BASALT
EN DEL AV OMEGAPOINT

Svenskt Säkerhetsindex® 2023

En årlig kartläggning av säkerhetsläget inom samhällsviktig verksamhet

I samarbete med

KANTAR

Rapporten i korthet

Innehåll

- Det upplevda hotet mot Sveriges samhällsviktiga verksamheter ökar, nästan 7 av 10 upplever en mer allvarlig hotbild, en ökning med 6% jämfört med ifjol.

- Hotbilden kopplad till verksamheternas informationssäkerhet upplevs vara allvarligast, 8 av 10 anser att hotet är allvarligt. Lägst är hotbilden kopplad till personalsäkerhet, endast 28% upplever den som allvarlig.

- Allmänheten upplever en allvarligare hotbild mot samhället, 73% upplever en allvarligare hotbild jämfört med 66% i fjol.

- Svenskt Säkerhetsindex® 2023 visar att endast 3% av allmänheten har mycket stor tilltro till beslutsfattarnas förmåga att skydda viktig infrastruktur, en alarmerande siffra med tanke på konsekvenserna om beslutsfattarna misslyckas med sitt uppdrag.

- Säkerhetsfrågan hos verksamheterna är både högt på agendan och budgeterad. Nästan 9 av 10 beslutsfattare anser att statusen för säkerhetsarbetet har ökat.

- Svenskt Säkerhetsindex® 2023 konstaterar att 1 av 5 verksamheter har ett otillräckligt verksamhetsskydd. Den vanligaste bristen är att organisationerna inte regelbundet övar en krisplan.

Ett steg mot ett säkrare samhälle

Under 2022 har det allmänna säkerhetsläget kraftigt förvärrats. Bara under hösten har flera allvarliga dataintrång skett mot kommuner, myndigheter och privata företag. Även personalsäkerheten är under luppen, med systematiska kartläggningar från antagonister.

Som ett av Sveriges ledande säkerhetsföretag har vi en viktig roll att fylla. Vårt syfte med Svenskt Säkerhetsindex® är att lyfta säkerhetsfrågorna till ett högre plan och skapa viktiga insikter för det kommande decenniet, så att vi tillsammans kan skapa ett säkrare samhälle.

Du läser just nu vår fjärde rapport, som visar att nästan 7 av 10 beslutsfattare upplever en allvarligare hotbild mot deras verksamhet än tidigare. Det största upplevda hotet är cyberattacker, som fortsätter att växa med en alarmerande hastighet. Runt om i världen ökade antalet attacker med 55 procent förra året, enligt Check Point Cyber Security Report.

Det finns mycket vårt samhälle behöver göra för att stå rustade inför en orolig framtid. Hotbilden är hög och alltjämt ökande, medan förmågan att stå emot hoten dessvärre är bristfällig. Vår undersökning visar dessutom att allmänhetens förtroende för statens förmåga är i gungning.

Även om mycket är mörkt finns några ljuspunkter. Säkerhetsfrågorna har klättrat högre upp på dagordningen och prioriteringen av dessa frågor hos myndigheter och företag ökar markant. Behovet av ett systematiskt arbete inom säkerhet är tydligt och företag och organisationer agerar genom att säkerhetsfrågorna nu lyfts upp till ledning och styrelser. I synnerhet står frågor runt säkerhetsskydd i fokus.

Genom att vi lyfter rätt frågor till rätt nivå har vi en möjlighet att tillsammans agera under de kommande åren, vilket höjer tröskeln för de som hotar vårt samhälle. I synnerhet antagonistiska staters underrättelsetjänster.

Ta del av rapporten samt begrunda vilket ansvar du har, eller kan ta, för att göra din organisation säkrare och bättre rustad mot kommande hot.

- Nicklas Haglund, VD Basalt

Allvarligare hotbild

Svenskt Säkerhetsindex® visar på en tydlig ökning av det upplevda hotet mot Sveriges samhällsviktiga verksamheter.

Under 2022 upplevde fler beslutsfattare, nästan 7 av 10 (65%)*, en allvarligare hotbild mot deras verksamhet, det är en ökning med 6% jämfört med i fjol. Enbart 1 av 100 upplever att hotbilden inte alls är allvarlig.

”Kriget i Ukraina pågår, den ekonomiska utvecklingen är under stor press, energiproduktionen riskerar att inte räcka till under vintern och efterdyningarna av Covid-19 skakar oss fortfarande. Utöver detta kan kriget i Ukraina trappas upp till ett krig mellan Ryssland och NATO.

Också kärnvapen kan komma att användas, inte bara i Ukraina utan också betydligt närmare eller till och med på svenskt territorium.

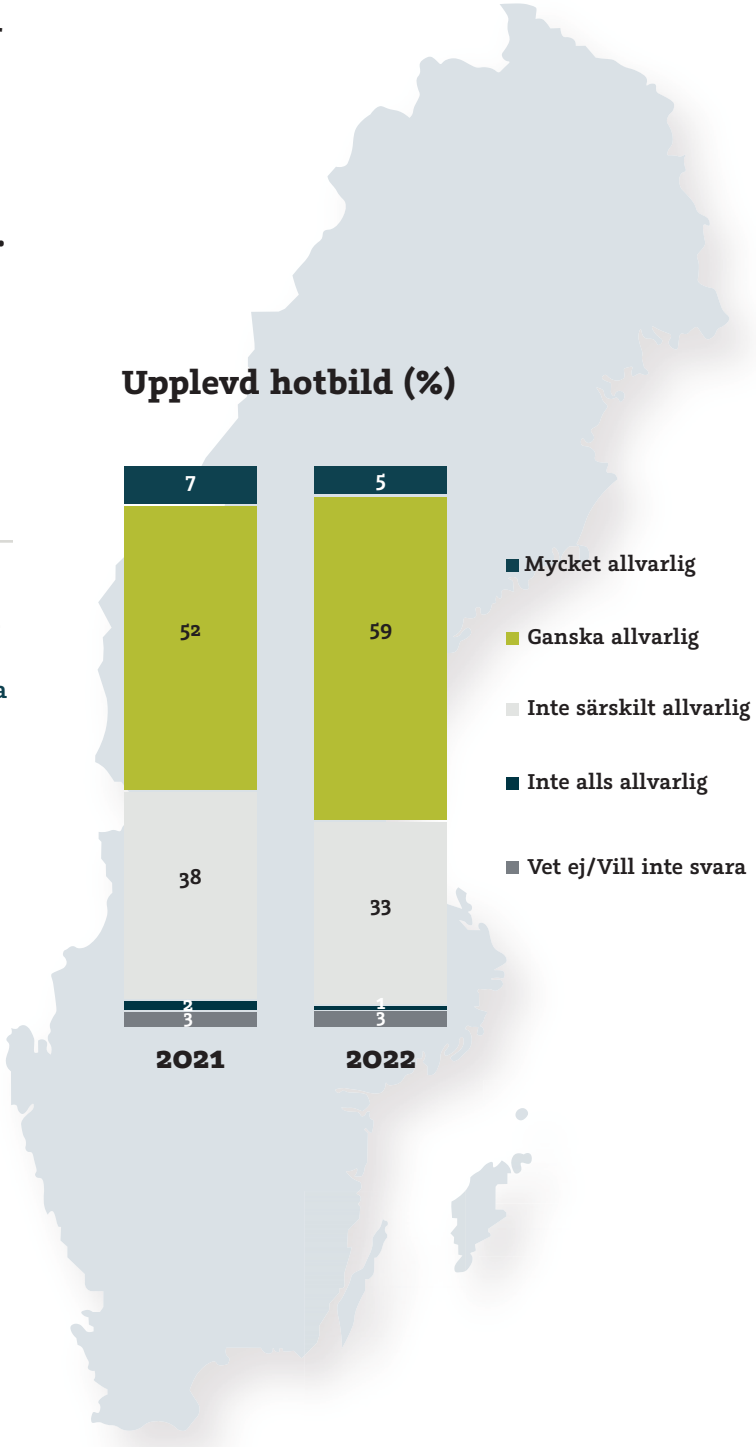
Svarta svanar som till exempel solstormar och vulkanutbrott med allvarlig påverkan på atmosfären eller det ekonomiska systemets kollaps, kan vi aldrig helt räkna bort.”

