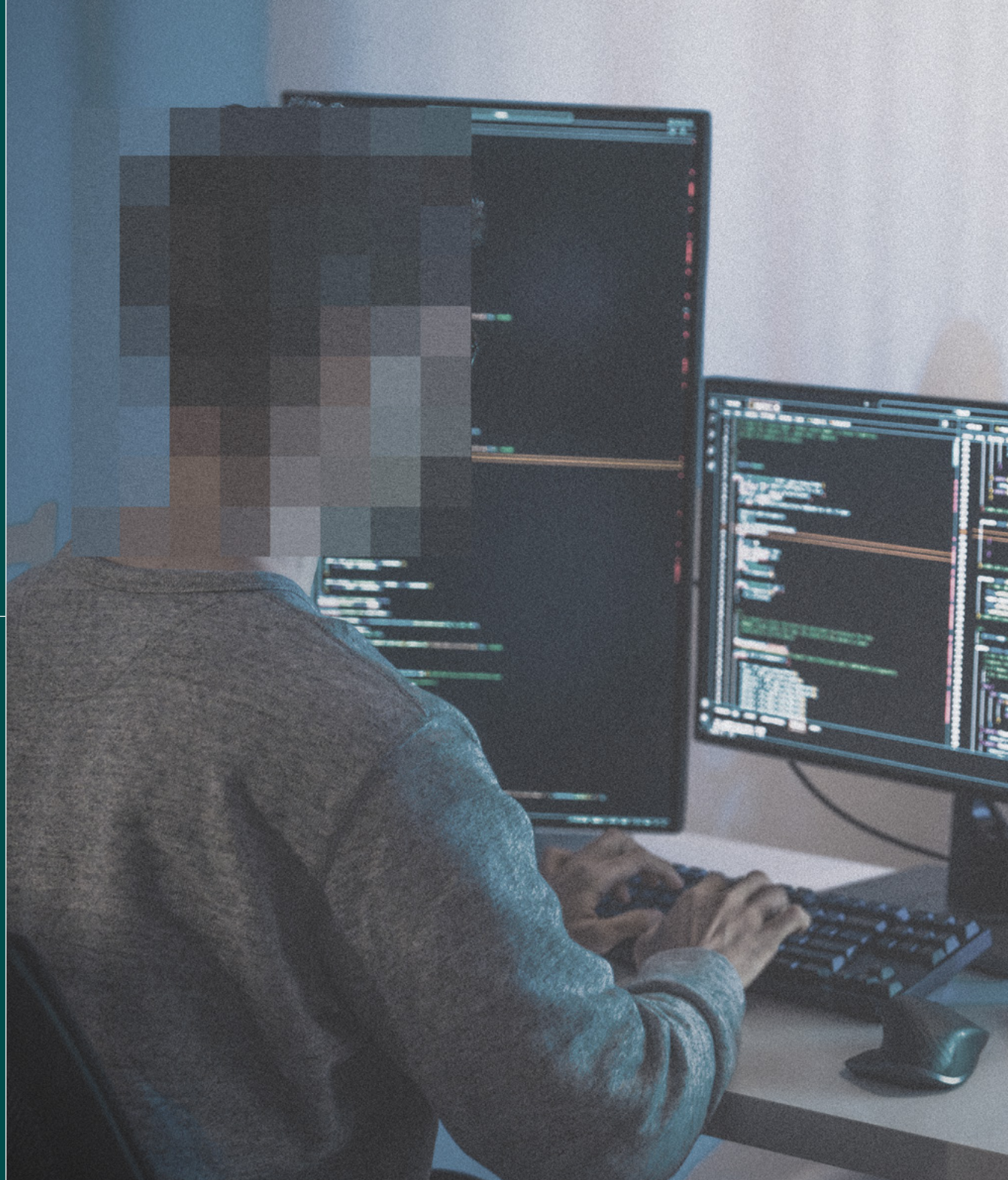
Handeln och den digitala brottsligheten

2025



Innehåll i rapporten

Inledning
Digitala brott – ett hot mot handelns verksamhet

Brott mot handelsföretag sker inte enbart i fysisk butik. Under de senaste åren har antalet digitala brott växt explosionsartat, och precis som i butikerna går trenden åt fel håll. Tyvärr tvingas man konstatera att ingen går säker. Såväl stora som små företag riskerar att drabbas av olika typer av digitala brott. Ibland med ödesdigra konsekvenser.

I rapporten du nu läser, ”Den digitala brottslighetens påverkan på handeln 2025”, påvisas att den digitala brottsligheten kostar handelsföretagen miljardbelopp årligen. Samtliga stora företag som tillfrågats har drabbats i någon utsträckning, men även medelstora och mindre företag uppger att attackerna blivit mer frekventa.

Det är inte bara kostsamt att utsättas för digital brottslighet. Även det brottsförebyggande arbetet blir för många handelsföretag en extra utgift, och för små- och medelstora företag är det den största utgiftsposten. I det rådande ekonomiska läget är ytterligare utgifter det sista företagen behöver, och kontinuerliga digitala attacker kan i värsta fall innebära att företag tvingas lägga ned sin verksamhet.

Med denna rapport vill Svensk Handel på allvar lyfta upp den problematik som den digitala brottsligheten medför. För tyvärr tvingas vi konstatera att brotten mot handeln ständigt tar sig nya uttryck. Därför är det viktigt att handelsföretagen, stora som små, säkrar upp sin verksamhet efter bästa förmåga. I detta arbete finns Svensk Handels säkerhetsavdelning tillgängligt. Vi är alltid bara ett samtal bort.

Nina Jelver, säkerhetschef Svensk Handel

Tyvärr tvingas man konstatera att ingen går säker.
Såväl stora som små företag riskerar att drabbas av olika typer av digitala brott. Ibland med ödesdigra konsekvenser.

01.

Om rapporten

Bakgrund
Så påverkar den digitala brottsligheten handeln – en nulägesbild

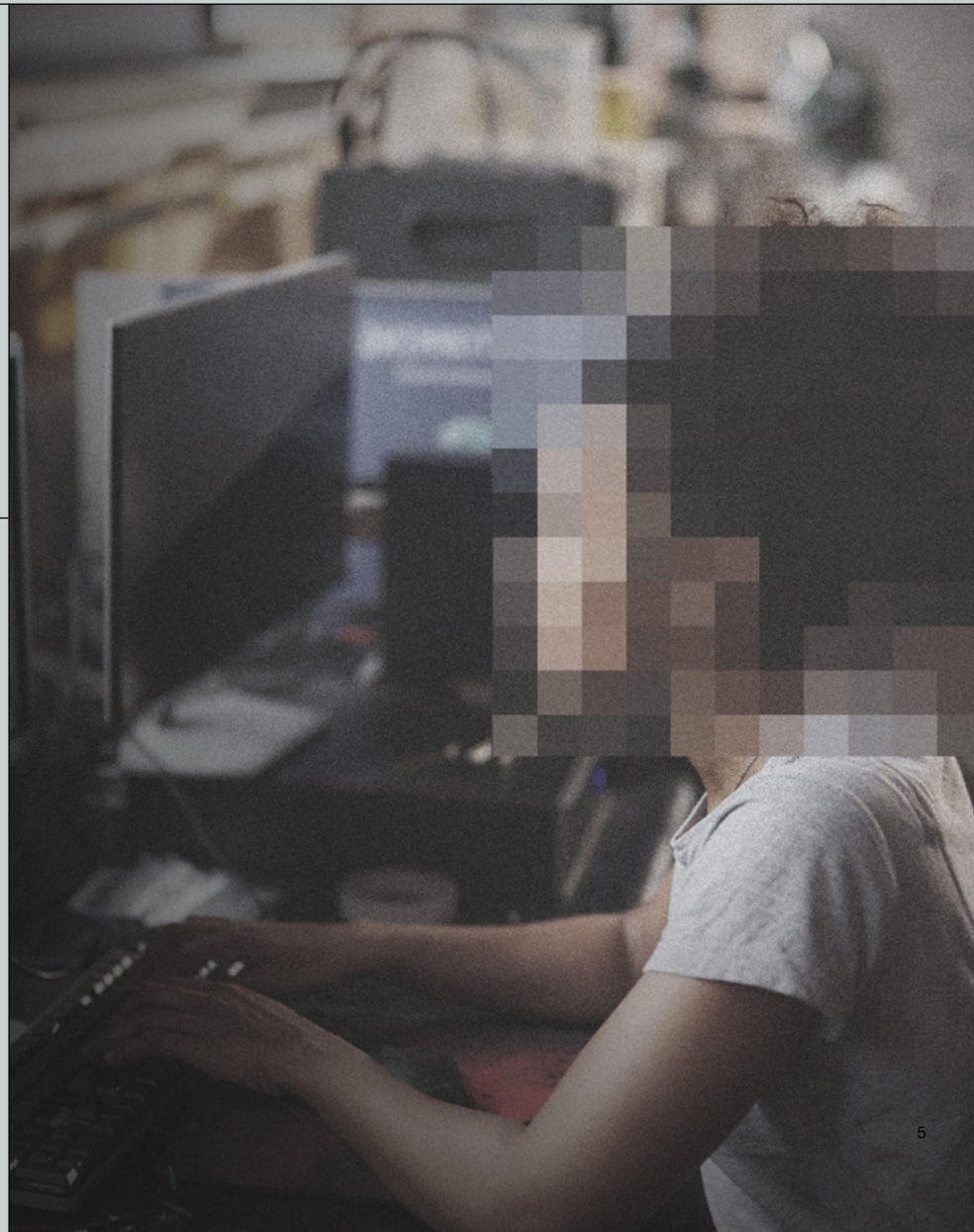
Svensk Handel genomför regelbundet undersökningar om hur brottslighet påverkar både den fysiska och digitala handeln.

Denna rapport berör hur utsatta företagen är, vilka konsekvenser det kan få och vilka behov de har i arbetet kring digital säkerhet.

I rapporten har begreppet digital brottslighet använts som ett samlingsbegrepp både för cyberbrott (angrepp mot den digitala miljön) och de bedrägerier som utförs med hjälp av i huvudsak digitala hjälpmedel.

Fler definitioner av begrepp som använts i rapporten följer på kommande sidor.

Denna rapport är den andra i ordningen där Svensk Handel undersöker den digitala brottsligheten och hur den påverkar handeln i Sverige.



