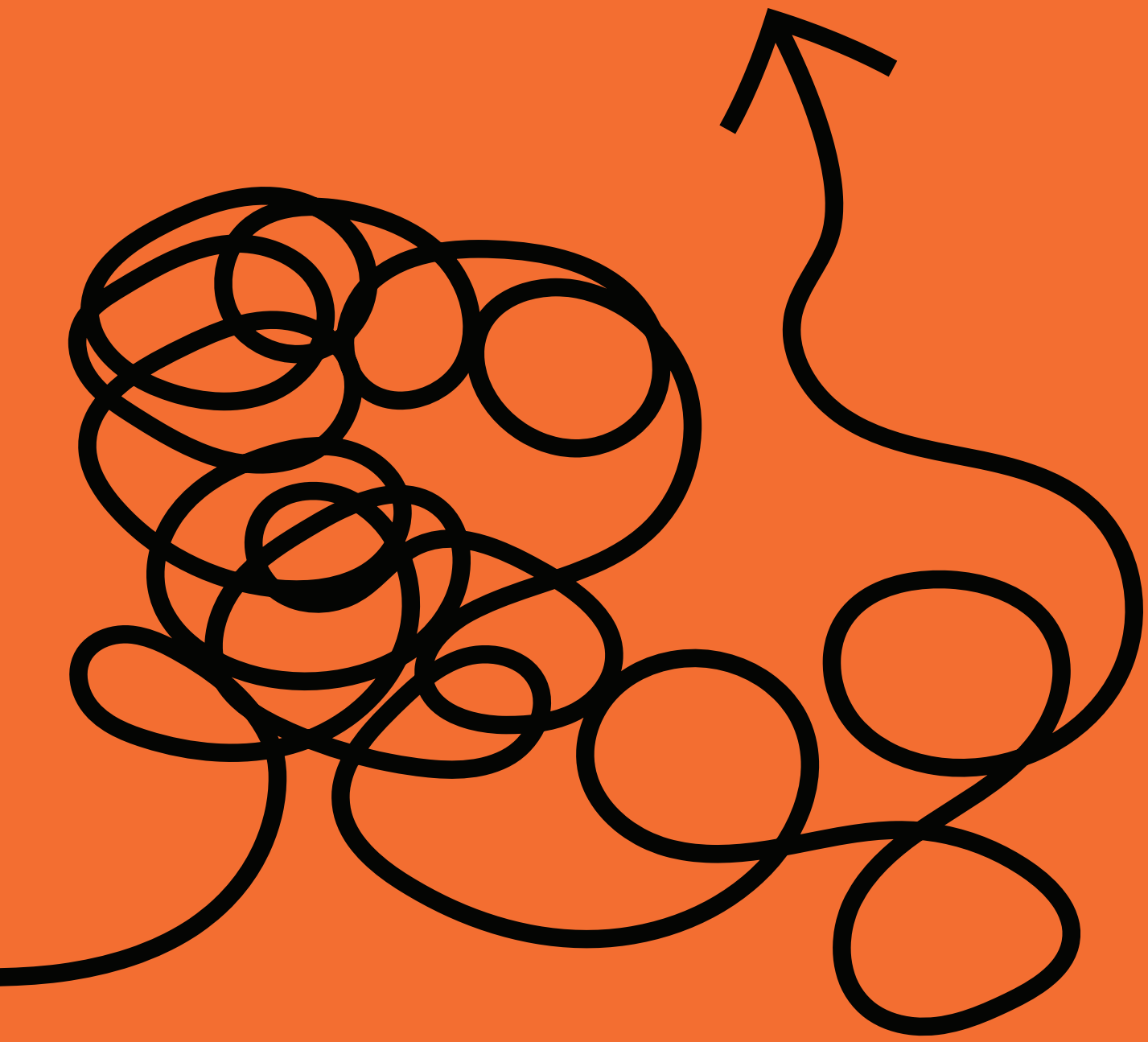
Tjänsteföretagen och stärkt cybersäkerhet i Sverige



Almega

Juni 2022

Innehåll

Sammanfattning

Hotet inom cyberområdet har ökat i takt med digitaliseringen och en successivt försämrad säkerhetspolitisk situation. Utpressningsattacker med skadlig kod, så kallade ransomware-attacker mot företag ökar snabbt. Enligt Försvarsmakten är cyberhotet det mest påtagliga hotet mot Sverige just nu med kontinuerliga försök till intrång och kartläggning av nätverk, något som flera tjänsteföretag märkt av. Denna rapport visar att en femtedel av tjänsteföretagen har blivit utsatta för cyberattacker de senaste tre åren, varav en majoritet är riktade och kvalificerade cyberattacker.[1]

Konsekvenserna av ett cyberangrepp är potentiellt stora, såväl för företagen som för samhället i stort, och ytterst för Sveriges säkerhet. I synnerhet om det drabbar tjänsteföretag som direkt och indirekt bedriver verksamhet eller levererar tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Det kan till exempel handla om tjänsteföretag verksamma inom vård och omsorg, elektronisk kommunikation, transporter och säkerhet, samt tjänsteföretag som bidrar med IT- och säkerhetslösningar till samhällsviktiga funktioner.

Utbyte och samverkan mellan tjänsteföretagen och myndigheterna lyser dock med sin frånvaro på det här området vilket framgår i den enkätundersökning vi har låtit genomföra. Flertalet tjänsteföretag uppger i enkäten att de i dag inte samarbetar med myndigheter avseende cybersäkerhet. Många företag upplever dessutom bristande intresse från myndigheterna att utveckla ett närmare samarbete, och även till viss del en bristande förståelse hos myndigheterna om vad företagen tillhandahåller som är av vikt för samhället. Över lag förefaller det även råda en osäkerhet bland de svarande kring vilka myndigheter tjänsteföretagen kan eller bör samarbeta med, alternativt få stöd av.[2]

Från tjänsteföretagens sida har man uttryckt såväl vilja som behov av samverkan och stöd med myndigheter. Att åstadkomma reellt utbyte och god samverkan mellan tjänsteföretag och det offentliga för att stärka arbetet med cybersäkerhet ligger i såväl näringslivets som offentlig sektors intresse. Skälet till det är bland annat att många tjänsteföretag upprätthåller eller säkerställer samhällsviktiga funktioner. Företagen har vidare ett egenintresse i att arbeta med cybersäkerhet eftersom det mildrar konsekvenserna som ett cyberangrepp kan leda till, såsom tid och kostnader att hantera och återställa system samt skadat förtroende hos kund.

1 Det vill säga avancerade och allvarliga attacker med större skada eller konsekvenser för tjänsteföretaget.

2 På fråga om vilka myndigheter som företagen gärna skulle arbeta närmare var det endast 23 procent av de tillfrågande som svarade, och av dessa svarade 45 procent att de inte visste.

Uppgifter om tjänsteföretagens budgeterade medel för cybersäkerhet och vidtagna åtgärder för att stärka beredskap att hantera ett cyberangrepp pekar på begränsade investeringar och förmågehöjande åtgärder. En orsak till detta ligger i att tjänsteföretagen i flera fall saknar förutsättningar att arbeta med cybersäkerhet, vilket i mångt och mycket grundar sig i att det är otydligt hur tjänsteföretagen bör, kan och förväntas ta sig an arbetet med att stärka den egna cybersäkerheten och bidra till samhällets cybersäkerhet.

Från tjänsteföretagens håll saknas tillgång till kvalificerad hotbildsbedömning och tillräcklig inriktning från myndigheternas sida inom området där det skulle vara befogat. Förbättrad kompetensförsörjning inom cybersäkerhetsområdet för tjänsteföretagen kommer att vara avgörande för hur tjänsteföretagen och Sverige kan minska sin sårbarhet.

