Dold brottslighet

– så drabbas tjänstesektorn av den rådande brottsligheten

Rapporten belyser hur tjänstesektorn drabbas av den rådande brottsligheten och bidrar med rekommendationer kring hur företagens brottsutsatthet kan motverkas.

Förord

Brottsligheten fortsätter att öka i Sverige. Det gäller såväl den grova organiserade kriminaliteten som de så kallade mängdbrotten, så som bedrägeri och skadegörelse. Parallellt med denna utveckling har även brottsligheten ändrat karaktär till att bli alltmer digitaliserad och gränsöverskridande, vilket utmanar vår traditionella brottshantering som utgått från att kriminaliteten är lokal och geografiskt begränsad.

Att konsekvenserna av den rådande brottsligheten är omfattande och allvarliga framgår inte minst genom den årliga nationella trygghetsundersökningen som för 2023 visar att hela 53 procent av befolkningen känner oro över brottsligheten samtidigt som förtroendet för polisen minskar. Resultatet understryker därmed det brådskande behovet att bryta brottslighetens utveckling för att motverka dess skadliga följdverkningar.

En särskilt utsatt grupp för denna brottslighet är näringslivet. Det är dock en målgrupp vars utsatthet inte framgår i den officiella statistiken, vilket innebär att den inte heller syns i beslutsunderlagen för det brottsbekämpande arbetet på nationell, regional och lokal nivå. I den officiella bilden över brottslighetens utveckling är därmed tjänsteföretagen en fortsatt dold målgrupp som riskerar att hamna i skymundan för prioriterade åtgärder.

Almega, som representerar cirka 12 000 företag i ett 60-tal branscher inom den privata tjänstesektorn, vill därför bidra till att belysa problembilden genom att redogöra för hur specifikt tjänstesektorn drabbas av brottsligheten.

Relevanta och effektiva åtgärder kräver att bilden av brottsligheten är heltäckande annars riskerar inte heller brottsbekämpningen bli det. Med denna rapport, som är den första i sitt slag som fokuserar på tjänstesektorns brottsutsatthet, bidrar vi just till den bilden och identifierar de åtgärder som vi ser motverkar den brottslighet som drabbar tjänsteföretagen.

Rapporten är författad av Moa Tivell, näringspolitisk expert på Almega.

Stockholm, maj 2024

Fredrik Östbom, näringspolitisk chef Almega

Innehåll

Sammanfattning och slutsatser

Den ökade brottsligheten fortsätter att vara en högprioriterad politisk fråga. De allvarliga konsekvenserna från den grova organiserade kriminaliteten har skapat en intensiv samhällsdebatt med krav på handlingskraft.

I skymundan av denna utveckling riskerar övrig brottslighet och till viss del det brottsförebyggande arbetet hamna. Det gäller även en hårt brottsdrabbad målgrupp vars utsatthet inte redovisas särskilt för i den officiella statistiken. Nämligen näringslivet.

Denna rapport syftar därför till att belysa problembilden kring hur tjänstesektorn drabbas av den rådande brottsligheten, som ett bidrag till den samlade bilden av svenska företags brottsutsatthet. Att denna problembild blir ordentligt belyst är viktigt för att relevanta och effektiva åtgärder ska kunna identifieras.

Rapporten är baserad på en digital enkät som genomfördes bland Svenskt Näringslivs medlemmar under 2023 för att undersöka företagens utsatthet för brott under de senaste tolv månaderna. De inkomna svaren har därefter brutits ner per näringslivssektor, vilket för den privata tjänstesektorn inneburit svar från1 205 företag. Detta motsvarar en svarsfrekvens på 36 procent.

Resultatet från undersökningen visar att 45 procent av tjänsteföretagen har utsatts för brott under det senaste året. Det innebär att nästan hälften av företagen uppger att de drabbats av något eller några av de olika brottstyperna, antingen en eller upprepade gånger. Den sammantagna bilden som framkommer från undersökningen är därmed att tillsammans med övriga näringslivet är tjänsteföretagen en utsatt målgrupp för den rådande brottsligheten. En brottslighet som med all tydlighet ökar i omfattning och komplexitet, vilket leder fram till slutsatsen att näringslivets utsatthet riskerar öka om inte brottsutvecklingen bryts.

Det vanligaste brottet tjänsteföretag utsätts för är skadegörelse (31 %), följt av cyberbrott och inbrott som drabbar företagen i lika hög utsträckning (24 %). Resultatet visar på betydande risker för företag i form av materiella skador, intrång i egendom och digitala hot. Nästan vart fjärde företag svarar att de utsatts för stöld (ej snatteri), medan aningen färre drabbats av bedrägeri. Med anledning av den kraftigt ökade brottsligheten av just bedrägerier görs en särskild djupdykning inom just denna brottskategori där resultatet visar att tjänsteföretagen främst drabbas av fakturabedrägerier följt av phishing som innebär att någon på företaget har fått ett mejl eller sms där man uppmanats att klicka på en falsk länk.

På grund av näringslivets ökade digitalisering och den snabba teknikutvecklingen belyses särskilt hur cyberbrottsligheten drabbar tjänstesektorn. Resultaten visar att vart fjärde tjänsteföretag drabbats av cyberbrott, men precis som för bedrägerier, visar svaren endast fullbordade brott och därmed framgår inte de cyberattacker som lyckats avvärjas. Om även detta redovisats hade andelen utsatta företag uppenbarligen varit högre. Den bilden stärks från flera andra studier.

Sammantaget bidrar resultatet gällande bedrägerier och cyberbrottslighet med att förtydliga hur brottsligheten blir alltmer digitaliserad och komplex, vilket även genererar allt högre brottsvinster. Detta styrks genom bilden av att trots att andelen företag som utsatts för cyberbrott inte förändrats i relation till föregående år så har kostnaden för denna brottslighet trefaldigats. Detta är en anmärkningsvärd ökningstakt som just tillskrivs bedrägerier som sker online eller via andra nätbaserade plattformar.

Ökningen av den digitaliserade brottsligheten är oroväckande, inte minst med tanke på den fortsatt snabba teknikutveckling inom artificiell intelligens (AI) som medför utvidgade möjligheter till exempelvis förfalskning och manipulation. Lika viktigt som att fortsätta arbetet med att stärka näringslivets cybersäkerhet, blir därmed att utveckla Polismyndighetens förmåga att hantera den växande digitala brottsligheten.

För att kunna motverka företagens brottsutsatthet spelar anmälningsbenägenheten en viktig roll. I undersökningen framgår att nästan fyra av tio brottsutsatta tjänsteföretag väljer att inte polisanmäla. Resultatet ligger på samma nivåer som för näringslivet i sin helhet och stärker bilden av att en stor del av den brottslighet som drabbar företag just inte kommer till polisens kännedom. Den främsta anledningen till att tjänsteföretagen inte polisanmäler handlar om att man anser att det inte leder till någon åtgärd eller till några positiva konsekvenser och en förbättrad situation för företaget.

Inte bara utsatthet för brott utan även en upplevd oro för att drabbas kan i sin tur få negativa konsekvenser. I denna undersökning har tjänsteföretagen fått besvara tre frågor om hur oro eller utsatthet för brott påverkat verksamheten. Totalt svarar sex procent att man avstått från att göra investeringar i verksamheten på grund av oro eller utsatthet för brott. Av samma anledning svarar fyra procent att det uppstått svårigheter att rekrytera personal och tre procent att man till och med övervägt att lägga ned delar av eller hela företagets verksamhet.

Rapporten avslutas med ett kapitel med reflektioner och rekommendationer till beslutsfattare i syfte att bidra till arbetet med att motverka brottsligheten som drabbar företag. För Sverige är det en uppenbar förlust när företag behöver investera och lägga tid på säkerhetslösningar i stället för att fokusera på verksamhetsutveckling och ytterligare tillväxt. Detta understryker vikten av att företagens brottsutsatthet blir ordentligt belyst och att relevanta åtgärder kommer på plats.

Almegas rekommendationer är:

1. **Säkerställ brottsförebyggande samverkan med näringslivet**

Säkerställ att det identifierade behovet av brottsförebyggande samverkan med näringslivet realiseras i praktiken av kommuner och relevanta myndigheter.

