Rapport: Förstudie om digital säkerhet för små och medelstora företag i Skåne

Författare och bidragsgivare: Thomas Rosenstatter (RISE), Janos Olajos (Mobile Heights), Linda Håkansson (IUC Syd) , Liza Johansson (IDEON), Pernilla Lavesson och Rebecka Nilsson (Media Evolution)

Datum: 2023-03-15

Rapporten är finansierad av Region Skåne – Verkställighet av Regionala utvecklingsnämndens budget för perioden juni-september 2022

Sammanfattning

Digital säkerhet används mot angripare eller hackare med olika motiv, t.ex. att stjäla känsliga uppgifter som immateriella rättigheter, neka vanliga användare tillgång till systemet (Denial of Service) eller tjäna pengar på information/data online genom att antingen utpressa offret eller sälja informationen på darknet. Sannolikheten att utsättas för en cyberattack ökar ständigt, dels på grund av samhällets växande uppkoppling i alla aspekter av vårt dagliga liv och å andra sidan på grund av den geopolitiska instabilitet vi just nu står inför p.g.a. den ryska invasionen av Ukraina. Med tanke på att små och medelstora företag står för 49 % av Sveriges ekonomi och står för 56 % av sysselsättningen[1] behöver vi ytterligare stödja dem i att göra deras företag cybersäkra mot attacker. I USA hävdar FBI att en våg av cyberattacker mot små och medelstora företag är att vänta när stora företag investerar i cybersäkerhet medan små och medelstora företag tenderar att vara "mjuka mål"[2], vilket sannolikt också är fallet för Sverige.

Rapporter som publicerats under de senaste två åren visar att cybersäkerhetsincidenter kommer att öka mot västländer, deras företag och

[1] https://www.oecd.org/cfe/smes/Sweden.pdf
[2] https://www.cnbc.com/2022/12/16/fbi-7-billion-lost-in-criminal-hacks-most-victims-small-businesses.html

individer. Ett exempel på en kraftfull cyberattack som inträffade i Sverige var en så kallad Denial of Service-attack mot Trafikverkets internetleverantör TDC och DGS som i slutändan ledde till störningar i tågschemat och följaktligen förseningar runt om i Sverige (RISE, 2022). Denial of Service-attacker syftar till att göra en viss resurs, såsom en webbplats eller en server, otillgänglig för normal användning. En annan typ av attacker som orsakat rubriker under de senaste åren är så kallade ransomware-attacker där angriparen kräver lösen i utbyte mot att göra en resurs eller information tillgänglig igen (ENISA, 2022). Coop, till exempel, har blivit ett offer för en sådan attack, även om endast "passivt" då en av deras mjukvaruleverantörer blev attackerad, men det tvingade Coop att stänga ner sina butiker tillfälligt. Ransomware-attacker har blivit ett särskilt problem eftersom brottslingar har utvecklat en ny affärsmodell som heter "Ransomware as a Service (RaaS)" som gör denna mer tillgänglig. Microsoft uppger i sin årliga (Microsoft, 2022) rapport att 93 % av ransomware-attackerna beror på otillräcklig kontroll av åtkomstprivilegier inom det attackerade nätverket. Dessutom framhåller Microsoft också att *social engineering* fortfarande är ett allvarligt hot eftersom riktade attacker ofta resulterar i framgång.

Sammantaget är cybersäkerhet en möjlighet för våra företag att fortsätta växa och förnya sig. 100 procent säkerhet är eftersträvansvärt, men kan förmodligen aldrig uppnås. Ändå måste säkerhetsåtgärder för att försvara sig, skydda data och reagera på attacker finnas på plats och kontinuerligt uppdateras och utvärderas. Dessutom måste företag ha adekvata verktyg och processer på plats när det kommer till hur säkerhetsincidenter ska hanteras.

Resultaten av vår onlineundersökning med 26 svarande som arbetar i små och medelstora företag i Skåne visar att det fanns minst en individ i varje attackscenario som sa att de medvetet varit offer för en sådan attack. Attackscenarionerna vi identifierade var: nätverk/server hackad, datastöld eller kryptering, virus-/malwareinfektion, smartphonehack och nätfiske-e-post. Vidare menar vi att denna undersökning också belyser ett missförstånd av cyberattacker och deras inverkan. Till exempel, av de fem attackscenarierna bedömdes de tre första ha störst inverkan, medan smartphones som hackades och nätfiske-e-post mest bedömdes ha en liten eller medelstor inverkan på företaget. Detta belyser också en något begränsad förståelse för komplexiteten i cyberattacker, eftersom de sista typerna av attacker är det första steget för angripare att få tillgång till systemet och i slutändan äventyra hela IT-infrastrukturen i ett företag. Betydelsen av *social engineering*/nätfiske-attacker identifieras också i Cybersäkerhet i Sveriges

rapport 2022 av Nationellt Cybersäkerhetscenter. Positivt är att vår studie indikerar att människor har blivit mer medvetna om de olika typerna av attacker, särskilt om nätfiskeattacker eftersom hälften av de tillfrågade angav att de varit utsatta för sådana attacker tidigare. Detta beror sannolikt också på det pedagogiska arbetet riktat till allmänheten.