Det krävs även kommunikativa åtgärder från myndigheternas sida för att påvisa det stöd och samverkansformat som i dag finns. Det är inte en helt enkel uppgift som företag att navigera och se sin roll och vart man ska in i det stora lapptäcke av aktörer och arrangemang som finns inom cyberområdet. Det finns däremot exempel på lyckade samarbeten som samverkan mellan Post- och telestyrelsen och teleoperatörerna inom elektronisk kommunikation. Detta är något som flera kan ta inspiration av och bygga vidare på. I rapportens avslutande del lyfts förslag som har framkommit i dialog med tjänsteföretagen som syftar till att stärka såväl tjänsteföretagens som samhällets motståndskraft.

Inledning

Cyberhotet mot Sverige

"Cybersäkerheten och de sårbarheter ett digitaliserat samhälle står inför har fått ökad uppmärksamhet. Men ännu, vill jag hävda, inte den uppmärksamhet de förtjänar. Det handlar om komplexa hot, som kräver engagemang på högsta nivå på myndigheter och företag. Intrång är kostsamma och svårhanterade."[3]

Björn Lyrvall, generaldirektör Försvarets radioanstalt

I takt med digitaliseringen och en successivt försämrad säkerhetspolitisk situation har hotet inom cyberområdet ökat. För ett högteknologiskt land som Sverige innebär detta fler sårbarheter, ökade beroenden och att fler företag utsätts för attacker. Både Säkerhetspolisen och Försvarets radioanstalt (FRA) beskriver cybersfären som en av de främsta arenorna som kriminella och främmande makt använder i antagonistiska syften. Det innebär allt ifrån finansiell vinning, inhämtning av information och informationspåverkan till att slå mot samhällsviktiga funktioner och skapa splittring. Dessutom bedömer flera experter att Rysslands invasion av Ukraina också kan innebära ett ökat cyberhot mot Sverige. Militära underrättelse- och säkerhetstjänsten (Must) har konstaterat att cyberhotet just nu är det mest påtagliga säkerhetshotet mot Sverige, något som flera av tjänsteföretagen redan märkt av.[4] [5]

Tjänsteföretag både levererar och använder sig av digitala lösningar och system för sin verksamhet. Direkt och indirekt handlar det i flera fall om verksamheter, tjänster eller infrastruktur som tjänsteföretagen levererar eller bidrar till och som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Effekterna av en cyberattack på tjänsteföretagen kan därmed få stora konsekvenser för samhällsviktiga funktioner och samhällsviktig verksamhet. Tjänsteföretagens förmåga att hantera cyberhot är därför avgörande för Sverige som en attraktiv och välfungerande marknad och i förlängningen – Sveriges säkerhet. De kan även ha en avgörande roll för att Sverige ska kunna motstå och hantera en situation med höjd beredskap och ytterst krig.[6] [7]

Cyberangrepp är inte bara ett allvarligt hot mot säkerhetskänsliga verksamheter utan också mot enskilda tjänsteföretag samt samhället i stort.[8] Som konstateras i den nationella strate-

3 Försvarets radioanstalts årsrapport 2021. Medarbetare i demokratins tjänst.

4 Säkerhetspolisens årsbok 2021.

5 Försvarsmakten. (2022). Cyberangrepp största hotet just nu.

6 SOU 2019:51. Näringslivets roll inom totalförsvaret: Betänkande av Utredningen om totalförsvarets försörjningstrygghet. Stockholm: Elanders Sverige AB.

7 Säkerhetspolisens årsbok 2021.

8 Säkerhetspolisens årsbok 2021.

gin för samhällets informations- och cybersäkerhet är arbetet med cybersäkerhet nödvändigt för att näringslivet ska kunna utveckla och tillhandahålla konkurrenskraftiga varor och tjänster. I ett större perspektiv är det också en viktig förutsättning för svensk tillväxt och konkurrenskraft.[9] Det digitaliserade och i hög grad sammankopplade samhället innebär att effekterna av ett cyberangrepp kan få stora konsekvenser inte bara för den aktör som utsätts utan också för andra aktörer och deras verksamhet.[10] Det ligger därmed i samtliga aktörers intresse, såväl offentliga som privata, att adressera cyberhoten och arbeta med cybersäkerhet. Från de tjänsteföretag som vi talat med har det uttryckts såväl vilja som behov av samverkan och stöd med myndigheter.

Åtgärderna för att möta cybersäkerhetshoten behöver i högre grad utgå ifrån företagens behov och förutsättningar, inte hur staten hittills har varit organiserad. Cybersäkerhetspolitiken behöver stärka de som levererar säkerhetstjänster, de som använder dem och Sverige som marknad, i tillägg till brottsbekämpning, totalförsvar och andra samhällsviktiga frågor.

Om undersökningen

Med anledning av den ökade hotbilden mot Sverige och utmaningarna inom cybersäkerhetsområdet har Almega låtit genomföra en undersökning tillsammans med 4C Strategies om tjänsteföretagens arbete med cybersäkerhet och förutsättningar för att hantera den ökade hotbilden, samt samverkan mellan staten och näringslivet. Som en del av undersökningen har vi intervjuat elva initierade chefer från olika branscher[11] i tjänstesektorn med ansvar för säkerhet, informationssäkerhet, IT-säkerhet och säkerhetsskydd. Intervjuerna syftade till att få en djupare förståelse för hur tjänsteföretagen arbetar med cybersäkerhet, vilka utmaningar som finns samt hur samverkan med myndigheter fungerar.

Intervjusvaren har kompletterats med en enkätundersökning som gått ut till Almegas medlemmar som ombetts svara på ett antal frågor rörande deras arbete med cybersäkerhet, upplevd hotbild och utmaningar samt samverkan med statliga aktörer.

Svaren från såväl intervjuerna som enkäten har anonymiserats och redovisas här i sammanställd form. Svarsfrekvensen på frågorna i enkätundersökningen har varierat, vilket har påverkat möjligheterna att dra konkreta slutsatser.[12] Även bredden på representerade branscher och storlek på företag i undersökningen gör att också frågan om tjänsteföretagens fokus på cybersäkerhet varierar.

Fokus för denna rapport är tjänsteföretagen, det vill säja företag inom den privata tjänstesektorn. Med tjänstesektorn menas branscherna G45 till T98 i Nationalräkenskaperna.

Med termen cybersäkerhet åsyftas i denna rapport den delmängd av informationssäkerhet som omfattar skydd av informationssystem mot antagonistiska hot om att slå ut samhällskritisk verksamhet eller att genomföra brott riktade mot företag. Informationssäkerhet inbegriper teknisk säkerhet (IT-säkerhet) och administrativ säkerhet (regler och rutiner).

9 Skr. 2016/17:213. Nationell strategi för samhällets informations- och cybersäkerhet.

10 Sveriges Radio. (2022) Har cyberattackerna ökat med kriget i Ukraina? Hämtad 4 april 2022.

11 Teknikföretag, säkerhetsföretag, medieföretag, transportföretag, vårdföretag, tjänsteförbunden och innovationsföretag.

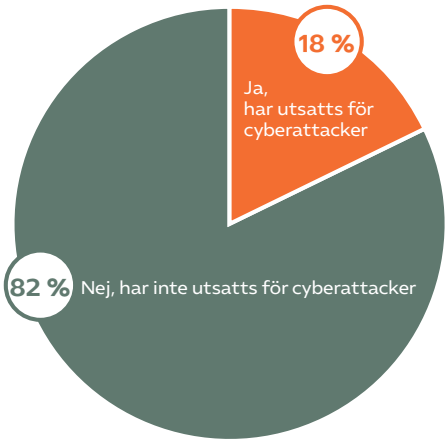
12 Totalt svarade 618 tjänsteföretag på enkätundersökningen.