2. **Redovisa officiell statistik över företagens brottsutsatthet**

Utveckla officiell statistik genom att ta fram nya brottskoder samt en nationell trygghetsundersökning bland företag som fångar upp mörkertalet.

3. **Prioritera mängdbrotten och samordna den digitala brottsbekämpningen**

Prioritera mängdbrotten genom stärkt kapacitet i lokalpolisområdena och hantera den alltmer digitaliserade brottsligheten genom samordnad polisiär förmåga.

4. **Utveckla digital polisanmälan**

Öka företagens låga anmälningsbenägenhet genom att utveckla möjligheten till digital polisanmälan.

5. **Inför ett trygghetsavdrag**

Kompensera företagen för omfattande investeringar i egna säkerhetslösningar för att förebygga och skydda sig mot brott och ordningsstörningar.

Resultat

I denna del redovisas resultatet gällande andelen tjänsteföretag som utsatts för brott under de senaste tolv månaderna.[1] Vidare redovisas vilken typ av brott företagen drabbats av, följt av en fördjupning inom bedrägerier med anledning av den kraftigt ökande brottsligheten inom just denna brottskategori. Därefter redovisas dels företagens benägenhet att polisanmäla, dels några av de ytterligare konsekvenser som brottsligheten medför för de brottsutsatta företagen.

Tjänstesektorns utsatthet för brott

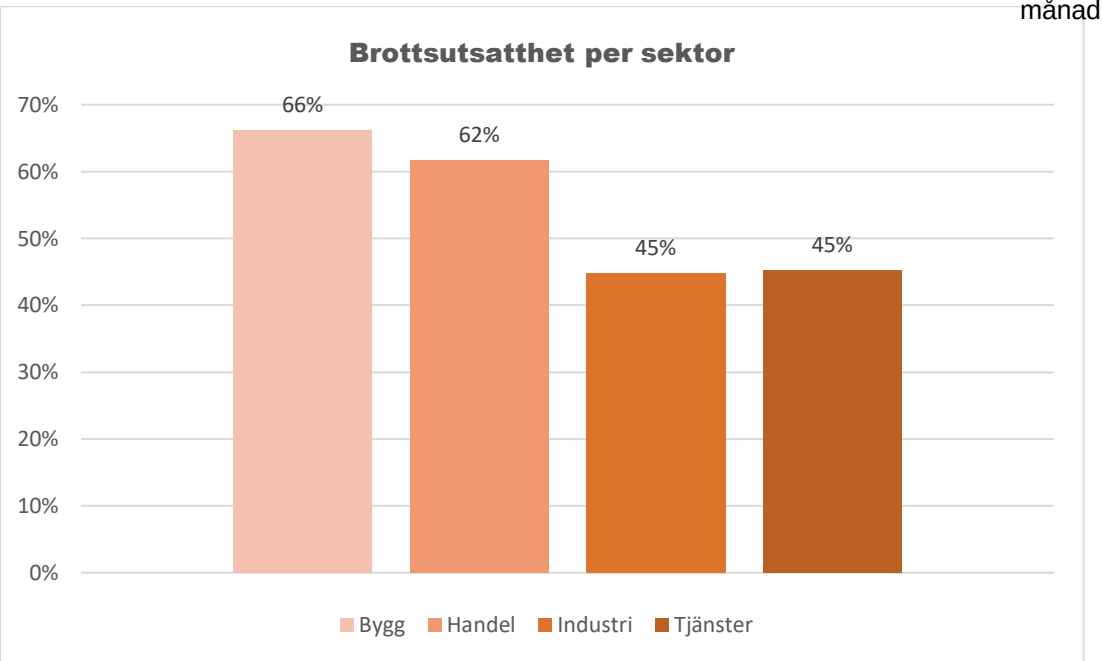
Resultatet från undersökningen visar att 45 procent av tjänsteföretagen har utsatts för brott under det senaste året. Det innebär att nästan hälften av företagen uppger att de drabbats av något eller några av de olika brottstyperna, en eller upprepade gånger. Detta resultat ger alltså en samlad bild av andelen företag som drabbas vilket belyser företagens utsatthet och brottslighetens utbredning.

För att förstå tjänstesektorns utsatthet i förhållande till övriga näringslivet framgår även övriga sektorer i diagram 1. Från resultatet går att utläsa att tjänstesektorn och industrin är relativt förskonade jämfört med bygg- och handelssektorn vars företag är brottsutsatta i högre utsträckning.[2]

45%

Av tjänsteföretagen har utsatts för brott under de senaste 12 månaderna.

Diagram 1. Andelen företag i respektive sektor som anger att de utsatts för brott, en eller flera gånger, under de senaste tolv månaderna



Källa: Svenskt Näringsliv

På grund av att inga tidigare jämförbara undersökningar genomförts som fokuserat på specifikt tjänsteföretagens brottsutsatthet saknas möjlighet att

[1] Undersökningen genomfördes 2023 och frågor ställdes om företagens utsatthet för brott under de senaste tolv månaderna.
[2] Dessa fyra sektorer representerar samtliga företag som ingick i Svenskt Näringslivs undersökning.

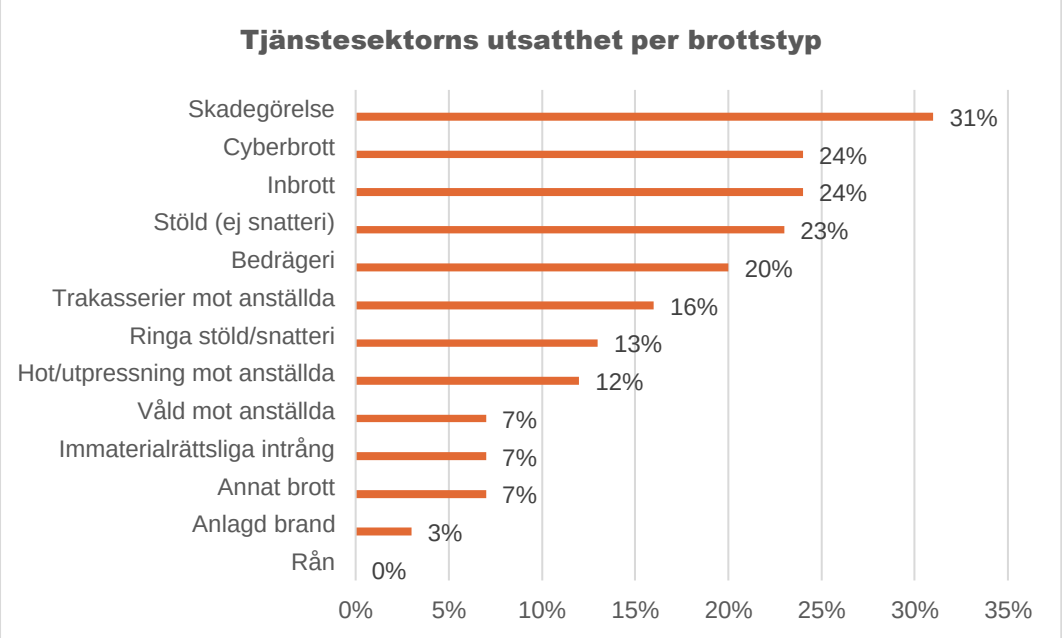
beskriva hur denna brottslighet utvecklats över tid. Dock finns en snarlik enkätundersökning från 2022 som genomfördes av Svenskt Näringsliv där tjänsteföretag tillfrågades om de utsatts för brott under en kortare tidsperiod jämfört med denna undersökning.[3] Trots att studien inte är helt jämförbar indikerar svaren att ingen stor förändring skett gällande andelen företag inom tjänstesektorn som utsätts för brott.[4] Siffrorna fångar dock inte upp brottslighetens allvarlighetsgrad eller antalet gånger företagen drabbats.

Den sammantagna bilden som framkommer från undersökningen är att brottsligheten som drabbar tjänstesektorn är utbredd. Att nästan hälften av företagen utsatts för brott under det senaste året påvisar att kriminaliteten påverkar förutsättningarna att bedriva företag i Sverige.