- Anders Brännström, strategisk rådgivare, Basalt

”Eftersom många affärskritiska verksamhetsprocesser är direkt beroende av att informationens konfidentialitet, integritet och tillgänglighet kan säkerställas genom hela informationskedjan, har informationssäkerhetsarbetet i allt högre grad gått från att vara enbart värdebevarande till att även vara värdeskapande.

Genomtänkta och rätt implementerade säkerhetsåtgärder skyddar nämligen inte bara verksamhetens informationstillgångar, utan bidrar också till att optimera den produktivitet och kreativitet som informationen faciliterar.”

– Per Nyberg, CISO, Basalt



Fråga: Hur bedömer du den nuvarande hotbilden mot er verksamhet? Med extern hotbild menar vi hot från en eller flera agerande aktörer som kan få negativ effekt om de sätts i verket. Vi menar inte t.ex. en naturkatastrof eller pandemi.

Källa: Kantar
Bas: Alla (200)
*Top box, de som svarat mycket allvarlig + ganska allvarlig

Hotet kopplat till personalsäkerheten underskattat

Hotbilden kopplad till verksamheternas informationssäkerhet i form av cyberattacker upplevs vara allvarligast bland verksamhetsskyddets tre områden; informationssäkerhet, personalsäkerhet och fysisk säkerhet. 8 av 10 anser att hotet mot informationssäkerheten är allvarligt (s 23 figur 1:1). Hotet mot den fysiska säkerheten (obehörigt tillträde till områden eller byggnader där en aktör kan få tillgång till skyddsvärd information) upplever en tredjedel (31%) som allvarlig (s 23 figur 1:3).

Lägst är hotbilden kopplad till personalsäkerhet (dvs. oavsiktliga eller avsiktliga riskbeteenden hos egen personal kopplade till informationssäkerhet endast 28% upplever den som allvarlig (s 23 figur 1:2). Att hotet kopplat till personalsäkerhet är lägst kan bero på att det underskattas. Det kan även finnas ett obehag att konfrontera sina medarbetare såväl som en osäkerhet kring hur man bör ta sig an frågorna.

”Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas enligt säkerhetsskyddslagen. Det är även lämpligt att låta personer som ska delta i verksamhet med höga skyddsvärden i övrigt, genomgå en säkerhetsprövning som en verksamhetsskyddsåtgärd. En sådan säkerhetsprövning kan dock inte omfatta en registerkontroll eller särskild personutredning men har ändå ett stort värde och innebär att risken att få in fel personer i verksamheten minskar.

Det finns i det aktuella samhällspolitiska läget skäl att ta personalsäkerheten på allvar!”

– Yvette Glantz – Jurist, säkerhetskonsult, Basalt

”Det är viktigt att anställningen föregås av en utredning som i tillräcklig mån säkerställer att personen är trovärdig och lojal. Oavsett om anställningen avser en tjänst inom en klädesbutik, en fordonstillverkare eller försvaret, kommer den anställde i kontakt med känslig information. Och innan anställningskontraktet signeras måste den chefen kunna veta med tillräcklig säkerhet att personen är trovärdig och lojal.”

- Jana Thorén, Konsultgruppchef, Basalt

65% upplever en allvarlig hotbild idag

Källa: Kantar
Bas: Beslutsfattare (200)

77%

8 av 10 upplever att hotbilden kommer att öka ytterligare

78%

Källa: Kantar
Bas: Beslutsfattare (200)

anser att verksamhetsskydd är strategiskt viktigt för verksamheten

Vad innebär verksamhetsskydd?

Säkerhetsskydd regleras i säkerhetsskyddslagen och säkerhetsskyddsförordningen. Verksamhetsskydd och säkerhetsskydd omfattar i stort samma åtgärder men har olika syften. Säkerhetsskydd ska skydda Sveriges säkerhet och verksamhetsskydd ska skydda verksamheten. Ofta är de faktiska handgreppen och åtgärderna runt informationssäkerhet, personalsäkerhet och fysisk säkerhet likartade inom både verksamhetsskydd och säkerhetsskydd.

Verksamhetsskydd* innebär skydd mot inre och yttre hot som är riktade mot verksamheten och det omfattar tre huvudsakliga områden; informationssäkerhet, personalsäkerhet och fysisk säkerhet.

*När det gäller verksamheter som omfattas av säkerhetsskyddslagen så benämns verksamhetsskydd i stället som säkerhetsskydd.

Allmänheten har oroande lågt förtroende för beslutsfattarna

Årets undersökning visar att allmänheten upplever en allvarligare hotbild mot samhället jämfört med i fjol, 73% upplever en allvarligare hotbild jämfört med 66%.

