkerhet? Gör en insats du med, bli bättre på säkerhetsskydd, det gynnar alla.

Attack mot BankID – så hanterades angreppet

På kvällen den 23 februari 2021 utsattes BankID-systemet för ett allvarligt överbelastningsangrepp via internet. Tryggare Samhälle har talat med företagets säkerhetschef Andreas Bergqvist om incidenten.

Text: Hans-Erik Nilsson

Foto: Finansiell Id-Teknik

BankIDs äkerhetschef Andreas Bergqvist.

Med sina över åtta miljoner användare i Sverige och 17 miljoner genomsnittliga inloggningar per dygn är det ingen överdrift att kalla BankID den mest kritiska delen av det svenska samhällets digitala infrastruktur.

Under tidsperioderna 19:45-20:15 och 21:45-22:10 den aktuella aftonen kunde BankID-användarna uppleva problem med att logga in eller att svarstiderna var längre än normalt.

– Detta scenario både övar vi på och har väl etablerade processer samt skydd mot. Så när väl attacken riktades mot oss så var all relevant personal mycket snabbt på bollen att avvärja den. Vi arbetade aktivt med att se till att alla skydd som behövdes hela tiden var aktiva och med det säkerställdes att våra slutanvändare kunde använda vår infrastruktur även fast attacken pågick, förklarar Andreas Bergqvist..

Kommunikation och transparans

Andreas Bergqvist pekar på att en viktig aspekt när en verksamhet blir utsatt för en nätattack är att behålla lugnet och stödja sig på de förberedelser som man gjort och se till att rätt kompetens jobbar med rätt sak.

– I vår hantering är kommunikation en väldigt viktig del, att alla som undrar får svar för att skapa både en förståelse av vad som händer och vad vi gör för att lösa problemet. Transparens är bra när det kommer till dessa typer av händelser, säger Andreas Bergqvist.

Överbelastningsangrepp

Ett överbelastningsangrepp kallas på itspråk för en ddos-attack. Förkortningen ddos uttyds ”distributed denial of service” och innebär att en tjänst på nätet bombarderas med en enorm mängd datatrafik, vilket då hindrar användare från att ansluta till tjänsten. I vissa fall kryper hastigheten, bandbredden, ned till snigelfart. Ddos-attacker kan dessutom utföras i utpressningssyfte. Vid just den här attacken förekom inga meddelanden eller krav på lösensumma från angriparna, vilket gör syftet är höljt i dunkel. Därutöver är det svårt att klarlägga vilka förövarna är och var i världen de befinner sig.

– Attacken skedde med hjälp av ett så kallat botnet, en samling av datorer som en angripare kapat och med hjälp av dem skickar massiva datamängder för att på så sätt överbelasta våra system. Det är en form av attack som i sig är väldigt svår att spåra då de kapade datorerna är utspridda i olika länder och de personer och företag som äger dem vet i regel inte om att just deras dator är med i en cyberattack, säger Andreas Bergqvist.

Kapade datorer

I och med systemet hanterar drygt 5 000 företag, myndigheter och organisationer som använder BankID för identifiering och underskrift i sina e-tjänster är det rimligt att anta att några av tjänstens egna kunder helt omedvetet var en del av attacken.

– Angripare som använder sig av botnets gör det för att det är ett kraftfullt verktyg som kan anpassas relativt enkelt och kan användas till olika former av cyberangrepp, allt ifrån överbelastningsattacker till informationsstölder. Det är också svårt att spåra då ett botnät kan bestå av tusentals datorer och servrar från ovetande privatpersoner och företag, placerade i flera olika länder. Detta gör att arbetet för brottsbekämpande myndigheter blir mycket svårt när det kommer till att försöka hitta personerna bakom, säger Andreas Bergqvist.

Angriparna varierar tillvägagångssätt

Överbelastningsattacker är ett hot mot alla verksamheter som har en digital närvaro på nätet och det är viktigt att man planerar, övar och har verktyg att sätta mot när en sådan attack inträffar.

– Som en del i Sveriges digitala infrastruktur ser vi givetvis många attacker av den här sorten. Det som många misstar sig på är att de tror att alla överbelastningsattacker går att likställa med varandra. Så är det inte, angripare försöker hela tiden att ändra tillvägagångssätt för att försöka slå ut digitala måltavlor och det är därför det är så viktigt att man har ett väl inövat försvar samt att hela tiden se över de digitala skydden, menar Andreas Bergqvist.

Viktigt samarbete

Samarbete bland de verksamheter som hanterar skyddsvärd information, eller bekämpar de som vill stjäla densamma, är mycket betydelsefullt för att effektivt kunna försvara sig mot digitala hot.

– Självklart samverkar vi med andra, både företag och myndigheter. Det ger en god beredskap. Vi polisanmäler alltid brott som riktas mot oss, vilket vi givetvis även gjorde i detta fall. Jag är av uppfattningen att för få företag väljer att anmäla när de utsätts för ett cyberbrott, säger Andreas Bergqvist.

Extrem upptid

Den så kallade upptiden för BankID-tjänsten är imponerande 99,99 procent på ett år, vilket i internetsammanhang är liktydigt med en superstabil leverans av datapaket över nätet.

– Med snart 20 års erfarenhet och mycket hög expertis inom säkerhet och teknik kan våra användare, företag och myndigheter lita på Bankid. Vår målsättning är att fortsatt utveckla och erbjuda digital identifiering och elektronisk underskrift som är snabb, säker och värnar om användarnas integritet, avslutar Andreas Bergqvist.

SÅ ANVÄNDER DU BANKID PÅ ETT SÄKERT SÄTT

- Läs alltid texten som visas i BankID-appen och kontrollera var du loggar in och vad du skriver under. Är du osäker, välj avbryt.
- Lämna aldrig ut koder från ditt BankID till någon annan.
- Använd aldrig ditt BankID på uppmaning av någon annan person.
- I BankID-appen kan du se vilka identifieringar och underskrifter du gjort. Kolla historiken.

Foto: Bankid

Ulrica Heinrici, SSF:s utbildningschef, om säkerhetsskyddslagen:

”Det finns många frågor att ställa rörande regeringens nya lagförslag”

SSF Stöldskyddsföreningen står inför en höst, fullmatad med aktiviteter, inte minst när det gäller utbildning kring säkerhetsskyddslagen.

Tryggare Samhälle har intervjuat Ulrica Heinrici, ny utbildningschef om hur hon ser på sin och SSF:s roll som när det gäller utbildning gällande säkerhetsskydd och andra områden inom det brottsförebyggande området.

Text: Lennart Alexandrie

Ulrica Heinrici, ny utbildningschef på SSF.

Ulrica Heinrici kommer närmast från Swedbank där hon har arbetat som utbildningsexpert och dessförinnan var hon utbildningschef och utbildningsansvarig inom IT-säkerhet.

Vad är din roll som utbildningsansvarig på SSF?

– Jag ansvarar för att verksamheten systematiskt ska öka kvalitén på utbildningarna. Jag har dessutom det övergripande verksamhets -och ekonomiansvaret. Jag arbetar med framför allt strategiska frågor i samverkan med enheten och ledningsgrupp.