Cyberhotet och tjänsteföretagen

En femtedel av tjänsteföretagen har utsatts för cyberattacker

Cyberhoten både ökar och utvecklas snabbt. Ransomware[13] är fortsatt det största och mest allvarliga hotet för medelstora och stora företag och antalet ransomware-angrepp ökade 2021 med 26 procent jämfört med 2020. Ökningen av cyberattacker beror bland annat på ökad automatisering och rekrytering av individer och grupper som agerar på uppdrag av kriminella.[14] Vidare är cyberhotet enligt Försvarsmakten det största säkerhetshotet mot Sverige just nu med kontinuerliga försök till intrång och kartläggning av nätverk.[15] Även Säkerhetspolisen varnar för en ökad risk för cyberangrepp i och med Rysslands invasion av Ukraina och det försämrade säkerhetsläget.[16]

Figur 1: Andel tjänsteföretag som utsatts för cyberattacker de senaste tre åren.



Vår undersökning visar att en femtedel av tjänsteföretagen uppger att de har blivit utsatta för cyberattacker de senaste tre åren (se figur 1). Cirka hälften av tjänsteföretagen som utsatts för cyberangrepp anger även att andelen riktade och kvalificerade cyberattacker[17] har ökat de senaste tre åren. En femtedel anger att de ligger på ungefär samma nivå som

13 Ransomeware (utpressnings- eller gisslanprogram) syftar på utpressning genom att filer låses och bar öppnas mot betalning.

14 Trusec. (2022). Cyberkriminella har bytt taktik.

15 Försvarsmakten. (2022). Cyberangrepp största hotet just nu.

16 Säkerhetspolisen. (2022). Cyberangrepp ständigt pågående hot mot Sverige. Hämtat den 5 april 2022.

17 Det vill säga avancerade och allvarliga attacker med stora konsekvenser för företaget.

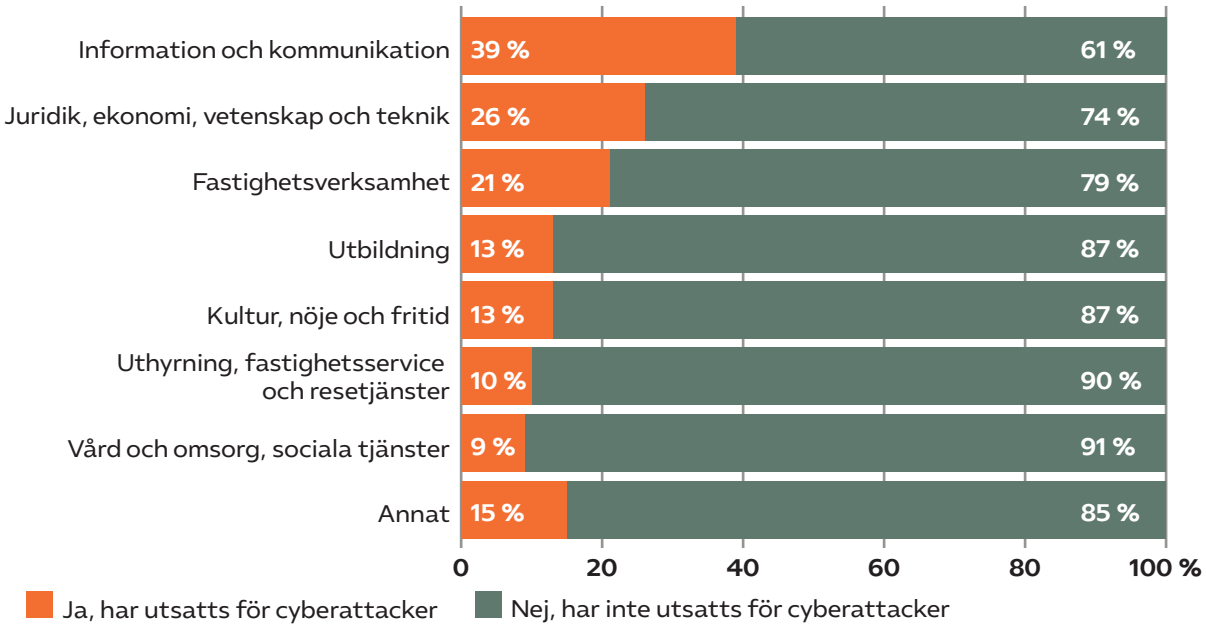
tidigare.[18] Det tyder på att en majoritet av angreppen som sker mot tjänsteföretagen uppfattas som kvalificerade och riktade angrepp. Denna bild bekräftas av de chefer för säkerhet, informationssäkerhet, IT-säkerhet och säkerhetsskydd som intervjuats, där ungefär en femtedel svarar att deras företag utsatts för kvalificerade och riktade cyberangrepp som har fått konsekvenser för företaget. Samtidigt konstaterar samtliga intervjupersoner som vi talat med att det finns ett konstant "brus" och mer eller mindre ständiga försök till attacker, varav vissa även är riktade attacker.

"Försök till att hacka våra system sker dagligen"

Intervjusvaren indikerar en varierande syn på vad tjänsteföretagen bedömer vara ett cyberangrepp. Det som beskrivs som "det dagliga bruset" med mindre försök till attacker tycks av flera inte bedömas som en cyberattack. Enligt vår enkätundersökning har en stor majoritet av Almegas medlemmar inte blivit utsatta för en cyberattack. Huruvida alla dessa företag är helt förskonade från cyberattacker eller om det dagliga "bruset" inte är av den omfattning att de upplever det som en cyberattack går inte att utläsa från enkätsvaren.

Samtalen med chefer i branschen tyder emellertid på att vissa tjänsteföretags grundläggande IT-säkerhet och säkerhetsarbete ligger på en nivå där mindre kvalificerade attacker avvärjs och att företagen därmed inte märker av eller är medveten om de försök till cyberattacker som sker. Det finns därmed en möjlighet att försök till cyberangrepp, som kanske är av mindre karaktär eller inte får konsekvenser för företagen, är högre än vad resultatet från vår enkätundersökning påvisar. En intervjuperson konstaterade att "...**de attacker som man nu märker av och som får konsekvenser är attacker som är mer sofistikerade. Som svar på frågan om det är fler attacker nu skulle jag säga att det är ungefär lika många attacker som sker och får en effekt nu som för tre år sedan.**"

Figur 2: Ungefärlig andel inom olika branscher i tjänstesektorn som utsatts för cyberattacker de senaste tre åren.



Anm: 2 procent av respondenterna svarade "vet ej".

18 Av de som utsatts för cyberattacker kunde cirka 30 procent inte bedöma om attackerna har ökat eller minskat, och cirka 3 procent svarade att det minskat.

Vår enkätundersökning visar på att bland Almegas medlemmar är tjänsteföretag inom informations- och kommunikationsbranschen mest utsatta för cyberangrepp, följt av tjänsteföretag inom juridik, ekonomi, vetenskap och teknik (se figur 2). Det kan finnas flera anledningar till att just dessa branscher sticker ut. Det kan vara att dessa branscher i högre grad bygger på eller är beroende av tekniska system och därmed mer aktivt arbetar med frågorna, alternativt använder de fler system som också kan utsättas för angrepp. Det kan också vara så att tekniska säkerhetslösningar i dessa branscher möjliggör tidig varning och upptäckt i högre utsträckning. Det är rimligt att anta att det också speglar angriparens värdering av de informationstillgångar och skyddsvärden som finns inom dessa branscher.

Huruvida tjänsteföretagen upplever att de är utsatta för cyberangrepp är något som kan påverka hur tjänsteföretagen uppfattar hoten inom cyberområdet. Om man som företag inte utsätts för cyberangrepp så upplevs hotet inom cyberområdet förmodligen som lägre.

