Är det it-säkert?

En undersökning om företagares utsatthet för it-relaterade brott, kontakter med polisen och åtgärder för att skydda företaget mot digital brottslighet

Oktober 2022

företagarna

INNEHÅLL

Rapportens författare
Olivia Dahlman

Policyansvarig
Pontus Lindström

SAMMANFATTANDE RESULTAT

FÖRETAGENS UTSATTHET FÖR IT-RELATERAD BROTTSLIGHET

- 76 procent av Sveriges företagare har blivit utsatta för någon form av it-relaterad brottslighet vid minst ett tillfälle under det senaste året.
- Den vanligaste formen av it-brott som drabbar företagare är phishing (nätfiske), där 55 procent av de tillfrågade svarade att de någon gång under det senaste året har mottagit e-post från en avsändare som utgav sig för att vara någon annan i syftet att få tillgång till personliga uppgifter.
- 31 procent svarade att de i mycket hög eller ganska hög utsträckning oroar sig för att deras företag ska bli utsatt för it-relaterade brott.

ANMÄLNINGSBENÄGENHETEN BLAND SVERIGES FÖRETAGARE

- Endast 13 procent av de företagare som någon gång under det senaste året blivit utsatt för it-relaterad brottslighet valde att polisanmäla händelsen/händelserna. Den främsta anledningen till att många låter bli att göra det är att man inte ser någon poäng med att anmäla.
- Av de företagare som gjorde en polisanmälan uppgav 69 procent att ärendet lades ned. Endast 1 procent av polisanmälningarna resulterade i åtal.
- 57 procent av företagarna svarade att de inte alls eller enbart till viss del känner ett starkt förtroende för polisens förmåga att utreda och lösa it-relaterade brott.

FÖRETAGENS IT-SÄKERHET

- De vanligaste säkerhetsåtgärderna bland Sveriges företagare är en användning av antivirusprogram och/eller brandväggar (78 procent), följt av molnlagring av viktig information (54 procent) och digital brevlåda för myndighetspost (48 procent).
- 83 procent av de tillfrågade svarade att det saknas en plan för incidenthantering på deras företag. 78 procent saknar en utarbetad policy för vad som ska göras vid minsta misstanke om brott från ett inkommande e-post, sms eller telefonsamtal.

MEST EFTERFRÅGADE ÅTGÄRDER

- Nästan hälften av företagarna instämde helt i påståendet att it-säkerhet bör prioriteras högre inom politiken.
- 59 procent höll helt eller till stor del med om att informations- och kunskapsutbytet mellan företag och myndigheter när det gäller it-säkerhet bör förbättras.
- Var tredje företagare svarade Vet ej när de ombads ta ställning till huruvida de upplever att det finns god tillgång till stöd, verktyg och/eller information från myndigheter när det gäller it-säkerhetsfrågor.

OM UNDERSÖKNINGEN

Denna rapport bygger på en webbaserad enkätundersökning där Företagarnas medlemspanel har fått besvara och ta ställning till en mängd olika frågor och påståenden som rör it-brottslighet och digital säkerhet. Enkäten genomfördes mellan 21 september – 7 oktober 2022, där antalet respondenter var 1 216 företagare med bred representation sett till olika branscher, företagsstorlekar och geografisk hemvist. Svarens fördelning har korrigerats för att efterlikna den nationella företagarstrukturen, med hjälp av en modell baserad på SCB:s statistik över antal företagare i Sverige. Konkret görs detta genom att korrigerande vikter räknas fram för olika företagsstorlekar (antal anställda), kön, ålder och bransch.

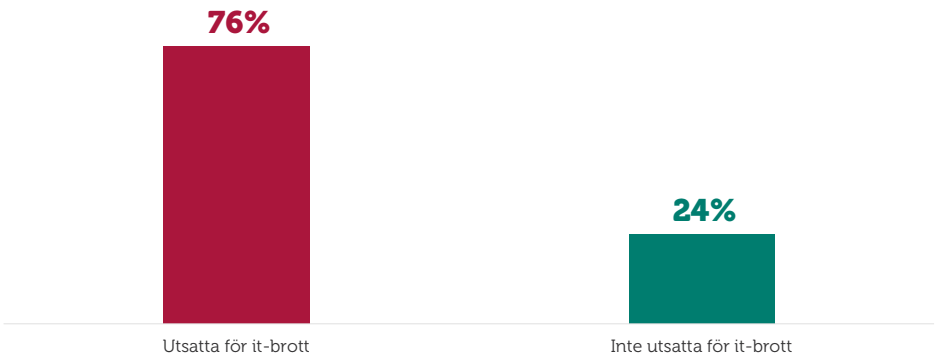
Syftet med denna undersökning är att belysa i vilken omfattning mindre företag i Sverige drabbas av it-brott och på vilket sätt den sortens utsatthet i sin tur kan påverka både företagare och anställda, såväl som samhället i stort. Genom att undersöka företagarnas beteenden på internet såväl som inställningar till området it-säkerhet hoppas enkätresultaten också kasta ljus på potentiella förbättringsområden i det brottsförebyggande arbetet, både på organisatorisk och nationell nivå. Detta görs med ambitionen att öka medvetenheten och kunskapen kring it-säkerhetsfrågor ur ett företagarperspektiv, för att på så sätt stärka förmågan att skydda det egna företaget mot digitala brott och bedrägeriförsök.