Varför tackar du ja till jobbet som utbildningschef på SSF?

– SSF Stöldskyddsföreningen har byggt upp en unik erfarenhet och kompetens inom säkerhetsområdet. Den kompetensen ville jag vara med och lyfta så att flera organisationer får ta del av utbildningsutbudet.

> ***Organisationer som har säkerhetskänslig verksamhet skall göra en säkerhetsskyddsanalys som syftar till att utreda behovet av säkerhetsskydd.***

Vad är dina främsta prioriteringar när det gäller utvecklingen av SSF:s utbildningsverksamhet?

– Att hålla utbildningsutbudet uppdaterat mot de behov som marknaden stöter på. Därför måste vi ha skarpa och pedagogiska utbildare, enkla anmälningslösningar och flexibilitet vad det gäller deltagarens behov av utbildningsmiljö. I nuläget är ju de flesta av våra utbildningar så kallat blandat lärande. Det gör att vi varierar olika lärmetoder och genom att använda en kombination av olika inlärningssätt så förstärks medarbetarnas ingångar till inlärning.

Säkerhetsskyddslagen infördes 2018 och håller på att uppdateras. Hur bidrar SSF till att hålla företag och andra organisationer uppdaterade om lagens innebörd?

– Vi håller webinarier för att sprida kunskap om vad den nya säkerhetsskyddslagen innebär. Dessutom har vi tagit fram en kortare utbildningsserie som skall ge mer matnyttig kunskap inom detta område.

Säkerhetsskyddslagen förändras i takt med att hotbilder förändras, hur påverkar det SSF:s utbildningsverksamhet?

– Det gäller att hela tiden att vara uppmärksam och lyssna på utbildningsbehoven som kan förändras snabbt beroende på vad som sker i omvärlden. Därför försöker vi hela tiden att vara flexibla och variera vårt utbildningsutbud efter det att villkoren för kompetensutveckling för organisationer förändras.

Företag som inte omfattas av Säkerhetsskyddslagen, bör de ändå informera sig eller utbilda sig säkerhetssk

– Ja absolut, det kan ju hända att de faller inom ett avtal för ett annat företag som handhar säkerhetskänslig verksamhet. Ledningssystemet och det grundläggande skyddet är fundament för de organisationer som kommer i kontakt med säkerhetsklassade uppgifter.

Så vad behöver man primärt då kunna?

– Organisationen i stort behöver ha koll på vad man skall oroa sig för, vem som ska göra vad, vem som fattar beslut om viktiga förbättringar, hur man mäter hur det går, vad du eller kanske någon annan ska göra om det sker en incident, och hur den ska rapporteras och hanteras. Lagförslaget innebär ju exempelvis att säkerhetsskyddschefen får en mer framträdande och drivande roll i säkerhetsskyddsarbetet.

Kan du ge exempel på delar i säkerhetsskyddslagen tror du är mest intressanta för just dessa företag?

– Organisationer som har säkerhetskänslig verksamhet skall göra en säkerhetsskyddsanalys som syftar till att utreda behovet av säkerhetsskydd. Ibland behöver organisationen hjälp med alla steg i säkerhetsskyddsanalysen där målet är att klargöra vilka säkerhetskänsliga och säkerhetsskyddsklassade uppgifter en verksamhet behandlar, för att säkerhetsskyddsanalysen ska hållas uppdaterad.

Det finns många frågor att ställa rörande regeringens nya lagförslag på säkerhetsskyddet för det innebär nya krav på olika verksamhetsutövare och avtalen mellan olika led.

Slutligen, vad är på gång den närmaste tiden när det gäller utbildningar i SSF:regi?

– Vi ska lansera vår nya utbildningsserie inom säkerhetsskydd, där man själv kan välja om man vill gå en eller fler av utbildningarna i serien. Varje utbildning bygger på verklighetsbaserade scenarier med tillhörande reflektionsfrågor där vi utgår ifrån praktiska exempel inom säkerhetsskyddsanalys, säkerhetsprövning eller informationssäkerhet. Utbildningen omfattar individuellt lärande inför kurstillfället och lärarledd undervisning samt repetition och summering med tillgång till checklistor och fördjupningsmaterial.

Något annat som ligger i närtid?

– Ja, vi är på gång att lansera digitala diplom som äkthetsbevis på genomförd utbildning hos Stöldskyddsföreningen. Det kommer att kunna delas på exempelvis LinkedIn vilket gör att deltagare kan intyga och verifiera genomförd SSF-utbildning på ett tillförlitligt sätt. Diplomet bygger på en säker blockchain-metod. Det är en databas som lagras i många kopior, som gör det extra svårt att manipulera originaldokumentationen.

Vilka blir först att tilldelas dessa diplom?

– Först ut är våra diplomerade säkerhetschefer som på ett tillförlitligt sätt kan visa sina arbetskontakter att de har genomgått Diplomerad Säkerhetschef hos Stöldskyddsföreningen.

AR Medias grundare mottog Stora Säkerhetspriset 2021

I samband med att Säkerhetsbranschen arrangerade Säkerhetsdagen den 2 september utdelade branschorganisationen för första gången den nyinstiftade utmärkelsen Stora säkerhetspriset. Mottagare blev AR Medias grundare Lennart Alexandrie.

– Jag känner mig hedrad och stolt över att få motta detta fina pris från Säkerhetsbranschen. Det är alltid roligt att få uppskattning för det man gör och det man har gjort, kommenterar prisvinnaren.

Lennart Alexandrie (mitten) mottog Stora Säkerhetspriset av Säkerhetsbranschens vd, Joakim Söderström och styrelseordförande Kettil Stenberg i samband med Säkerhetsdagens bankett.

Säkerhetsdagen arrangerades på Quality Stockholm Hotel med cirka 200 deltagare på plats. Under den avslutande banketten presenterades Säkerhetsbranschens vd Joakim Söderström vinnaren av Årets Säkerhetspris och läste upp juryns motivering.

”Lennart har genom sitt engagemang och driv för säkerhetsbranschen varit med och påverkat utvecklingen framåt. Inte minst genom Sectech, Detektor Awards och SNOS bidrar Lennart med att lyfta innovationer och driva på utvecklingen kring säkerhetslösningar och branschfrågor såväl i Sverige som på den internationella marknaden.”

På scenen tackade Lennart Alexandrie juryn men också sina medarbetare på AR media.

Stora Säkerhetspriset tilldelas en person som verkar inom säkerhetsbranschen och som på ett utmärkande sätt ha bidragit till branschens utveckling, nytänkande, synlighet eller framgång.

– Det här priset ska lyfta de viktiga personer som med sitt hårda arbete bidrar till att utveckla och förbättra branschen. Vi arbetar i en bransch med många engagerade och duktiga personer, och vi är väldigt glada om vi kan lyfta fram några av dem. Vi hade tre riktigt bra finalister det här första året, och även om det bara är en som kan ta hem pokalen så var alla helt klart värdiga vinnare, kommenterar Joakim Söderström, vd för Säkerhetsbranschen.