Cybersäkerhet i och utanför Sverige

För att hitta aktuella trender kring cyberattacker inom Sverige, men även i världen i stort, har vi granskat rapporter publicerade 2022 och 2021 som ger en analys av cybersäkerhetshotet (hotlandskapet) från olika håll. Vi granskade:

- rapporten Cyberhot mot Sverige (RISE, 2022) av RISE (ett oberoende, statligt forskningsinstitut) som riktar sig till ledare och beslutsfattare
- rapporten "ENISA Threat Landscape 2022" (ENISA, 2022) sammansatt av Europeiska unionens byrå för cybersäkerhet, som identifierar de främsta hoten och riskerna såväl som hotaktörer och attacktekniker.
- rapporten "Internet Organized Crime Threat Assessment" (Europol, 2021) som i 2021 års upplaga fokuserar på förändringarna i cyberbrottslighet jämfört med föregående år. En rapport för år 2022 har ännu inte publicerats.
- rapporten ”Cybersäkerhet i Sverige 2022” från Nationellt Cybersäkerhetscenter beskriver i första delen hoten och attackerna och fokuserar i den andra delen på lämpliga motåtgärder.
- Microsofts "Digital Defense Report 2022" (Microsoft, 2022) ger en översikt över 2022 års hotlandskap samt hur deras försvarsmekanismer kunde förhindra framgången för olika attacker.

Sammantaget identifierar alla Denial of Service (DoS)-attacker, mer specifikt Distributed DoS (DDoS), ransomware-attacker och dataintrång och doxning. Dessutom tillhandahåller ENISA i sin rapport ett bredare spektrum av hot och nämner också specifikt *social ingenjörskonst*, desinformation och attacker i leveranskedjan. Alla rapporter lyfter också fram att cybersäkerhet blir viktigare i takt med att fler och fler delar av samhället kopplas upp, vilket leder till en ökad attackyta för angripare men ökar också attackernas genomslagskraft. Nedan förklarar vi kort attackerna samt deras inverkan på organisationerna.

Denial of Service (DoS)-attacker är attacker som riktar sig mot tillgängligheten av resurser, tjänster som webbplatser och själva datat. Även om den här typen av attacker inte är nya anses de fortfarande vara ett av de största hoten. Till exempel Mirai Botnet[3] som blockerade användare från att komma åt de tjänster som tillhandahålls av stora företag, som Spotify, Twitter, Sony och Amazon i hela USA

[3] https://www.cloudflare.com/en-gb/learning/ddos/glossary/mirai-botnet/

och Europa[4] genom att utföra en DDoS-attack på Dyn, en leverantör av domännamnstjänster (DNS). Ett mer ”lokalt” exempel på en DDoS-attack är attacken mot Trafikverkets internetleverantörer[5] (TDC och DGC) som resulterade i tågförseningar över hela Sverige. Som framhållits i (RISE, 2022) har DoS-attacker direkt inverkan på vårt samhälle och kan leda till allvarliga konsekvenser när kritisk infrastruktur (t.ex. energi, transport eller banksektorn) påverkas.
Vidare kan det också få allvarliga konsekvenser för små och medelstora företag som inte kan tillhandahålla sina kunder de tjänster som leder till ekonomisk förlust och en negativ inverkan på ryktet om incidenten hanteras på ett felaktigt sätt. Små och medelstora företag kanske inte är huvudmålet för DDoS-attacker eftersom de måste riktas mot en specifik tjänst, men de kan påverkas indirekt eftersom tjänsteleverantören (t.ex. Dyn) kan vara måltavla.

Ransomware-attacker syftar till att ta kontroll över offrets tillgångar (t.ex. data) genom att kryptera dem och kräva lösen i utbyte mot krypteringsnyckeln, med andra ord "återlämnande av tjänstens tillgänglighet" (ENISA, 2022). Ett slående exempel är attacken mot mjukvaruföretaget Kaseya som drabbade flera svenska företag. Till exempel behövde Coop stänga sina butiker i flera dagar då kassasystemet påverkades av denna attack.
Ransomware-attacker är redan ett allvarligt hot och verkar fortfarande öka. En anledning är en ny "affärsmodell" kallad Ransomware as a Service (RaaS) där en grupp kriminella utvecklar ransomware genom att utnyttja en viss sårbarhet i datorsystemet och erbjuda andra kriminella att använda detta "verktyg" i utbyte mot en andel. av vinsten. Därför kan vem som helst kunna använda detta verktyg och rikta en attack mot även små och medelstora företag genom att använda till exempel *social engineering* som beskrivs nedan (Microsoft, 2022).

Social Engineering-attacker består av ett brett utbud av aktiviteter eftersom de syftar till att utnyttja mänskligt beteende för att få obehörig åtkomst till offrets dator (användare avslöjar sitt lösenord) eller annan information/åtkomst (åtkomst till sitt bankkonto). Det slutliga målet är att övertyga eller locka människor att öppna skadliga webbplatser eller ladda ner skadligt innehåll som gör att angriparen i slutändan kan komma åt offrets dator. (ENISA, 2022) belyser det breda utbudet av *social engineering* och nätfiske. Nätfiske kan till exempel antingen riktas mot en bred grupp, t.ex. skickar angriparen ett e-postmeddelande som utger sig för att vara offrets bank, eller riktar sig mot specifika individer eller organisationer (kallat spjutfiske). I likhet med RaaS finns Phishing as a Service där brottslingar utvecklar så kallade kits som innehåller redan färdigt material. Ett annat mer "fysiskt" exempel är användningen av QR-koder, som noterats i (ENISA, 2022), där attacker lanserades med QR-koder som ledde till en skadlig webbplats och distribuerades i syfte att locka offren att skicka in sina inloggningsuppgifter och ekonomisk information.