Tillvägagångssätt
Om undersökningen

Undersökningen genomfördes under perioden november 2024 – januari 2025 med hjälp av kombinerade metoder:

Del 1

Intervjuer med experter inom Polismyndigheten, Truesec, Svensk Dagligvaruhandel, Axfood och Stadium med syftet att få en förståelse för digital brottslighet och ringa in för undersökningen relevanta områden. De intervjuade experterna utgör även referensgrupp för undersökningen i syfte att säkerställa dess innehåll och relevans.

Del 2

Semistrukturerade intervjuer med åtta säkerhetschefer med representanter från några av de största företagen inom dagligvaruhandeln och sällanköpshandeln.

Del 3

Enkätundersökning med 285 ekonomiansvariga för små och medelstora företag inom handeln. En webbaserad enkätundersökning genomfördes under perioden november 2024 – januari 2025.

Del 4

En telefonundersökning med ekonomiansvariga i små företag inom handeln genomfördes i februari 2025.

Definitioner i rapporten

Små företag

Definieras som de svarande i en telefonundersökning genomförd av Norstat på uppdrag av HUI, med en tonvikt på små företag. Medianföretaget hade 1-9 anställda.

Medelstora företag

Definieras som de svarande i webbenkäten som genomfördes av HUI, med en tonvikt på medelstora företag. Medianföretaget hade 10-24 anställda.

Stora företag

Definieras som de svarande i intervjustudien som genomfördes av HUI, med en tonvikt på stora företag. Medianföretaget hade över 500 anställda.

Tillvägagångssätt
Referensgrupp

Referensgruppen för undersökningen har bestått av

Marcus Murray, Truesec

Marcus Murray är grundare av Truesec och en av Sveriges främsta experter inom cybersäkerhet. Marcus har över 20 års erfarenhet av arbete kring hur organisationer bäst kan skydda sig, upptäcka och hantera cyberintrång, både internationellt och i Sverige. Marcus är även en eftertraktad föreläsare på Techkonferenser runt om i världen.

Lotta Mauritzson, Polismyndigheten

Charlotta Mauritzson är samordnare vid polisens nationella bedrägericentrum. Hon har gedigen erfarenhet av olika typer av bedrägerier, som utgör en stor del av den digitala brottsligheten.

Jan Olsson, Polismyndigheten

Jan Olsson har arbetat över 30 år inom Polisen, varav 15 år med nätrelaterade brott. Han var med och grundade Nationellt Bedrägericentrum och är nu verksamhetsutvecklare vid Nationellt it-brottscentrum. Jan är en av landets främsta experter inom cyberbrottslighet och internetrelaterade brott. Hans arbete sträcker sig också utanför Sveriges gränser i form av föreläsningar och samarbeten med bland annat Interpol.

Patricia Lindén, Stadium

Patricia Lindén är IT security manager på Stadium och ansvarar för det operativa arbetet inom IT-säkerhet där hon har över 15 års erfarenhet. Patricia arbetade tidigare med informationssäkerhet inom försvarsindustrin. Hon är också en ofta anlitad föreläsare.

Elin Ryrfeldt, Axfood

Elin Ryrfeldt är CISO på Axfood där hon jobbar med att skydda en av Sveriges största dagligvaruaktörer. Hon har bred kunskap inom bland annat compliance, informationssäkerhet, riskhantering, krishantering och ledningssystem.

Ulrika Dahlin, Svensk Dagligvaruhandel

Ulrika Dahlin är beredskapsansvarig hos Svensk Dagligvaruhandel. Hon har lång erfarenhet av dagligvaruhandeln och har arbetet inom såväl livsmedelssäkerhet och miljöfrågor som risk- och säkerhetsfrågor. På Svensk Dagligvaruhandel jobbar Ulrika med att företräda dagligvaruhandelns intressen i beredskapsfrågor.

Begrepp och definitioner som används i rapporten

Attackvektorer

Attackvektorer är metoder eller ingångar som en eller flera angripare använder sig av för att utnyttja sårbarheter i ett system eller hos en individ.

Cyberbrott

Cyberbrott riktar in sig mot digitala nätverk, tjänster, produkter eller plattformar.

Dataintrång

Dataintrång innebär att utan tillstånd få åtkomst till en IT-miljö eller dess uppgifter, ofta med syfte att stjäla, ändra, eller radera information.

Deepfake

Deepfake är en AI-baserad teknik som trovärdigt imiterar människan i ljud och bild. I brottsliga sammanhang används Deepfakes för att exempelvis få tillgång till information eller pengar genom att bedragare utger sig för att vara en inflytelserik person.

Digitala bedrägerier

Digitala bedrägerier inkluderar stulna kortuppgifter, bedrägliga internetköp eller betalningar, bedrägliga e-postmeddelanden, falska webbsidor eller plattformar med skadligt uppsåt.

Digitala brott

Digitala brott är alla brott som helt eller delvis begås i anslutning till digital teknik, inklusive cyberbrott.

Insiderbrott

Insiderbrott innebär utnyttjande av en individs tillgång till en organisations resurser, information eller system i olagliga syften.

Ransomware

Ransomware är en skadlig programvara som oftast blockerar åtkomsten till system med syfte att utpressa den drabbade organisationen till betalning.

Nätfiskebedrägeri (phishing)

Nätfiske (phishing) är en metod där individer vilseleds att självmant och ovetandes lämna känslig information som inloggningsuppgifter, personuppgifter eller kreditkortsuppgifter genom exempelvis formulär.

Sabotage

Sabotage är en medveten handling som syftar till att förstöra, skada eller störa verksamhet, infrastruktur, system eller resurser.

Social manipulation

Social manipulation är en påverkansmetod som förmår individen att utföra specifika handlingar eller lämna ut känslig information genom mänsklig interaktion.

02.

Kostnader och konsekvenser

Digital brottslighet påverkar hela handeln

Huvudinsikter
Digital brottslighet påverkar hela handeln

01.

Osynlig brottslighet

Stora- och medelstora företag är överrepresenterade bland de drabbade i undersökningen. Samtliga av de stora företagen uppger att de drabbats på något sätt. Omfattningens av företagens utsatthet är trots detta sannolikt större då mörkertalet döljer brott som inte anmäls, inte upptäcks, eller av andra anledningar inte nämns.

02.

Kostsamt förebyggande arbete

Större företag drabbas av mer avancerade angrepp med risk för större skada och har därför ofta tvingats lägga resurser på säkerhetsavdelningar och förebyggande IT-lösningar. De mindre företagen blir istället personberoende och mer sårbara, där lyckade angrepp kan få förödande konsekvenser.

03.

Stor oro för intäktsbortfall

Den digitala brottsligheten skapar oro. De medelstora företagen uppger att de främst vill undvika minskade intäkter, medans de stora företagen tenderar att främst oroar sig för minskat förtroende.

Omvärldsläget ökar hotbilden

Osäkerhet påverkar

Hotbilden mot Sverige från utländska aktörer förändrades med Rysslands invasion av Ukraina. Den organiserade brottsligheten har samtidigt tagit en allt större plats i samhället. Detta ger en ökad risk för digital brottslighet samtidigt som vardagen präglas av en allmän oro.

Flera uppmärksammade IT-attacker

Konsekvensen av digital brottslighet kan vara förödande. Mest omskrivet i närtid är attacken mot IT-leverantören Tietoevry under 2024 och när Coops kassor slogs ut genom attacken mot leverantören Kaseya 2021. Båda var så kallade Ransomware-attacker och påverkade verksamheter över hela världen.

Förebyggande arbete viktigt

Effektivt förebyggande arbete mot digital brottslighet kan vara avgörande för handelns utveckling, stärkt konkurrenskraft och kundernas förtroende. Vikten av att vara på sin vakt, att vara medveten om vilka hot och risker som finns och att ha rätt verktyg betonas av experterna i studien.

Större företag mest oroliga

De stora företagen oroar sig i störst utsträckning för digital brottslighet. Detta kan bero på att de generellt drabbas av mer avancerade angrepp i kombination med större risk vid skada, främst sett till hög omsättning, värdefulla data eller kostnad vid driftstopp. Större företag har också fler, ofta utländska, underleverantörer och mer komplexa system, vilket gör att de i större utsträckning kan drabbas indirekt av attacker riktade mot en underleverantör.

”Mitt jobb är att oroa mig för vad som kan hända och att vidta åtgärder. Målet är att aldrig behöva uppleva arbetsdagen som när Coop drabbades av ett intrång, och butikerna behövde stänga.”