Övriga två finalister var Martin Bjurhem, vd för Bevakningsbranschens Yrkes- och Arbetsmiljönämnd och Malin Svensson, tidigare brandsäkerhetstekniker och instruktör inom brand och räddning.

Sectechs projektlchef, Deniz Baykal.

Sectech först att slippa smittskyddsrestriktioner

Den 7 september meddelade regeringen att man tar bort begränsningarna för hur många som får delta i offentliga tillställningar. Det betyder att 20-årsjubilerande Sectech den 27–28 oktober blir det första större säkerhetseventet i Skandinavien som arrangeras utan särskilda smittskyddsrestriktioner.

Sectech är vanligen en kompakt säkerhetsmässa med teknikfokus där många utställare och besökare möts på en relativ liten yta. Med hänsyn till pandemin kommer det inte vara så 2021. Istället präglas utställningsdesignen av utrymmen för att möjliggöra social distansering. Breda gånger och sunda avstånd mellan montrarna möjliggör säkra avstånd mellan besökare och utställningspersonal.

– De åtgärderna är redan tagna och kommer bestå. De nya direktiven till trots kommer vi även tillämpa andra åtgärder för att säkerställa att Sectech blir ett tryggt event för såväl utställare som besökare, säger Deniz Baykal, Sectechs projektchef, som ser väldigt positivt på regeringens besked.

– Ja, så klart. Nu är förutsättningarna de allra bästa för att Sectech ska bli just den mötesplats som så många av oss har efterlängtat, säger hon.

Förutom en fullbokad utställning kommer Sectech arrangera seminarier och paneldiskussioner som kretsar kring trender och viktiga frågor som rör marknaden för fysisk säkerhet, framför allt när det gäller teknikbaserade tjänster. AI, smarta städer och cybersäkerhet är några av de mer highlightade ämnena som tas upp.

Kenny Stamatopoulos, trygghetsambassadör 2020.

Kenny Stamatopoulos utses retroaktivt till årets Trygghetsambassadör 2020

Tankesmedjan Säkerhet för näringsliv och Samhälle samt publikationen Securityuser.com utser varje år en trygghetsambassadör. Under förra årets pandemi uteblev dock själva prisceremonin, som istället kommer att ske den 20 september på Friends Arena i samband med toppmatchen AIK–IFK Göteborg.

Platsen motiveras av att mottagaren av ”Årets Trygghetsambassadör 2020” är Kenny Stamatopoulos, före detta fotbollsmålvakt i AIK, numera målvaktstränare i klubben.

Kenny Stamatopoulos utsattes för ett mutförsök inför ett toppmöte i fotbollsallsvenskan 2017. Han valde att polisanmäla och vittna i det rättsliga efterspelet, vilket ledde till en fällande dom, som Högsta domstolen fastställde 2020.

I motivationen till 2020 års val av trygghetsambassadör skriver juryn:

”Med sitt agerande har Kenny Stamatopoulos inte bara gjort fotbollen och idrotten en stor tjänst, utan även samhället i stort. Mediauppmärksamheten kring rättsfallet har dessutom lyft problemet med matchfixning i Sverige till en ny nivå.

Kenny Stamatopoulos civilkurage, integritet och känsla för fair play gör honom till ett föredöme för alla som vill se en utveckling där matchfixningsförsök och andra allvarliga brott beivras.

Därför är Kenny Stamatopoulos en mycket värdig mottagare av utmärkelsen Årets Trygghetsambassadör 2020”. Prisceremonin kommer ske i samband med matchstart (AIK–IFK Göteborg) på Friends Arena den 20 september kl 19.30.

Antalet banktrojaner ökade med 65 procent under 2021

Antalet användare som attackerades med Qakbot - en kraftfull banktrojan, under de första sju månaderna 2021 växte med 65 procent jämfört med samma period 2020, vilket visar att detta hot blir alltmer påtagligt för allmänheten.

Banktrojaner gör det möjligt för cyberbrottslingar att stjäla pengar från offrens nätbankkonton och e-plånböcker. Därför anses de vara ett av de farligaste exemplen på skadlig kod. Qakbot identifierades redan 2007, men har under de senaste åren utvecklats väldigt mycket, vilket har gjort Qakbot till en av de mest hotfulla banktrojaner som finns.

Kan undgå upptäckt

Utöver de välkända funktionerna, som att registrera tangentbordets aktivitet, samt stjäla lösenord och cookies, har uppdateringarna av Qakbot inkluderat tekniker som gör att banktrojanen kan minimera eller stänga av sin aktivitet om den tror att den är på väg att identifieras av säkerhetslösningar. Därtill har Kaspersky-forskare upptäckt att de senaste versionerna av Qakbot har förmågan att stjäla e-post från den attackerade maskinen. Dessa e-postmeddelanden kan sedan användas för olika typer av bedrägerier som riktas mot kontakter i offrets adresslista.

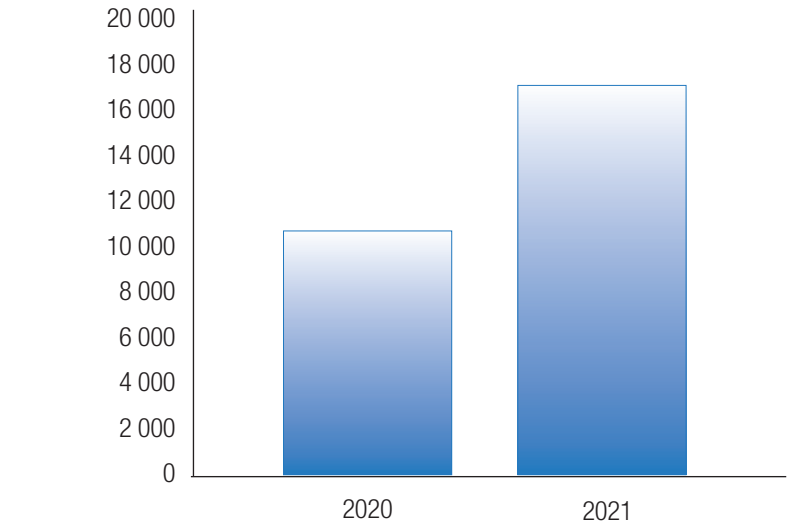
Svårstoppad

Det är osannolikt att Qakbot stoppas inom en snar framtid. Denna skadliga programvara får hela tiden nya uppdateringar och hotaktörerna bakom den fortsätter att lägga till nya funktioner och uppdatera sina moduler för att maximera intäkterna. Tidigare har vi sett Qakbot spridas aktivt via Emotet-botnätet. Detta botnät togs ner i början av året, men att döma av infektionsstatistiken, som har ökat i jämförelse med förra året, har aktörerna bakom Qakbot hittat nya sätt att sprida denna skadliga programvara, säger Haim Zigel, säkerhetsanalytiker på Kaspersky.

Så skyddar du dig mot Oakbot

För att undvika hot som Qakbot rekommenderar Kasperskys experter att du:

- Inte klickar på länkar i skräppostmeddelanden eller öppnar dokument som bifogas i dem.
- Använder en internetbank med multifaktorautentisering.
- en pålitlig säkerhetslösning som kan hjälpa dig att kontrollera att webbadressen du besöker är säker och öppna alla webbplatser i en skyddad version för att förhindra stöld av känslig data (exempelvis finansiell information).