Tjänstesektorns utsatthet per brottstyp

De företag som angett att de utsatts för brott har fått ange vilken typ av brott de drabbats av. Det vanligaste brottet tjänsteföretag utsätts för är skadegörelse, följt av inbrott och cyberbrott som drabbar företagen i lika hög utsträckning. Resultatet visar på betydande risker för företag i form av materiella skador, intrång i egendom och digitala hot. Av de brottsutsatta företagen svarar nästan vart fjärde att de utsatts för stöld (ej snatteri), medan aningen färre drabbats av bedrägeri. Värt att notera är att grafen nedan (diagram 2) endast redogör för fullbordade bedrägerier och inte bedrägeriförsök. I följande kapitel görs en djupdykning i företagens utsatthet för olika typer av bedrägerier och bedrägeriförsök.

Diagram 2. Andelen tjänsteföretag som utsatts för olika typer av brott, en eller flera gånger, under de senaste tolv månaderna



Källa: Svenskt Näringsliv

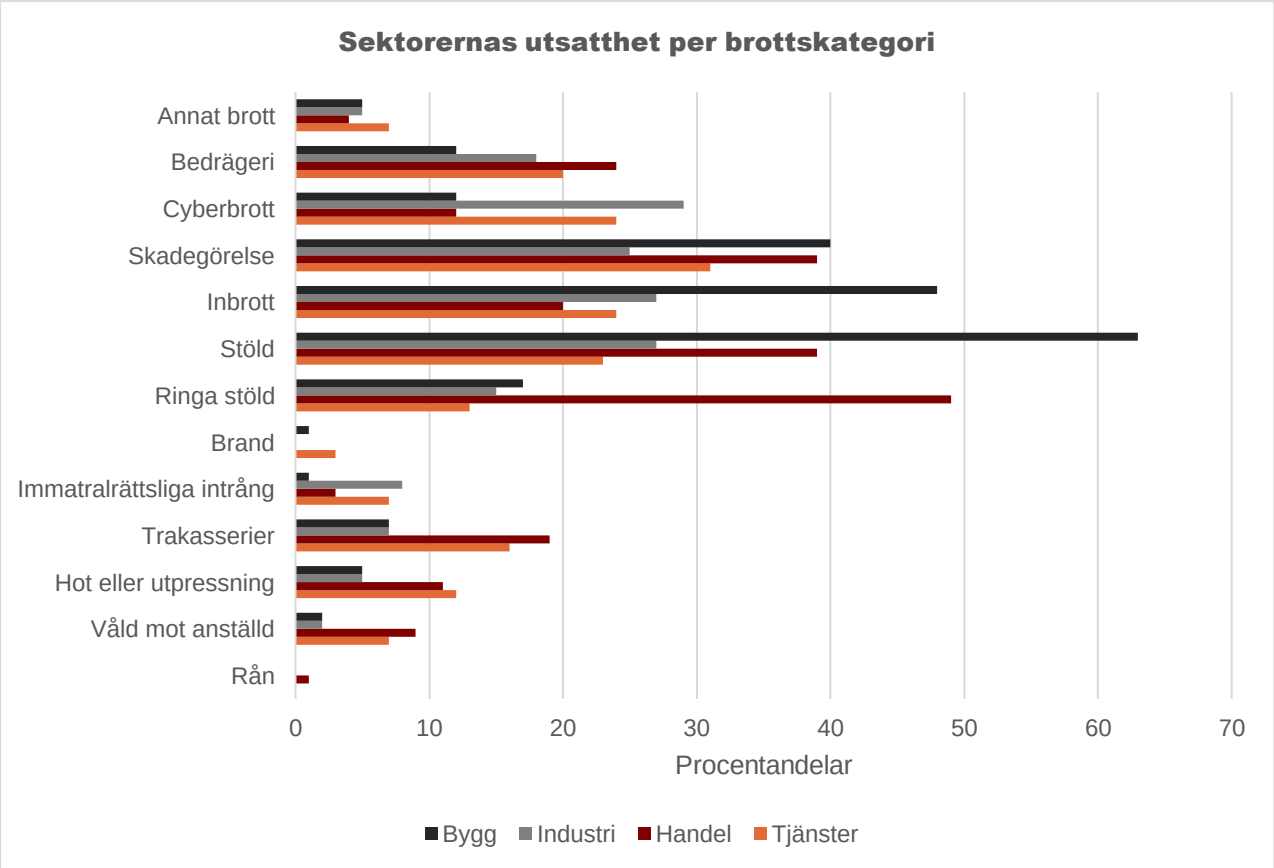
[3] Tidsperioden gällde de senaste 6 månaderna, jämfört med de 12 månader som varit aktuellt för undersökningen som ligger till grund för denna rapport.
[4] 41% av tjänsteföretagen svarade att de hade utsatts för brott under de senaste 6 månaderna.

Vidare framgår att brott som hot/utpressning mot anställda, trakasserier mot anställda och våld mot anställda förekommer, om än i mindre utsträckning, vilket är att betrakta som positivt med tanke på tjänstesektorns höga personaltäthet.

Sju procent av de brottsutsatta företagen anger att de drabbats av immaterialrättsliga intrång. Denna typ av brottslighet omfattar ett brett spektrum av handlingar som bryter mot upphovsrätt, varumärkesintrång och patentintrång, vilka ofta genomförs via digitala metoder. Den immaterialrättsliga brottslighet kan därmed betraktas som en del av den växande cyberbrottsligheten och utvecklas med teknikens framsteg.

Diagram 3 visar tjänstesektorns utsatthet per brottstyp i förhållande till övriga delar av näringslivet. Från resultatet går att utläsa att tjänstesektorn är jämförelsevis förskonade vad gäller viss typ av brottslighet. Detta gäller även den brottstyp som drabbar tjänsteföretagen värst, nämligen skadegörelse, där både bygg- och handelssektorn drabbas hårdare. Liknade resultat går att se vad gäller exempelvis stöld där övriga tre sektorer och framför allt byggsektorn utsätts värre.

Diagram 3. Andelen brottsutsatta företag inom respektive sektor, fördelat på brottskategori



Källa: Svenskt Näringsliv

Det finns ingen brottstyp där tjänstesektorn enskilt sticker ut som särskilt drabbad i förhållande till övriga näringslivet. I diagram 3 framgår dock att anställda inom både handeln och tjänster utsätts för trakasserier, hot och fysiskt våld i högre

grad än inom bygg och industrin, men i det stora hela går det att konstatera att denna typ av brottslighet inte drabbar företagen lika hårt som exempelvis tillgrepps- och skadegörelsebrotten.

Tjänstesektorns utsatthet för cyberbrottslighet

Näringslivets ökade digitalisering och den fortsatt snabba teknikutvecklingen gör det särskilt intressant att titta närmare på hur cyberbrottsligheten drabbar tjänstesektorn. Resultaten visar att denna brottslighet drabbar både industri- och tjänstesektor hårdare än bygg och handel. Totalt anger 24 procent av de brottsutsatta tjänsteföretagen att de drabbats av cyberbrott vilket innebär att detta, tillsammans med inbrott, är den näst vanligaste brottstypen som drabbar tjänsteföretag idag. Precis som för bedrägerier, visar dock resultatet gällande cyberbrott, fullbordade brott och därmed framgår inte de cyberattacker som lyckats avvärjas. Om även detta redovisats hade andelen utsatta företag uppenbarligen varit högre.

Bilden av tjänsteföretagens utsatthet för cyberbrott stärks från flera andra studier, däribland Almegas undersökning om företagens cybersäkerhet som visade att uppemot 20 procent av tjänsteföretagen varit utsatta för cyberattacker.[5] Så även av Svenskt Näringslivs rapport från slutet av 2023 som visar att hela 28 procent av de tillfrågade företagen drabbats av cyberattacker de senaste 12 månaderna.[6] Här är det dock på sin plats att betona att det än så länge inte finns någon vedertagen definition av begreppet cyberbrottslighet, vilket innebär att det i vissa fall även kan inkludera det som kallas för cyberbaserade bedrägerier.[7] Detta medför att det även i denna rapport kan finnas en viss felmarginal vid redovisningen av andelen företag som drabbas av cyberbrott respektive bedrägerier eftersom dessa begrepp används om vartannat.