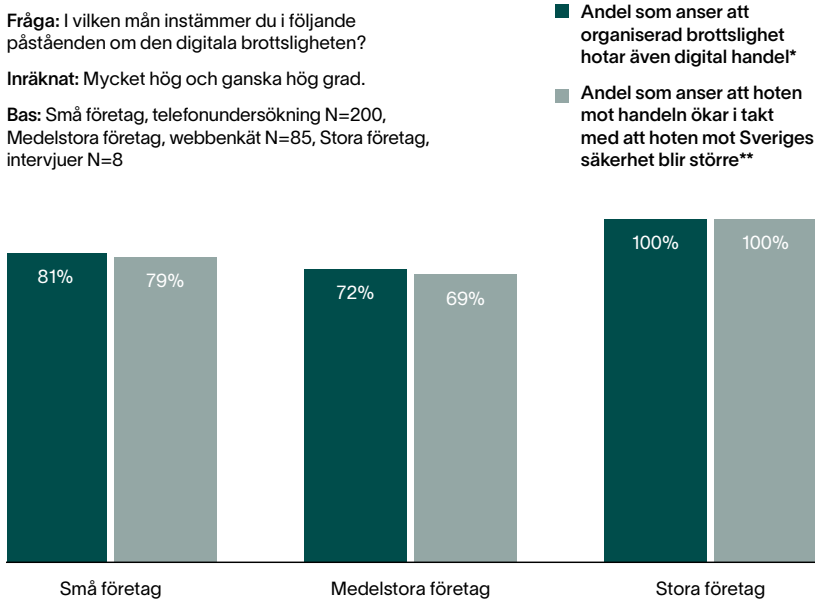
Säkerhetschef inom detaljhandelsföretag

Företagen är medvetna om den ökade digitala hotbilden mot handeln

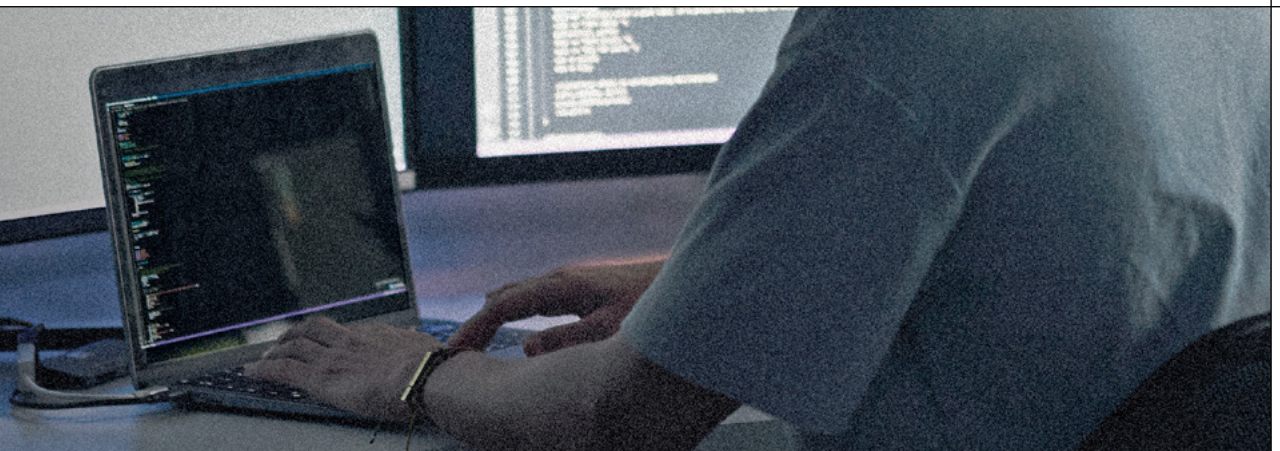
Fråga: I vilken mån instämmer du i följande påståenden om den digitala brottsligheten?

Inräknat: Mycket hög och ganska hög grad.

Bas: Små företag, telefonundersökning N=200, Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8



*Organiserad brottslighet hotar även handeln digitalt.
** Hoten mot handeln ökar när hoten mot Sveriges säkerhet är större.



”En utmaning vi behöver hantera är att en förändrad hotbild i omvärlden måste balanseras mot kompetens, teknisk förmåga och resursbehov. Utmaningen är att hitta den balansen. Även om man har pengar att investera i skydd så finns det inte folk på marknaden som kan.”

Säkerhetschef inom detaljhandelsföretag

Små företag sällan drabbade

Den digitala utvecklingen har bidragit till en ökad produktivitet i näringslivet och lägre priser i detaljhandeln. Det är idag få verksamheter som inte har inslag av datorisering och digital teknik. I takt med den ökade digitaliseringen har även riskerna ökat. Den digitala miljön är global och kan angripas från hela världen.

Stora företag drabbas hårdast

Att samtliga stora företag i undersökningen uppger att de har utsatts för digital brottslighet belyser allvaret i situationen. De stora företagen tenderar även att utsättas för olika former av digital brottslighet, ofta via kriminella organisationer i utlandet. 63 procent av de största företagen uppger att de har drabbats av överbelastningsattacker, 38 procent har drabbats av dataintrång och hela 75 procent har drabbats av andra digitala brott så som fakturabedrägeri.

Små företag avviker

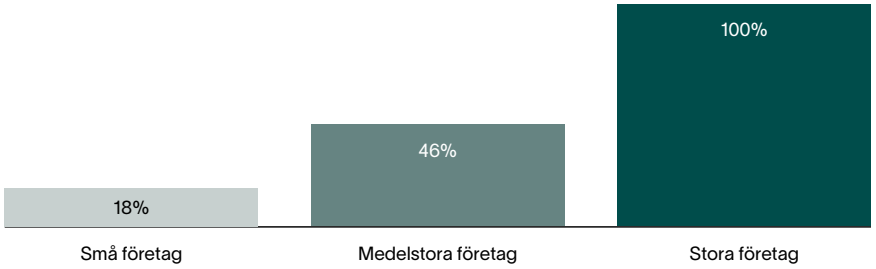
En betydande del av de mindre företagen uppger att de inte har drabbats av digitala brott. Detta beror sannolikt på att mindre företag inte är lika prioriterade måltavlor för digital brottslighet på samma sätt som stora företag.

De små företagen tenderar att drabbas mer av phishing och bluffakturor, vilka delvis rensas bort automatiskt av spamfilter eller alternativt inte tolkas som digital brottslighet. Det kan också vara så att företagen saknar rutiner och kunskap för att kunna upptäcka de intrångsförsök eller andra former av digital brottslighet som de drabbas av.

Alla stora företag har drabbats av digital brottslighet

Fråga: Utsattes ert företag för någon form av digital brottslighet det senaste året?

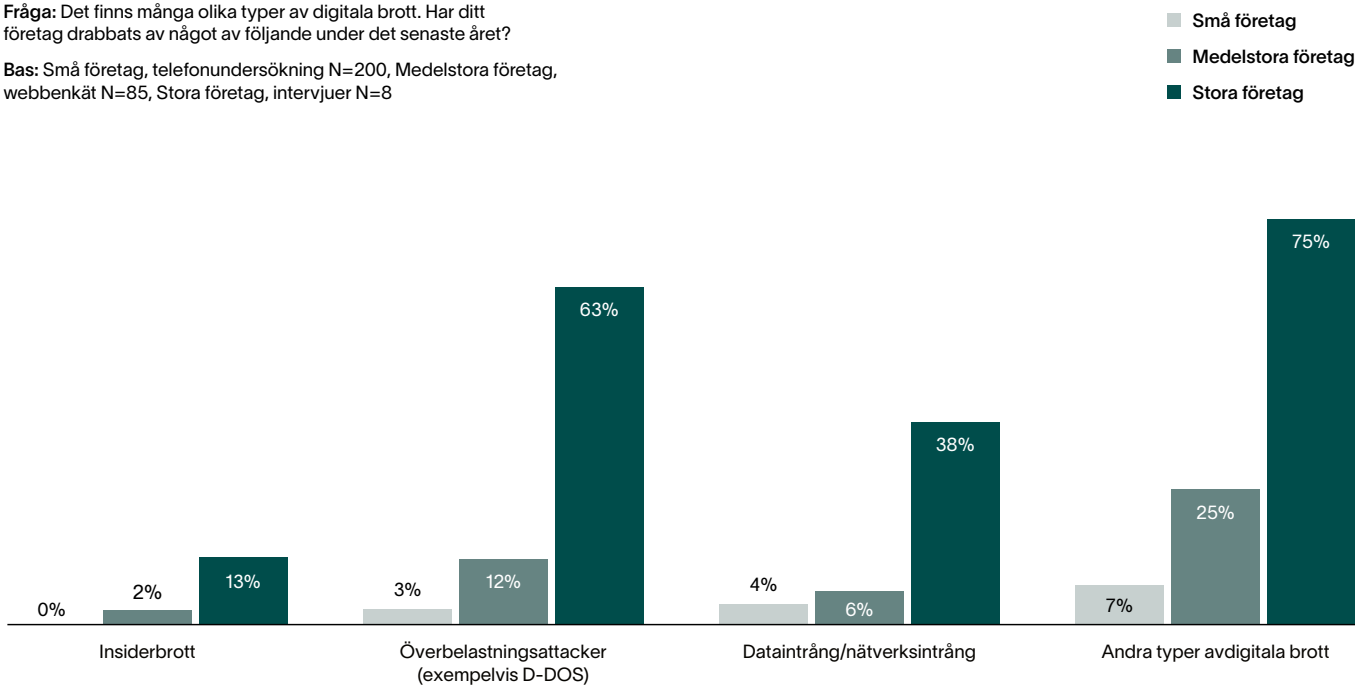
Bas: Små företag, telefonundersökning N=200, Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8



Andel företag som drabbats av brott i respektive brottskategori

Fråga: Det finns många olika typer av digitala brott. Har ditt företag drabbats av något av följande under det senaste året?

Bas: Små företag, telefonundersökning N=200, Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8



Den digitala brottsligheten kostar miljardbelopp

Den digitala brottsligheten kostar miljarder varje år

Kostnaderna för den digitala brottsligheten uppgår idag till miljardbelopp varje år. I Svenskt Näringslivs mätning uppgick de direkta kostnaderna för cyberkriminalitet till cirka 9 miljarder kronor i Sverige år 2023.[1] Utöver detta tillkommer indirekta kostnader och intäktsbortfall kopplade till brottsligheten.

Trots dessa enorma summor underskattas med all säkerhet cyberbrottslighetens kostnader. Den verkliga kostnaden är dock med all sannolikhet ännu större då mörkertalet är enormt.

Stora företag oroar sig mer

Frågan om digital brottslighet ter sig något annorlunda än traditionell brottslighet i butik. När det kommer till svinn och butiksstölder tenderar dessa att vara en konsekvens av butikens läge och produkterna som säljs. Större företag är inte avsevärt mer utsatta än mindre företag enbart på grund av sin storlek.

I den digitala världen är det annorlunda. Ett större företag utgör vanligtvis en mer attraktiv måltavla för olika angripare eftersom det finns en potentiellt större ekonomisk vinning i att angripa dem. I Svensk Handels undersökning har samtliga stora företag drabbats jämfört med knappt hälften av de medelstora och endast 18 procent av de små.

Större företag är således mer riskutsatta och konsekvenserna blir mer omfattande vid ett intrång. Samtidigt har stora företag betydligt större och mer utvecklade säkerhetsavdelningar och en helt annan förmåga att hantera angrepp än små företag har.