[4] https://coverlink.com/case-study/mirai-ddos-attack-on-dyn/
[5] https://computersweden.idg.se/2.2683/1.690504/ddos-bakom-tag-forseningar

En motåtgärd till enklare former av nätfiskeattacker var införandet av multifaktorautentisering, där användare måste verifiera sin identitet genom en annan kommunikationskanal, t.ex. SMS, push-notiser som kräver att användaren godkänner inloggningen. Sådana lösningar förbättrar definitivt IT-systemets säkerhet, men de senaste attackerna kan kringgå det, t.ex att ett offer får kontinuerliga förfrågningar på sina mobiltelefoner som ber användaren att acceptera/lita på inloggningen (även om de inte startade inloggningen själva). Till en början kan de ignorera dessa meddelanden, men efter några timmar eller dagar kan offret vara berett att acceptera det för att "bli av med det" eller av misstag acceptera en av dessa förfrågningar. Och bara ett enda "acceptera" behövs för att angriparen ska få tillgång till systemet (eftersom angriparen redan har fått lösenordet genom *social engineering* eller via darknet). Denna attack kallas *MFA fatigue*[6].
Social Engineering är ofta det första steget för angripare att få tillgång till systemet eller information och därför är det viktigt att utbilda anställda för att öka medvetenheten om sådana tekniker.

Skadlig programvara på mobiltelefoner har också ökat under de senaste åren, eftersom framgångsrikt installerad skadlig programvara kan användas för att övervinna multifaktorautentiseringen där skadlig programvara används för stöld av svarskoderna eller till och med låter dem acceptera dem (Europol, 2021).

Dataintrång och doxning är ofta riktade attacker mot individer eller organisationer. Till exempel blev Riksidrottsförbundet flera gånger måltavla mellan december 2017 och maj 2018 av den ryska militären (GRU)[7]. Säkerhetspolisen menar att detta var ett försök från Ryssland att distrahera från sin egen dopningsskandal genom att peka ut och smutskasta andra länders idrottare. Andra former av doxying är när personlig information som adresser eller telefonnummer publiceras,. Ett annat exempel är inblandningen under val där information som erhållits genom hacks (som uppnås genom social engineering) publicerats vid kritiska tidpunkter (RISE, 2022).
Små och medelstora företag kanske inte är målgruppen för doxingattacker, men beroende på organisationens affärstillgångar kan de vara mål så att angriparen får kunskap eller affärshemligheter (immateriella rättigheter), även kallat cyberspionage.

[6]https://www.bleepingcomputer.com/news/security/mfa-fatigue-attacks-are-putting-your-organization-at-risk/
[7]https://www.sakerhetspolisen.se/download/18.650ed51617f9c29b552287/1649683389251/Sakerhetspolisen_arsbok%202021.pdf

Resultat från undersökning med 26 svar.

För att undersöka de aktuella utmaningarna och behoven hos små och medelstora företag i Skåne genomförde vi en webbenkät som 26 anställda/VD:ar/ägare svarade på. Undersökningen var uppbyggd i tre delar, dvs (i) allmänna frågor om personerna och företaget de arbetar i, (ii) hotbedömning och (iii) bedömning av förmågan att hantera. De specifika frågorna visas i bilaga 1.

Bakgrundsinformation

Figur 1 och figur 2 visar lite bakgrundsinformation om de svarandes företag. Figur 1 visar fördelningen av små och medelstora företag i termer av storlek; 11 svarande arbetar på småföretag med färre än 10 anställda, 9 svarande i småföretag med färre än 50 och 6 respondenter i medelstora företag med färre än 250. Vidare visar figur 2 variationen i de svarandes position och primärsektorn för företaget. Tolv av de 26 svarande var antingen VD eller ägare till företaget, fyra ansvarade för IT och 10 var anställda inklusive chefsbefattningar utanför VD. Med tanke på denna fördelning av anställningsstatus inkluderar resultaten inte bara den anställdes erfarenhet av cybersäkerhet, utan också erfarenheten och åsikten från den högre ledningen inklusive ägarna. Den primära sektor som företagen tillhör är också bred och omfattar produktion, tjänster, mjukvara/elektronik, men även marknadsföring/kommunikation och ett arkitektföretag. Denna variation i storlek, position och segment är fördelaktig eftersom undersökningen täcker uppfattningen hos ett stort urval, samtidigt som resultaten endast kan ses som indikatorer på nuvarande uppfattningar om cybersäkerhetsfrågor snarare än en komplett bild.