Nästan varannan person (45%) tror att det är sannolikt att vi drabbas av långvariga strömavbrott, det är en ökning med 9 procent från förra året. Man tror även att det är troligt att bli hackad på sociala medier och att få sina personliga bilder/konversationer läckta (46%). Allmänheten tror också att det är sannolikt att journaluppgifter läcks från sjukvårdens digitala sjukvårdssystem (44%).

Top 3 mest sannolika händelserna enligt allmänheten

1 Dina personliga/privata bilder och konversationer är inte längre under din egen kontroll

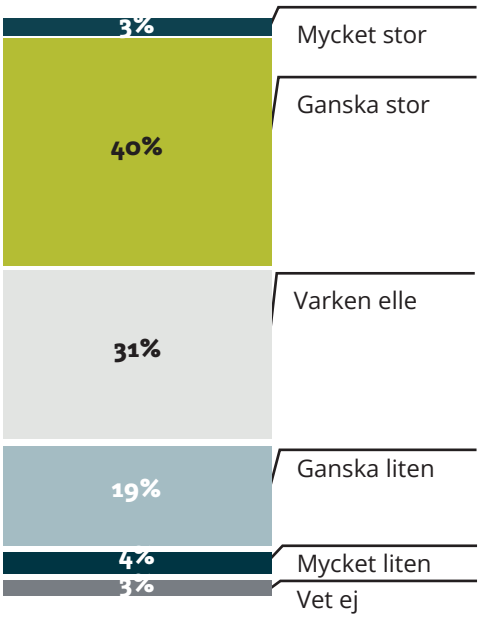
2 Det blir strömavbrott i samhället under flera dagar

3 Journaluppgifter läcks från sjukvårdens digitala sjukvårdssystem

Sveriges beslutsfattare måste ligga steget före och därigenom förebygga att samhället bland annat drabbas av cyberattacker. Dock visar Svenskt Säkerhetsindex® siffror på att endast 3% av allmänheten har mycket stor tilltro till beslutsfattarnas förmåga att skydda viktig infrastruktur, en alarmerande siffra med tanke på konsekvenserna om beslutsfattarna misslyckas med sitt uppdrag.

Tilltro till beslutsfattarnas förmåga att skydda viktig infrastruktur

Källa: Kantar
Bas: Allmänheten (1000)



”Utan att på något sätt vara alarmist uttrycker den siffran något mycket allvarligt i samhället. Allmänhetens uppfattning om ledarskapet och ledningen grundar sig som alltid på vad ledarskapet har visat sig kunna hantera.

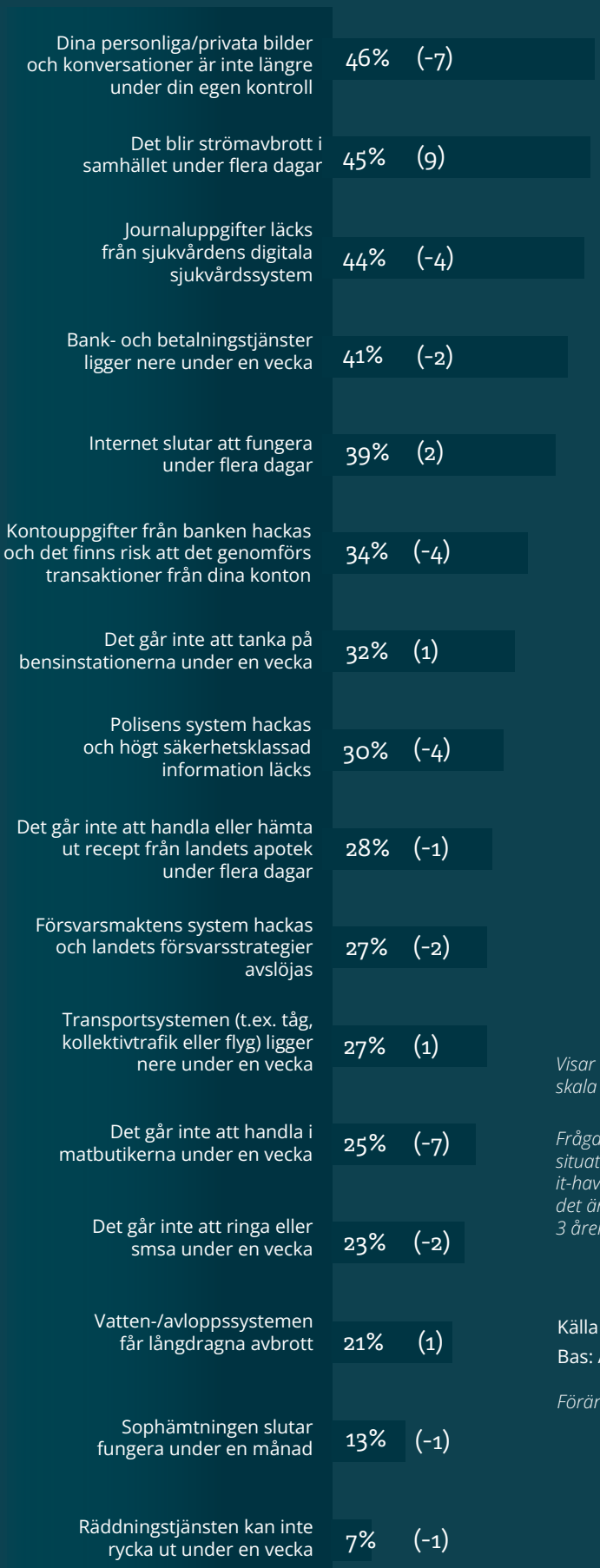
Om beslutsfattarna i samhället i god tid fattar och genomför riktiga beslut blir allmänhetens tilltro till dem högre, om inte blir den som nu katastrofalt låg.”

Anders Brännström,
Strategisk rådgivare, Basalt

”Den uppenbara slutsatsen är att i stort är Sveriges ledarskap på det här området underkänt. Det finns säkert positiva undantag men överskuggande är situationen absolut inte tillräckligt bra.”

Anders Brännström,
Strategisk rådgivare, Basalt

Hur troligt anser du att det är att följande inträffar inom de närmaste 3 åren?