Varierande grad av investeringar och förmågehöjande åtgärder i cybersäkerhet

> **"Skulle gärna se att mer resurser läggs på cybersäkerhet men då inga större incidenter sker uppfattas det högre upp som att det man gör fungerar. De ser då inte varför pengar ska läggas på något som tycks fungera."**

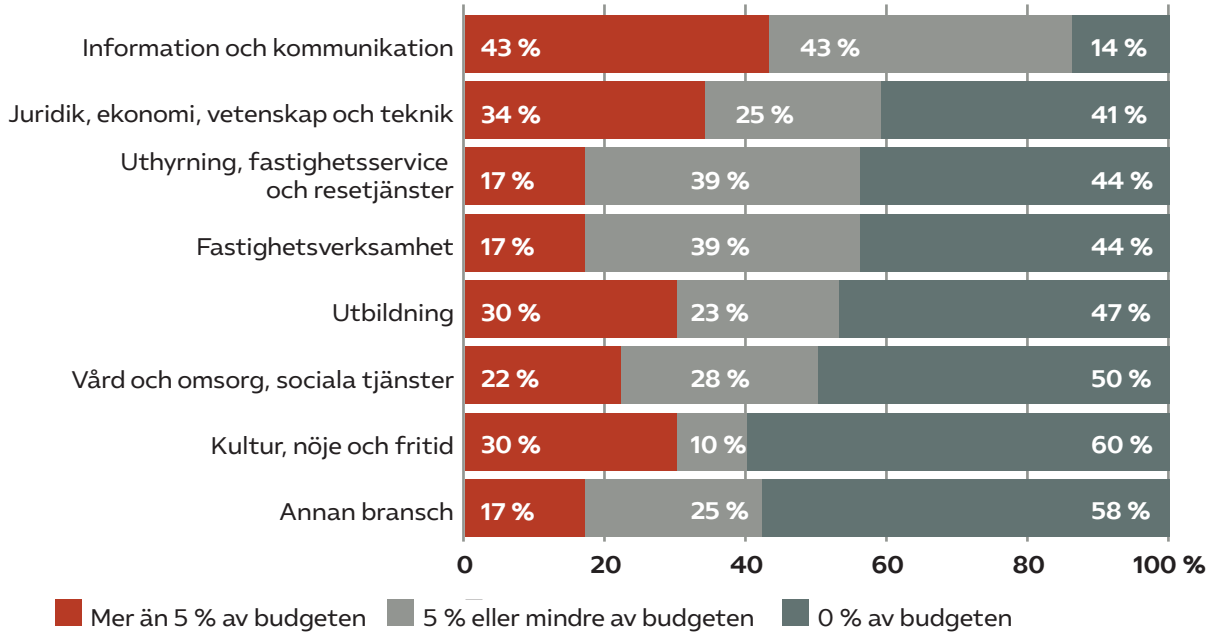
Åtgärder för att stärka företags förmåga att skydda sig mot angrepp är viktiga. Det kräver bland annat finansiella investeringar i cybersäkerhet. Enligt en ny undersökning lägger svenska verksamheter i snitt 5,2 procent av IT-budgeten på cybersäkerhet.[19] Av de som svarade i vår undersökning uppgav nästan 40 procent att de inte har några budgeterade medel för cybersäkerhet. Företag i informations- och kommunikationsbranschen budgeterade som väntat mest till cybersäkerhet, följt av tjänsteföretag inom juridik, ekonomi, vetenskap och teknik (se figur 3). Det är även de två branscher där flest företag angett att de utsatts för cyberangrepp.

I snitt hälften av företagen i övriga branscher svarar att de inte har några budgeterade medel för cybersäkerhet. Mindre än en femtedel av dessa företag har utsatts för cyberangrepp de senaste tre åren, vilket kan vara en anledning till att företagen inte budgeterat särskilda medel för cybersäkerhet.

I verkligheten är bilden mer komplicerad än så och många av de mindre företagen har få eller inga egna IT-system utan är helt beroende av externa leverantörer. Satsningar på cybersäkerhet är sällan en renodlad kostnadspost. För många företag är säkerhet inbyggt i lösningar från externa leverantörer. På samma sätt är det många gånger ordinarie IT-personal som arbetar med att lösa cybersäkerhetsfrågor inom ramen för sina normala arbetsuppgifter. Dessa företag kan därmed ha ett stort engagemang inom området utan att det syns i budgeten.

19 Radar. (2021). Svensk cybersäkerhet 2021: Svenska förutsättningar, marknad, trender, hotbild, attacker, åtgärder och praktiska råd.

Figur 3: Andel av IT-budget som läggs på cybersäkerhet inom olika branscher i tjänstesektorn



Anm: 48 procent av respondenterna svarade "vet ej" eller ett annat svar som inte gick att tolka.

Huruvida företag har medel särskilt avsedda för cybersäkerhet är en indikator på om företagen investerar i att stärka sin förmåga inom cybersäkerhet. Finansiella investeringar behövs men den viktigare frågan är vilka åtgärder företagen väljer att investera i.

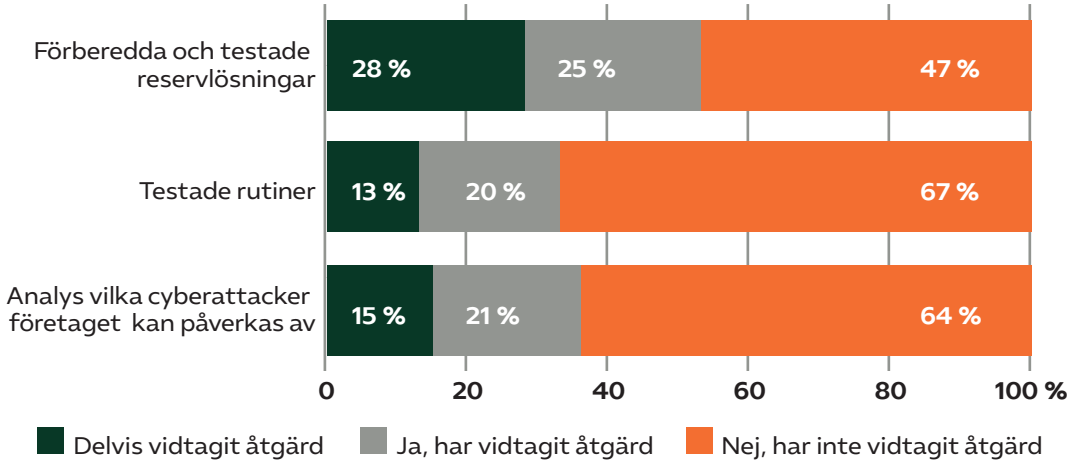
> "Just insikten att man inte är – eller kan bli – helt osårbar är viktig när man jobbar med cybersäkerhet. Det man kan göra är att arbeta skade- och riskreducerande."

Skyddsåtgärder är en viktig åtgärd för att avvärja och minska risken för negativa konsekvenser av cyberangrepp. Att fullt ut skydda sig mot cyberangrepp är emellertid en omöjlig uppgift. Företag behöver därför vara förberedd på att cyberattacker kan inträffa och vidta åtgärder för att kunna hantera dem.

I Myndigheten för samhällsskydd och beredskaps (MSB) rapport[20] om cybersäkerhet i Sverige 2020 redogör myndigheten för ett antal åtgärder som kan stärka förmågan att hantera ett cyberangrepp. Det inkluderar bland annat att göra en analys över vilka cyberhot organisationer kan påverkas av samt att säkerställa att det finns testade rutiner för hur cyberattacker anmäls, bedöms och hanteras. Det inbegriper även att ha en plan B i form av förberedda och testade alternativ om ordinarie IT-system inte fungerar.

20 Myndigheten för samhällsskydd och beredskap. (2022). En inblick i Sveriges cybersäkerhet: Årsrapport it-incidentrapportering 2021.