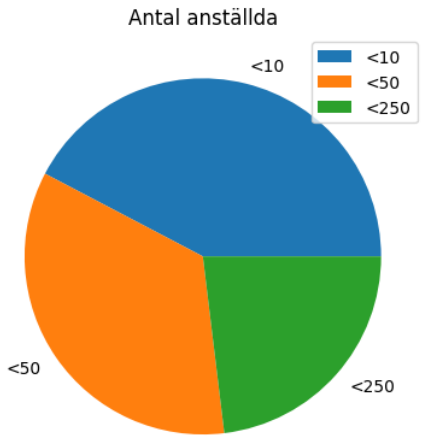
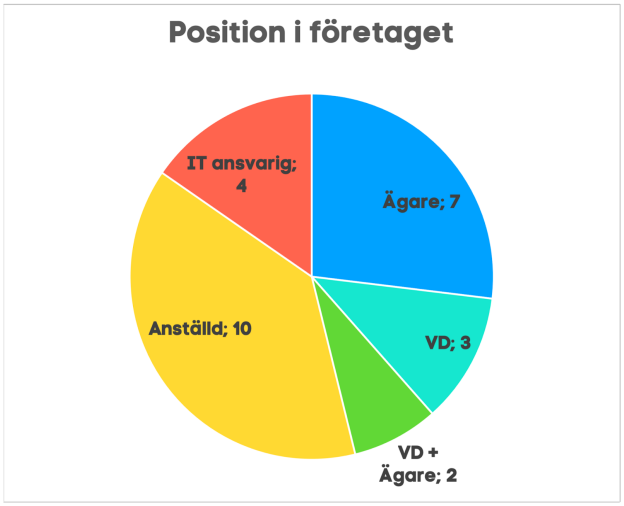
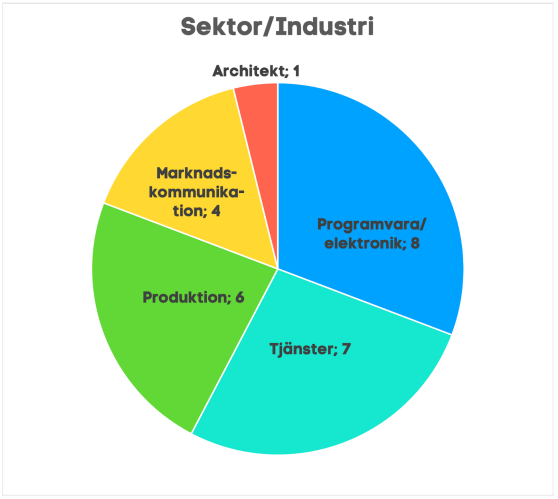


Bild 1. Fördelning på storlek hos SME som svarat





(a) (b)

Bild 2a. Fördelning av de svarandes position och **Bild 2b.** Fördelning av sektor.

Hotbedömning

I denna del av enkäten strävar vi efter att få insikter i de svarandes egen uppfattning, till exempel om de tror/vet att de redan minst en gång varit offer för en cyberattack eller inte, hur sannolikt de tror att de kommer att bli offer samt attackernas severitet. För dessa frågor identifierade vi följande hotscenarier liknande (Wilson, 2022):

- nätverket eller servrarna har hackats
- data har stulits eller krypterats (ransomware)
- ett system är infekterat med skadlig programvara
- en mobil enhet har äventyrats
- nätfiske-e-postattack

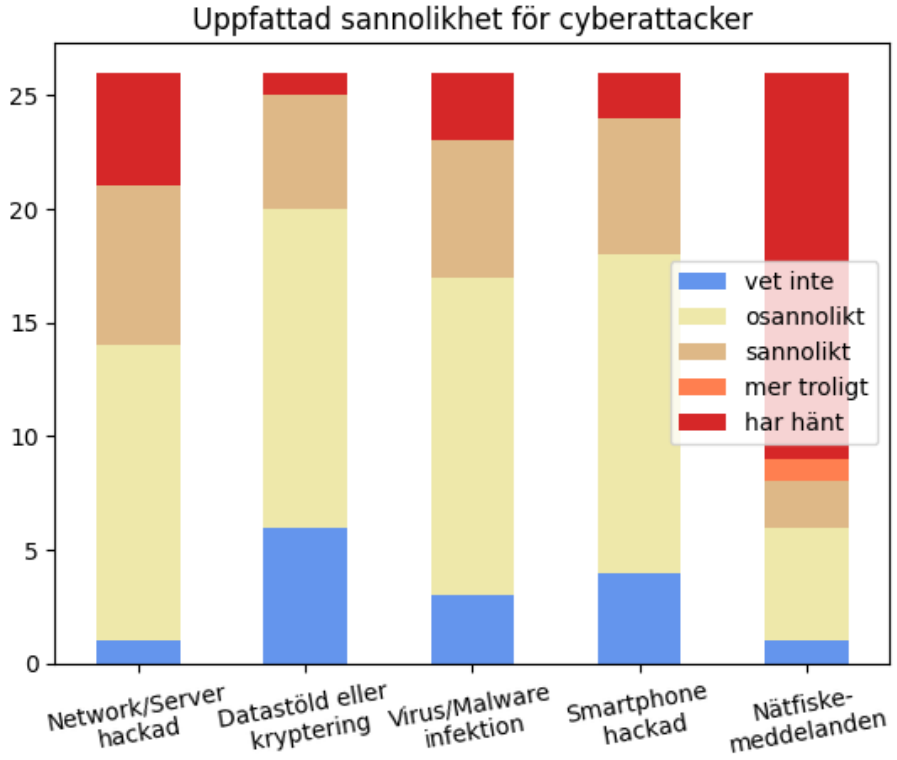


Bild 3. Histogram över de 5 scenarierna och den bedömda sannolikheten att drabbas av dessa.