Visar andelen som svarat 4-5 på en 5-gradig skala där 1=Inte alls troligt och 5=Mycket troligt

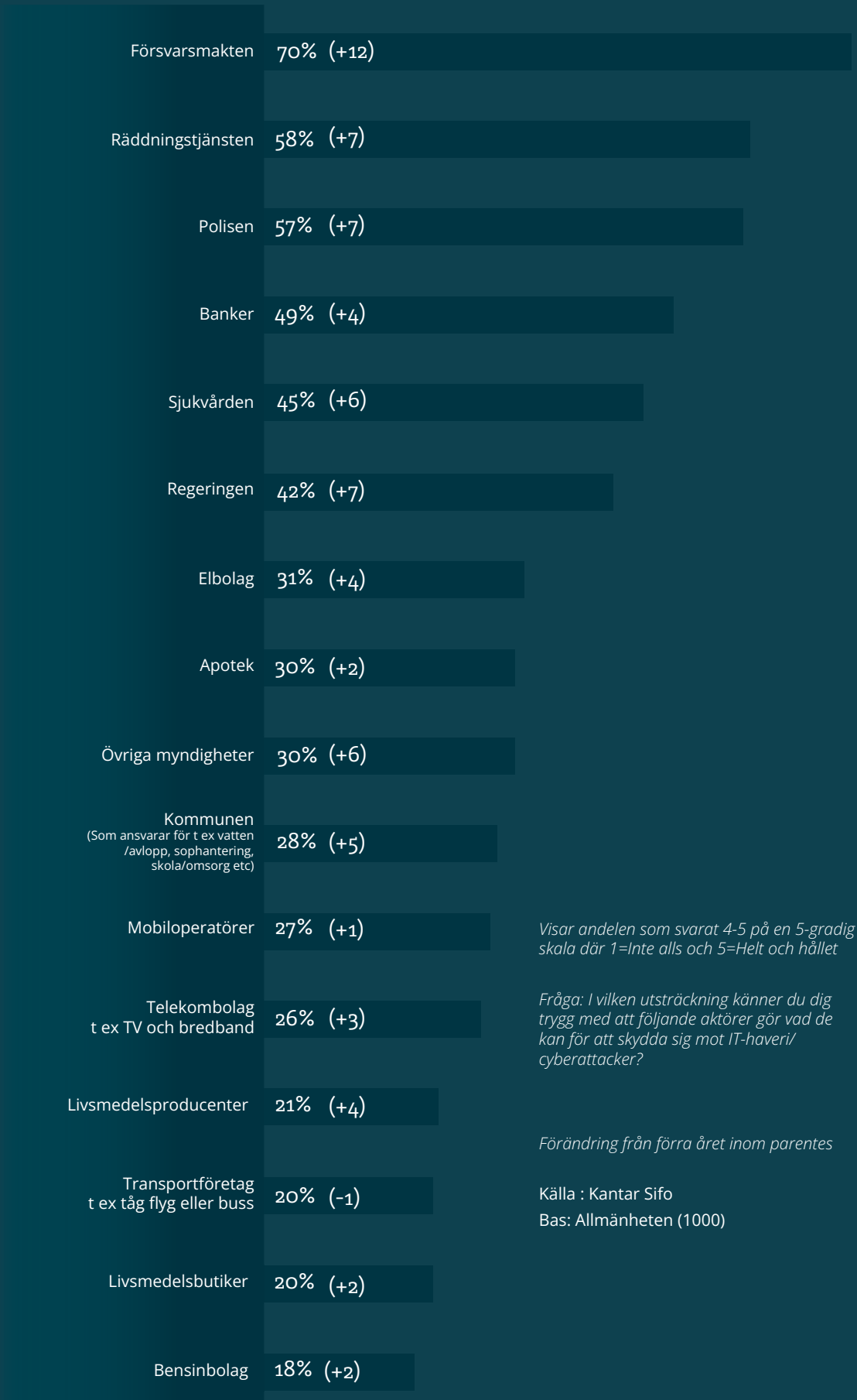
Fråga: Vi kommer nu att lista några olika situationer som skulle kunna uppstå till följd av it-haveri/cyberattacker. Hur troligt anser du att det är att följande inträffar inom de närmaste 3 åren?

Källa : Kantar Sifo

Bas: Allmänheten (1000)

Förändring från förra året inom parentes

Upplevd trygghet i att aktörer gör vad de kan för att skydda sig mot haveri



Visar andelen som svarat 4-5 på en 5-gradig skala där 1=Inte alls och 5=Helt och hållet

Fråga: I vilken utsträckning känner du dig trygg med att följande aktörer gör vad de kan för att skydda sig mot IT-haveri/ cyberattacker?

Förändring från förra året inom parentes

Källa : Kantar Sifo

Bas: Allmänheten (1000)

Säkerhetschef – det nya statusyrket

I år konstateras att säkerhetsfrågan hos verksamheterna både är högt på agendan och budgeterad. Nästan 9 av 10 (87%) beslutsfattare anser att statusen för säkerhetsarbetet har ökat, bara 1 av 100 anser att den har minskat (s 23 figur:2).

Säkerhetschefer har också fått mer pengar att röra sig med, 70% av organisationerna anger att deras säkerhetsbudget har ökat de senaste åren (s 23 figur:3).

Trenden med ökat fokus på säkerhetsarbete ser även ut att hålla i sig då 65% förutspår att budgeten kommer fortsätta att öka (s 23 figur:4).

”I många år har det sagts att säkerhet- och säkerhetsskyddschef är bland det mest ensamma yrket som finns. Detta är definitivt under förändring!

Dagens säkerhet- och säkerhetsskyddschef är inte längre en ensamvarg. Yrket kräver ett brett spektrum av kompetenser och samarbetsytor. Att förstå verksamheten, att se helheten är en av de allra viktigaste aspekterna för dagens och morgondagens säkerhets- och säkerhetsskyddschef.”

– Ron Egly, Säkerhetsskyddschef, Basalt

”Det krävs en stark integration med specialister inom personalsäkerhet, fysisk säkerhet, informations-säkerhet, it-säkerhet, operativt it-arbete och inte minst en stark förankring i det dagliga arbetet. Olika interna och externa nätverk bidrar också till en väl avvägd beslutsfattning samtidigt som det bidrar till att öka kompetensen.”

– Ron Egly, Säkerhetsskyddschef, Basalt

1 av 5 har ett otillräckligt verksamhetsskydd

Basalts definition av ett ”heltäckande verksamhetsskydd” utgår från de elva kriterierierna som spänner över informationssäkerhet, personalsäkerhet och fysisk säkerhet, med fokus på ett systematiskt och kontinuerligt arbetssätt. Genom att tydligt uppfylla samtliga kriterier anses man ha ett heltäckande verksamhetsskydd. Följande sex kriterier (av de totalt elva) är helt avgörande. Om någon av dessa kriterier inte är uppfyllda, bedömer Basalt att organisationen har ett ”otillräckligt verksamhetsskydd”.