Antal Kaspersky-användare som stött på Qakbot: sju månader 2020 mot sju månader 2021 (Källa: Kaspersky Security Network)

> ***Banktrojaner gör det möjligt för cyberbrottslingar att stjäla pengar från offrens nätbankkonton och e-plånböcker.***

Svenska IT-ansvariga: nätfiskeattackerna har ökat

En global undersökning visar att svenska företag tillhör de som haft den största ökningen av nätfiskeangrepp sedan pandemin började. Drygt åtta av tio (83 procent) av de tillfrågade IT-ansvariga upplever att nätfisket ökat. Det kan jämföras med det globala genomsnittet 70 procent.

Israel mest drabbat

Israel är det land där flest företag uppger att de sett en ökning av antalet nätfiskeattacker – 90 procent. I andra änden ligger Italien där 57 procent av de tillfrågade anger att nätfisket ökat.

I undersökningen som genomförts av IT-säkerhetsföretaget Sophos framgår att skillnaden mellan hur olika branscher och områden drabbats är relativt liten. Globalt tillhör dock statliga verksamheter, myndigheter, tjänstesektorn samt sjuk- och hälsovården de mer drabbade.

– Det är uppenbart att cyberkriminella sett pandemin och ökat hemarbete som en möjlighet. Tyvärr kan nätfiske ibland uppfattas som ett relativt avgränsat hot men i många fall är det precis så större och mer komplexa angrepp börjar. En enskild medarbetare som oavsiktligt laddar ner skadlig kod eller uppger sina inloggningsuppgifter kan vara fullt tillräckligt för att angreppet ska övergå i en storskalig och kostsam attack med ransomware, kommenterar Per Söderqvist, IT-säkerhetsexpert på Sophos.

Företagen satsar på utbildning

Per Söderqvist menar att det är positivt ändå att totalt nittio procent uppger att deras företag genomför något slags utbildningsprogram inom IT-säkerhet.

– Samtidigt ligger det en stor utmaning i att få de här insatserna att anpassas och fungera för personal som inte har särskilt mycket förkunskap om teknik och IT-säkerhet. Det bästa är naturligtvis om medarbetarna aldrig nås av angriparnas e-post och nätfiske. I dag kan effektiva säkerhetslösningar stoppa en stor andel av nätfiskeangreppen men det behövs fortfarande kunskap och vaksamhet hela vägen ut i organisationen, säger Per Söderqvist.

83 procent av de tillfrågade IT-ansvariga upplever att nätfisket ökat.

Svar från 5 400 IT-ansvariga

Undersökningen ”Phishing Insights 2021” bygger på information från 5 400 IT-ansvariga vid företag i trettio länder, däribland USA, Storbritannien, Kina, Japan, Brasilien, Tyskland, Frankrike, Italien, Indien och Sverige. I Sverige medverkade 100 IT-ansvariga. Samtliga medverkande arbetar i organisationer med mellan 100 och 5 000 användare. Undersökningen har genomförts av Vanson Bourne på uppdrag av Sophos. Vanson Bourne är ett oberoende företag specialiserat på marknadsundersökningar.

Experter varnar för sårbarheter i Bluetooth

Forskare på Singapore University of Technology and Design har hittat 16 stycken allvarliga sårbarheter i Bluetooth, skriver Computer Sweden. Sårbarheterna gör att hackare kan installera skadlig kod eller utföra Ddos-attacker.

Sårbarheterna finns i chip från flera olika tillverkare, bland annat Intel, Qualcomm, Texas Instruments, Infineon (Cypress) och Silicon Labs.

Intel lovar att försöka åtgärda sårbarheterna omgående medan till exempel Qualcomm och Texas Instruments menar att de inte kommer att vidta åtgärder såvida inte ”kunderna begär det”.

En anledning till att risken att drabbas bedöms som relativt liten är att hackarna kommer att behöva befinna sig i närheten.

MSB får uppdrag om cybersäkerhets-center

MSB får i uppdrag att förbereda för och lämna förslag på hur ett nationellt samordningscenter för forskning, innovation och tillämpning inom cybersäkerhet ska kunna inrättas vid myndigheten under 2022.

Sverige utsätts dagligen för allvarliga cyberattacker som riskerar att skada samhället och demokratin. Det kan bland annat handla om utpressningsvirus där filer tas gisslan i syfte att tvinga den drabbade att betala en lösensumma.

I uppdraget till MSB ingår bland annat att lämna förslag om hur den nationella kompetensgemenskapen ska byggas upp, bland annat i relation till det nationella cybersäkerhetscentret, samt lämna förslag om en långsiktig samverkansstruktur för berörda myndigheter och aktörer, såväl nationella som internationella.

Uppdraget ska genomföras i samverkan med Verket för innovationssystem (Vinnova) och Myndigheten för digital förvaltning (Digg). MSB ska ha en dialog med RISE Research Institutes of Sweden AB och andra aktörer som bedöms vara relevanta vid genomförandet, skriver regeringen.

Det nationella samordningscentret ska vara kopplat till det europeiska kompetenscentret för cybersäkerhet inom näringsliv, teknik och forskning som inrättades i somras enligt Europaparlamentets och rådets förordning. Uppdraget ska redovisas senast den 17 november 2021.

– Vi behöver mer forskning och innovation inom cybersäkerhet för att exempelvis minska systemfel och förhindra cyberattacker, säger inrikesminister Mikael Damberg.

I uppdraget till MSB ingår bland annat att lämna förslag om hur den nationella kompetensgemenskapen ska byggas upp, bland annat i relation till det nationella cybersäkerhetscentret.

Den förvärrade ransomware-krisen sätter rekord för lösensummor

Under årets första halvår steg den genomsnittliga betalningen till kriminella i samband med ransomware-angrepp med 82 procent till 570 000 dollar, cirka 4,9 miljoner kronor, enligt en rapport från Unit 42.

Ökningen kommer efter att den genomsnittliga betalningen redan förra året steg med 171 procent till nära 312 000 dollar, 2,7 miljoner kronor. Siffrorna, som sammanställts av säkerhetskonsultgruppen Unit 42, bekräftar att ransomware-krisen bara blir värre när kriminella företag ökar sina investeringar i lönsamma utpressningsoperationer.

Fyrdubbel utpressning

Ökningen av ”fyrdubbel utpressning” är en oroande trend som Unit 42 upptäckte när de studerade en mängd ransomware-fall från första halvåret 2021. Ransomware-grupper använder nu ofta hela fyra metoder för att tvinga sina offer att betala:

1. Kryptering: Offret betalar för att åter få tillgång till krypterade data och utsatta datorsystem som slutar fungera eftersom de nödvändiga filerna är krypterade.

2. Datastöld: Hackare släpper ut känslig information om lösensumman inte betalas. (Denna trend ökade starkt 2020.)

3. Denial of Service (DoS): Ransomware-grupper skapar olika former av oreda som stänger ner offrens offentliga webbplatser.