Sammantaget bidrar resultatet gällande bedrägerier och cyberbrottslighet till att förtydliga hur brottsligheten blir alltmer digitaliserad och komplex, vilket även genererar allt högre brottsvinster. Detta styrks av ny statistik som konstaterar att trots att andelen svenska företag som utsatts för cyberbrott inte förändrats i relation till föregående år, så har kostnaden för denna brottslighet trefaldigats. Detta är en anmärkningsvärd ökningstakt som just tillskrivs bedrägerier som sker online eller via andra nätbaserade plattformar.[8]

Den digitala brottslighetens skenande kostnader är i ljuset av den fortsatt snabba teknikutvecklingen därmed oroväckande. Inte minst sett till utvecklingen inom artificiell intelligens (AI) med exempelvis möjlighet att manipulera ljud och bild, så kallad deepfake, som öppnar upp för att skapa falskt innehåll som kan användas för bedrägeri, utpressning eller annan digital kriminalitet. Å andra sidan kan AI också användas för bättre möjligheter att öka säkerheten och till exempel upptäcka attacker, bedrägerier med mera.

Utifrån bilden av en alltmer kostsam och sofistikerad cyberbrottslighet blir därmed företagens förmåga att skydda sig allt viktigare. Detta kräver i sin tur både god kunskap om cybersäkerhet och finansiella investeringar i säkerhetslösningar,

[5] Tjänsteföretagen och stärkt cyberäkerhet i Sverige. Almega, 2022.
[6] Svenskt Näringsliv – cybersäkerhet företag. 2023.
[7] Stockholms handelskammare (2022). Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid? Stockholm: Stockholms handelskammare.
[8] Brottslighetens kostnader 2023. Svenskt Näringsliv.

vilket det idag råder brist på inom tjänstesektorn enligt Almegas egen undersökning från 2022. I den framgick att uppemot 40 procent av tjänsteföretagen inte har några budgeterade medel för cybersäkerhet och att det fanns en bristande beredskap för cyberangrepp. Det blev därtill tydligt att tjänsteföretagen efterfrågade en utvecklad samverkan, informationsdelning och kompetensutveckling med offentliga aktörer i syfte att stärka sin cybersäkerhet.[9]

I linje med dessa önskemål, har behovet av stärkt samverkan även uppmärksammats på flera olika håll. Bland annat genom Riksrevisionens granskning av regeringens arbete med att stärka informations- och cybersäkerheten i Sverige, där man konstaterade att arbetet saknat sammanhållen styrning samt att relevanta intressenter såsom näringslivet, inte involverats i någon större omfattning.[10] I linje med Riksrevisionens rekommendationer har därefter Nationellt cybersäkerhetscenter fått ett förtydligat uppdrag att stärka samverkan med näringslivet just inriktat på ökad informationsdelning och kunskapsspridning. Att detta uppdrag inte försenas ytterligare, så som varit fallet, är helt vitalt för att näringslivets sårbarhet inte ska riskera att öka. Utöver detta påbörjade arbete är det också viktigt att centret organiseras så att det kan närma sig företagen. I dag riktas stort fokus till arbetet som säkerhets- och underrättelsemyndigheter inom centret bidrar med. Med NIS2-lagstiftningen[11] och totalförsvarsarbetet behöver centret nå längre ut till verksamheterna, men också tillsyns-, sektors- och beredskapsmyndigheter.

Sammantaget är det positivt att initiativ och åtgärder utformats som besvarar tjänsteföretagens efterfrågan för att kunna stärka sin cybersäkerhet. Fortfarande kvarstår dock det faktum att förutom den alltmer avancerade cyberbrottsligheten utvecklas även mängdbrotten till att bli mer digitaliserade, varav bedrägerier är ett tydligt exempel på detta. Skiljelinjerna mellan det som tidigare sågs som cyberattacker och den övriga digitala brottsligheten suddas därmed alltmer ut när exempelvis skadlig programvara används vid utpressning, vilket betraktas som just bedrägeri. Lika viktigt som att fortsätta arbetet med att stärka näringslivets cybersäkerhet, blir därmed även att utveckla Polismyndighetens förmåga att hantera den växande digitala brottsligheten.

Cyberbrottslighetens utveckling mot en allt större spännvidd med allt från mer traditionell brottslighet så som bedrägerier och utpressning, till immaterialrättsliga intrång och cyberattacker pekar därtill på behovet av mer övergripande samordning i det brottsbekämpande och förebyggande arbetet.

Medan informations- och cybersäkerhet i hög utsträckning kan vara en marknadsledd verksamhet, så kan ett av de viktigaste bidragen från det offentliga vara att utöver kunskapsdelning och samordning även öka kompetensförsörjningen inom området.

Tjänsteföretagens utsatthet för bedrägerier

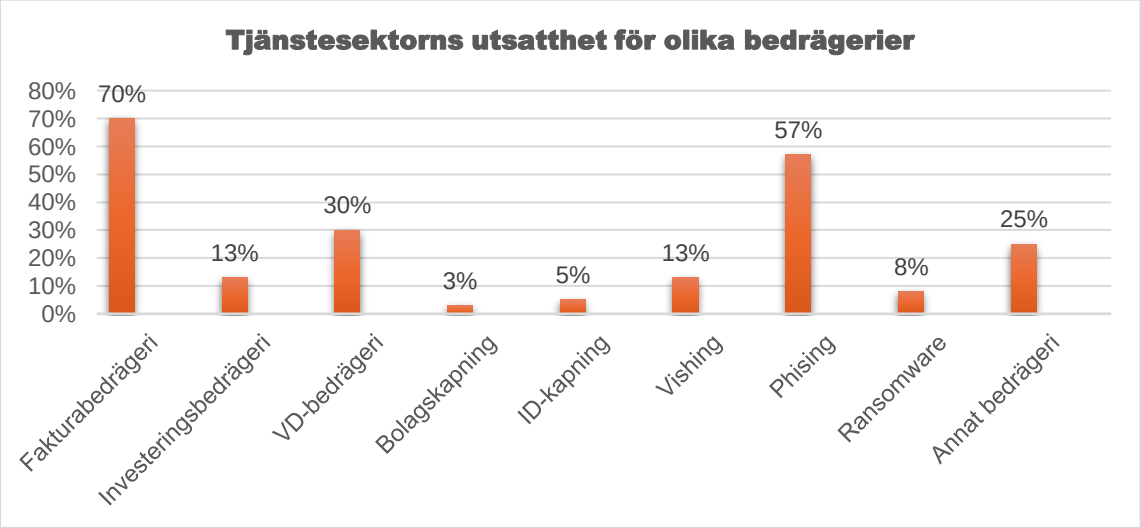
Enligt statistik från Brottsförebyggande rådet (Brå) ökade antalet anmälda bedrägeribrott i Sverige med 22 procent under 2023 jämfört med 2022. Denna ökning representerar den största uppgången bland alla brottskategorier under

[9] Tjänsteföretagen och stärkt cybersäkerhet i Sverige. Almega 2022.
[10] Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig, Riksrevisionen 2023. RiR 2023:8.
[11] NIS2-direktivet beslutades av EU den 14 december 2022. Direktivet syftar till att uppnå en hög gemensam cybersäkerhetsnivå och ställer tydligare krav på bland annat riskanalyser och olika säkerhetsåtgärder. Den 23 februari 2023 tillsatte regeringen en utredning som har till uppdrag att införa NIS2 i svensk lagstiftning. Utredningen har lämnat delbetänkandet SOU 2024:18 Nya regler om cybersäkerhet med förslag om hur NIS2-direktivet ska implementeras och föreslår att förslagen ska träda i kraft den 1 januari 2025.

året, men eftersom företag inte redovisas särskilt i den officiella statistiken går det inte att utläsa hur denna kraftigt ökade brottslighet drabbat tjänstesektorn.