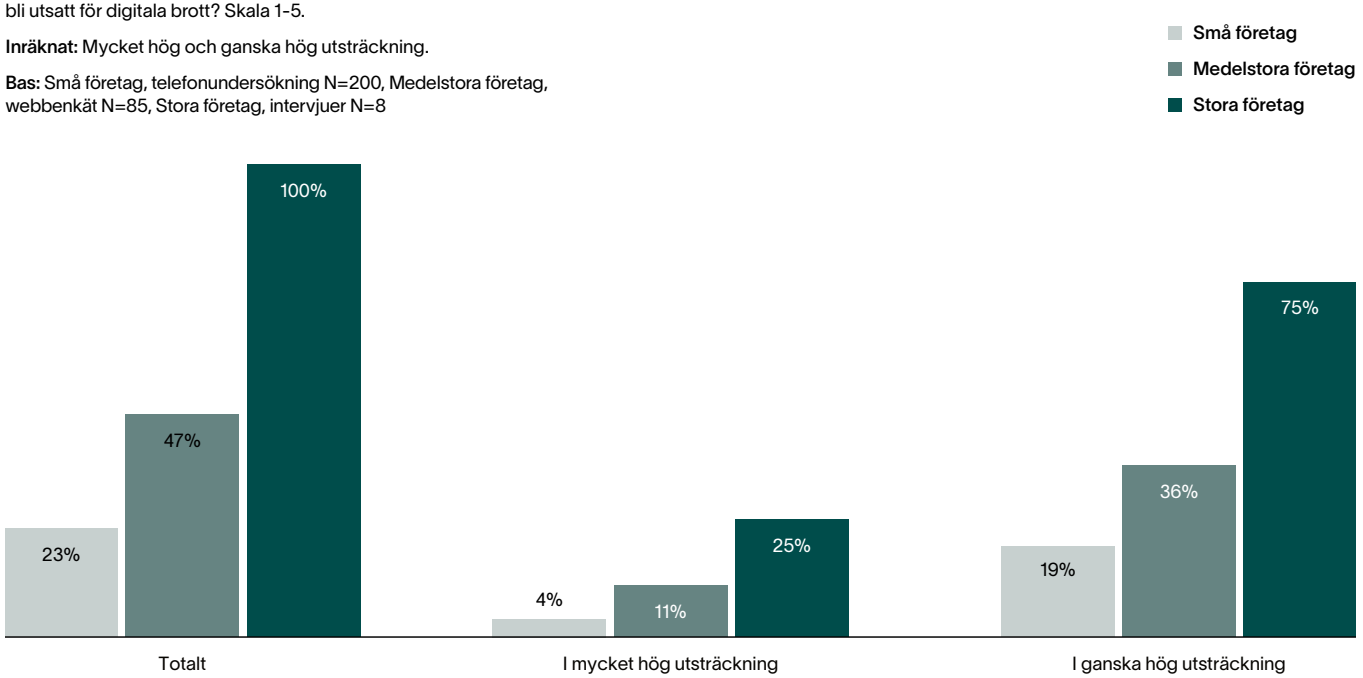
[1] Svenskt Näringsliv, 2023

Stora företag har högst medvetenhet gällande utsatthet för digitala brott och oroar sig därför i högre utsträckning

Fråga: I vilken utsträckning oroar du dig över att ditt företag ska bli utsatt för digitala brott? Skala 1-5.

Inräknat: Mycket hög och ganska hög utsträckning.

Bas: Små företag, telefonundersökning N=200, Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8



Minst

9 miljarder

i direkta kostnader uppgår den digitala brottsligheten till per år.

Kostsamt att förebygga brott

Stora kostnader förknippade med att förhindra brott

Undersökningen ger en inblick i hur det förebyggande arbetet påverkar företagen. Digitala säkerhetssystem är den vanligast förekommande kostnaden både för små och medelstora företag.

Kostnader för expertis och utbildning

Externa konsulter och expertis är den näst vanligaste kostnaden bland medelstora företag. Bland de små företagen är det istället något vanligare att bekosta utbildningsinsatser.

Utbildningsinsatser kring grundläggande IT-kunskap och de vanligaste säkerhetsriskerna kan göra stor skillnad, likaså utbildningar kring säkerhetsrutiner, i synnerhet för de små företagen.

Få företag har en dedikerat ansvarig för digital säkerhet

27 procent av de medelstora företagen uppger att de har haft kostnader för dedikerad personal och 38 procent att de har haft kostnader för externa konsulter. Att ha intern kompetens är vanligare på stora företag. I ett större företag ökar komplexiteten och riskutsattheten snabbt och därmed också vikten av kompetens.

27%

Endast 27% av de medelstora företagen har haft kostnader för personal som dedikerat ansvarig för digital säkerhet

Topplista: De mest prioriterade säkerhetsåtgärderna bland företagen i detaljhandeln

Företagens vanligaste kostnadsposter inom digital säkerhet

Bas: Medelstora företag, webbenkät N=85, Små företag, telefonundersökning N=200

Medelstora företag		Små företag	
01.	Kostnad för digitala säkerhetssystem	01.	Kostnad för digitala säkerhetssystem
02.	Kostnad för externa konsulter och expertis	02.	Kostnad för utbildning
03.	Kostnad för utbildning	03.	Kostnad för externa konsulter och expertis

Oro för minskat förtroende och minskade intäkter

Störst oro bland de stora företagen

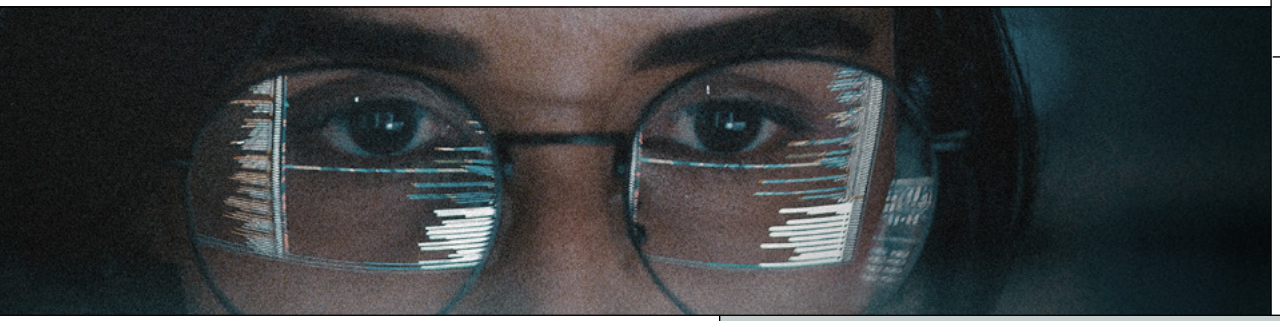
Oron för att utsättas för olika typer av digitala brott hos stora företag speglas av riskmedvetenhet och förberedelsegrad.

Nästan alla stora företag oroar sig för intrång som leder till någon form av sabotage som är skadligt för verksamheten. En majoritet av företagen i undersökningen uppger att minskade intäkter är den största risken med digital brottslighet.

Direkta och allvarliga konsekvenser

När det kommer till uteblivna intäkter på grund av digital brottslighet är det tydligaste exemplet IT-attacken som drabbade bland annat Coop 2021 där butikskassor slogs ut.

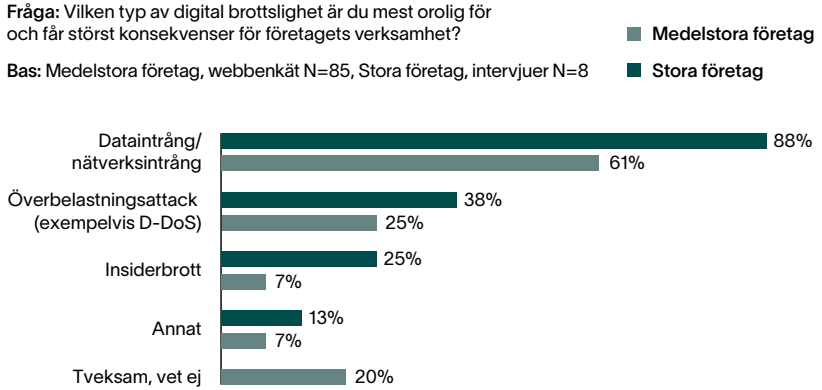
En annan stor risk är minskat förtroende bland kunderna, i synnerhet för de stora företagen. De medelstora företagen uppger att den tredje största risken är minskad möjlighet att utveckla verksamheten, exempelvis att inte våga implementera vissa tekniska lösningar på grund av de ökade säkerhetsriskerna.



De digitala brott som företagen är mest oroliga för

Fråga: Vilken typ av digital brottslighet är du mest orolig för och får störst konsekvenser för företagets verksamhet?

Bas: Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8



”E-handeln låg nere i en vecka, vilket påverkade försäljningen och kundtjänsten. Fysiska butiker kunde hålla öppet men hade begränsningar i varuförsörjningen.”

Säkerhetschef inom sällanköpsvaruhandeln

”Intrång leder i regel till tre saker: avbrott i verksamheten, att information stjäls, eller kostnader för att återställa IT-miljön.”

Säkerhetsansvarig inom detaljhandeln

Vad är den största risken med digital brottslighet i handeln?

Medelstora företag		Stora företag	
01.	Minskade intäkter för företagen	01.	Minskat förtroende hos kunderna
02.	Minskat förtroende hos kunderna	02.	Minskad tillgänglighet/beredskap för kunderna
03.	Minskade möjligheter att kunna utveckla verksamheten	03.	Minskade intäkter för företagen

Intervju med Jan Olsson
Den professionella cyberbrottsligheten fungerar som ett företag

Jan Olsson är kriminalkommissarie och arbetar på NOA – polisens nationella operativa avdelning. Jan har en lång karriär inom cyber- och nätrelaterad brottslighet och har även arbetat internationellt i samarbete med Europol och Interpol.

Vilka är de främsta hoten mot svensk IT-säkerhet?

Det är många som underskattar hur professionell den organiserade cyberbrottsligheten är idag. Globala kriminella organisationer som bedriver den här typen av brottslighet fungerar som väl-organiserade internationella företag, där man går till jobbet varje dag i syfte att göra intrång och begå brott. Även människan är en stor attackvektor idag, och det är viktigt med personalutbildning vid sidan av IT-systemet.

Hur ser IT-säkerheten ut hos företag i handeln idag?

Tyvärr är säkerheten bland svenska detaljhandels-företag idag generellt ganska låg. De stora företagen har professionella säkerhetsavdelningar men bland mindre företag är kunskapen ofta sämre. Ett vanligt problem för mindre företag är att man sällan övar eller ens testar backuperna på sin data. När man väl behöver dem så visar det sig ofta att de inte fungerar.

Det finns en betydande specialisering som gör det möjligt för de kriminella att rekrytera den specialist-kompetens de behöver. Detta kallas för ”crime as a service” och det finns en stor kriminell marknad för att köpa såväl kompetens som tjänster och befintliga sårbarheter eller uppgifter som någon annan kommit över.

> Under de kommande åren kommer utvecklingen inom Artificiell Intelligens att medföra utmaningar, både i Sverige och internationellt. Enkla bedrägerier kan nu göras mer sofistikerade och riktade genom AI, vilket gör dem mer effektiva. Massutskick av bedrägerimejl kan se betydligt mer trovärdiga ut än tidigare, och produceras på vilket språk som helst.