4. Trakasserier: Cyberkriminella informerar kunder, affärspartners, anställda och media att organisationen hackats.

Även om det är sällsynt att man faller offerför alla fyra utpressningsmetoderna är det en trend att att ransomware-grupper tar till fler metoder när offren inte betalar efter kryptering och datastöld, enligt Unit 42 Ransomware Threat Report, som under förra året påvisade att dubbel utpressning då var starkt ökande. De nya rönen visar att utpressarna nu fördubblar det antal metoder de använder. Genom dessa nya utpressningsmetoder har ransomware-grupperna också blivit girigare.

5,3 miljoner dollar – genomsnittlig lösensumma

I de fall som Unit 42 granskade under första halvåret 2021 var det genomsnittliga lösensummekravet 5,3 miljoner dollar. Det är en ökning med 518 procent från förra årets 847 000 dollar.

Den högsta kravet konsulterna hittade mot ett enskilt offer var 50 miljoner dollar mot 30 miljoner förra året. Dock försökte Revil nyligen med ett nytt tillvägagångssätt genom att erbjuda en universell dekrypteringsnyckel för 70 miljoner dollar till alla organisationer som berörts av Kaseya VSA-attacken. Man sänkte snart kravet till 50 miljoner dollar och en universell dekrypteringsnyckel till Kaseya kom så småningom, men det är oklart hur stor, om ens någon, betalning som gjorts.

Den största bekräftade betalningen hittills i år var 11 miljoner dollar, vilket JBS SA avslöjade efter en kraftig attack i juni. Den största bekräftade betalningen förra året var 10 miljoner dollar.

Forsatt förvärring att vänta

Unit 42 förutser att ransomware-krisen kommer att förvärras under de kommande månaderna, eftersom cyberbrottsgrupper ytterligare skärper sin taktik för att tvinga sina offer att betala. Dessutom utvecklas nya tillvägagångssätt för att göra attackerna mer störande.

Till exempel har företaget börjat se att ransomware-grupper krypterar en typ av programvara som kallas en hypervisor, vilket kan skada flera virtuella händelser som kör på samma server. Vi förväntar en ökad inriktning på hypervisorer och annan infrastrukturprogramvara under de kommande månaderna. Efter attacken som använde Kaseyas fjärrhanteringsprogramvara till att distribuera ransomware till tjänstleverantörer och deras kunder, tror vi också på en ökad inriktning på dessa grupper.

Foto: Tegulhjati Pras / Pixabay

Offret betalar för att åter få tillgång till krypterade data och utsatta datorsystem som slutar fungera eftersom de nödvändiga filerna är krypterade.

Allt fler småföretag drabbas

Trots att lösensummorna förutspås fortsätta sin uppåtgående trend förväntas många utpressare fokusera på marknadens svagare led och konsekvent ge sig på små företag som saknar resurser för en stor investering i cybersäkerhet. Hittills i år har Unit 42 observerat grupper, inklusive NetWalker, Suncrypt och Lockbit, som kräver och tar in betalningar från 10 000 till 50 000 dollar. Även om ett lösenkrav kan verka relativt litet kan sådana summor ha förödande inverkan på ett litet eller medelstort företag.

Skadliga koden som drabbade Sverige särskilt hårt

Den mest utbredda skadliga koden i Sverige under juli var Snake Keylogger. Den drabbade uppskattningsvis nära 8,5 procent av de svenska verksamheterna, vilket är avsevärt högre än globalt där drygt 3 procent av verksamheterna drabbats, visar en ny rapport från Check Point Software Technologies.

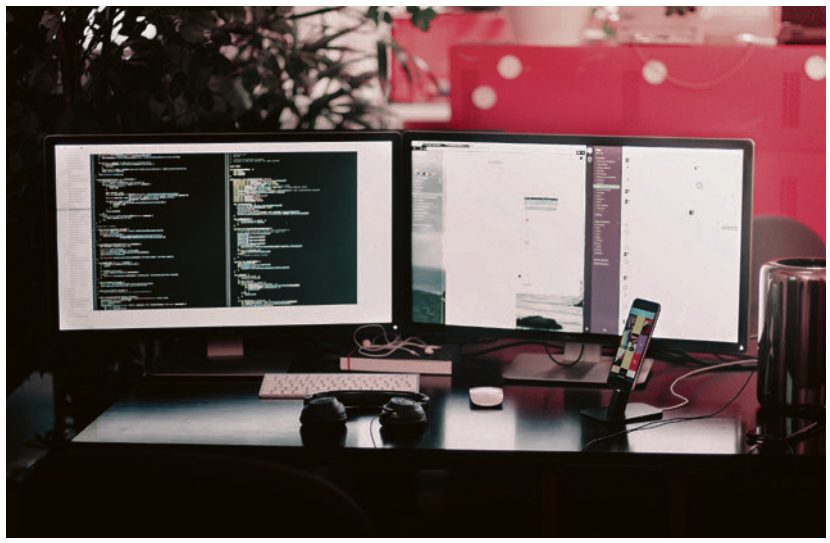


Foto: Pixabay

Under de senaste veckorna har Snake Keylogger vuxit snabbt via nätfiske-mejl med olika innehåll och mot olika branscher över hela världen.

Snake Keylogger är en skadlig kod som registrerar hur användare trycker på tangentbord på datorer eller mobiltelefoner, främst för att stjäla inloggningsuppgifter. Snake Keylogger upptäcktes första gången i november 2020. Under de senaste veckorna har Snake Keylogger vuxit snabbt via nätfiske-mejl med olika innehåll och mot olika branscher över hela världen. Snake Keylogger utgör ett stort hot mot användares integritet och nätsäkerhet, eftersom den skadliga koden kan stjäla praktiskt taget alla typer av privat information.

Välj unika inloggninguppgifter

Keylogger-attacker kan orsaka mycket stor skada eftersom användare ofta använder samma lösenord och användarnamn för flera olika tjänster.

– Kommer cyberkriminella åt ett användarnamn och lösenord kan det möjliggöra tillgång till alla användarens tjänster som använder samma inloggningsuppgifter. Vi rekommenderar därför också att användare bör ha unika inloggningsuppgifter för varje tjänst, säger Mats Ekdahl, säkerhetsexpert hos Check Point Software.

Skiftande prisbild på hackforum

Det går för närvarande att köpa Snake Keylogger på olika hackforum. Priset varier mellan 25 och 500 dollar beroende på vilken servicenivån som erbjuds.

Keyloggers som Snake distribueras ofta via nätfiskemeddelanden, varför det är viktigt att vara uppmärksam på felstavningar i länkar och e-postadresser och aldrig klicka på misstänkta länkar eller öppna obekanta bilagor, menar Check Point.

Minska lösenordsberoendet

Beroendet av enbart lösenord kan också minskas genom att implementera multifaktor-autentisering eller andra typer av inloggningsteknik, som exempelvis SSO (Single-Sign on).

”Dåligt förberedda företag öppnade upp för fler cyberattacker”

Cisco och Conscia låtit göra internationell undersökning om distansarbete och cybersäkerhet. Den visar på låg beredskap hos såväl svenska som utländska bolag när tjänstemän i allt högre utsträckning gick över till distansarbete till följd av pandemin.