Kriterierna som måste uppfyllas för att ha ett tillräckligt verksamhetsskydd

Vi arbetar fullt ut med riskhantering

Vi har en fungerande och fullt implementerad policy kring informationssäkerhet

Vi har en krisplan som vi övar med viss regelbundenhet

I samband med rekrytering säkerställer vi att medarbetaren inte utgör en säkerhetsrisk

Vi har handlingsplaner för att återställa våra system eller vår verksamhet så snabbt som möjligt

Vi har tydliga rutiner för hur vi skulle återställa verksamheten efter ett it-haveri

Svenskt Säkerhetsindex® 2023 konstaterar att 1 av 5 verksamheter har ett otillräckligt verksamhetsskydd.

Den vanligaste bristen är att organisationerna inte regelbundet övar en krisplan - 12% gör inte detta. Det betyder att man inte tar steget från att ha en plan på papper till att faktiskt öva och testa den.

Den näst vanligaste bristen är att man nyanställer utan att genomföra tillräckliga säkerhetskontroller - 9% gör inte det. Det finns därmed en risk att rekrytera medarbetare vars beteenden riskerar att skada organisationen allvarligt.

”För att maximera affärsnyttan av verksamhetens säkerhetsarbete krävs ett systematiskt och strukturerat tillvägagångssätt, där de mest skyddsvärda tillgångarna identifieras och analyseras utifrån ett hot-, risk- och sårbarhets-perspektiv.

Resultatet av denna kartläggning blir sedan de grundläggande ingångsvärden som krävs för att i nästa steg kunna definiera och implementera anpassade och effektiva säkerhetsåtgärder, både av teknisk och organisatorisk karaktär.”

– Per Nyberg, CISO, Basalt

För att uppnå ett heltäckande verksamhetsskydd ska samtliga kriterier stämma in på verksamheten

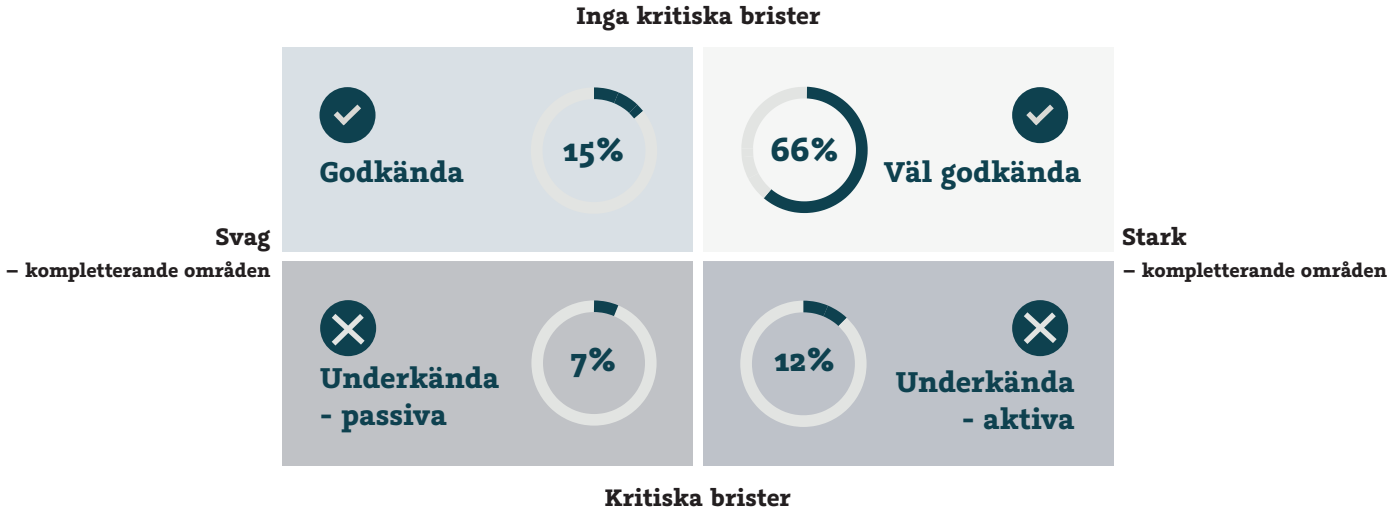
Undersökningens resultat visar att 24% av verksamheterna har ett heltäckande skydd vilket är en ökning på 3 procent jämfört med i fjol.

Diagrammet visar andelen av beslutsfattarna som uppfyller respektive kriterium enligt definition. För att en verksamhet ska anses ha ett heltäckande verksamhetsskydd enligt denna ska samtliga kriterier vara uppfyllda.

Källa : Kantar
Bas: Beslutsfattare (200)

Oroväckande vanligt med ett bristande verksamhetsskydd

Många organisationer inom samhällsviktiga verksamheter har mycket kvar att göra. Vad man ska prioritera beror på vilket läge man befinner sig i inom ramen för matrisen. Även ambitiösa organisationer kan ha prioriterat fel trots att de har många delar som är på plats. Analysera din organisation och fundera på var ni befinner er.



Godkända

Dessa organisationer har inte kritisk exponering i nuläget men saknar en systematik i arbetet.

Säkerhetsarbetet är komplext och det är viktigt att ledningsgruppen är djupt involverad så att inte delar missas på grund av silo-strukturer. En inventering av vita fläckar ger ofta en bra roadmap för budgetarbetet.

Åtgärd: Säkerställ att det finns ett systematiskt arbetssätt och en tydlig kvalitetsäkringsprocess. Överväg certifiering mot t ex ISO 27001.

Väl godkända

Dessa organisationer har mycket på plats och inga kritiska brister. Men säkerhetsarbetet är ständigt pågående och det är viktigt att systematiken finns kvar även i ett längre perspektiv.

Genom genomlysning av både rutiner och total-kostnaden för säkerhetsarbetet går det också ofta att hitta synergieffekter och möjligheter att effektivisera.

Åtgärd: Arbeta vidare med sitt systematiska säkerhetsarbete och säkerställa att samtliga kriterier är prioriterade.

Underkända – passiva

Dessa organisationer har kritiska brister och är heller inte aktiva inom kompletterande områden.

Här krävs en kulturförändring och scenario-planering för att tydligt medvetandegöra den risk som verksamheten exponeras för.