Figur 4: Förberedande åtgärder som tjänsteföretagen vidtagit för att hantera cyberangrepp



Som går att utläsa i figur 4 anger omkring två tredjedelar av tjänsteföretagen att de inte har gjort en analys över vilka cyberhot de kan påverkas av. Ungefär lika många anger att de inte har testade rutiner för hur cyberattacker anmäls, bedöms och hanteras. Därtill anger omkring hälften av tjänsteföretagen att de inte har några förberedda eller testade alternativ om ordinarie IT-system slutar att fungera. Cirka en tredjedel av tjänsteföretagen i vår undersökning har inte vidtagit några av dessa förberedande åtgärder. Över lag indikerar det en bristande beredskap för cyberangrepp bland ett flertal av företagen.

Undersökningen visar samtidigt att en del av tjänsteföretagen har vidtagit förberedande åtgärder. Omkring en femtedel av tjänsteföretagen har fullt ut, eller delvis, vidtagit samtliga tre ovannämnda åtgärder och en fjärdedel svarade att de har, eller delvis har, testade rutiner och reservlösningar (se figur 4). Av de företag som vidtagit samtliga tre åtgärder är det återigen tjänsteföretag inom kommunikation och information[21] samt inom juridik, ekonomi, vetenskap och teknik[22] som sticker ut, men även tjänsteföretagen inom vård, omsorg och sociala tjänster.[23]

Uppgifter om budgeterade medel för cybersäkerhet och vidtagna åtgärder för att stärka beredskap att hantera ett cyberangrepp pekar på varierande grad av investeringar och förmågehöjande åtgärder. Tjänsteföretagens branschtillhörighet och den upplevda hotbilden utgör möjliga förklaringar till vilka finansiella investeringar och åtgärder som företagen väljer att göra.

Tjänsteföretagens storlek utgör en annan möjlig variabel där större företag över lag har mer resurser, och i vissa fall även fler krav och större behov av att arbeta med cybersäkerhet. Mindre företag å andra sidan, som generellt har begränsade resurser och inte utsatts för angrepp, har svårt att motivera eller ser inte ett behov av investeringar i cybersäkerhet. Dock har även större företag som vi intervjuat också tagit upp utmaningen med att motivera investeringar i cybersäkerhet för företagets ledning när man inte utsatts för en större cyberattack som föranlett större konsekvenser för företaget.

21 24 procent av de svarande är tjänsteföretag verksamma inom kommunikation och information.

22 21 procent av de svarande är tjänsteföretag verksamma inom juridik, ekonomi, vetenskap och teknik.

23 15 procent av de svarande är tjänsteföretag verksamma inom vård, omsorg och sociala tjänster.

Ytterligare en utmaning avseende investeringar i cybersäkerhet är att veta vilken nivå av cybersäkerhet som är eftersträvansvärt, eller förväntat, och som bör utgöra en miniminivå för att stärka sin egen men också den samlade motståndskraften i samhället. Det är även en av anledningarna som tjänsteföretagen i enkäten har angett till varför man ser behov av en ökad samverkan med myndigheterna.

Invasionen av Ukraina och skiftet i cyberhotet

Flera myndigheter och experter har varnat för att Rysslands invasion av Ukraina innebär ett ökat cyberhot mot Sverige. Detta är något som några av de större tjänsteföretagen har märkt av. Några beskriver hur de redan innan den förnyade invasionen av Ukraina i februari 2022 noterat en ökning av cyberattackerna som riktats mot dem.

Efter invasionen vittnar företagen även om att inriktningen på cyberattackerna har skiftat. I samband med upptrappningen till invasionen av Ukraina konstaterade ett företag att syftet med attackerna gick från att i huvudsak handla om ekonomisk vinning till att skapa störningar i verksamheten. Två andra företag har i närtid identifierat cyberattacker mot deras verksamhet som med största sannolikhet bedöms ha utförts av en statsaktör. Ett av dessa företag misstänker att en kvalificerad attack man utsatts för var en storskalig övning inför cyberangrepp mot Ukraina. En ökning i antal belastningsattacker uppmärksammades också av ett företag som intervjuats. Samtliga är konkreta exempel på en ökad hotbild inom cyberområdet.

Även om det framför allt är större företag som tycks ha noterat en ökad hotbild så innebär det inte att risken för angrepp är lägre för mindre företag. Mindre företag är också måltavlor och det är ofta dessa företag som attacker riktas mot då de generellt sett är mer oskyddade. För små och medelstora företag blir de ekonomiska konsekvenserna dessutom ofta mer betydande. Att många små och medelstora företag har koppling till större företag eller andra aktörer som bedriver samhällsviktig verksamhet innebär också att dessa företag kan utgöra en ingång för en antagonist till andra verksamheter.[24] [25]

Utmaningarna att hantera cyberhoten är stora

> **"Arbetet bygger på föränderlig kunskap. Cyberhoten och de tekniker som används uppdateras och förändras konstant."**

Den övergripande utmaningen i cybersäkerhetsarbetet är förmågan att hålla jämna steg med hotaktörer och helst ligga före i att identifiera sårbarheter och upprätta skydd mot möjligt intrång i IT-systemen. Eftersom cyberhoten och de tekniker som används konstant utvecklas innebär det att företagen kontinuerligt behöver arbeta med att utveckla och stärka sina skydd. Att systemen blir alltmer komplexa och ihopkopplade gör det även svårt att veta hur säkerheten ser ut i hela kedjan. Ett cyberangrepp mot en aktörs system kan, som tidigare konstaterats, också komma att riskera störningar eller intrång i en annans företagens egna system.

24 Avast.com (2022). Vad är en attackyta?

25 Forbes.com (2022). Small Businesses Are More Frequent Targets Of Cyberattacks Than Larger Companies: New Report

Den andra större utmaningen som flera tjänsteföretag nämner är den mänskliga faktorn och behovet av att öka säkerhetsmedvetandet hos personalen. Personalens misstag eller bristande säkerhetsmedvetande kan leda till att en antagonist lyckas ta sig in i systemen och därmed kringgå det skydd man byggt upp (se faktaruta nedan). Det finns aktörer som specifikt riktar sig mot anställda och erbjuder finansiell ersättning mot att få tillträde till organisationens system.[26] Det räcker därmed inte att endast investera i att upprätta säkra system utan det behövs även kunskapshöjande insatser, samt rutiner och processer för hur företaget ska gå till väga om det utsätts för ett cyberangrepp eller om ett misstag av personalen har begåtts.

Fakta: Den mänskliga faktorn – exempel på utmaningar.

- Det finns exempel på grupperingar som betalar målföretagens egna anställda för att de ska ge tillträde till företagens interna system, och på så sätt få ett första fotfäste. Väl inne verkar de inte vara speciellt bekymrade över att dölja sina spår, och använder sig av mer eller mindre avancerade metoder för att få tillträde till data som den anställde själv inte har tillgång till.
- På det här sättet har grupper lyckats ta sig in i flera större företag. De hämtar hem känslig information, raderar den från företaget och bedriver sedan olika former av utpressning.
- De tar sig också in i företagets krishanteringskanaler och kan på så sätt följa hur företagen bedriver sitt incidenthanteringsarbete.
- Det är svårt att med enbart tekniska metoder skydda sig mot den här typen av attacker.

Enkätundersökningen och intervjuerna tyder även på att en central utmaning också ligger i osäkerhet i hur tjänsteföretagen bör och kan ta sig an arbetet med att stärka cybersäkerheten, inklusive vad företagen bör prioritera och fokusera vid. Tjänsteföretagen behöver tillgång till kompetens inom cybersäkerhet för att kunna möta problemen. Att anställa personal med kompetens inom cybersäkerhet är dock ytterligare utmaning som tjänsteföretagen står inför. Mer än tre fjärdedelar av företagen uppger att det är ganska eller mycket svårt att hitta personer med rätt utbildning och eller kompetens.