Vilka risker ser du för just handelns företag i Sverige?

Skalbarheten är helt annorlunda idag än tidigare, det vill säga att angripare kan göra anrop varifrån som helst. Ligorna kan angripa företag över hela världen, eller attackera digitala tjänster och underleverantörer. Det är vanligt att retailaktörer drabbas i andra hand, som kunder till dessa IT-leverantörer. Detta drabbade Coop via det amerikanska företaget Kaseya och ett antal svenska retailföretag via Tietoevry.

Vilka är de främsta säkerhetsåtgärderna för att skydda sin verksamhet mot digital brottslighet?

Det finns en del enkla åtgärder som ger effekt mot kriminella intrång. Relativt små ändringar som veri-fiering med BankID har minskat förekomsten av vissa typer av brott avsevärt. Flerfaktorautentisering för att komma åt känsliga uppgifter gör det också svårare för de kriminella.

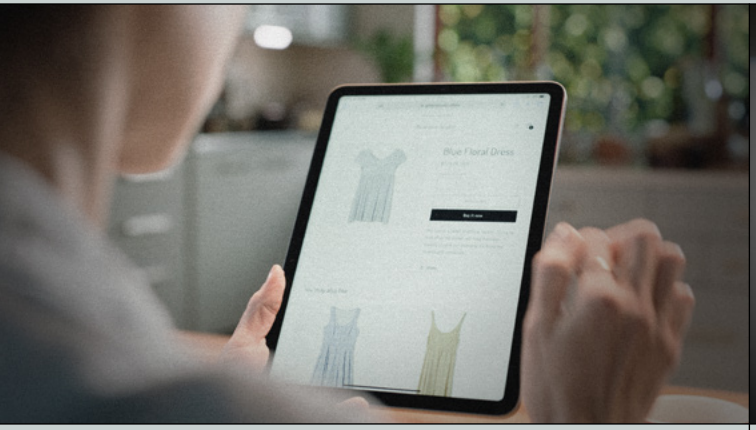
Jan Olsson,
kriminalkommissarie,
NOA – polisens nationella operativa avdelning

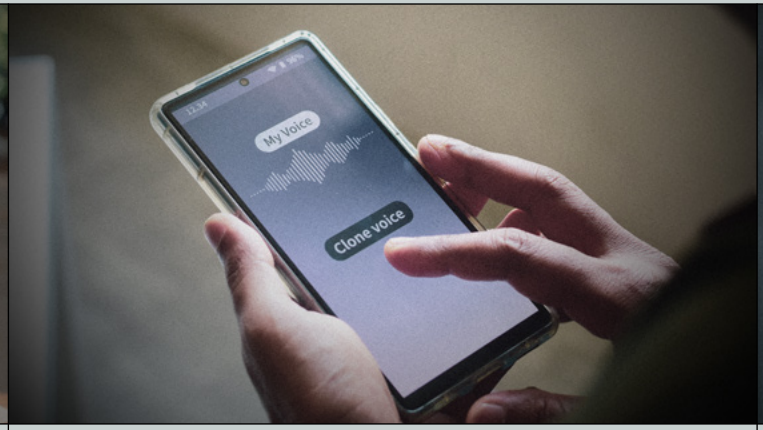
03.

En alltmer komplex brottslighet

Nya brottsformer och bedrägerier utmanar handeln

Huvudinsikter
Nya brottsformer och bedrägerier utmanar handeln





01.

En alltmer komplex brottslighet utförs av olika professionella aktörer

En stor del av den digitala brottsligheten utförs av, eller åt, den organiserade brottsligheten. Brottsvinsterna kan i förlängningen utgöra en del av mer omfattande upplägg som exempelvis penningtvätt. Utförarna är mycket kunniga. Det förekommer annonser av illegala tjänster på digitala plattformar likt vilken kommersiell verksamhet som helst, ofta benämnt *Crime As A Service.*

02.

Bedrägerier drabbar alla företag i handeln

Den tekniska utvecklingen och AI möjliggör alltmer avancerade bedrägerier där individen är mer utsatt än tidigare. Bedrägerier förekommer i olika former, ibland specifikt inriktade mot vissa verksamheter, ibland riktade mot en vidare krets.

03.

Ständig förändring ökar utsattheten

Utsattheten för digitala brott varierar över tid. Oavsett företagsstorlek finns en oro. Nya brotts- och bedrägerimetoder såsom social manipulation, deepfakes och falska webbsidor har ökat i takt med den tekniska utvecklingen i samhället.

Medveten riskhantering avgörande

De digitala brotten är osynliga

Antalet digitala brott ökar, blir allt mer sofistikerade och svårare att upptäcka.

Det gör dagens brottslandskap komplext och inte helt lätt att kartlägga. Handelns viktiga roll i samhället gör branschen till en av många måltavlor för hotaktörer i digitala miljöer.

Förståelse för företagets utsatthet är avgörande

Antalet skydd som erbjuds för att stå emot olika digitala hot är många, och det kan vara svårt att hitta rätt.

Ett effektivt förebyggande arbete ställer större krav på medvetenhet och riskhantering inom företaget, oavsett storlek.

Det är avgörande att företagen förstår sin verksamhet och dess unika sårbarheter för att kunna identifiera och hantera hot, och därefter välja besluta om förebyggande åtgärder.

"Om det finns sätt att bryta sig in på i en digital miljö kommer det att ske förr eller senare."

Säkerhetsansvarig inom detaljhandeln

Utsattes ert företag för någon form av digital brottslighet det senaste året?

Bas: Små företag, telefonundersökning N=200, Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8.

18%

av de små företagen uppger att de blivit utsatta för brott.

46%

av de medelstora företagen uppger att de blivit utsatta för brott.

100%

av de stora företagen uppger att de blivit utsatta för brott.

Upplever ni att företaget är mer eller mindre sårbart eller hotat av digitala attacker idag än för tre år sedan?

Bas: Små företag, telefonundersökning N=200, Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8.

38%

av de små företagen upplever att de är mer sårbara för digitala attacker idag än för tre år sedan.

59%

av de medelstora företagen upplever att de är mer sårbara för digitala attacker idag än för tre år sedan.

63%

av de stora företagen upplever att de är mer sårbara för digitala attacker idag än för tre år sedan.

Stor variation bland aktörerna som utför digitala brott

Svensk Handel har inom ramen för samverkansgruppen med Svensk Dagligvaruhandel tagit fram en indelning av de primära hotaktörer som utför digitala brott gentemot handeln

Nationalstatliga aktörer

Nationalstatliga aktörer är hotaktörer som agerar på uppdrag av, eller styrs av, nationalstater utifrån geopolitiska motiv. En ökande trend är att stater använder cyberkriminella så kallade hackers for hire* (hackare att hyra) för att främja sina intressen.

Detta suddar ut gränserna mellan olika typer av hotaktörer och stärker samtidigt de nationalstatliga aktörernas kapacitet. Kända aktörer inom detta område är Kina, Ryssland, Nordkorea, Vietnam, Iran och Syrien.

Cyberkriminella hotaktörer

Cyberkriminella hotaktörer är individer eller organiserade grupper som begår brott i den digitala miljön, främst i syfte att uppnå egen ekonomisk vinning.

Vanliga angreppsmetoder inkluderar utpressningsattacker och nätfiske där drabbade tvingas eller vilseleds att utföra penningöverföringar eller lämna ifrån sig känslig information.

Cyberkriminella

Till skillnad från de mer avancerade cyberkriminella hotaktörerna finns det även grupper av kriminella som begår enklare digitala brott. Dessa bedragare riktar sig inte bara mot handeln, utan även mot handelns kunder.

Cyberterrorister

Cyberterrorister genomför politiskt eller ideologiskt motiverade cyberattacker som kan innebära hot om, eller resultera i, våld. Vissa cyberterrorister har kopplingar till nationalstatliga aktörer, medan andra agerar på egen hand eller på uppdrag av en icke-statlig grupp.

Hacktivister

Hacktivister kan vara organisationer, enskilda individer eller grupper av varierande storlek och förmåga, vars agerande främst drivs av ideologiska motiv.

Hacktivister använder tekniska medel för att genomföra dataintrång och cyberattacker i syfte att sprida sitt budskap. Deras angrepp kan riktas mot en bred uppsättning mål, exempelvis individer, organisationer, myndigheter och andra samhällsaktörer.

Spänningssökare

Spänningssökare är individer som ägnar sig åt cyberaktiviteter främst för spänningens och utmaningens skull snarare än för ekonomisk vinning eller politiska syften.

Insiders

Insiders är medarbetare, partners eller andra som genom sitt arbete har tillgång till IT-system eller fysiska miljöer. Det som särskiljer dem är deras förtroendeställning inom ett företag eller en yrkesroll.

*** Hackers for hire**

”Hackare att hyra”. Dessa erbjuder sina tjänster till cyberkriminella eller nationalstatliga aktörer, antingen för ekonomisk vinning eller för att säkra sin egen trygghet. Dessa aktörer har ofta mycket hög kompetens och arbetar med tydlig specialisering och arbetsfördelning, vilket gör dem särskilt svåra att bekämpa inom ramen för cyberbrottslighet.

Bedrägerier drabbar alla företag i handeln

Stora företag mest drabbade av bedrägerier

Fråga: Vid bedrägeri: Har du som företagare/ditt företag blivit utsatt för något eller några av följande under det senaste året?

Bas: Små företag, telefonundersökning N=200, Mellanstora företag, webbenkät N= 85, Stora företag, intervjuer N=8.

Vanligast förekommande bedrägerierna i handeln	Små företag	Medelstora företag	Stora företag
Mottagit en bedrägerifaktura	33%	55%	100%
Bedrägeriförsök via e-post, sms eller telefon	24%	29%	100%
Levererat varor som inte betalats	14%	26%	N/A
Falska webbsidor som utger sig för att vara vår webbsida	7%	8%	88%

Digitala bedrägerier sker på olika sätt

Företagen inom handeln är utsatta för olika typer av bedrägerier. Undersökningen visar att fakturabedrägeri är den vanligast förekommande typen av bedrägeri för de olika företagen i undersökningen. De stora företagen är bedrägeriutsatta i högst utsträckning.

Bedrägerierna är svåra att mäta

Det finns ett mörkertal i statistiken för anmälda bedrägerier, både vid försöksbrott och fullbordade brott. Försöksbrotten är svåra att identifiera och fullbordade brott, framförallt omfattande, stannar internt.