I rapporten indikerar IT-cheferna att distansarbetet kommer att fortsätta vara högt på agendan hos många företag.

Distansarbetet har ökat markant i kölvattnet av pandemin och har satt digitaliseringen än högre upp för företagens prioriteringar runt om i världen. I såväl Sverige som i övriga världen visar det sig att företagen varit företagen dåligt förberedda på pandemins konsekvenser för arbetsplatserna.

I hög grad har företagen lämnat över ansvaret för den digitala säkerheten till medarbetarna.

– Osäkra uppkopplingar via hemmanätverk och ett alltför stort beroende av lösenord öppnade därför upp för ett ökat antal cyberattacker, säger Erik Arnberg, marknads- och kommunikationschef, Conscia Sverige AB.

> ***Osäkra uppkopplingar via hemmanätverk och ett alltför stort beroende av lösenord öppnade därför upp för ett ökat antal cyberattacker.***

Cyberattackerna ökade

Distansarbetet har sett en boom utan motstycke det senaste året där tusentals företag och hundratusentals svenskar nu, villigt eller motvilligt, jobbat utanför sin vanliga kontorsmiljö. Men vart tionde svenskt företag uppger att man inte alls var förberedd på distansarbetesboomen. Lite fler än var tredje, 36 procent, uppger att man var ganska förberedd. Samtidigt uppskattar 41 procent av de svenska företagen att antalet cyberattacker ökat under pandemin med 25 procent eller mer.

– Ransomware, nätfiske och datastöld är de tre huvudtyperna av attacker som hotar företag idag. Och när jobbdatorn kopplas upp från osäkra hemmanätverk och kanske används av flera familjemedlemmar som surfar eller klickar på okända länkar öppnar det upp för sårbarheter som en kontorsmiljö skulle sätta stopp för, säger Emanuel Lipshütz, CTO och Director Cybersecurity på Conscia Sverige.

Distansarbetet kräver nya rutiner

I rapporten indikerar IT-cheferna att distansarbetet kommer att fortsätta vara högt på agendan hos många företag. Och det innebär nya rutiner och nya former av samarbete att hantera. Liksom ett antal nya frågeställningar kring IT-miljön. Inte minst att stärka säkerheten hos användarna, något som 41 procent av företagen pekar på. Andra initiativ företagen prioriterar nu är att byta ut lösenordsanvändning mot flerfaktorautentisering.

– När vi frågade de svenska it-cheferna om de tror att någon CIO kan känna sig säker inför dagens cybersäkerhetshot svarade 96 procent nej, säger Emanuel Lipshütz.

Säkerheten högprioriteras

Och det är tydligt i rapporten att företagen prioriterar cybersäkerhet högre nu än innan pandemin. Nästan var fjärde svensk IT-chef klassar cybersäkerhet som extremt viktigt och över en tredjedel som viktigare än innan pandemin. Fyra av tio svenska företag avser också att öka sin budget för cybersäkerhet med minst 30 procent.

– Många företag och organisationer har behövt göra kompromisser med sina säkerhetspolicys under pandemin. Det är talande att undersökningens svenska IT-chefer pekar ut policyarbetet som det viktigaste att styra upp. Vi ser det i alla de zero trust-dialoger vi har med våra kunder, säger Henrik Bergqvist, cybersäkerhetschef, Cisco Sverige.

> ***Många företag och organisationer har behövt göra kompromisser med sina säkerhetspolicys under pandemin.***

För en elev som blivit av med sin dator kan det påverka veckor av skolarbete i förlorat material i väntan på att den gamla ska ersättas

350 skolstölder i månaden

Under vårterminen 2021 anmäldes 2141 stölder i skolor och på fritidshem där föräldrar och försäkringsbolag tvingades betala stora summor för att ersätta de stulna värdesakerna. Det är en minskning jämfört med året innan men under april–juni 2021 ökade stölderna och var högre än 2020 samma period.

Nu är verksamheten i skolorna i full gång igen och många elever har med sig cyklar, mobiltelefoner, kontanter, datorer och andra värdesaker till skolan.

Prata med barnen

Förutom att värdesakerna är stöldbegärliga är de även lätta att tappa bort eller glömma kvar på olika platser under dagen. Att behöva byta lås till hemmet på grund av borttappade/stulna nycklar eller att ersätta stulna teknikprylar är både kostsamt och tidskrävande. För en elev som blivit av med sin dator kan det påverka veckor av skolarbete i förlorat material i väntan på att den gamla ska ersättas.

– Det är viktigt att prata med sina barn och ungdomar om vad som är stöldbegärligt och informera om vad man ska tänka på. Dels för att öka medvetenheten hos unga om risken att bli av med sina saker men också för att få in ett brottsförebyggande tänk, säger Lina Nilsson, rådgivningsexpert på SSF Stöldskyddsföreningen.

Viktigt med säkra lösenord

I samband med skolstart bytte också många elever datorer och inloggning till skolans olika nätverk. För att minska risken att barnet bli utsatt för bedrägeri eller hackning är det även viktigt att barnens digitala produkter, dator och mobiltelefon skyddas med säkra lösenord.

SÅ KAN SKOLSTÖLDER FÖREBYGGAS

Det finns flera bra saker att tänka på som minskar risken att bli av med värdesaker och som framförallt ökar chanserna att få tillbaka dem igen. Här är några SSF-tips:

- Lämna inte värdesaker i skolans skåp, omklädningsrum, eller hängande i korridoren, utan ta med dem in i klassrummet eller gymnastiksalen.
- Lås fast cykeln i ramen i ett fast föremål med ett certifierat lås.
- Se till att ditt barn har säkra lösenord på dator och mobiltelefon.
- Sätt en Nyckelbricka från exempelvis SSF på hemnyckeln så ökar chansen att den kommer tillbaka om den kommer bort.
- Märk mobiltelefon, dator och cykeln med MärkDNA så blir de mindre stöldbegärliga och chansen ökar att du får tillbaka det som eventuellt stulits. Märk kläder med permanenta märkpennor.

Foto: Fredrik Hed / Pixabay

Enligt statistik från Polisen har båtstölderna hittills i augusti i år ökat i jämfört med samma period i augusti förra året.

Båtstölderna ökar

Nu har de flesta avslutat sina semestrar och så även båttjuvarna som är tillbaka och mer aktiva än under våren och sommaren. Enligt statistik från Polisen har båtstölderna hittills i augusti i år ökat i jämfört med samma period i augusti förra året. Även Larmtjänst rapporterar en tydlig ökning i augusti på vissa platser i landet.

Det blir nu mörkare och mörkare på kvällarna vilket underlättar för tjuven som kan arbeta mer ostört. Efter semestern då vi inte är lika aktiva på båtklubbar och bryggor och fram till dess att båtarna tas upp ur vattnet ökar ofta stölderna av båtar och båtmotorer.

– Se över vad du som båtägare eller båtklubb kan göra för att försvåra för tjuven, allt från certifierade lås på båtmotorn till belysning. Töm även båten på värdefull utrustning när du inte använder båten, säger Lina Nilsson expertrådgivare på SSF Stöldskyddsföreningen.