Tjänsteföretagen lyfter även fram utmaningen med att täcka de ökade kostnaderna som såväl tillskaffandet av kompetensen som arbetet med att stärka cybersäkerheten innebär.

> **"Alla system har sårbarheter, vilket i sig är en sårbarhet och det viktiga är att själva hitta och vara medvetna om dessa."**

Vad som också framkommer är att det från tjänsteföretagens håll saknas tillgång till kvalificerad hotbildsbedömning och tillräcklig inriktning från myndigheternas sida. De flesta tjänsteföretag uppger dessutom att de inte har något utbyte med myndigheter rörande cybersäkerhetsområdet.

26 Microsoft. (2022). DEV-0537 criminal actor targeting organizations for data exfiltration and destruction. Hämtat den 11 april 2022.

Förbättrad kompetensförsörjning inom cybersäkerhetsområdet för tjänsteföretagen samt utvecklande av samarbeten mellan företagen och myndigheterna kommer vara avgörande för hur tjänsteföretagen och Sverige minskar sin sårbarhet och stärker motståndskraften. Det finns flera exempel på goda samarbeten, till exempel inom telekomområdet. Där samarbetar Post- och telestyrelsen (PTS) och telekomoperatörer inom Nationella telesamverkansgruppen (NTSG). Det är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid allvarliga störningar i samhället. Det finns flera sådana samarbeten och inom flera sektorer är företag redan ålagda krav och skyldigheter genom lagstiftning.

Mer samverkan
– cybersäkerhet, tjänsteföretagen och myndigheter

Potentiellt stora konsekvenser

Generellt tycks tjänsteföretagen i enkäten uppfatta sannolikheten för att utsättas för en kvalificerad attack som låg – även om det varierar mellan branscherna. Samtidigt ligger det i tjänsteföretagens intresse att minska och hantera osäkerheter i omvärlden. Företag är ansvariga inför sina ägare att beakta hot och vidta rimliga försiktighetsåtgärder och inom flera områden finns lagkrav. Ett kontinuerligt arbete med det är att arbeta med riskhantering, vilket syftar till att skydda resurser och inkomstmöjligheter mot skador och bortfall så att verksamhetens mål kan nås till en så låg kostnad som möjligt. Därutöver är flera tjänsteföretag verksamma inom samhällsviktig verksamhet, vars tjänster därmed måste kunna levereras då de utgör en viktig del i Sveriges krishanteringsförmåga och totalförsvar.

> **"Även företagen behöver arbeta med cybersäkerhet utifrån ett egenintresse och bygga det som en del av, och något som bidrar till, affärsintressena. Börjar man där så kommer det andra [att arbeta med cybersäkerhet för att bidra till samhällets motståndskraft] falla in naturligt."**

För att analysera oönskade händelser används sannolikhet och konsekvens som mått på hur troligt det är att en viss händelse inträffar och vilka effekter den i så fall skulle få. Företagen värderar riskerna där sannolikhet och konsekvens vanligtvis viktas lika. Av det följer att en händelse med hög sannolikhet och medelhöga konsekvenser värderas högre (får ett högre riskvärde) än en händelse med mycket låg sannolikhet och katastrofala konsekvenser. Det kan innebära att hot med potentiellt katastrofala konsekvenser, men låg sannolikhet för att det inträffar, lämnas utan åtgärd. De potentiella konsekvenser av cyberangrepp som tjänsteföretagen anger är stora.

Cyberangrepp riskerar bland annat att orsaka driftstopp eller störningar i verksamheten, vilket i värsta fall innebär att företaget inte kan leverera en tjänst till kund. En cyberattack kan också medföra att data – däribland känsliga data såsom sekretessbelagda eller känsliga företagsdata – manipuleras, förvanskas, raderas eller stjäls. För tjänsteföretagen kan detta innebära skadat förtroende och missnöje hos kunderna. Allt detta riskerar att orsaka stora

ekonomiska förluster. Exempelvis på grund av förlorade kunder eller i och med den tid och de resurser som behöver läggas för att hantera och återställa, eller i värsta fall på nytt bygga upp, de system och material som gått förlorade.

Angrepp på tjänsteföretagen kan även få konsekvenser för samhället i stort, och i synnerhet för Sveriges säkerhet. Särskilt om det drabbar tjänsteföretag som direkt och indirekt bedriver verksamhet eller levererar tjänst eller infrastruktur som upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Det handlar exempelvis om samhällsfunktioner som till exempel transport; hälsa vård och omsorg; information och kommunikation; ordning och säkerhet samt barnomsorg och utbildning (se faktaruta nedan).

Fakta: Exempel på samhällsnyttiga funktioner som tjänsteföretagen bidrar med eller bidrar till.

- TRANSPORT
  Järnvägstransporter
  Sjötransporter
- HÄLSA, VÅRD OCH OMSORG
  Läkemedelsförsörjning
  Hälso- och sjukvård
- INFORMATION OCH KOMMUNIKATION
  Infrastruktur och tjänster för elektroniska kommunikationer
  Nyheter och samhällsinformation
  Infrastruktur och tjänster för lagring och bearbetning av information
  Post
- ORDNING OCH SÄKERHET
  Skyddsverksamhet
- BARNOMSORG OCH UTBILDNING
  Omsorg av barn
  Utbildning för barn och unga

Både sannolikheten och konsekvenserna kan i vissa fall vara små för det egna företaget. Däremot kan angrepp få konsekvenser för andra företag och aktörer, inklusive statliga aktörer. En angripare kan till exempel utnyttja tilliten mellan leverantörer och kunder för att hitta enklare vägar in i en verksamhet. Samhället i stort vinner på att det finns en sådan tillit mellan organisationer. Dock kan det också innebära att angrepp på ett företag kan sprida till, eller utgöra en inkörsport till, andra organisationer eller statliga aktörer.

Ännu svårare att överblicka är spridningsrisken mellan till synes orelaterade verksamheter. Lunchmenyn på den lokala restaurangen kan vara en utmärkt utgångspunkt för så kallade vattenhålsattacker. På restaurangens webbplats placeras infiltrationsprogram som infekterar besökarnas datorer. Programmet används sedan för att angripa ett annat företags nät.

"En attack behöver inte slå ut hela verksamheten för att få en stor inverkan. Det finns olika delar som får tjänster att fungera."

Ett cyberangrepp behöver inte vara omfattande och slå ut hela verksamheten för att det ska få konsekvenser. Cyberattacken som i juli 2021 slog ut kassasystemet som Coop använder sig av är ett exempel på detta. Matvaror levererades och fanns fortfarande i hyllorna. Det fanns tillgänglig personal och fungerade lokaler. Men eftersom kunderna inte kunde betala för varorna var man likväl tvungen att stänga butikerna. Det exemplet visar även på hur en attack riktad mot ett företag kan slå ut system som andra aktörer använder.

Cybersäkerhet – i allas intresse

Cybersäkerhet är en nödvändighet för att näringslivet ska kunna utveckla och tillhandahålla konkurrenskraftiga varor och tjänster, och i ett större perspektiv också en viktig förutsättning för svensk tillväxt och konkurrenskraft.[27] Ett cyberangrepp kan även få stora konsekvenser inte bara för den som utsätts utan också påverka andra aktörer och deras verksamhet.[28]

Som konstaterats av flera myndigheter utgör cyberhotet ett av de största hoten mot Sverige. Fördjupad samverkan mellan tjänsteföretagen och staten för att stärka arbetet med cybersäkerhet ligger i bådas intresse. Skälet till det är bland annat att många tjänsteföretag upprätthåller eller säkerställer samhällsfunktioner som är nödvändiga för samhällets grundläggande behov, värden eller säkerhet. Det handlar exempelvis om transporter, hälsa, vård och omsorg, information och kommunikation eller ordning och säkerhet. Många av de tjänster som företagen levererar är därmed samhällsviktiga och det ligger i statens intresse att den upprätthålls. Företagen har vidare ett egenintresse i att arbeta med cybersäkerhet, genom vilket de kan minska risken för de konsekvenser som ett cyberangrepp kan leda till.