Både hos drabbade företag och inom rättsväsendet finns en oklarhet i vilka typer av bedrägerier som skall anmälas, och även hur de sedan skall utredas.

Exempelvis sker regelbundet utskick av e-post som skulle kunna klassas som nätfiske (phishing) men som istället filtreras bort och slängs.

Vissa bedrägeriers komplexitet gör också att den drabbade inte alltid kan avgöra vad som är vad, särskilt för hybridbrott där flera metoder har använts i kombination.

Ytterligare en faktor är att drabbade känner stor skuld för det inträffade.

”Vi ser en mycket större frekvens bedrägerier generellt. Allt från beställningar av presentkort till falska fakturor. Vid de tillfällen där det går att utföra bedrägerier så gör man det.”

Vd inom sällanköpsvaruhandeln

SAMTLIGA

av de stora företagen i undersökningen har mottagit en bedräglig faktura.

Vd-bedrägerier och fakturabedrägerier
Hur går ett bedrägeri till?

I intervjuer med ett urval av företag som varit i kontakt med Svensk Handels Varningslista framkommer att vd-bedrägerier är ett vanligt förekommande tillvägagångssätt.

Medarbetaren är ingången

Vd-bedrägerier är en i huvudsak e-postbaserad metod där bedragaren utger sig för att vara en individ inom den egna organisationen eller en etablerad leverantör.

Redan vid första kontakt kan en påhittad tidigare dialog förekomma i e-postmeddelandet, där bedragaren använder inslag av stress och tidsbrist för att få till stånd en betalning.

De angrepp som kan klassas som vd-bedrägerier är olika sofistikerade. Vissa föregås av faktiska dataintrång, medan andra använder läckt eller i övrigt publik information för att inge trovärdighet.

Hur ska man hantera ett fakturabedrägeri?

Den som blir utsatt för ett vd-bedrägeri märker inte alltid att mailadressen från chef eller vd är felaktig, vilket gör det extra viktigt att förhålla sig till rutiner. Att granska hur mailet är skrivet och om det följer samma språk och form som avsändaren vanligtvis använder kan räcka långt. Fakturans innehåll kan också avslöja om det är ett bedrägeri eller ej. Detta gör det viktigt att verifiera innehållet, särskilt om fakturan inte kommit via det ordinarie systemet.

”Vi betalade aldrig. Det var ett misstänkt stort belopp på flera hundra tusen när vi oftast betalar fakturor på cirka 50 000.”

Bedrägeriutsatt inom branschorganisation

”Efter att ha drabbats av att någon utger sig för att vara jag i mail, har jag en ständig oro för att någon ska öppna en skadlig fil.”

Chef på litet företag inom sällanköpsvaruhandeln

Interna rutiner avgörande

Det är viktigt att företag förstår vilka typer av digitala brott och bedrägerier de riskerar att utsättas för vilket ställer krav på både rutiner och aktiv riskhantering.

Den mänskliga faktorn alltmer avgörande vid digitala brott

Social manipulation – den mänskliga faktorn

Social manipulation är en metod för att vilseleda en individ att omedvetet eller medvetet utföra en viss handling. Hotaktörer riktar ofta in sig på anställda som har höga administrativa IT-behörigheter, exempelvis IT-ansvariga. Den tekniska utvecklingen gör det lättare för hotaktörer att hitta ”rätt” måltavlor att utsätta för digitala brott. Det är därför mycket viktigt för företagen att öka kunskapen kring social manipulation i digitala miljöer.

Deepfakes och AI som verktyg

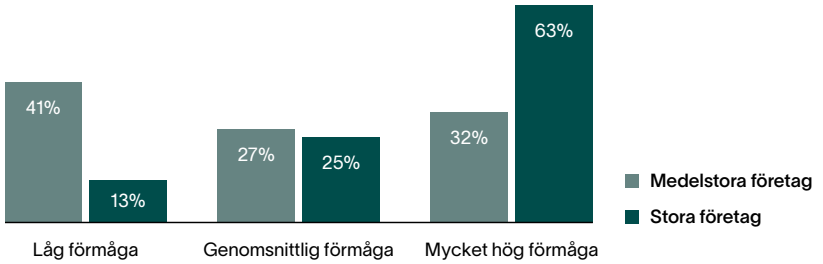
Deepfake är en AI-baserad teknik som kan användas till bedrägerier med inslag av social manipulation. Bedragaren antar en kapad eller fiktiv identitet, till exempel genom imitation av ett ansikte eller en röst, och uppmanar den drabbade att dela information eller utföra betalningar.

Experterna nämner att social manipulation förmodligen kommer att öka i och med den nya tekniken och att det kommer bli viktigare att förhålla sig skeptisk till exempelvis nya kontakter – till och med i röst- och videosamtal. Än viktigare är tydliga rutiner för även befintliga kontakter.

Förmåga att hantera insiderbrott

Fråga: Hur är er förmåga att hantera Insiderbrott?

Bas: Medelstora företag, webbenkät N=85, Stora företag, intervjuer N=8



Insiderbrott - ett växande hot

Större företag upplever att de har en hög förmåga att hantera insiderbrott, medan många medelstora företag upplever att de har en låg förmåga.

Enligt bland annat Truesec är frågan om säkerhetsfrågor inom företag viktig och ett område som är näraliggande exempelvis arbetsmiljöfrågor och företagskultur.

Säkerhetsgranskning av anställda blir allt viktigare både under och efter rekrytering, speciellt för tjänster som kommer i kontakt med känslig information.

Falska webbsidor orsakar förtroendeskada

Ett stort problem

Falska webbsidor och/eller domänadresser skapar problem både för konsumenter och företag. Metoderna är många.

Beroende på syfte kan besökaren av webbsidan förmås utföra olika handlingar så som att ovetandes ladda ner skadlig kod, beställa varor som inte existerar, beställa piratkopior, eller mata in känslig information.

Själva domänadresserna som leder till hemsidan kan utnyttjas till bedragarnas fördel genom att registrera dem med innehållandes vissa ord eller använda en struktur som vid första anblick ser ut att vara en seriös verksamhet.

Ibland används flera domänadresser i en kedja av vidarebefordringar där den första domänen ser mer trovärdig ut än slutmålet. Kedjan börjar då med ett SMS.

Varumärkesintrång skadar förtroendet för e-handeln

Falska webbsidor inom e-handel är ibland mycket skickligt utformade, vilket riskerar att ha en negativ påverkan på förtroendet för varumärket som drabbas. I grunden utgör sidorna varumärkesintrång, men syftet är i första hand riktat mot att skada konsumenten.

Problemet är mycket svårt att komma åt för de drabbade företagen och närmast omöjligt att skydda sig från.

Rättsväsendet har liknande utmaningar. De falska webbsidorna är medvetet registrerade med anonyma eller dolda uppgifter, de olika delarna sprids över landsgränser och tekniska detaljer bakom både domänadress och innehåll ändras regelbundet vilket gör utredning och lagföring mycket svår.

Köp på falska webbsidor en ingång till stöld av personuppgifter

En falsk webbsida kan ha flera syften. Sidor som i huvudsak säljer piratkopior kan samtidigt samla in dina betaluppgifter, vilket över tid ger värdefulla register av kortuppgifter att antingen använda eller sälja vidare.

Som psykologisk påtryckning lockar dessa hemsidor ofta med ovanligt bra priser. Det är svårt för konsumenter att kritiskt granska sidan vid köptillfället.

88%

av de stora företagen har blivit utsatta för att en falsk webbsida har skapats i deras namn.

”Kunder hör av sig om att de inte fått sina paket levererade. För oss är problemet ofta att hemsidan de beställt ifrån inte är vår. Då har kunden beställt från en butik som är väldigt lik vår webbshop. Detta är en konsekvens av SEO-poisoning, där falska hemsidor köper annonser i sökmotorer och sociala medier, där nya domäner skapas med namn som liknar riktiga varumärken.”

Säkerhetsansvarig inom sällanköpsvaruhandel

”Vi märker att falska webbsidor blir allt vanligare och att fler konsumenter råkar ut för det. Under 2024 har andelen anmälningar kring ämnet ökat. Troligtvis kommer problemet att fortsätta växa.”

Lotta Mauritzson, Polisens nationella bedrägericentrum

04.

Från digital utveckling till fokus på säkerhet

Företagens beredskap måste stärkas

Huvudinsikter
Företagens beredskap måste stärkas

01.

Mindre företag saknar god digital säkerhet

Små- och medelstora företag saknar god digital säkerhet, trots att handeln är en av de mest utsatta branscherna under de senaste åren. Små- och medelstora företag saknar såväl någon som ansvarar för den digitala säkerheten samt förståelsen för vad som kan hända vid en incident.

02.

Företagen behöver och vill öka sin egen medvetenhet

Företagen saknar idag tillräckligt med information om vilka de digitala riskerna är och hur de behöver skydda sig.

Företagen ser dock vikten av att informera och utbilda sin personal för att minska riskerna.

03.

Polis och andra myndigheter behöver samarbeta mer

Det finns en otydlighet bland företagen gällande när och hur man ska kontakta polisen och vad polisen kan göra i händelse av ett digitalt brott eller försök till brott.

Företagen inom handeln efterfrågar mer information och ett närmare samarbete med olika myndigheter för att kunna komma åt den digitala brottslighet som hotar branschen.

Majoriteten av företagen saknar god digital säkerhet

Trots tidigare attacker saknar företagen en god digital säkerhet

Under de senaste åren har ett flertal företag inom handeln utsatts för olika typer av digitala attacker. Detta har inneburit stora konsekvenser för företagens verksamheter. Trots att erfarenheterna från dessa attacker borde ha fått företagen att förstå allvaret med digitala brott, saknar de små och medelstora företagen fortfarande förmågan och rutinerna som krävs för att kunna hantera sin digitala säkerhet. Detta är något som kan få kostsamma konsekvenser inte bara för företagens intäkter utan även för samhället.

Digital säkerhet behöver tas på lika stort allvar som fysisk

De intervjuade säkerhetscheferna lyfter att grunden för en god digital säkerhet ligger i att prioritera digital säkerhet på samma sätt som fysisk. Få företag saknar en plan och en ansvarig för fysisk säkerhet medan en stor andel, cirka 60 procent, av de medelstora företagen idag saknar en ansvarig för den digitala säkerheten. Detta minskar möjligheten att ta frågan på allvar och kunna skydda sig mot digitala brott.