Utifrån undersökningen som ligger till grund för denna rapport kan vi dock se att 20 procent av de brottsutsatta tjänsteföretagen drabbats av bedrägeri under de senaste tolv månaderna, vilket därmed är den fjärde vanligaste brottstyp som tjänstesektorn drabbas av. I diagram 4 framgår vilken typ av bedrägeri företagen utsatts för samt att vissa företag drabbats upprepade gånger under de senaste tolv månaderna. Därmed överskrider totalen mer än 100 procent.

Diagram4. Andelen bedrägeriutsatta företag, fördelat på bedrägerikategori



Källa: Svenskt Näringsliv

Fakturabedrägeri är den allra vanligaste formen av bedrägeri och har drabbat 70 procent av de bedrägeriutsatta tjänsteföretagen. Näst vanligast är phishing som innebär att någon på företaget har fått ett mejl eller sms där man uppmanats att klicka på en falsk länk och behövt ange uppgifter som lösenord eller bankuppgifter. Vd-kapning är den tredje vanligaste bedrägeriformen och innebär att någon utgett sig för att vara företagets vd och förmått anställda att överföra tillgångar. Därefter kommer så kallad vishing som 13 procent av de bedrägeriutsatta tjänsteföretagen drabbats av, vilket innebär att någon på företaget har fått ett telefonsamtal där man utgett sig för att vara en bank, affärspartner, myndighet och lurat till sig känslig information. Vad gäller ransomware, som drabbat 8 procent av de bedrägeriutsatta tjänsteföretagen, så innebär detta att datorer eller filer har krypterats av skadlig programvara och endast kunnat låsas upp mot betalning.

Sett över tid så finns ingen tidigare undersökning att jämföra med för att förstå utvecklingen av olika typer av bedrägeribrott som drabbar tjänstesektorn. Om jämförelsen i stället görs kring hur bedrägerier i sin helhet (ej nedbrutet per bedrägerityp) drabbar tjänsteföretag indikerar resultaten att ingen större förändring skett jämfört med tidigare år.[12] Andelen som drabbas ligger i paritet med föregående år.

Resultatet är dock svårtytt och rymmer en mer komplex problembild. Enligt Brås statistik så har bedrägeribrotten som tidigare nämnts ökat dramatiskt under 2000-

[12] Statistik från undersökningen Brottslighetens kostnader 2022. Svenskt Näringsliv. Undersökningen gäller en tidsperiod på 6 månader vilket innebär att den inte är jämförbar med undersökningen som denna rapport baserar sig på.

talet (med undantag för året 2020–2021).[13] Detta gäller det totala antalet anmälda bedrägeribrott och därmed inte de som drabbar specifikt företag eller tjänstesektorn. Statistiken som Brå sammanställer visar att de anmälda bedrägeribrotten ökat med 52 procent sedan 2012. Jämfört med 2006 har de anmälda bedrägeribrotten ökat med 270 procent.[14] Utifrån denna statistik kan vi inte veta hur näringslivet drabbats av de ökande bedrägeribrotten, men det går att anta att utvecklingen även påverkat företagen. Det här är en bild som stärks utifrån flera studier som visar på att konsekvenserna från bedrägerier blir allt allvarligare. Detta sett både till den ekonomiska förlusten för det enskilda företaget och för samhället i stort eftersom vinsten till stor del investeras i annan illegal verksamhet.[15]

Utifrån definitionerna av dessa bedrägeribrott är det lätt att förstå begreppsförvirringen gällande cyberbrott och bedrägerier. De flesta av tillvägagångssätten för att utföra bedrägerier inbegriper i dagsläget digitala metoder. Det gäller oavsett om det rör fakturor, vd-bedrägeri eller olika former av kapningar där alltmer av den kriminella aktiviteten flyttar ut i den digitala miljön. Detta anses också vara anledningen, så som tidigare nämnts, till den oproportionerligt höga kostnadsutvecklingen för cyberbrott.

Bedrägeribrottens utveckling framstår därtill alltmer problematisk i vetskap om att bedrägerier är starkt sammankopplat med grov och organiserad brottslighet. Här har Polismyndighetens nationella bedrägericentrum i två olika studier beskrivit en påtaglig relation mellan den organiserade brottsligheten och bedrägeribrotten. Bedrägerier beskrivs vara en förhållandevis riskfri kriminell aktivitet som utgör en av de mest vinstdrivande verksamheter som organiserade kriminella aktörer kan ägna sig åt. Nationellt bedrägericentrum förklarar detta delvis med att bedrägeribrotten blivit alltmer komplicerade att utreda, bland annat på grund av en ökad användning av digital teknik. Här konstateras att trots ökad komplexitet så visar intern analys att Polismyndighetens brottsbekämpande förmåga inom bedrägeriområdet inte har anpassats i tillräcklig omfattning till utvecklingen.[16]

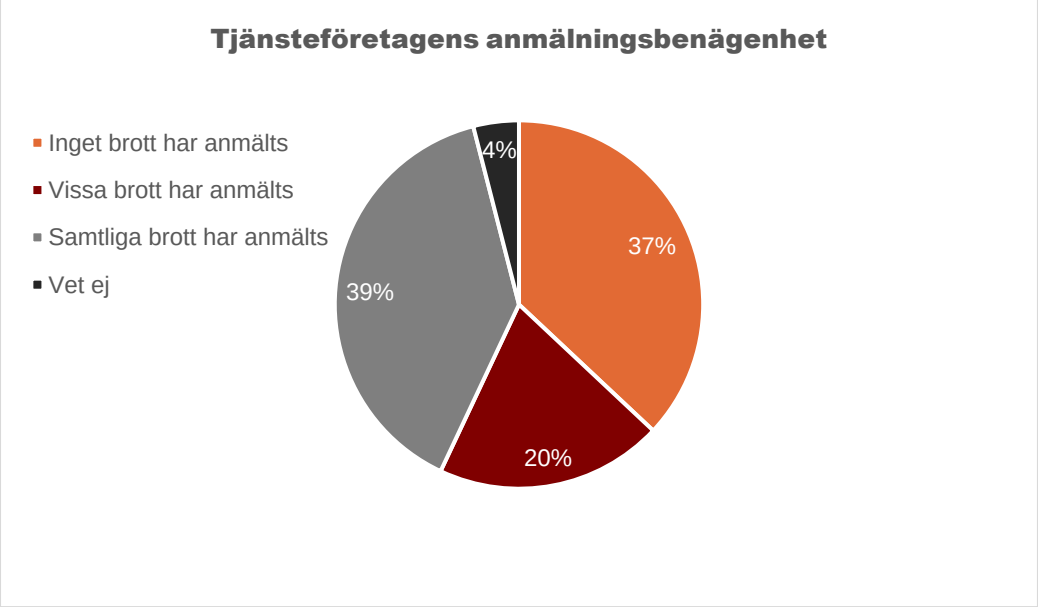
Tjänstesektorns anmälningsbenägenhet

Företagens anmälningsbenägenhet spelar en viktig roll för att polisen ska kunna prioritera och utveckla adekvata åtgärder inom det brottsbekämpande arbetet.

I undersökningen har därför tjänsteföretagen som angett att de utsatts för brott även tillfrågats i vilken utsträckning dessa brott har polisanmälts. I diagram 5 framgår att nästan fyra av tio brottsutsatta tjänsteföretag har valt att inte polisanmäla. En lika stor andel av företagen väljer att anmäla samtliga brott de utsatts för medan två av tio väljer att bara anmäla vissa brott. Resultatet ligger på samma nivåer som för näringslivet i sin helhet[17] och stärker bilden av att en stor del av den brottslighet som drabbar företag inte kommer till polisens kännedom.

Diagram 5. Andelen brottsutsatta tjänsteföretag som polisanmäler brott

[13] Enligt Brå minskade bedrägerier med cirka 10 % detta år. Främst minskade kortbedrägerierna, men vissa bedrägeriformer fortsatte att öka, däribland vishing.
[14] Brottsförebyggande rådet (2022)
[15] De organiserade bedrägerierna. 2021. De dödliga bedrägerierna 2022. Båda från Nationellt bedrägericentrum, Polismyndigheten.
[16] De dödliga bedrägerierna, Nationellt bedrägericentrum. 2022.
[17] Brottslighetens kostnader 2023. Svenskt Näringsliv.