Den upplevda sannolikheten för de identifierade hotscenarierna visas i bild 3. Den visar att alla de fem scenarierna har hänt tidigare. Det höga betyget av nätfiskemail indikerar också att medvetenheten om dem är mycket högre, troligen också på grund av offentliga kampanjer om nätfiskemail. En annan orsak till att ett så stort antal svarar att de blivit utsatta för detta och anser att de är sannolika kan också vara det faktum att sådana attackförsök också upplevs av många anställda som inte nödvändigtvis är i chefspositioner eller arbetar med att hantera IT-systemet. Vidare menade två av de tillfrågade att även nyare typer av attacker, som smartphonehackning händer. Smartphoneattacker är särskilt viktiga att tänka på, eftersom de inte bara kommer åt företagets nätverk, utan också används för tvåfaktorsautentisering. På grund av variationen av deltagare i denna studie samt att det inte fanns möjlighet att ställa uppföljningsfrågor kan vi inte tydligt säga varför vissa deltagare svarade att deras företag sannolikt inte kommer att uppleva dessa scenarier. Man kan bara gissa att dessa personer antingen tror att de har minskat risken på lämpligt sätt genom att implementera nödvändiga säkerhetsprodukter och -praxis, eller att de bara är väldigt optimistiska. Det senare stöds också av (Wilson, 2022) som hänvisar till flera skotska studier som pekar på att små och medelstora företag vanligtvis är mer optimistiska, möjligen för optimistiska!

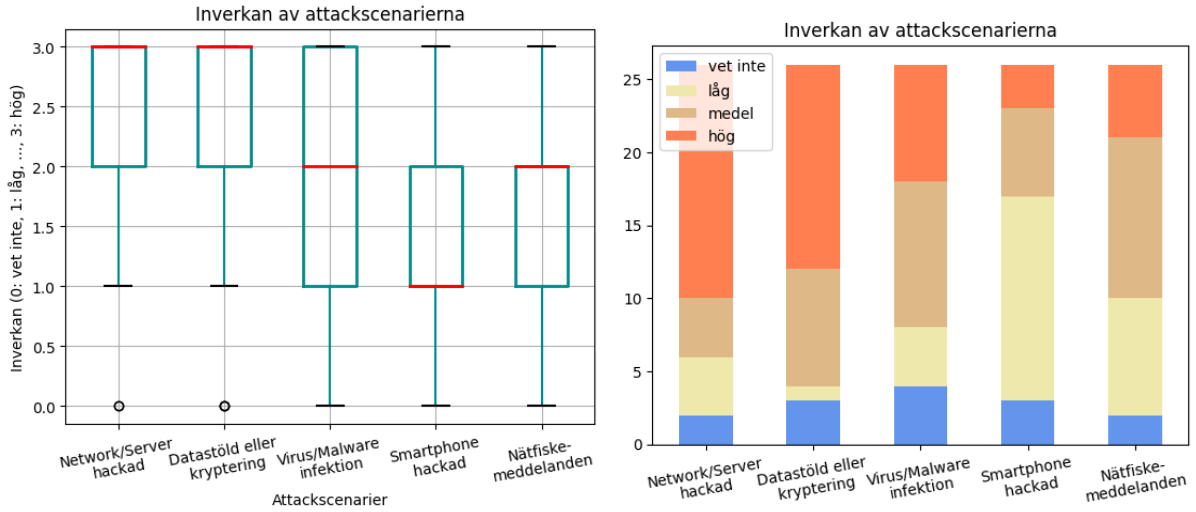


Bild 4. En boxplot och histogram visande den uppfattade påverkan på företaget för respektive attack.

När man betraktar den upplevda effekten av attackscenarierna hos små och medelstora företag, håller majoriteten med om att de tre första attackscenarierna, de mer traditionella, välkända attackerna, identifieras som hög och medelstor påverkan. De andra attackerna, dvs. smarttelefonen som hackas och nätfiske-e-post, identifieras dessa ha liten till medelstor inverkan på företagets verksamhet. Dessa attacker i sig kanske inte har så stor inverkan, men detta indikerar också att många av de tillfrågade kanske inte nödvändigtvis förstår konsekvenserna av en framgångsrik smartphonehack/nätfiske-attack som kan leda till att hela systemet äventyras.

Bedömning av förmågan att hantera

Den här delen av frågeformuläret syftar till att få insikter i de svarandes egna uppfattning om säkerhetsmekanismer, tekniker och produkter som hjälper till att minska risken för cyberattacker. Vi strävar till exempel efter att få mer insikt i deras uppfattning om deras effektivitet och kostnaden/förmågan att implementera dem. Följande säkerhetsmekanismer och metoder identifierades i (Wilson 2022) och utökades av oss:

- Användning av starka, unika lösenord för företagskonton.
- Regelbunden säkerhetskopiering av data.
- Förebyggande av skadlig programvara (skadlig programvara, inklusive virus) infektioner med hjälp av till exempel endpoint-skydd, brandväggar, etc.
- Konfiguration av mobila enheter så att de kan spåras på distans, raderas och låsas.