FÖRETAGENS UTSATTHET FÖR IT-RELATERAD BROTTSLIGHET

It-relaterad brottslighet är ett begrepp som omfattar en mängd olika brottstyper, med den gemensamma nämnaren att de utförs med hjälp av någon slags it-teknik. Ofta handlar det om phishing (nätfiske) där det på olika sätt ”fiskas” efter viktig information eller pengar, till exempel genom e-post eller sms som ser ut att komma från en trovärdig avsändare och där mottagaren uppmanas att klicka på en länk eller på annat sätt uppge sina person- och kontouppgifter. Andra exempel på it-brott är bluffakturor, dataintrång, samt olika slags virus och trojaner. En särskild form av virus som på senare tid har blivit allt vanligare är ransomware, även kallat utpressningsvirus, som låser datorer och mobiler och/eller krypterar filer och ”håller dem gisslan” i utbyte mot en lösensumma.

Årets enkätresultat visar att hela 76 procent av respondenterna har blivit utsatta för någon form av it-relaterad brottslighet under det senaste året (se figur 1). Utöver att vara en alarmerande hög siffra tyder det också på en stor ökning i utsatthet bland företagare jämfört med tidigare år, där det bland annat i en undersökning från 2019[1] enbart var 29 procent som svarade Ja på frågan om de någon gång under de senaste två åren blivit utsatta för it-brott.

Figur 1 Andelen företagare som har blivit utsatta för ett it-relaterat brott under det senaste året



Bas: Samtliga företag, n=1216.

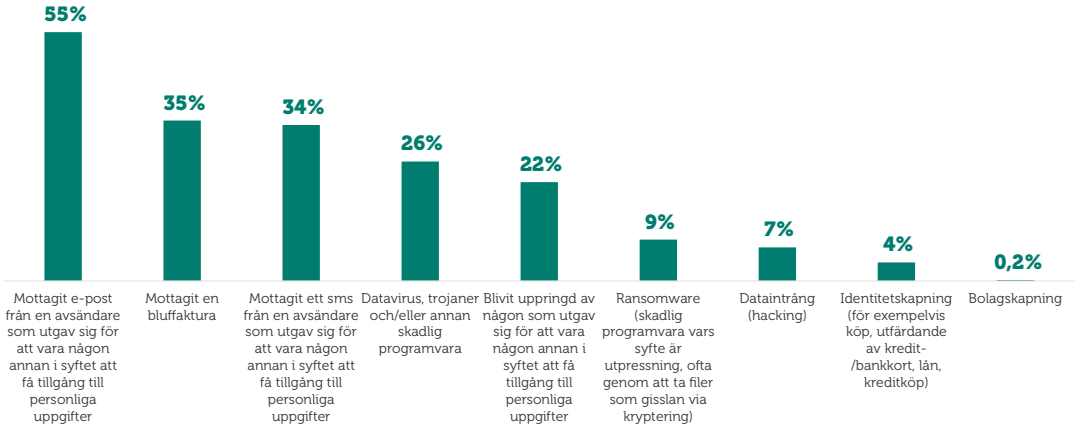
En möjlig förklaring till denna ökning kan vara att svarsalternativen i årets undersökning är formulerade på ett sätt som även fångar upp mer vardagliga former av it-brott som inte alltid uppfattas som just brottslighet, däribland phishingförsök via e-post, sms eller telefonsamtal. Detta tyder på att utsattheten kan vara mycket större än vad man tidigare har trott, vilket betonar vikten av att utöka medvetenheten och kunskapen kring de många olika former av it-brott som existerar.

1 https://www.foretagarna.se/nyheter/riks/2019/oktober/manga-saknar-verktyg-for-att-skydda-sig/

De vanligaste formerna av it-brott

Årets undersökning visar att phishing utgör den vanligaste formen av it-brott som drabbar Sveriges företagare (se figur 2). Av samtliga respondenter uppgav 55 procent att de vid minst ett tillfälle hade mottagit e-post från en avsändare som utgett sig för att vara någon annan i syfte att få tillgång till personliga uppgifter. Av enkätresultaten framgår det också att phishingförsök via e-post är betydligt vanligare än via sms eller telefonsamtal, som jämförelsevis hade drabbat 34 respektive 22 procent av de tillfrågade.

Figur 2 Andel som svarat Ja på frågan ”Har du som företagare/ditt företag blivit utsatt för något eller några av följande exempel på it-relaterade brott under det senaste året?”



Bas: Samtliga företag, n=1216

35 procent svarade också att de någon gång under det senaste året mottagit en bluffaktura. Här handlar det om att ha mottagit en digital eller fysisk faktura med uppmaningar om att betala för en tjänst och/eller produkt som inte har beställts eller avtalats om.