När det gäller stölderna handlar det ofta om beställningsjobb där man slaktar båten på exempelvis båtmotorer och utrustning som ofta hamnar utomlands men också på andrahandsmarknaden här i Sverige. Men det går att försvåra för tjuven och därmed minska risken att bli drabbad.

– Tyvärr finns det inga enkla lösningar för att skydda sig helt. Man måste utgå från de lokala förutsättningarna och hitta tillvägagångssätt för att försvåra för tjuven. Det är så vi arbetar inom Båtsamverkan. Att hjälpa och informera varandra om vad som fungerar och händer lokalt i regionen, säger Rino Carlsson, polis och nationell samordnare för Båtsamverkan.

FEM SSF-TIPS FÖR EN SÄKRARE FÖRVARING:

✓ Delta i Båtsamverkan! Det är viktigt att ha tillsyn på bryggor, marinor och hamnar under ALLA årstider.

✓ Sitter båtmotor kvar på båten, se till att den är fastlåst med godkänt certifierat lås.

✓ Ha ett kulhandskelås på släpet när båten står uppställd på tomten/båtklubben.

✓ Båt, motor och utrustning bör märkas med Märk-DNA och med stor fördel även förses med spårsändare och startspärr.

✓ Upprätta ett ”båtkort” med alla uppgifter på din båt, motor, utrustning, märkning m.m. så det snabbt kan anmälas om någonting blir stulet. Fotografera gärna!

Ny tjänst ska skapa säkrare samtal och försvåra telefonbedrägerier

Telefonbedrägerierna är ett växande problem som orsakar ökad känsla av otrygghet och stora ekonomiska förluster för de som drabbas. Nu inleder Stöldskyddsföreningen ett samarbete med säkerhetsföretaget Securifid, där de tillsammans ska skapa ett säkrare samtal för alla parter. Securifid har skapat en app som låter företag, myndigheter, organisationer och privatpersoner identifiera sig för varandra.

Lisa Hasselgren, vd och grundare till Securifid.

Stöldskyddsföreningen inleder ett samarbete med säkerhetsföretaget Securifid.

Stöldskyddsföreningen är en oberoende aktör som sedan 1934 arbetar med olika brottsförebyggande verksamheter mot både fysiska och digitala brott för att öka tryggheten i samhället. Genom samarbetet med Securifid utökar Stöldskyddsföreningen sin portfölj med digitala tjänster. Tillsammans ska de två organisationerna arbeta för att utveckla det brottsförebyggande arbetet i synnerhet gällande telefonbedrägerier.

– Vi ser ett allt större behov av säkra och pålitliga digitala lösningar som kan bidra till att förebygga brott. Securifids tjänst ligger helt i linje med vår verksamhet och genom vårt samarbete lyfter vi fram en tjänst som bidrar till ökad trygghet i samhället, säger Tomas Brühl, vd på Stöldskyddsföreningen.

– Det ska vara en självklarhet att kunna identifiera sig i ett samtal, oavsett om det är i rollen som tjänsteman eller privatperson, menar han vidare. Det skapar trygghet för alla parter, berättar Tomas Brühl, vd på Stöldskyddsföreningen.

Misshandel blev startpunkten

Idén till Securifid föddes när grundaren Lisa Hasselgren blev vittne till en misshandel. Hon filmade händelsen och fick kort därefter ett telefonsamtal från Polisen som ville ta del av bevismaterialet. Eftersom de inblandade hade sett när Lisa filmade blev hon osäker på om det faktiskt var Polisen som ringde. Det fanns inget sätt för henne att kontrollera att personen som ringde henne faktiskt var den som hen utgav sig för att vara och hon var rädd för att bli lurad.

Bidrar till rättssäkerheten

Securifid skapades ur det stora behovet för människor och organisationer att kunna identifiera sig för varandra. Ingen ska behöva tvivla på att det är vårdcentralen, banken eller myndigheten som ringer. Därigenom bidrar Securifid också till att upprätthålla rättssäkerheten i samhället.

– Samarbetet med Stöldskyddsföreningen är oerhört viktigt för att vi ska lyckas etablera oss på marknaden. Det krävs att vi har en stark, kunnig och trovärdig aktör med oss för att fler ska börja använda vår tjänst, säger Securifids grundare och vd Lisa Hasselgren.

Lisa Hasselgren hoppas att ännu fler företag och organisationer börjar använda Securifid för att värna om sina kunders och om medborgarnas trygghet, såväl som det egna ryktet.

– Tillsammans med Stöldskyddsföreningen kan vi sprida kunskapen om hur man kan förebygga bedrägerier med relativt enkla medel, utan att begränsa individens frihet, kommenterar hon vidare.

Securifid-tjänsten

Securifid är en nytänkande och säker identifieringstjänst som skapar trygga samtal mellan privatpersoner, företag, myndigheter och organisationer. Appen möjliggör säker identifiering via exempelvis BankID och Freja eID mellan två uppkopplade parter. Man kan ladda ner Securifid i App Store eller Google Play.

SSF bryter ny mark för digitala äkthetsbevis

Nu lanserar Stöldskyddsföreningen SSF ett nytt sätt att verifiera sin utbildning. Syftet är att öka säkerheten och värdet i arbetsdokument. Säkerhetsarbetet blir allt viktigare i företag och organisationer och det gäller också vid nytillsättning och rekryteringar vid arbetstillfällen.

I mer än 50 år har Stöldskyddsföreningen genomfört säkerhetsutbildningar som ger praktiska verktyg för att skapa en trygg och säker arbetsplats. Nu kan utbildningsdeltagarna dessutom få ett digitalt och modernt dokument att visa upp sin nyvunna kunskap inom säkerhet

Baserad på bockchain-metod

Utbildningsdeltagarna kan få ett digitalt SSF diplom för sina utbildningar hos Stöldskyddsföreningen. Diplomet bygger på en säker blockchain-metod. Det är en robust databas som lagras i många kopior, som gör det svårt att manipulera originaldokumentationen. Det gör att du kan lägga ut ditt Diplom på arbetsnätverk såsom LinkedIn.

Diplomerade säkerhetschefer

Först ut i denna lansering är diplomen för Diplomerad Säkerhetschef, som verkligen kan behöva styrka och bekräfta sin säkerhetskompetens. Genom True Cert och SSF så kan säkerhetschefer på ett tillförlitligt sätt visa sina arbetskontakter att man har genomgått Diplomerad Säkerhetschef hos Stöldskyddsföreningen.

– Nu tar vi diplomen in i framtiden, menar säkerhetsexperten Tomas Devenyi. Den blivande arbetsgivaren kan enklare kontrollera intygets ursprung och äkthet, vilket ju är av extra vikt när det handlar om säkerhet i allmänhet och säkerhetsutbildningar i synnerhet, påtalar han vidare.