- En process som övervakar publiceringen av säkerhetsuppdateringar och ytterligare stödjer identifieringen av berörda system inklusive en uppdateringsplan.
- Övervakning av IT-infrastrukturen och bearbetning av säkerhetsvarningar (d.v.s. att ha ett Security Operation Center (SOC) eller dess uppgifter implementerade).

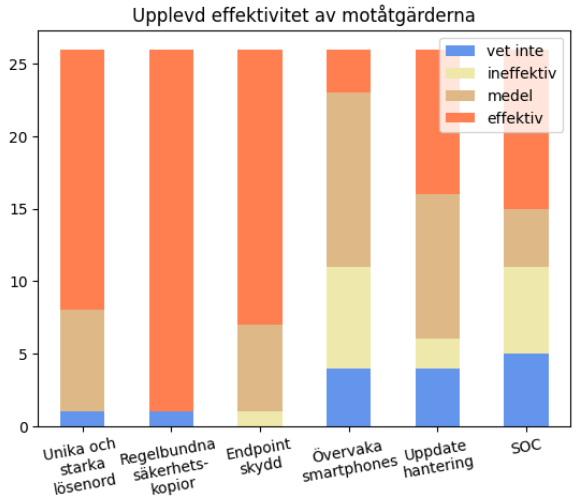


Bild 5

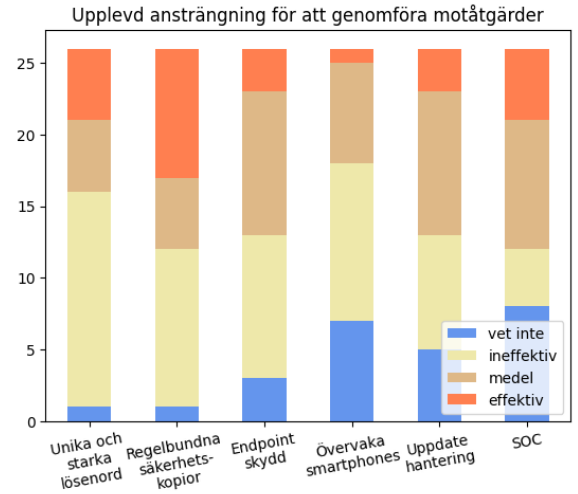


Bild 6

Bild 5. Upplevd effektivitet av en rad motåtgärder. **Bild 6.** Upplevd ansträngning att implementera en rad motåtgärder.

Den upplevda effektiviteten hos säkerhetsmekanismerna och metoderna som visas i figur 5 belyser att traditionella och välkända säkerhetslösningar, såsom användningen av starka unika lösenord, att ta regelbundna säkerhetskopior av data och ha brandväggar och antivirusprogram upplevs vara mer effektiva än metoder som är jämförbart nyare, det vill säga övervakning och hantering av smartphones, uppdateringshanteringsprocesser och att ha ett säkerhetsoperationscenter. Detta stöds också av det faktum att fler svarande valde alternativet vet ej för de tre sistnämnda metoderna. Resultaten om den upplevda ansträngningen/kostnaderna i figur 6 stödjer antagandet att nyare metoder och deras effektivitet är mindre kända för ett större antal av de svarande. Att ha rutiner för säkerhetsövervakning (en SOC) på plats rekommenderas också av Nationellt Cybersäkerhetscenter eftersom det krävs upptäckt av förändringar i systemet för att någon skall reagera på den pågående, möjligen ganska komplexa attacken.

Upplevda utmaningar

Slutligen frågade vi också om de utmaningar de svarande ser som viktiga i framtiden. Mer exakt frågade vi dem om hur de uppfattar följande utmaningar:

- Kostnaderna för att introducera säkerhetsprodukter, som ny hårdvara som brandväggar eller ny programvara som slutpunktsskydd.
- Placeringen av säkerhetsanordningar (t.ex. effektiv placering av en brandvägg).
- Den övergripande bristen på förståelse av konsekvenserna av attacker och varför säkerhetspraxis/produkter måste implementeras.
- De anställdas acceptans att följa de definierade säkerhetsprotokollen.
- Nedtoning av hot om cyberattacker som påpekas av företagsledningen (t.ex. "det här kommer inte att hända oss, vem skulle hacka oss?")