"Alla, såväl privata som offentliga sektorn, är ihopkopplade och ligger något nere så kommer det påverka flera."

Dagens sammankopplade och digitaliserade samhälle visar på betydelsen av nära samverkan mellan staten och företagen. De stora utmaningarna talar för att etablera närmare samarbeten och en fördjupad dialog om hur cybersäkerheten kan stärkas gemensamt. Att flera tjänsteföretag dessutom bedriver, eller bidrar till, samhällsviktig verksamhet innebär att bristande cybersäkerhet i något led riskerar få allvarliga konsekvenser för samhällets skyddsvärden.

"Det finns en skev bild och tilltro till att alla har sina egna resurser inom offentlig sektor, men de förlitar sig oftast på privata företag som levererar varor och tjänster av vikt för funktionaliteten i deras verksamhet"

Tyvärr lyser utbyte och samverkan mellan tjänsteföretagen och myndigheterna i hög grad med sin frånvaro i den enkät som vi har genomfört. Mer än nio av tio tjänsteföretag uppger att de i dag inte samarbetar med myndigheter avseende cybersäkerhet. Ett antal tjänsteföretag beskriver hur de upplever bristande intresse från myndigheterna att utveckla ett närmare

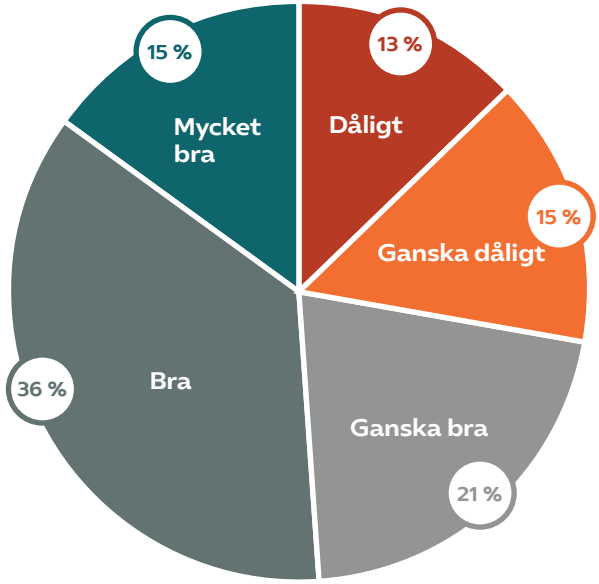
27 Skr. 2016/17:213. Nationell strategi för samhällets informations- och cybersäkerhet.

28 Sveriges Radio. (2022) Har cyberattackerna ökat med kriget i Ukraina? Hämtad 4 april 2022.

samarbete, och även till viss del en bristande förståelse hos myndigheterna om vad företagen tillhandahåller som är av vikt för samhället.

Över lag förefaller det även råda en osäkerhet kring vilka myndigheter tjänsteföretagen kan eller bör samarbeta med, alternativt få stöd av.[29] I våra intervjuer med tjänsteföretag framkom att en av anledningarna till detta är att flera myndigheter ansvarar för olika aspekter kopplat till cybersäkerhet, såsom myndigheter med ansvar inom en särskild sektor eller aspekt inom cybersäkerhet (till exempel MSB, Säkerhetspolisen och Polisen) eller myndigheter med samverkans- eller tillsynsansvar. Detta leder till osäkerhet vilken myndighet man kan och bör samverka med eller söka stöd från.

Figur 5: Svar på frågan "Hur bra fungerar samarbetet med statliga aktörer?"



Som framgår ovan (figur 5) så anser emellertid den lilla andel tjänsteföretag som samarbetar med statliga myndigheter att samarbetet över lag fungerar bra. Bland aktörer som företagen samarbetar med omnämns framför allt Polisen, MSB, regioner och kommuner, Säkerhetspolisen, Integritetsskyddsmyndigheten (IMY) och till viss del även Försvarsmakten och FRA. Det finns därmed exempel på gott samarbete att bygga vidare på.

Samtliga tjänsteföretagen som intervjuats har uttryckt en vilja till ökat utbyte och samarbete med myndigheter. Flera av de utmaningar som tjänsteföretagen lyfter fram är också områden de uttryckt behov och ett stort mervärde av samverkan med, men även stöd från, statliga aktörer. Dessa utmaningar är inte unika för företagen utan utmaningar som även statliga aktörer står inför. Det finns också exempel på lyckade samarbeten som samverkan mellan tillsynsmyndigheten Post- och telestyrelsen (PTS) och teleoperatörerna inom elektronisk kommunikation i Nationella telesamverkansgruppen (NTSG). Det är ett frivilligt samarbetsforum med syfte att stödja återställandet av den nationella infrastrukturen för elektroniska kommunikationer vid allvarliga störningar i samhället som startade 2005.

29 På fråga om vilka myndigheter som företagen gärna skulle arbeta närmare var det endast 23 procent av de tillfrågande som svarade, och av dessa svarade 45 procent att de inte visste.

Tjänsteföretagens förslag för stärkt cybersäkerhet

Från tjänsteföretagens sida har man uttryckt såväl vilja som behov av samverkan och stöd. Det blir tydligt att behovet är stort av en tydligare styrning och inriktning. Det behöver bli tydligare vilka förväntningar som ligger på företagen avseende cybersäkerhet samt vilken miniminivå som företag inom olika sektorer behöver och förväntas ha. Kravställningarna i dag uppfattas av vissa som alltför generiska. Vad är det företagen behöver ta höjd för och på vilka grunder? Flera tjänsteföretag pekar även på vikten av finansiellt stöd eller kostnadsersättning, vilket utgör ett möjligt verktyg för att påskynda och lyfta den samlade motståndskraften i samhället.

Utöver tydligare styrning, och tydligare förväntansbild på tjänsteföretagen, efterfrågar tjänsteföretagen tydliga och anpassade riktlinjer och vägledningar utifrån exempelvis företagsstorlek och i vissa fall även bransch. De ser också ett behov av rådgivnings- och stödfunktioner, inklusive tillhandahållande av resurser som arbetar förebyggande eller kan stödja vid attack i form av ett responsstöd. Att företagen får ta del av information och lägesbilder från myndigheterna avseende hot, typer av attacker och identifierade sårbarheter är ytterligare en viktig komponent för att stärka cybersäkerheten.

Det stöd och former för samverkan som företagen har behov av för att stärka cybersäkerheten finns till viss del i dag, både som information från myndigheter och tjänster från till exempel IT-säkerhetskonsulter. Det finns därmed möjligheter att utveckla det existerande statliga stödet för att tillgodose det, exempelvis genom att utveckla och anpassa MSB:s vägledningar och utveckla det stöd om CERT-SE bistår med, där det är lämpligt utan att störa marknaden. CERT-SE är Sveriges nationella CSIRT (Computer Security Incident Response Team) med uppgift att stödja samhället i arbetet med att hantera och förebygga IT-incidenter.

Man skulle även kunna se över möjligheterna för att vidareutveckla forumen för informationsdelning och informationssäkerhet samt de nätverk som i dag finns inom ett antal områden där staten har en särskild roll. Därtill finns också möjligheter att utveckla stödåtgärder genom det nyligen inrättande Nationellt cybersäkerhetscenter där det är lämpligt. Avseende Nationellt cybersäkerhetscenter uttrycks en förhoppning från tjänsteföretagens sida om att det även kan bli ett forum för dialog och samverkan samt utgöra en aktör som kan sprida information och dela lägesbilder, vilket centret också har som uppdrag.