Åtgärd: Säkerställ att ledning har rätt kompetens för att initiera och driva ett systematiskt säkerhets- arbete.

Underkända – aktiva

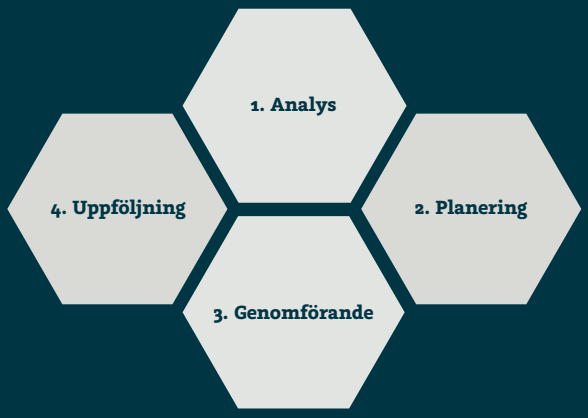
Dessa organisationer har kritiska brister som måste åtgärdas, samtidigt som man istället satsar inom mindre kritiska områden.

Att prioritera rätt och arbeta med helheten på ett systematiskt sätt är viktigare än att vara bäst på varje enskilt område.

Åtgärd: Säkerställ att ledning har rätt fokus och prioriteringar för att driva ett systematiskt säkerhetsarbete.

Systematiskt säkerhetsarbete

För att en organisation ska kunna skydda sig mot yttre och inre hot, behöver ledningen säkerställa att man har ett holistiskt och systematiskt förhållningsätt till säkerhets-arbetet. PDCA-modellen är en välbeprövad interativ process som driver ständig förbättring över tid.



”Man skulle behöva ha ett mer systematiskt säkerhetsarbete och få ut säkerhetsfrågorna i ledningsgruppen.”

– Beslutsfattare, kommun

Stort utrymme att göra mer

Genom att jobba systematiskt och vidta åtgärder för att bättre kunna möta hoten mot verksamheten kan man uppnå ett tillräckligt verksamhetsskydd.

Beslutsfattarna upplever att det finns mer åtgärder att vidta som skulle kunna minska hoten mot verksamhetsskyddets tre områden. Nästan 7 av 10 beslutsfattare (66%) anser att de definitivt kan vidta ytterligare åtgärder kring it-säkerhet. För personal-säkerheten och den fysiska säkerheten anser drygt 40% att de definitivt kan vidta ytterligare åtgärder.

Varför görs inte mer idag?

Anledningarna till att beslutsfattarna inte gör mer är främst grundat på resursbrist samt att det är ett kontinuerligt arbete där man upplever att det alltid finns mer att göra. Dessutom förändras hotbilden konstant och det är därför svårt att hinna ställa om.

”Det är ett föränderligt hotlandskap och förändrad riskbild, ändrade lagkrav och teknisk utveckling, som innebär att vi kontinuerligt behöver byta åtgärder. Vi måste vidta ytter-ligare säkerhetsskyddsåtgärder, för att stå rustade”.

– Säkerhets-/beredskapschef, konsultverksamhet

”Omvärlden förändras i snabb takt, det är svårt att hinna med i omställningsarbetet.”

– it-chef, kommun

Källa: Kantar
Bas: Beslutsfattare (200)

Fyra tydliga förbättringsområden för att bli mer organiserade gällande verksamhetsskydd

Ökade resurser

Genom att våga satsa mer resurser på säkerhetsarbetet stärks verksamheters skydd inifrån och kan således förebygga de förödande konsekvenser som följer av bland annat cyberattacker.

De investeringar en organisation tar nu minskar risken för betydligt större kostnader i ett senare skede.

Mer kompetens

Öka kompetensen och förståelsen för vikten av verksamhetsskydd i hela organisationen.

Genom att få ut säkerhetstänket i organisationens alla led kan samtliga medarbetare hjälpa till att upptäcka samt förebygga hot.

Tydlig ansvarsfördelning

Ett tydligt ägarskap över säkerhetsfrågorna förebygger att de hamnar mellan stolarna. Det säkerställer även att frågorna sätts på agendan och ökar möjligheten för dem att hamna högre upp på dagordningen.

Med andra ord lägger det en bra grund för att arbeta med frågorna på ett mer systematiskt sätt genom hela organisationen.

Systematiskt arbete

Det är viktigt att implementera ett systematiskt arbetssätt för att bli mer organiserade.

Med hjälp av tydliga riktlinjer, uppföljning och styrning så förblir inte beredskapsövningar och krisplaner enbart en strategi på papper utan de kan även verkställas på ett tryggt sätt.

Framgångsfaktorer för att vara organiserade gällande verksamhetsskydd /säkerhetsskydd

”Säkerhetsorganisationen ligger direkt under ledningsgruppen”

– Säkerhets-/beredskapschef, transportmedelsindustrin

”Hög kompetens, tydliga processer. Framtagna styrstöddokument. Ett säkerhetsteam omhändertagande av informationssäkerhet, fysisk och personalsäkerhet”

- Säkerhets-/beredskapschef, konsultverksamhet

”Samarbete, tydligt ägarskap i olika frågor”

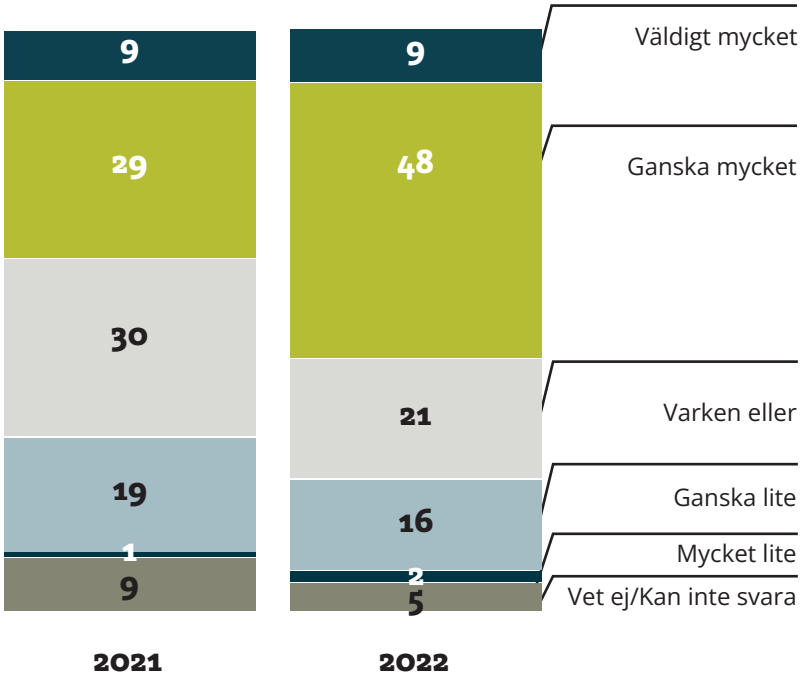
- Säkerhets-/beredskapschef, finanssektor