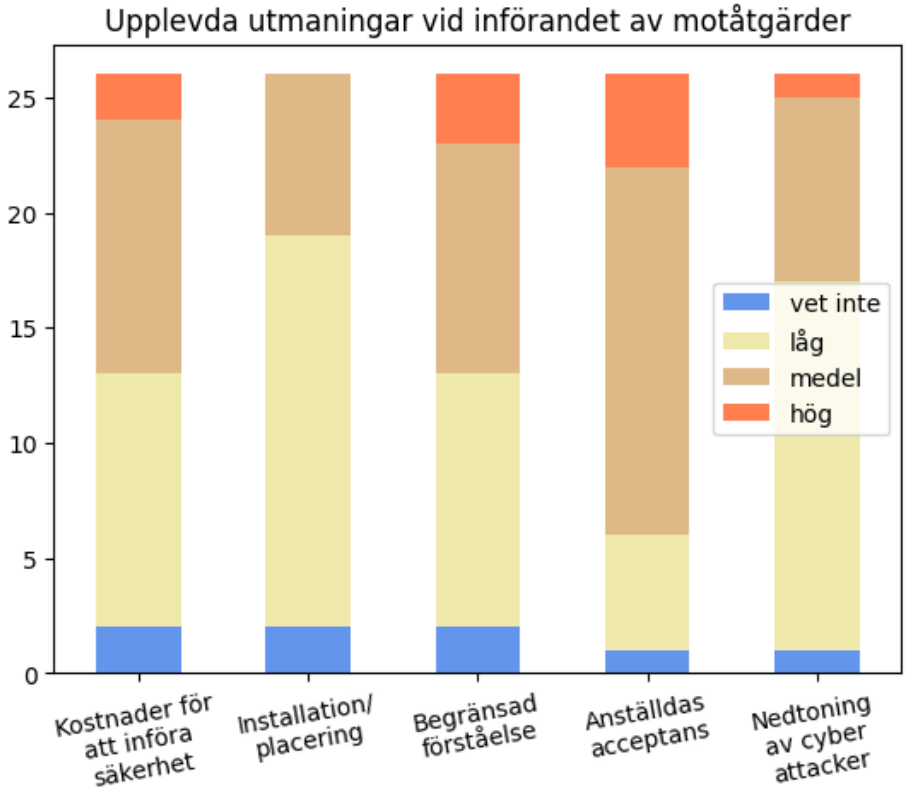


Bild 7. Histogram av upplevda utmaningar vid införandet av motåtgärder.

Bild 7 visar att anställda skall följa de definierade säkerhetsrutinerna är det största bekymret för de svarande. Detta följs av den begränsade förståelsen av cybersäkerhetspraxis och varför de behövs, och kostnaderna för att implementera säkerhetsprodukter/-protokoll. Särskilt har majoriteten av VD:ar och ägare indikerat att nedtoning av cybersäkerhet inte är ett allvarligt problem i deras företag (8 låga, 3 besvarade medelhöga och 1 hög). Som tidigare nämnts är denna studie ett litet urval med olika bakgrund och befattningar, men man kan dra slutsatsen att de svarande på högre chefsbefattningar har blivit mer medvetna om cybersäkerhet och behovet av att skydda sitt företag.

Slutsatser

I denna rapport ger vi en översikt över de utmaningar som svenska och europeiska myndigheter samt internationella företag har när det gäller cybersäkerhet. Denna översikt ska ses som en bra utgångspunkt som gör det möjligt för läsaren att få mer detaljerad information i de rapporter som vi hänvisar till. Eftersom angripare och hackare arbetar över nationella gränser kan vi tydligt se att alla rapporter identifierar liknande cybersäkerhetshot, mer specifikt, (i) hotet om avancerade DDoS-attacker (Distributed Denial of Service), (ii) ransomware-attacker, (iii) social engineering-attacker för att i slutändan få tillgång till företagets nätverk/IT-system, (iv) användning av skadlig programvara på datorer och mobiltelefoner, och (v) dataintrång där data publiceras eller säljs på den darknet.
Utifrån denna översikt och vetenskaplig forskning har vi konstruerat en undersökning för att få en överblick över de aktuella behoven hos små och medelstora företag i Skåne. Enkäten besvarades av 26 deltagare i olika positioner och som arbetar i företag från olika sektorer, som mjukvara/elektronik, service och produktion.

Undersökningen visar att det finns en medvetenhet om cybersäkerhet bland små och medelstora företag och deras svar visar att de är mer medvetna om traditionella cybersäkerhetsmetoder och produkter (t.ex. brandväggar, antivirus, säkerhetskopiering). Nyare produkter eller praxis, såsom definierade procedurer för övervakning av säkerhetsuppdateringar och spårning av vilka system som påverkas, och kontinuerlig övervakning av IT-infrastrukturen och bearbetning av säkerhetsvarningar som liknar en SOC är mindre kända för deltagarna i undersökningen.

Sammantaget tror vi att insikterna från denna undersökning visar att små och medelstora företag behöver en bättre förståelse för hur cyberattacker utförs nuförtiden, det vill säga att de inte bara är riktade till ett specifikt mål, utan snarare mycket automatiserade. Därför behövs också stöd till små och medelstora företag med utbildningsmaterial eller workshops för att få en djupare förståelse för hur attacker utförs nuförtiden och även vad en framgångsrik attack kan betyda för deras verksamhet. I likhet med vad som föreslås av (Wilson, 2022) kan det också vara fördelaktigt att tillhandahålla mer detaljerad information riktad till små och medelstora företag via en webbplats.

Citat och referenser

European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape 2022*. ENISA, October 2022. *ENISA Threat Landscape 2022*, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Europol. *Internet organised crime threat assessment 2021*. Europol, 2021. *IOCATE 2021*, https://www.europol.europa.eu/publications-events/main-reports/iocta-report.

Microsoft. *Microsoft Digital Defense Report 2022*. Microsoft, 2022. *Microsoft Digital Defense Report 2022*, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us

Nationellt Cybersäkerhetscenter. *Cybersäkerhet i Sverige 2022 - Del 1: Hot, metoder, brister och beroenden*. Nationellt Cybersäkerhetscenter, 2022. *Nya rapporter om cybersäkerhet*, https://www.ncsc.se/aktuellt/nya-rapporter-om-cybersakerhet/.