De stora företagen har en god digital säkerhet

De stora företagen som medverkat i undersökningen har samtliga uppgett att de har en god förmåga att upptäcka intrång snabbt, liksom rutiner och policys för vad som exponeras och kunskap om hur de ska hantera misstankar om brott. I intervjuerna med säkerhetscheferna framkommer däremot att det finns en otydlighet kring när polis ska kontaktas i samband med digitala brott. Det finns ett behov av att förenkla samarbetet med polisen och andra myndigheter. Till skillnad från de mindre företagen i undersökningen har de stora företagen en organisation där flertalet personer jobbar dedikerat med digital säkerhet, vilket möjliggör en annan typ av trygghet och reaktionshastighet. Något som också krävs med tanke på de mer komplexa system företagen har och den hotbild som finns kring dessa.

49%

av de medelstora företagen saknar förmåga att upptäcka intrång snabbt.

60%

av de medelstora företagen vet inte när de ska kontakta polisen vid digitala brott.

Vilka av följande förmågor har ert företag?

Andel av företagen som har följande förmågor	Små företag	Medelstora företag	Stora företag
Förmåga att upptäcka intrång snabbt	61%	51%	100%
Inhyrd expertis vid akuta kurser	55%	46%	75%
Rutiner för vad som exponeras mot internet	44%	51%	100%
Policy för vad som ska göras vid misstanke om brott	61%	54%	100%
Dedikerat ansvarig för digital säkerhet	52%	41%	100%
Kännedom om när polis ska kontaktas	59%	40%	88%
Plan för incidenthantering	52%	39%	88%

Satsningar på information och utbildning

Att informera personalen ses som det viktigaste för att öka säkerheten

För att stärka sin förmåga satsar många företag på information riktad till personalen om vad som kan hända och hur de kan skydda sig mot olika typer av digitala hot.

Något som också lyfts i expertintervjuerna är att en ökad medvetenhet hos medarbetarna uppges minska risken för social manipulation.

Det är viktigt att löpande informera personalen om olika kända angreppsmetoder och att de hela tiden utvecklas, där förebyggande åtgärder anpassas efter varje typ av bedrägeririsk verksamheten kan drabbas av.

72%

av de medelstora företagen kommer framåt att satsa på information till personal.

"Vi jobbar mycket med intern information och försöker få till mer utbildningar. Det är det jag ser som viktigast, där måste vi lägga mest fokus."

Säkerhetschef inom sällanköpsvaruhandeln

"Den viktigaste frågan i vår organisation är att vi ökat riskmedvetenheten. Vi kan inte förhindra allt utan vi måste lära oss och vara kritiska till de mail som dyker upp i mailkorgen."

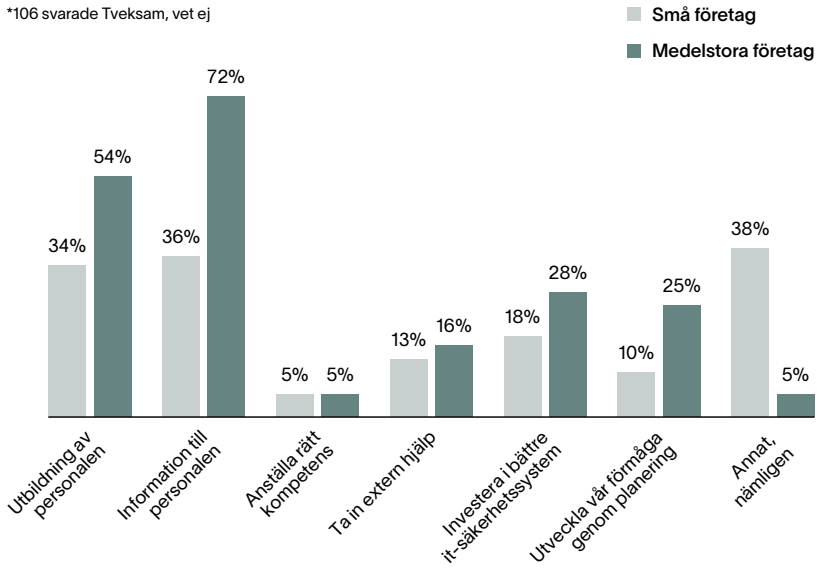
Vd inom sällanköpsvaruhandeln

Information och utbildning är de främsta satsningsområdena

Fråga: Vad kommer ni att satsa på för att öka den digitala säkerheten under de kommande åren?*

Bas: Små företag N=118, Medelstora företag N=61

*106 svarade Tveksam, vet ej



Företagen vet inte vad de ska göra om något händer

Majoriteten av de små och medelstora företagen saknar en plan för incidenthantering

Att planera och öva på vem som ska göra vad om något händer är en viktig del av den grundläggande säkerheten enligt experterna i studien. Undersökningen visar dock att många av de små och medelstora företagen idag saknar en tydlig plan för incidenthantering

Många saknar alternativa betalsystem

Även om de senaste årens attacker som har drabbat flertalet företag inom handeln har visat på vikten av att ha flera olika betalsystem, saknar många av företagen just detta. Enligt webbundersökningen saknar nästan hälften av de medelstora företagen fortfarande alternativa betalsystem.

45%

av de medelstora företagen saknar ett alternativt betalsystem.

61%

av de medelstora företagen saknar en plan för incidenthantering.

”Det viktigaste är att upprätthålla den ordinarie verksamheten. Likt en brandövning har vi nödövningar som en intern säkerhetsrutin. En typ av nödövning är att personalen får jobba utan tillgång till systemen, och då får öva på att exempelvis styra lagret manuellt.”

Säkerhetschef inom dagligvaruhandeln

86%

av de medelstora företagen uppger att de saknar tillräcklig information för att kunna skydda sig.

”Ubikey, Authenticator och flera betalningslösningar minskar risken för att bli attackerad, men man blir inte immun bara för att man har infört sådana åtgärder.”

Expert inom digital säkerhet

Utmaning att polisanmäla

Företagen vet inte när och hur de ska kontakta polisen

En stor andel av företagen uppger att de inte vet när de ska polisanmäla ett intrång eller olika typer av digitala brott. Även bland de stora företagen i undersökningen framkommer det att det är otydligt när och hur man ska göra en polisanmälan och på vilket sätt polisen kan hjälpa till när något hänt. Förståelsen för och samarbetet med polisen upplevs som tydligare när det gäller andra typer av brott, exempelvis stölder i butik. Idag uppger 64 procent av de medelstora företagen att de inte anmält de digitala brott som de har utsatts för men nästan lika många, 57 procent, önskade att det skulle vara enklare att komma i kontakt med polisen.

Låg anmälningsbenägenhet

En anledning till att så få företag anmäler de brott som de har utsatts för är bilden av att anmälningarna läggs ner trots att företagen upplever att det finns bevis för det som inträffat. Enligt undersökningen uppger 78 procent av de medelstora företagen som har anmält en incident att ärendet lades ner. Detta påverkar sannolikt anmälningsbenägenheten vid framtida incidenter.

En annan anledning som framkommer i de öppna svaren i undersökningen är det faktum att företagen är rädda för de aktörer som ligger bakom brotten. Vissa av företagen vittnar om att de har blivit utsatta för hot av kriminella gäng om de valt att polisanmäla ett digitalt brott.

Enligt företagen har viljan att anmäla digitala brott minskat.

”Vi blev lurade på cirka 500 000 kronor och polisanmälde. Det fanns bevis men trots detta lades ärendet ner. I ett andra skede blev vi hotade av gängkriminella, men inte heller det togs upp av polisen.”

Svarande inom sällanköpsvaruhandeln

”Man hade kunnat drömma om en digital insatsstyrka, men det finns inte ännu.”

Svarande inom sällanköpsvaruhandeln

”Det blir irrelevant när man är på utredningsstadiet för då har det redan hänt. Det hade varit mer relevant att få proaktiv hjälp från polisen: det här skulle kunna hända.”

Vd inom sällanköpsvaruhandeln

64%

av de medelstora företagen anmälde inte de digitala brott som de utsatts för.

60%

av de medelstora företagen vet inte när de ska kontakta polisen gällande digitala brott.

57%

av de medelstora företagen vill att det ska vara enklare att komma i kontakt med polisen.

Handeln efterlyser samarbete med myndigheterna

Handeln eftersöker ett närmare samarbete mellan näringsliv och myndigheter

Handeln är en central del av Sveriges ekonomi och en av landets viktigaste branscher. De hot som handeln utsätts för är desamma som Sverige som land utsätts för och för att kunna agera eftersöker handeln ett närmre samarbete mellan näringsliv och myndigheter. För att kunna agera gentemot den digitala brottsligheten vill handeln:

- Dela information om aktuella hotbilder mot Sverige, svenska företag och organisationer.
- Samverka och dela operativ information om pågående händelser.
- Gemensamt identifiera och dela lärdomar om de kriminella hotaktörernas angreppssätt och hur man bäst skyddar sig mot dessa.

Lagar och regler efterfrågas

Små och medelstora företag uppger i undersökningen att tydligare lagar och regler skulle leda till en bättre digital säkerhet.

Rädslan för att bli utsatt minskar möjligheten att förstå företagens behov

Under rapportens framtagande blev det tydligt att det finns en rädsla hos de deltagande företagen att ställa upp på intervjuer. Exempelvis ställdes frågan om vem som genomför undersökningen, om det verkligen var på uppdrag av Svensk Handel eller om undersökningen i sig är ett bedrägeri.

Rädslan hos företagen gör det svårt att kartlägga utsattheten och därmed även möjligheten att hitta gemensamma åtgärder för att motarbeta den digitala brottsligheten.

I vilken mån instämmer ni i följande påståenden om digital brottslighet?

Andelen företag som instämmer i ganska hög och hög grad	Små företag	Medelstora företag	Stora företag
Det krävs mer samverkan mellan näringsliv och myndigheter för att lösa den digitala brottsligheten	70%	75%	88%
Tydligare lagar och regler skulle göra den digitala säkerheten bättre	63%	52%	38%
Vi får tillräckligt med stöd från polisen vid digitala brott	13%	12%	74%
Det borde vara enklare att få kontakt med polisen vid digitala brott	40%	57%	63%

”Vi eftersöker mer samverkan mellan myndigheter och näringsliv. Tanken när NCSC startades var att Sverige skulle få en expertmyndighet kring digital brottslighet. Vi får se vad som händer nu när FRA har tagit över ledarskapet.”