Svårt att manipulera

Papperskopior och betyg är lätta att förfalska inför en tillsättning av en arbetsroll och därför är det enklare att kontrollera dessa digitalt via en säker källa. Det är svårt för arbetsgivaren att göra efterkontroller när det gäller betyg och intyg. När allt fler bedrägerier gäller pappersdokument, så handlar om att det visa upp tillitsfulla dokument vid en arbetsintervju. Som ett led i att försvåra dessa bedrägerier så kommer nu digitala diplom som är svårare att manipulera.

SSF startar företagsdel på säkerhetskollen.se

I november förra året lanserade SSF Säkerhetskollen som en heltäckande tjänst för information om digitala brott. Lanseringen riktade sig till allmänheten med funktioner som rådgivning, varningar om pågående brottsförsök och möjlighet att ge tips. Nu lanserar SSF även en företagsdel på Säkerhetskollen.

Digitala brott som bedrägerier är ett stort problem i samhället, inte bara för allmänheten utan i allra högsta grad även för företag. Förra året polisanmäldes totalt närmare 220 000 digitala brott av olika slag. Det pågår ständiga bedrägeriförsök för att lura företag att betala falska fakturor men även försök till att komma åt möjlighet till IT-intrång.

SSF lanserar därför en företagsdel med särskild inriktning mot att minska risken för intrång i IT-systemen. Erfarenheterna och innehållet kommer förutom SSF vanliga rådgivningsarbete även från SSF samarbete med MSB kring cybersäkerhetsnormen SSF 110 som avhandlar åtgärder för att förebygga intrång i IT-system.

– På Säkerhetskollen Företag hittar du även aktuell information, utbildning om att jobba säkert digitalt, säkerhetsguider kring bland annat ransomware, vd-bedrägerier och mycket annat. Bäst är att själv besöka sidan och bekanta sig med dem, säger Thomas Brûhl, vd för SSF.

Nu lansers en företagsdel på Säkerhetskollen.se som syftar till att minska risken för intrång i IT-system.

Med företagsdelen så kompletterar SSF Säkerhetskollen så den även fyller de behov som finns för företagare inom små och medelstora företag.

– Gå in och testa ditt företags säkerhet och läs mer om hur du kan certifiera dig inom området, avslutar Thomas Brûhl.

Dataintrång mot sociala medier och e-tjänster fortsätter öka

Under en längre tid har dataintrång mot sociala medier och e-tjänster ökat drastiskt. Från januari 2021 till juli 2021 så ökade anmälningarna med 40 procent, tittar man längre tillbaka, från juli 2020, så är ökningen 119 procent fram till idag. Enbart i juli 2021 så polisanmäldes 587 dataintrång mot sociala medier och e-tjänster, vilket är en ökning med ca 16 procent jämfört med månaden innan.

Det vi sett det senaste året, när vi samtidigt levt i skuggan av en pandemi, är att dejtingsajterna till stor del tagit över scenen som mötesplats och att användningen av olika sociala medier ökat på liknande sätt. Ärenden som kommer in till Stöldskyddsföreningens digitala tjänst, säkerhetskollen.se, visar att konton hackas på Facebook och andra sociala medier där man försöker lura användare på deras personliga uppgifter.

– Skydda dina konton genom att använda säkerhetsåtgärder som exempelvis tvåfaktorsautenticering. Sedan så ska du självklart inte klicka på okända länkar som kan förekomma i sociala medier, mejl och sms säger Paul Pintér, Rådgivare mot digitala brott vid SSF Stöldskyddsföreningen.

Att kunna skilja falska konton från andra är inte helt enkelt, men det finns saker att vara uppmärksam på när meddelandet handlar om att:

- Jag är i knipa behöver ett snabblån.
- Jag behöver låna dina inloggningskoder till bankdosan då min är trasig.
- Samla in pengar till behövande.
- Jag vill ha ditt telefonnummer.
- Jag vill att du ska skicka verifikationskoden som du har fått.

Konsekvenserna av dessa intrång är att människor bland annat kan bli utsatta för bedrägeri. Här är SSF tips för att undvika dataintrång.

- Ha starka och unika lösenord för varje tjänst, helst en lösenordsfras.
- Lämna aldrig ut några privata uppgifter till någon annan.
- Använd om möjligt en lösenordshanterare.
- Aktivera tvåfaktorinloggning där det går.
- Klicka aldrig på några länkar som du är osäker på.
- Tacka inte ja till okända personers vänförfrågan utan att ha gjort en gedigen research kring personen ifråga.
- Logga ut från det sociala mediet så fort du slutat att använda det.
- Kontrollera alltid suspekta meddelanden som kommer från ”vänner”.

Säkra din mobil mot QR-kod-bedrägerier

Koder har funnits länge i vårt samhälle, koder har använts till bland annat att kryptera information, gömma information eller förvandla en typ av information till en annan typ, det är just detta som QR koden gör.

QR står för Quick Response och är en standard för så kallade rutkoder, denna kod utvecklades av ett japanskt företag redan 1994 som en lösning på den begränsade EAN-koden (streckkoden). Dessa QR koder kan tyvärr också användas av bedragare.

Tvådimensionell kod

QR koden är en tvådimensionell kod, vilket betyder att den kan läsas uppifrån ned samt från höger till vänster, för att på detta sätt lagra mer information än en vanlig streckkod (EAN) som bara kan läsas uppifrån och ned. Mönstren i QR-koderna representerar exempelvis webbadresser, telefonnummer eller texter upp till 4 000 tecken.

Så kan QR-koder användas

QR-koder kan användas för att:

- Länka direkt för att ladda ned appar.
- Autentisera konton online och verifiera inloggningsuppgifter hos banker och e-tjänster såsom Swish, 1177 och Kivra.
- Få åtkomst till Wi-Fi genom att lagra krypteringsinformation såsom SSID, lösenord och krypteringstyp.
- Skicka och ta emot betalningsinformation.

Kan drabba användare hårt

Eftersom QR-koder innehåller stora mängder data är det möjligt att de kan användas för att dölja information som används för nätfiske. Smarta hackare kan också använda QR koder för att rikta användare till dolda nedladdningar av skadlig programvara eller tvinga användarens mobiltelefon att skicka meddelanden till betalnummer.

– Om din smartphone tillåter installation av säkerhetsprogram som kontrollerar webbplatser för skadligt innehåll och nedladdad programvara för skadlig programvara, se till att du installerar ett sådant program. Det finns skadliga kod ute som kan infektera de flests mobiltelefoner som finns på marknaden, säger Paul Pintér, rådgivare digitala brott vid SSF

Se till att du kommit rätt

När en användare tar ett foto av en QR -kod visas länken som den lagrar först på enhetens skärm; cyberbrottslingar använder emellertid också förkortningstjänster för webbadresser, exempelvis ”bit.ly” för att dölja den slutliga adressen som har lagrats i QR koden, vilket kan leda till en sida med skadlig kod som stjäl användarens referenser eller till en nätfiskewebbplats. När du har öppnat en appbutik eller en webbplats i din webbläsare, se till att QR koden har tagit dig till den plats du förväntade dig att gå.

Det finns skadliga kod ute som kan infektera de flests mobiltelefoner som finns på marknaden, säger Paul Pintér, rådgivare digitala brott vid SSF.

Foto: Gerd Altmann / Pixaby