”Utbildning vad gäller säkerhetsskydd, personal och medarbetare”

- Verksamhetschef, media

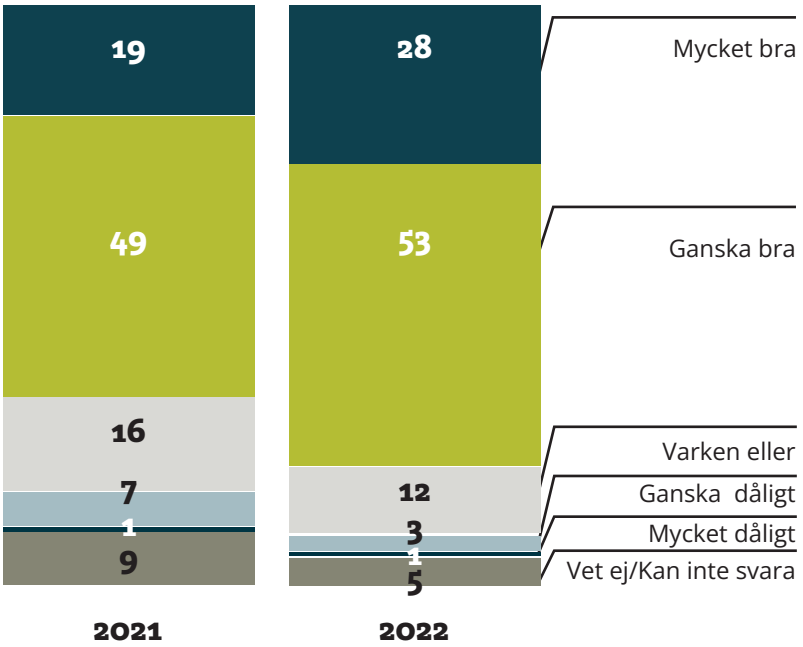
Hur mycket kompetens man upplever att verksamheten har gällande verksamhetsskydd/säkerhetsskydd

Källa: Kantar
Bas: Beslutsfattare (200)



Hur organiserad man upplever att verksamheten är gällande verksamhetsskydd/säkerhetsskydd

Källa: Kantar
Bas: Beslutsfattare (200)



Experternas tankar om insikterna från Svenskt Säkerhetsindex® 2023

Vi hoppas att du har fått mycket nyttig information om både det allvarliga och det hoppfulla som vårt samhälle och vi som organisationer står inför.

På kommande sidor får du ta del av reflektioner om insikterna från tre av våra experter.

Att omsätta ord i handling

Det är tydligt i årets version av Svenskt Säkerhetsindex® att medvetenheten är stor kring allvaret i hoten mot vår information och våra informationssystem. Tillsammans med kunskapen följer också viljan att åtgärda bristerna men ändå fortsätter incidenter med allvarliga följder att rapporteras i massmedia. För att minska och hantera dessa incidenter mer effektivt behövs ett annat engagemang i säkerhetsarbetet.

Vilka som är ansvariga för säkerheten kan definieras på flera olika sätt: ledningen är alltid ytterst ansvarig, en säkerhetschef med sin stab har ett uttalat ansvar att skydda organisationen och har varje medarbetare ansvar för säkerheten i sitt arbete. Men det finns en grupp som normalt förbises, till dess en incident inträffar. Den grupp som vi alltför ofta missar är de funktionsansvariga, ibland kallade produktägare, systemägare, avdelningschef eller motsvarande. Det finns uttalade krav och löpande uppföljning för tex ekonomi, personal och leverans men finns motsvarande krav och uppföljning på detaljerad nivå för säkerhet? Utredningen och ansvaret är minst lika omfattande för säkerhetsincident som för en missad budget, trots de olika förutsättningarna.

Den som anställer personal har ett ansvar att sätta rätt lön, att anlita personer med rätt kompetens och rätt vilja. Men anställningen innebär också att ge mandat att verka och hantera information i organisationen under lång tid på olika nivåer. Därför är det tankeväckande att bara 28% av de tillfrågade beslutsfattarna anser hotbilden som allvarlig sedd till personalsäkerhet (s 23 figur:1:2).

Det är viktigt att anställningen föregås av en utredning som i tillräcklig mån säkerställer att personen är trovärdig och lojal. Oavsett om anställningen avser en tjänst inom en klädesbutik, en fordonstillverkare eller försvaret kommer den anställde i kontakt med känslig information. Och innan anställningskontraktet signeras måste den chefen kunna veta med tillräcklig säkerhet att personen är trovärdig och lojal.

Slutligen har den som ansvarar för ett område också informationssäkerhet inom ansvaret. Ansvar för säkerhet följer två viktiga fundament; den som har kunskap har säkerhetsansvar, och den som har mandat har säkerhets-ansvar. Därför blir den som är utsedd som ansvarig för ett område med automatik också ansvarig för säker-heten inom det området och ska följas upp för säkerheten.

Genom att arbeta aktivt med säkerhet hos funktionsansvariga, ställa krav, stötta och följa upp, på samma sätt som vi gör med finans och personal kan vi höja det faktiska skyddet i företaget. Och vi uppnår det som inom systemutveckling kallas ”security by design”, alltså att säkerheten är en del av det dagliga arbetet och inte ett sidospår.

Det är dags att vi omsätter ord i handling och tillämpar säkerheten i det dagliga arbetet, där den gör verklig skillnad.

Jana Thorén
Konsultgruppchef, Basalt

Vad kan hända om man har fel person på insidan?

En person som inte är pålitlig ur säkerhetssynpunkt kan ställa till stor skada för en verksamhet. Det kan t.ex. handla om uppsåtligt röjande av skyddsvärd information, i värsta fall sådan som kan skada Sveriges säkerhet.

I Sverige har under senare tid två allvarliga fall av spioneri upptäckts. Båda fallen handlade om uppgiftslämnande till den ryska underrättelsetjänsten GRU. Bedömningen är att de upptäckta fallen bara är ”toppen på ett isberg” och att underrättelseinhämtningen mot Sverige är omfattande.