Källa: Svenskt Näringsliv

Den främsta anledningen till att tjänsteföretagen inte polisanmäler är att man inte anser att det leder till någon åtgärd eller till en förbättrad situation för företaget. Den näst vanligaste orsaken till att tjänsteföretagen väljer att inte polisanmäla handlar om att händelsen inte upplevs tillräckligt allvarlig trots att det är ett brott. Detta svar öppnar dock upp för tolkningsutrymme och skulle kunna spegla att man vant sig vid en viss grad eller typ av brottslighet.

Brottslighetens ytterligare konsekvenser

Att brottsligheten äter sig in i samhället har blivit ett uttryck som förekommer allt oftare för att belysa brottslighetens omfattande konsekvenser. Inte bara utsatthet för brott utan även en upplevd oro för att drabbas kan påverka våra liv och de beslut vi fattar inför framtiden.

I denna undersökning har tjänsteföretagen fått besvara tre frågor om hur oro eller utsatthet för brott påverkat verksamheten. Totalt svarar sex procent att man avstått från att göra investeringar i verksamheten på grund av oro eller utsatthet för brott. Av samma anledning svarar fyra procent att det uppstått svårigheter att rekrytera personal och tre procent att man till och med övervägt att lägga ned delar av eller hela företagets verksamhet.

Trots att procentandelarna är låga så understryker statistiken att brottsligheten kan få stora konsekvenser och påverka viktiga framtidsbeslut. Att investeringsviljan hämmas och kompetent arbetskraft blir mer svårrekryterad innebär tillväxthinder och att företagens utvecklingspotential inte tillvaratas fullt ut. Att ett antal företag dessutom anser att brottsligheten påverkar deras verksamhet i sådan hög grad att de övervägt avveckling belyser just vilka allvarliga konsekvenser brottsligheten kan få i långa loppet.

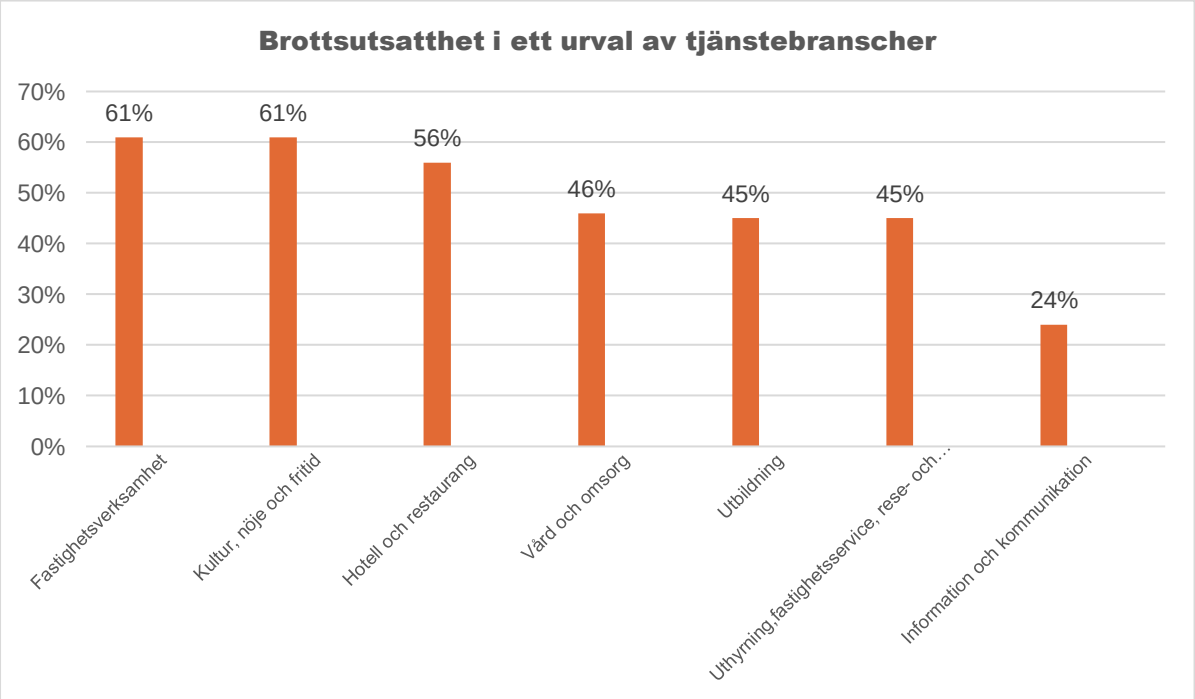
Sammantaget visar dock resultatet att i dagsläget så fortsätter tjänsteföretagen i hög utsträckning att bedriva sin verksamhet enligt plan utan att låta sig påverkas av den utbredda brottsligheten.

Läget i utvalda tjänstebranscher - kommentar utifrån tidigare studier

Denna rapport bygger på en undersökning som genererat svar från totalt 1 205 tjänsteföretag. Antalet svarande för respektive bransch inom tjänstesektorn är därmed i de flesta fall för få för att kunna analysera och jämföra hur olika delar av sektorn drabbas. Men utifrån två andra nyligen publicerade rapporter går det ändå att få en bild hur vissa branscher inom tjänstesektorn drabbas av brott.[18] I Svenskt Näringslivs nationella undersökning, som ligger till grund för rapporten Brottslighetens kostnader 2023, framgår att bland de tre värst drabbade branscherna tillhör två av dessa tjänstesektorn.

Inom både fastighetsverksamhet och kultur, nöje och fritid har drygt 60 procent av företagen utsatts för brott under det senaste året. Även hotell- och restaurangbranschen är hårt drabbat, där över hälften av företagen utsatts. I diagram 6 redovisas hur vissa utvalda tjänstebranscher drabbats under de senaste tolv månaderna enligt Svenskt Näringslivs undersökning. Inom exempelvis vård och omsorg, utbildning och inom stödtjänster i form av uthyrning, fastighetsservice och resetjänster utsätts företagen i lägre grad. Som minst drabbad av de utvalda branscherna sticker informations- och kommunikationsbranschen ut där ungefär vart fjärde företag utsatts för brott under det senaste året.

Diagram 6. Andelen brottsutsatta företag i ett urval av tjänstebranscher



Källa: Svenskt Näringsliv

[18] Brottslighetens kostnader 2023. Svenskt Näringsliv. Företagens trygghetsundersökning 2023, Stiftelsen tryggare Sverige.

I Stiftelsen Tryggare Sveriges undersökning bekräftas bilden i stort hur dessa branscher inom tjänstesektorn utsätts för brott. Fastighetsverksamhet samt hotell och restaurang framstår även här som ett par av de värst drabbade branscherna. Den enda märkbara skillnaden mellan de två undersökningarna gäller branschen kultur, nöje och fritid, som i Svenskt Näringslivs undersökning framstår som en av de värst drabbade, men som i Tryggare Sveriges rapport i stället är en av de minst utsatta branscherna.[19] En förklaring till detta anses vara skillnader i undersökningarnas metodik vilket innebär att undersökningarna inte är helt jämförbara. Slutsatserna kring brottsutsattheten i specifikt denna bransch blir därmed osäkra, vilket pekar på behov av ytterligare undersökningar.

Sammanfattningsvis går det att konstatera att brottsligheten drabbar tjänstesektorn brett, men att den slår olika hårt beroende på bransch. Likt tidigare år fortsätter fastighetsverksamheten vara särskilt hårt utsatt och drabbas mer än dubbelt så hårt som informations- och kommunikationsbranschen som är en av de minst drabbade. Sett till tjänstesektorns bredd, med branscher inom vitt skilda affärsverksamheter, är denna spännvidd inte särskilt uppseendeväckande.

Reflektioner och rekommendationer

Denna rapport är skriven för att lyfta fram och beskriva tjänstesektorns brottsutsatthet. Att uppemot hälften av tjänsteföretagen utsätts för brott på årlig basis pekar på brottslighetens utbreddhet. Utöver de enskilda kostnader och lidande som brottsligheten medför för det enskilda företaget får detta negativa konsekvenser för samhället som helhet.