Det krävs även kommunikativa åtgärder från myndigheternas sida för att påvisa det stöd och samverkansformat som i dag finns. En övergripande utmaning för tjänsteföretagen avseende samverkan med, men även stöd från, statliga myndigheter ligger i att flera myndigheter arbetar med cybersäkerhet och att det därmed inte finns en väg in. Rätt väg in kan också vara beroende av vilken sektor tjänsteföretaget är verksamt inom. Det är inte en helt enkel uppgift som företag att navigera och se sin roll och vart man ska in i det stora lapptäcke av aktörer och arrangemang som finns inom cyberområdet.

> **"För att samarbetet ska kunna utvecklas behöver någon form av kulturskifte ske i myndighetssfären – all information kan inte vara hemligt. På myndighetssidan behöver man också inse mervärdet av att samarbeta och dela information och lägesbild med företagen."**

Ett kulturskifte behöver även ske inom myndighetssfären där dialog och utbyte av information uppmuntras. Att dela information kan vara en utmaning i frågor som är förknippade med känslig eller sekretessbelagd information. Samtidigt är delandet av information ett viktigt medel i att stärka cybersäkerheten då man genom detta bland annat i ett tidigt skede kan identifiera sårbarheter, stärka förebyggande åtgärder och öka beredskapen för ett potentiellt angrepp. Det finns därmed ett behov av att se över hur man säkert kan dela information.

Det finns flera goda exempel på privat-offentlig samverkan från andra länder som tjänsteföretagen har erfarenhet från, där det bland annat har skapats grupperingar för statliga och privata aktörer som till exempel är involverade i samhällskritisk verksamhet. Därigenom skapas bland annat ett kontaktnät, vilket är av stort värde för att exempelvis dela information och uppmärksamma om identifierade hot och sårbarheter. Några länder som omnämnts och som kan ligga till grund för utvecklandet av samverkan är Norge, Finland och Nederländerna.

Förslag på åtgärder från tjänsteföretagen

Nedan sammanfattas de förslag som har framkommit i dialog med tjänsteföretagen, och som syftar till att stärka såväl tjänsteföretagens som samhällets motståndskraft.

Upprätta format för samverkan

- Se över möjligheter för att vidareutveckla operativa nätverk för samverkan mellan företag och offentlig sektor inom fler branscher.
- Utveckla format för samverkan utifrån lärdomar från andra länder, exempelvis Norge, Finland och Nederländerna.

Informationsdelning

- Upprätta kommunikationskanaler och forum genom vilka företag kan rapportera in men också ta del av information, aktuella lägesbilder samt dela med sig av sektorsvisa lägesbilder.
- Uppmärksamma pågående cyberattacker eller identifierade sårbarheter.

Kunskapsspridning

- Dela goda exempel och bästa praxis avseende förebyggande cybersäkerhet, exempelvis genom MSB, Nationellt cybersäkerhetscenter eller genom befintliga nätverk.

Anpassade riktlinjer och råd

- Utveckla sektorsspecifika riktlinjer och vägledningar för hur företag kan arbeta med cybersäkerhet och vilka grundläggande krav eller funktioner som bör finnas, särskilt till företag som bedriver samhällsviktig verksamhet och där staten kan bidra med något som privata aktörer inte kan.
- Målgruppsanpassa riktlinjer och vägledningar till små och medelstora företag, inklusive tydliggörande av vilken nivå på cybersäkerhet som mindre företag bör ha där det finns det finns en statlig kravbild.
- Utveckla metoder för systematiskt arbete med cybersäkerhet anpassade till mindre företag, vilka ofta har begränsade resurser, där det inte finns tillräckligt stöd från marknaden.

Resursstöd

- Genom Nationellt cybersäkerhetscenter erbjuda lämpligt stöd till de som arbetar förebyggande eller kan stödja vid attack, exempelvis i form av ett responsstöd.
- Se över möjligheten att vidareutveckla det stöd som CERT-SE i dag ger till att utöver rådgivning vid en IT-incident även inkludera resursstöd där det finns särskilda behov.

Källor

Enkät

Enkätundersökning genomförd mellan februari och mars 2022 som gått ut till Almegas medlemmar som ombetts svara på ett antal frågor rörande deras arbete med cybersäkerhet, upplevd hotbild och utmaningar samt samverkan med statliga aktörer.

Intervjuer

Intervjuer genomförda mellan februari och mars 2022 med företrädare för teknikföretag, säkerhetsföretag, medieföretag, transportföretag, vårdföretag, tjänsteförbund och innovationsföretag.

Referenser

Försvarets radioanstalts årsrapport 2021. Medarbetare i demokratins tjänst. https://fra.se/download/18.3262020817e4dcd6ffc210/1648022049159/FRAarsrapport_2021_uppslag.pdf

Försvarsmakten. (2022). Cyberangrepp största hotet just nu. https://www.forsvarsmakten.se/sv/aktuellt/2022/03/cyberangrepp-storsta-hotet-just-nu/

Microsoft. (2022). ACTINIUM targets Ukrainian organizations. Hämtat den 11 april 2022. https://www.microsoft.com/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/

Myndigheten för samhällsskydd och beredskap. (2022). En inblick i Sveriges cybersäkerhet: Årsrapport it-incidentrapportering 2021. https://rib.msb.se/filer/pdf/29894.pdf

Paloalto Networks. (2022). Russia's Gamaredon aka Primitive Bear APT Group Actively Targeting Ukraine. Hämtat den 11 april 2022. https://unit42.paloaltonetworks.com/gamaredon-primitive-bear-ukraine-update-2021/

Radar. (2021). Svensk cybersäkerhet 2021: Svenska förutsättningar, marknad, trender, hotbild, attacker, åtgärder och praktiska råd. https://orangecyberdefense.com/se/rapport-om-svensk-cybersakerhet-2021/

Skr. 2016/17:213. Nationell strategi för samhällets informations- och cybersäkerhet. https://www.regeringen.se/4a095b/contentassets/00a3e76fcee44f54af2399b82ee1307f/skr-201617-213-bilaga-uppdatering-om-genomforandet.pdf

SOU 2019:51. Näringslivets roll inom totalförsvaret: Betänkande av Utredningen om totalförsvarets försörjningstrygghet. Stockholm: Elanders Sverige AB. https://www.regeringen.se/4ad9c6/globalassets/regeringen/dokument/forsvarsdepartementet/sou/sou-2019-51-naringslivets-roll-inom-totalforsvaret.pdf

Sveriges Radio. (2022) Har cyberattackerna ökat med kriget i Ukraina? Hämtad 4 april 2022. https://sverigesradio.se/artikel/har-cyberattackerna-okat-med-kriget-i-ukraina#:~:text=N%C3%A4r%20Ryssland%20startade%20kriget%20i,presskonferens%20om%20cyberangrepp%20i%20Sverige.

Säkerhetspolisen. (2022). Cyberangrepp ständigt pågående hot mot Sverige. Hämtat den 5 april 2022. https://www.sakerhetspolisen.se/ovriga-sidor/nyheter/nyheter/2022-03-11-cyberangrepp-standigt-pagaende-hot-mot-sverige.html

Säkerhetspolisens årsbok 2021. https://www.sakerhetspolisen.se/download/18.650ed51617f9c29b552287/1649683389251/Sakerhetspolisen_arsbok%202021.pdf

Truesec. (2022). Cyberkriminella har bytt taktik. Pressmeddelande 14 februari 2022, https://press.truesec.se/posts/pressreleases/cyberkriminella-har-bytt-taktik

www.almega.se
info@almega.se
08 762 69 00

Sturegatan 11
114 36 Stockholm