Vanligaste orsaken till att skyddsvärda uppgifter röjs är dock slarv och okunskap. Mot denna bakgrund är det viktigt att personalen får utbildning i säkerhetsskydd, bl.a. hur skyddsvärd information ska hanteras. Utbildning av personalen utgör en del av personalsäkerheten enligt säkerhetsskyddslagen (2018:585).

En händelse som innebär att skyddsvärd information röjs, oavsett om det är ett uppsåtligt eller oaktsamt röjande, riskerar att skada förtroendet för verksamheten. En hög nivå på säkerheten – även personalsäkerhet – är därför av strategisk betydelse för en verksamhet.

Den som genom en anställning eller på något annat sätt ska delta i säkerhetskänslig verksamhet ska säkerhetsprövas enligt säkerhetsskyddslagen. Det är även lämpligt att låta personer som ska delta i verksamhet med höga skyddsvärden i övrigt, genomgå en säkerhetsprövning som en verksamhetsskyddsåtgärd. En sådan säkerhetsprövning kan dock inte omfatta en registerkontroll eller särskild personutredning men har ändå ett stort värde och innebär att risken att få in fel personer i verksamheten minskar.

Det finns i det aktuella samhällspolitiska läget skäl att ta personalsäkerheten på allvar!

Yvette Glantz
Jurist och säkerhetsskyddskonsult, Basalt

Säkerhet börjar i ledningen

Säkerhets- och säkerhetsskyddschefens roll i samhället blir allt synligare och rollen förändras mycket snabbt. En generell omvärldsförändring och en stark teknikutveckling innebär nya utmaningar och angreppsvektorer, som tillsammans med förändringar i lagar och förordningar påverkar arbetet ytterst påtagligt.

Morgondagens säkerhets- och säkerhetsskyddschef kräver ett brett spektrum av kompetenser och samarbetsytor. Att på djupet förstå verksamheten och samtidigt kunna se helheten är en av de allra viktigaste aspekterna för dagens och morgondagens säkerhets- och säkerhetsskyddschef.

Förutom säkerhets- och säkerhetsskyddsfrågor krävs ett allt starkare fokus på affärsmannaskap samt ett systematiskt arbete med risk management och kontinuitetshantering. Vidare ställer rollen krav på strategisk planering, analys, metodutveckling, förändringsledning, förankringsarbete och kommunikation.

För att möta den inre och yttre hotbilden behöver en modern säkerhetsorganisation vara förutseende och proaktiv inom samtliga ämnesområden och discipliner. Dessutom krävs en stark integration med specialister inom personalsäkerhet, fysisk säkerhet, informationssäkerhet, it-säkerhet, operativt it-arbete och inte minst en stark förankring i det dagliga arbetet. Olika interna och externa nätverk bidrar också till en väl avvägd beslutsfattning samtidigt som det bidrar till att öka kompetensen.

Komplext? Absolut, men ett gott säkerhetsarbete gör att verksamheten fungerar samt att nya affärsmöjligheter skapas.

Ron Egly
Säkerhetsskyddschef, Basalt

Så gjordes kartläggningen

Kartläggningen har gjorts av Basalt i samarbete med Kantar* och baseras på telefonintervjuer som genomfördes i oktober och november 2022. 200 beslutsfattare inom samhällsviktig verksamhet deltog i undersökningen. Personerna som deltog i undersökningen sitter i verksamhetens ledningsgrupp och/eller ansvarar för eller påverkar beslut kring IT och/eller säkerhetsfrågor.

Under samma tidsperiod genomfördes mot allmänheten en webbundersökning i Sifos panel. Där deltog 1000 personer från ett riksrepresentativt urval.

*) Kantar är världens ledande data-, insikts- och konsultföretag som tillhandahåller insikter och rådgivning till kunder över hela världen. Kantar har över 25 000 anställda verksamma på 90 marknader.

Beslutsfattare

Antal intervjuer	200
Tidsperiod för datainsamlingen	21 Oktober - 14 November 2022
Metod	Telefonintervjuer

Allmänheten

Antal intervjuer	1000
Tidsperiod för datainsamlingen	17 Oktober - 25 November 2022
Metod	Online i Kantar Sifos webbpanel

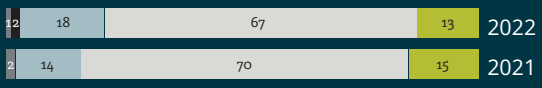
Appendix

Figur:1

Upplevd hotbild mot olika delar av verksamheten (%)

Vet ej/Vill inte svara | Inte alls allvarlig | Inte särskilt allvarlig | Ganska allvarlig | Mycket allvarlig

1:1 Upplevd hotbild mot informationssäkerhet



1:2 Upplevd hotbild mot personalsäkerhet

1:3 Upplevd hotbild mot fysisk säkerhet

Fråga: Hur bedömer du den nuvarande hotbilden kopplat till... informationssäkerhet/personalsäkerhet/fysisk säkerhet?
*Top Box: mycket allvarlig + Ganska allvarlig
**Low Box inte särskilt allvarlig + Inte alls allvarlig

Figur:2

Hur har statusen för säkerhetsarbetet i din verksamhet förändrats?

Vet ej | Den har minskat | Den har förändrats | Den har ökat

Figur:3

Hur har er säkerhetsbudget sett ut under de senaste tre åren?

Vet ej | Den har minskat | Den har förändrats | Den har ökat

Figur:4

Hur kommer er säkerhetsbudget att förändras under det kommande året?

Vet ej | Den kommer att minska | Den kommer att förändras | Den kommer att öka

Andel %

Källa: Kantar
Bas: Beslutsfattare (200)

BASALT
EN DEL AV OMEGAPOINT

Om Basalt

Basalt är ett av Sveriges ledande säkerhetsföretag. Vi hjälper företag, myndigheter och kommuner att skydda sin mest värdefulla information och kritiska verksamhet mot inre och yttre hot.

Vi skyddar din verksamhet genom att skapa ett systematiskt säkerhetsarbete, leverera nyckelfärdiga it-lösningar samt erbjuda seniora konsulttjänster med djup kompetens inom verksamhetsskydd och säkerhetsskydd.

Tillsammans skapar vi en säker värld där du, dina medarbetare, dina kunder och dina kunders kunder känner sig trygga.

I samarbete med

KANTAR