För Sverige innebär det uppenbara förluster när företag behöver investera och lägga tid på egna säkerhetslösningar i stället för att fokusera på verksamhetsutveckling och ytterligare tillväxt. Detta understryker därmed vikten av att brottsligheten som drabbar företag behöver prioriteras i högre grad än i dag och att näringslivet betraktas som ett brottsoffer snarare än ett brottsverktyg. Utifrån detta perspektiv behöver företagen även ges stärkta förutsättningar att stå emot den alltmer problematiska arbetslivskriminaliteten, däribland genom möjligheten till bakgrundskontroller.

Inom arbetet för att motverka brottsligheten som drabbar företag anser Almega att flera relevanta åtgärder bör vidtas. I detta kapitel presenteras dessa åtgärder och sammanfattas i form av rekommendationer under respektive stycke.

Säkerställ utvecklad samverkan med näringslivet

De senaste åren har stort fokus riktats mot det brottsförebyggande arbetet. Sedan 2017 finns ett nationellt program som syftar till att skapa förutsättningar för ett strukturerat och långsiktigt brottsförebyggande arbete i hela samhället.[20] Måluppfyllelsen utvärderas årligen av Brå som i den senaste upplagan

[19] Företagens trygghetsundersökning 2023. Stiftelsen Tryggare Sverige.
[20] Tillsammans mot brott – ett nationellt brottsförebyggande program. Regeringens skrivelse 2016/17:126.

konstaterar att det finns potential att utveckla samverkan med externa aktörer, däribland näringslivet.[21] Även Polismyndigheten lyfter fram i sin brottsförebyggande strategi behovet av ett mer proaktivt förhållningssätt, där man i stället för att reagera och rycka ut, blir bättre på att agera innan ett brott sker eller upprepas. Inom detta arbete betonas särskilt betydelsen av samverkan med flertalet aktörer, däribland näringslivet.[22]

Även inom det nationella cybersäkerhetsarbetet har behovet av stärkt samverkan med näringslivet uppmärksammats. I april 2023 gav regeringen därför ett förtydligat uppdrag till Nationellt Cybersäkerhetscenter (NCSC) om att stärka samverkan genom att bland annat bidra med lägesbilder, kompetensutveckling och informationsdelning. Utifrån Almegas egna undersökningar går detta helt i linje med vad tjänsteföretagen efterfrågar för att stärka den egna informations- och cybersäkerheten. Dock har NCSC arbete försenats, men nu påbörjats vilket är ett steg i rätt riktning. I det måste det ligga att centret organiseras och får en huvudman som underlättar för informationsutbyte och skapar goda möjligheter att nå ut brett till privata verksamheter. Inom arbetet bör även de förebyggande insatserna riktas mer fokus eftersom säkerheten börjar inom driftsäkerheten.

Ytterligare ett konkret initiativ för att i högre grad stärka samverkan med näringslivet kan ses genom den nya lagen om kommunernas ansvar inom det brottsförebyggande arbetet som trädde i kraft den 1 juli 2023. I lagen förtydligas kommunens ansvar att skriva överenskommelser med relevanta aktörer, vilket exemplifieras med näringslivet. Värt att notera är dock otydlighet kring begreppet ”relevanta aktörer” vilket öppnar upp för tolkningsutrymme. Det finns därmed ett behov av uppföljning och eventuellt förtydligande för att säkerställa att näringslivets perspektiv finns med i den kartläggning och den åtgärdsplan som kommunerna enligt lagen nu ska ta fram.

Sammantaget finns det därmed ett tydligt identifierat behov av stärkt samverkan med näringslivet inom det brottsförebyggande arbetet. Almega ser positivt till de initiativ som hitintills tagits, men betonar behovet av uppföljning för att säkerställa att arbetet leder till realiserad och resultatinriktad samverkan med företagen för att minska deras brottsutsatthet.

- **Rekommendation: Säkerställ att det identifierade behovet av övergripande samverkan med näringslivet inom det brottsförebyggande arbetet realiseras i praktiken.**

Detta bör göras med fokus på Polismyndighetens och Nationellt Cybersäkerhetscenters verksamhet samt genom en utvärdering hur kommunerna lever upp till sitt nya brottsförebyggande ansvar.[23] Rekommendationen kan genomföras som en granskning av Riksrevisionen.

Officiell statistik med nya brottskoder och trygghetsundersökning

Enligt den nya lagen om kommunernas ansvar att kartlägga brottsligheten ska denna utgå från officiell statistik från Brå och Polismyndigheten.[24] Problematiskt blir därmed att företagens brottsutsatthet inte redovisas i denna statistik. Risken

[21] Det brottsförebyggande arbetet i Sverige – Nuläge och utvecklingsbehov 2023. Brå.
[22] Polismyndighetens strategi för det brottsförebyggande arbetet. PM 2022:12.
[23] Lag (2023:196) om kommuners ansvar för brottsförebyggande arbete.
[24] Prop2022/23:43.

blir följaktligen återigen att kommunernas kartläggning, som ska ligga till grund för en åtgärdsplan, inte innefattar näringslivets utsatthet. Detta belyser vikten av att officiell statistik kommer på plats för att syftet med den nya lagen – att minska brottsligheten genom ett kunskapsbaserat brottsförebyggande arbete – ska kunna uppnås.

Framtagande av officiell statistik försvåras i sin tur av bristen på brottskoder för brott som drabbar företag. Det innebär att även om ett uppdrag skulle föreligga så finns det i dag inte möjlighet att sammanställa en heltäckande bild av brott som polisanmälts av företag. Det belyser därmed vikten av att nya brottskoder tas fram för att säkerställa att företagens brottsutsatthet kan sammanställas i officiell statistik.

Även om officiell statistik tas fram kvarstår problematiken kring att endast fyra av tio tjänsteföretag väljer att anmäla, vilket medför ett utbrett mörkertal. Allt sammantaget innebär detta att i syfte att säkerställa att företagens brottsutsatthet blir belyst på ett mer heltäckande vis så behövs även en återkommande nationell trygghetsundersökning genomföras med fokus på näringslivet. På så vis skapas, trots företagens låga anmälningsbenägenhet och bristande brottskoder, en mer heltäckande bild av företagens brottsutsatthet. Detta blir även ett särskilt viktigt underlag som kommunerna inom sitt nya lagstadgade uppdrag kan utgå från för att kunna göra en kartläggning och åtgärdsplan för brottsligheten i sitt geografiska område.

- **Rekommendation: Redovisa officiell statistik över företagens brottsutsatthet.**

  För att möjliggöra detta behövs nya brottskoder samt en återkommande nationell trygghethetsundersökning bland företag. Rekommendationen kan realiseras genom uppdrag till Brå.

Prioritera mängdbrotten och samordna den digitala brottsbekämpningen

Endast fyra av tio tjänsteföretag väljer att anmäla samtliga brott de blivit utsatta för. Att anmälningsbenägenheten är så låg handlar främst om att företagen inte tror att en anmälan leder till något resultat. Detta medför inte bara ett omfattande mörkertal där denna brottslighet inte kommer till polisens kännedom, utan än allvarligare – det pekar på en bristande tilltro till polisens förmåga att upprätthålla lag och ordning. En slutsats som dessutom delvis bekräftas i Riksrevisionens granskning av polisens förmåga att hantera mängdbrott, [25] vilket är den typ av brottslighet som utgör den stora bulken av brottslighet som drabbar både privatpersoner och företag.[26]

Riksrevisionens slutsats är att polisen inte bekämpar mängdbrotten på ett effektivt sätt och konstaterar att trots stora anslagsökningar, fler anställda och en genomgripande omorganisation har resultaten, sett till uppklaring av mängdbrott, blivit sämre. Bland orsakerna till polisens bristfälliga hantering pekas bland annat på ett ständigt dränage av utredningsresurser från lokalpolisområdena som ska vara basen i polisens verksamhet. I stället flyttas resurser för att hantera den

[25] Polisens hantering av mängdbrott – en verksamhet vars förmåga behöver stärkas. Riksrevisionen 2023. RiR 2023:2.
[26] Det rör sig om exempelvis skadegörelse, inbrott och bedrägeri som kan innebära allvarlig skada, ekonomiska förluster och som dessutom har starka samband med grov organiserad brottslighet.

grova organiserade brottsligheten. Detta medför att anmälda brott som har förutsättningar att utredas blir liggande eller avskrivs direkt. Riksrevisionen anser att detta innebär ett allvarligt läge eftersom brottsutsatta riskerar att inte få sin trygghet och säkerhet tillgodosedd, vilket i sin tur kan leda till att förtroendet för rättsväsendet minskar. Ett resultat som vi redan nu ser inom tjänstesektorn där just tilltron till polisen sviktar.