Svarande inom dagligvaruhandeln

”Det krävs god informationsdelning mellan privata aktörer och myndigheter för att stärka Sveriges cyberresiliens.”

Säkerhetschef inom dagligvaruhandeln

”Det största digitala hotet i handeln idag är AI. Detta påverkar redan förtroendet mellan människor, då till exempel deepfakes och AI-röster blir mer trovärdiga. Innan kunde man se stavfel i phishingmailen, men nu är de skickligt utförda.”

Säkerhetschef inom sällanköpsvaruhandeln

Intervju med Patricia Lindén
Stadium lyfter vikten av att förbereda sig

Stadium drabbades i januari 2024 av en ransomware-attack som IT-leverantören Tietoevry utsattes för. Utifrån den erfarenheten understryker Stadiums IT Security Manager Patricia Lindén vikten av att vara förberedd inom företaget när en IT-attack sker, oavsett hur bra det tekniska skyddet är. Att ha en krishanteringsplan gjorde det lättare för Stadium att hantera situationen.

Vad hände när ni drabbades av intrånget?

Det första tecknet var att våra system började indikera ett onormalt beteende men just där och då förstod vi inte omfattningen. Först när vi pratade med leverantören på lördagsmorgonen kunde de bekräfta att de hade utsatts för en säkerhetsincident och därför stängt ner vår tillgänglighet till data i det datacenter som var drabbat. Vi startade upp vår krisledning omgående med första mötet innan frukost, första av cirka trettiofem under en period på cirka tre veckor. Senare på lördagen fick vi reda på att det rörde sig om ransomeware-attack.

Vad blev konsekvenserna för Stadium?

Situationen varade i ungefär fem veckor, däremot var vår e-handel nere i en vecka, vilket gjorde att vi inte kunde komma åt vårt affärssystem. Våra fysiska butiker kunde vara öppna, men i och med att vi inte hade tillgång till affärssystemet fick vi ingen överblick på lagerstatus.

Vi fick också ägna ett stort fokus på intern och extern kommunikation för att mildra oro, i och med att varumärket kan påverkas negativt av den här typen av händelser.

> Frågan som företag bör ställa sig är 'hur skyddar vi det som är viktigast först?' genom att undersöka vad som skulle göra mest ont om man förlorade det.

Det innebar i sin tur också mycket arbete för kundtjänst och andra delar av verksamheten, som en följd av att det vanliga arbetet skakades.

Hur gick ni till väga för att hantera attacken?

I och med vårt förebyggande arbete med digital säkerhet följde vi vår krishanteringsplan. Efter attacken jobbade vi konstant i krisledningen i tre veckors tid innan vi var tillbaka till någon form av normalitet.

Något som är positivt är den ökade medvetenheten om vikten av digital säkerhet och att vi kommer vara ännu mer förberedda nästa gång.

Vi polisanmälde attacken i Svensk Handels app, i ett ärende tillsammans med vår IT-leverantör. Det tog däremot flera månader innan vi fick bekräftat att polisen arbetade med ärendet, och det är fortfarande öppet.

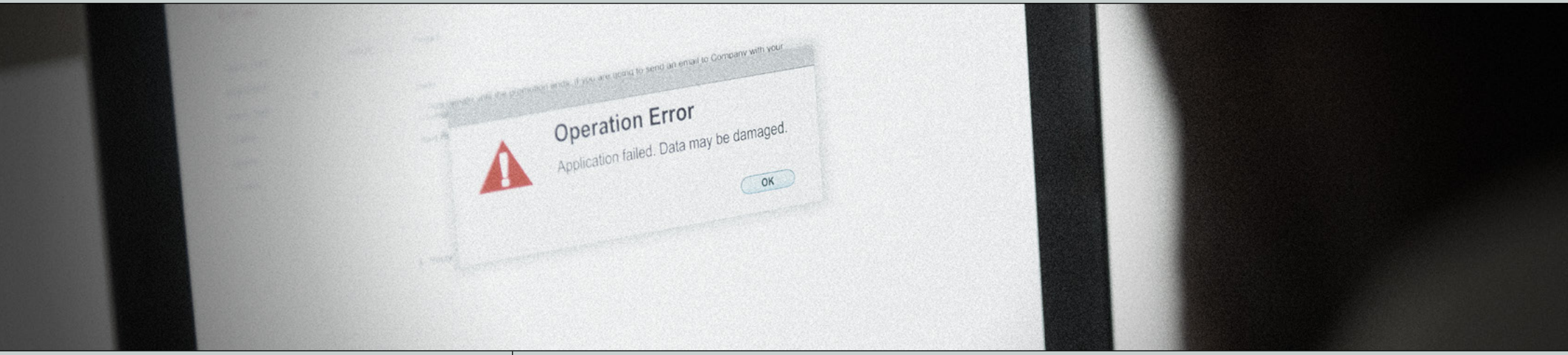
Hur utsatt är handeln för digitala brott?

Handelns utmaningar är lika stora som för resten av samhället i och med det osäkra omvärldsläget. Det gäller att vara påläst kring digital brottslighet, och att ligga steget före. Att identifiera var saker och ting gör mest skada inom verksamheten, och att ha en plan för hur man gör när ett intrång sker är viktigt för att vara förberedd – oavsett om man har säkrat sin digitala miljö eller ej.

05.

Slutord

Slutord från Svensk Handel



Svensk Handel har tagit fram denna rapport i syfte att lyfta problematiken kring digital brottslighet och dess påverkan på svenska företag.

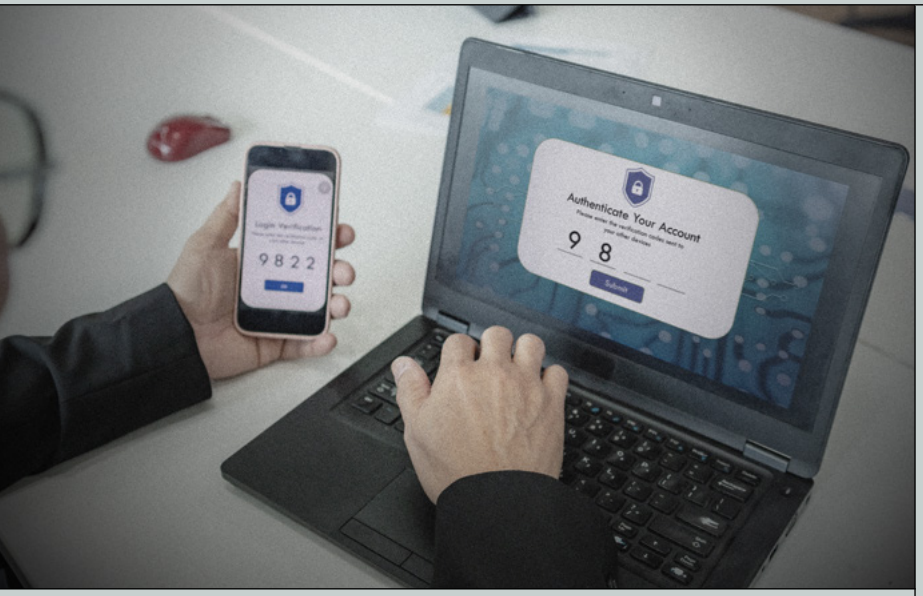
Rapporten belyser också vad handelsföretagen själva kan göra för att förebygga risken att utsättas. Det är viktigare än någonsin att säkerställa god beredskap och riskmedvetenhet.

Förhoppningen är att de svar och vittnesmål som utgör rapporten kan utgöra ett bra underlag för såväl beslutsfattare som opinionsbildare.

Låt oss tillsammans få frågan om den digitala brottsligheten högt upp på agendan!

DEN DIGITALA BROTTSLIGHETEN ÄR HÄR FÖR ATT STANNA

Så kan företagens digitala säkerhet öka



Om du skulle drabbas, här är åtgärderna när digital brottslighet är ett faktum:

- Om du inte har kompentensen internt, ta hjälp utifrån direkt.
- Polisanmäl händelsen i ett tidigt skede.
- Isolera attacken genom att stänga av internetåtkomst för de smittade enheterna och/eller de påverkade nätverken.
- Spara undan alla krypterade/påverkade system, så att dessa inte förstörs i återställningsprocessen.
- Säkra kritiska loggar. Exempelvis brandvägg och VPN.
- Utred hur de tog sig in, vilka bakdörrar som har placerats och vilken data som har läckt.
- Kommunicera inte med hotaktörer.
- Betala inte!

Utbildning och medvetenhet

- Se till att alla anställda är medvetna om riskerna med digitala brott.
- Ordna regelbundna utbildningar och uppdateringar om cybersäkerhet.
- Säkra en alternativ kontaktväg.

Uppdatera och säkra system

- Se till att datorer, servrar, nätverksutrustning och programvara är uppdaterade med de senaste säkerhetsuppdateringarna.
- Använd en pålitlig och uppdaterad antivirus-programvara och brandvägg för att förhindra intrång.
- Arbeta kontinuerligt med att upptäcka, prioritera och fixa säkerhetsbrister.
- Säkra högpriviligierade konton och se till att systemadministratörer har olika konton för olika system (AD Tiering).

Säkerhetskopiering av data

- Utför regelbundna och automatiska säkerhets-kopieringar av företagets viktiga data.
- Testa regelbundet återställningsprocessen på flera system parallellt.
- Lagra säkerhetskopior på extern plats. Exempelvis med separat Active Directory, nätverk, och på separat hårdvara.

Läs mer på www.svenskhandel.se/sakerhetscenter

Övervakning

- Övervaka IT-systemen kontinuerligt för att upptäcka pågående attacker tidigt.
- Tänk på att många attacker sker utanför kontorstid.
- Se över vilka loggar som sparas och hur länge dessa sparas.

Användning av säkra lösenord

- Kräv starka och unika lösenord för alla systemadministratörer och användare.
- Implementera tvåfaktorautentisering för extra säkerhet.

Nätverkssäkerhet

- Konfigurera brandväggar och övervaka nätverks-trafiken för att upptäcka ovanlig aktivitet.
- Begränsa åtkomsten till nätverket baserat på behov.

Incidenthantering och beredskapsplan

- Utveckla en tydlig plan för hur företaget ska hantera en ransomware-attack.
- Öva på och uppdatera beredskapsplanen regelbundet.
- Se över mandat för de som leder incidenten.
- Planera för kriskommunikation både internt och externt.

Svensk Handel