RISE Research Institutes of Sweden. *Cyberhot mot Sverige - En sammanfattning för ledare och beslutsfattare*. RISE, September 2022, https://www.ri.se/sites/default/files/2022-09/Rapport%20Cybers%C3%A4kerhet.pdf.

Martin Wilson, Sharon McDonald, Dominic Button & Kenneth McGarry (2022): It Won't Happen to Me: Surveying SME Attitudes to Cyber-security, Journal of Computer Information Systems, DOI:10.1080/08874417.2022.2067791

Appendix 1

Utkast till intervjufrågor – Förstudie Cybersäkerhet i små och medelstora företag

Intervjufrågorna är delvis baserade på det arbete som gjorts i (Wilson, 2022).

Bakgrundsinformation, öppna frågor

- Vilken position har du i företaget XYZ?

[exempel: ägare, chef, anställd]

- Hur länge har du arbetat i denna position i företaget XYZ?

[i år är decimaler okej]

- Hur länge har du arbetat i liknande befattningar?

[i år, är decimaler okej]

- Vilken typ av produkt eller tjänst är din kärnprodukt ELLER vilken sektor? (t.ex. programvara, finansiella tjänster, kreativ sektor …)
- När grundades företaget?

[i år, är decimaler okej]

- Hur många anställda har företaget?

[<10, <50, <250]

Bedömning av hot

Vi betraktar följande scenarier av attacker och ställer två följdfrågor till intervjupersonen om deras uppfattning av påverkan och beredskap kring en sådan attack.

1. Nätverk eller servrar hackas.
2. Data stjäls eller krypteras.
3. Systemen infekteras med skadlig programvara.
4. Mobila enheter utsätts för attacker
5. Nätfiske (Phishing) via e-postattack.

Upplevd sårbarhet:

- Har du varit utsatt för ett sådant scenario av attacker tidigare? [JA NEJ]
    - Om inte,

Hur troligt känner du att det här scenariot kommer att inträffa inom ditt företag?

[vet ej, osannolikt 1, … , troligt 3]

- Om ja,

Hur ofta har företaget blivit utsatt för en sådan attack?

[antal gånger]

Upplevd påverkansgrad:

- Ange vilken inverkan detta scenario skulle ha på ditt företag om det inträffade (i termer av förlorad tid, data, pengar och skada på ditt företags rykte).

[vet ej, låg effekt 1, … , hög effekt 3]

Därefter överväger vi förebyggande mekanismer och ställer några frågor till intervjupersonen om kostnaderna, effektiviteten och själv effektiviteten.

Förmåga att förebygga

För var och en av följande förebyggande åtgärder ställer vi två frågor.

1. Använder starka, unika lösenord för mina företagskonton.
2. Ta regelbundna säkerhetskopior av data.
3. Förebygger infektioner med skadlig programvara (t.ex. genom endpoint-skydd, brandväggar, …).
4. Konfigurerar mobila enheter så att de inte kan spåras på distans, raderas och låsas.
5. En process för att övervaka nyligen publicerade säkerhetsuppdateringar, identifiera de berörda systemen och installera uppdateringarna i tid.
6. Övervakning av IT-infrastrukturen och säkerhetsvarningar (via ett så kallat Security Operation Center - SOC)

- Vänligen ange effektiviteten av denna skyddsåtgärd när du överväger deras effektivitet när det gäller att skydda ditt företag från cyberattacker.

[vet ej, ineffektiv 1, …, effektiv 3]

- Betygsätt din insats/kostnad för att implementera och underhålla denna skyddsåtgärd för ditt företag (insatsen avser nödvändiga färdigheter, kunskaper och kostnader).

[vet ej, låg ansträngning 1, …, hög ansträngning 3]

Företagets syn/frågor inom cybersäkerhet

Vilka är de största utmaningarna eller hindren för att säkra ditt företags infrastruktur och tjänster? Betygsätt följande frågor med *[vet ej, 1 låg, …, 3 hög]*

- Kostnaderna för att införa säkerhetsåtgärder (t.ex. ny hårdvara som brandväggar eller mjukvara som slutpunktsskydd, webbserverskydd)
- Installation av säkerhetsåtgärder (t.ex. att placera brandväggen effektivt)
- Övergripande begränsad förståelse för vilken inverkan attacker kan ha och varför vissa säkerhetsåtgärder behöver implementeras.
- De anställdas acceptans och (tekniska) förmåga att följa rutinerna

- Nedtoning av cyberattacker av högre ledning (t.ex. "det här kommer inte att hända oss, vem skulle hacka oss?")

Vilka andra utmaningar ser du i ditt företag för att effektivt skydda ditt företag från cyberattacker?
[öppen fråga]

Syftet med frågorna
Hot- och copingbedömning ger oss mer information om vad de tycker är mest utmanande baserat på teknikimplementering, deras medvetenhet och hur det påverkar deras verksamhet. Dessutom ger frågorna kring företagets attityd/frågor när det gäller cybersäkerhet oss mer information där de kämpar (eller inte gör det). Med den öppna frågan hoppas vi dessutom få några ytterligare utmaningar som vi kanske inte hade tänkt på annars.