Sammantaget pekar slutsatserna på betydelsen av att Polismyndigheten mäktar med att hantera - vid sidan av det ökade fokuset på den grova brottsligheten - de mängdbrott som trots allt drabbar flest personer och företag. Dessutom blir detta en del i helheten att bekämpa den grova brottsligheten eftersom de är starkt sammanlänkade. Inte minst genom att brottsvinsterna från den stora ökningen av bedrägerier återinvesteras i den grova brottsligheten. Bekymmersamt är därför att Polismyndigheten själv redogör för att bedrägerierna blivit alltmer komplicerade att utreda.[27] Bland annat på grund av digitaliseringen och den snabba teknikutvecklingen som även innebär att denna typ av brottslighet genomförs utan geografiska begränsningar. De digitaliserade bedrägerierna utmanar därmed polisens traditionella fokus på att hantera brottsligheten lokalt. Detta pekar mot behovet av att även samordna förmågan för att möta den alltmer digitaliserade brottsligheten. Nya siffror som visar att kostnadsutvecklingen för cyberbrott skenar, till stor del på grund av de digitaliserade bedrägerierna, understryker därtill behovet av att se till att det finns förmåga att bryta denna ohållbara utvecklingstakt.[28]

- **Rekommendation: Prioritera mängdbrotten och samordna den digitala brottsbekämpningen**

  Polismyndigheten behöver dels prioritera mängdbrotten genom stärkt kapacitet i lokalpolisområdena, dels hantera den alltmer digitaliserade och gränsöverskridande brottsligheten genom att samordna den polisiära förmågan. Rekommendationen kan realiseras genom ett förtydligat uppdrag inom Polismyndighetens regleringsbrev.

Utveckla digital polisanmälan

Anmälningsbenägenheten behöver öka för att företagens brottsutsatthet ska komma till polisens kännedom. Uppenbart är att en tidskrävande och komplicerad process blir alltför kostsam för ett brottsutsatt företag, särskilt om det inte finns en tilltro att en anmälan gör någon skillnad eller leder till åtgärder, så som framkommit i den här rapporten.

I dag finns möjlighet att göra en digital anmälan för ett antal typer av brott, men i de flesta fall måste man fortfarande ringa in till Polismyndigheten. Det gäller även företag som endast i ett fåtal fall kan göra en digital anmälan i rollen som näringsidkare. Utformningen och handhavandet med digital anmälan har kritiserats av Riksrevisionen för att leda till merarbete för polisen snarare än att skapa en effektiv ärendehantering.[29] Detta sätter alltså fingret på att anmälningsförfarandet inte fungerar för vare sig för polisen själva eller för de anmälande företagen.

Det finns därmed stor potential att utveckla en digital anmälan för att underlätta och effektivisera både för de brottsutsatta företagen och för Polismyndigheten,

[27] Polismyndighetens årsredovisning 2023.
[28] Brottslighetens kostnader 2023. Svenskt Näringsliv.
[29] Polisens hantering av mängdbrott – en verksamhet vars förmåga behöver stärkas. Riksrevisionen 2023. RiR 2023:2.

som även kritiserats för alltför långa svarstider när anmälan tas emot via telefon.[30] Inspiration går här att få genom en nordisk utblick, där exempelvis Finland utvecklat ett digitalt anmälningsförfarande för företag genom en särskild företagssida.

- **Rekommendation: Utveckla det digitala anmälningsförfarandet.**

  Polismyndigheten behöver arbeta för att öka anmälningsbenägenheten genom att utveckla och underlätta möjligheten att anmäla digitalt. Detta kan göras genom att ta fram en särskild företagssida för anmälan på polisens hemsida.

Inför ett trygghetsavdrag

Svenska företag vidtar idag i stor utsträckning egna åtgärder för att förebygga och skydda sig mot brott och ordningsstörningar. Det framgår i en undersökning från Svenskt Näringsliv som visar att uppemot fyra av tio företag investerar i någon eller några säkerhetshöjande åtgärder.[31] Dessa investeringar täcker allt från kamerabevakning och väktare till it-säkerhet och lås. Sammantaget uppgår värdet av företagens egna säkerhetsåtgärder till 34 miljarder kronor under det senaste året.

Statistiken återspeglar därmed att trots företagen redan bidrar med betydande skattesummor till staten och kommunen för att upprätthålla lag och ordning så finns ett stort behov att ytterligare stärka den egna säkerheten. Detta innebär i praktiken att de betalar dubbla kostnader för att öka den egna tryggheten och skydda sig mot brottsligheten. I syfte att lätta den ekonomiska bördan som detta medför skulle ett trygghetsavdrag kunna införas som innebär en möjlighet att dra av en del av kostnaderna för säkerhetsåtgärder gentemot skatten. Detta skulle även bidra till att uppmuntra investeringar som leder till ökad trygghet och ett säkrare samhällsklimat samt till ett bättre utredningsunderlag till Polisen vid händelse av brott om till exempel fler företag investerar i kameraövervakning och passersystem.

Ett trygghetsavdrag vore en betydelsefull åtgärd och en del i att prioritera företagens brottsutsatthet i högre grad än idag. Förslaget i sig skulle i Almegas åsikt även vara tillämpbart i vidare bemärkelse och vara relevant för att uppmuntra privatpersoners investeringar för att öka den egna tryggheten.

- **Rekommendation: Inför ett trygghetsavdrag med möjlighet för företag att dra av delar av kostnaden för investeringar i säkerhetslösningar så som larm, väktare och kamerabevakning.**

[30] Ibid samt Polismyndighetens årsredovisning 2023.
[31] Brottslighetens kostnader 2023. Svenskt Näringsliv.

Referenser och litteratur

Almega. Tjänsteföretagen och stärkt cybersäkerhet i Sverige. 2022.

Brottsförebyggande rådet. Kriminalstatistik 2023.

Brottsförebyggande rådet. Det brottsförebyggande arbetet i Sverige – Nuläge och utvecklingsbehov 2023.

Brottsförebyggande rådet. Nationell trygghetsundersökning 2023.

Brottsförebyggande rådet (2022). Bedrägerier och ekobrott.

Lag (2023:196) om kommuners ansvar för brottsförebyggande arbete.

Nationellt bedrägericentrum, Polismyndigheten. De organiserade bedrägerierna. 2021.

Nationellt bedrägericentrum, Polismyndigheten. De dödliga bedrägerierna 2022.

Polismyndigheten. Polismyndighetens strategi för det brottsförebyggande arbetet. PM 2022:12.

Polismyndighetens årsredovisning 2023.

Proposition 2022/23:43. Kommunernas ansvar inom det brottsförebyggande arbetet.

Regeringens skrivelse. Tillsammans mot brott – ett nationellt brottsförebyggande program. 2016/17:126.

Riksrevisionen. Regeringens styrning av samhällets informations- och cybersäkerhet – både brådskande och viktig. 2023. RiR 2023:8.

Riksrevisionen. Polisens hantering av mängdbrott – en verksamhet vars förmåga behöver stärkas. Riksrevisionen 2023. RiR 2023:2.

Stiftelsen Tryggare Sverige. Företagens trygghetsundersökning 2023.

Stockholms handelskammare. Cyberbrott mot svenska företag – hur bygger vi en säkrare framtid? (2022).

Svenskt Näringsliv. Brottslighetens kostnader 2022.

Svenskt Näringsliv. Brottslighetens kostnader 2023.

Svenskt Näringsliv. Cybersäkerhet företag. 2023.