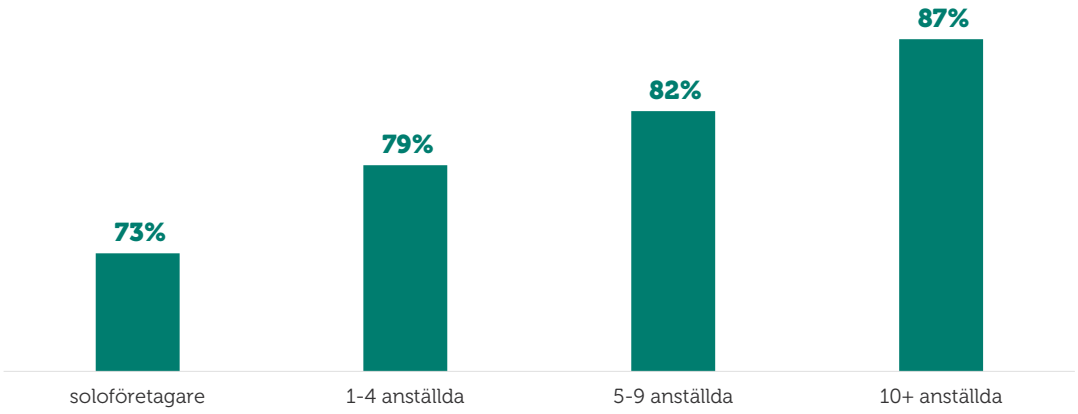
26 procent uppgav att de blivit utsatta för skadlig programvara i form av datavirus, trojaner eller liknande. När det gäller specifikt ransomware ligger motsvarande siffra på nio procent.

Sju procent av enkätens respondenter uppgav att de blivit utsatta för dataintrång, följt av fyra procent som hade drabbats av någon form av identitetskapning. Av de mindre vanliga formerna av it-brott som drabbar företagare finns även bolagskapning, där enbart 0,2 procent svarade att de hade blivit utsatta under det senaste året.

Skillnader i utsatthet beroende på företagsstorlek

Som visas i figur 3 utsätts företag med anställda för it-brott i betydligt högre utsträckning än soloföretagare.

Figur 3 Andelen företagare som har blivit utsatta för it-brott, utifrån företagets storlek.



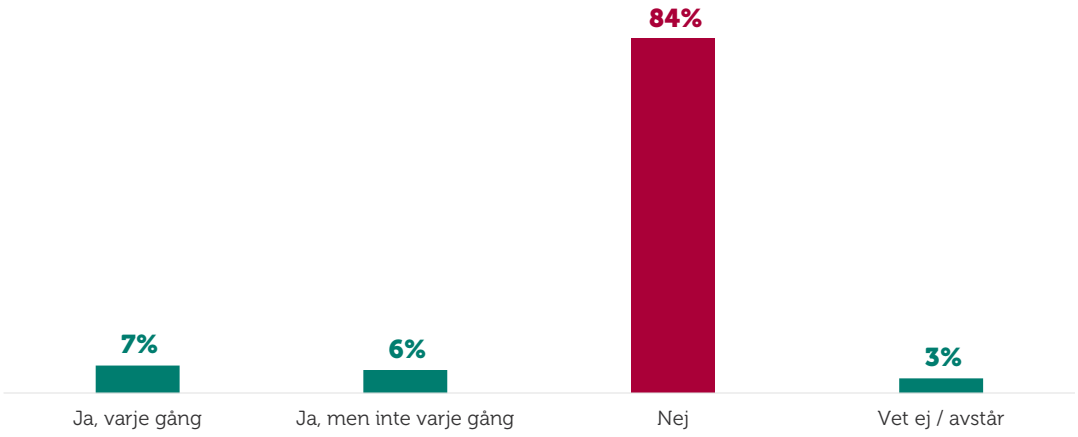
Bas: Samtliga företag, n=1216. Notera att y-axeln är bruten.

Att 87 procent av de respondenter som någon gång under det senaste året har blivit utsatta för it-brott driver ett företag med mer än tio anställda, jämfört med 73 procent av soloföretagare, visar att sambandet är starkt mellan företagets storlek och dess utsatthet för it-relaterad brottslighet. En förklaring till detta skulle exempelvis kunna vara att större företag utgör mer eftertraktade, lönsamma och attraktiva offer på grund av att de i många fall omsätter mer än mindre företag. Att ett större företag ofta är mer synligt, både fysiskt och digitalt, kan också vara något som drar mer uppmärksamhet och lockar till sig flera förövare. Ytterligare en förklaring är givetvis också att antalet personer som riskerar att till exempel klicka på en skadlig länk är fler om det finns anställda i bolaget. Det gäller särskilt under de tider på året då företag säsongsanställer personal som kanske inte alltid känner till företagets säkerhetsrutiner.

ANMÄLNINGSBENÄGENHETEN BLAND SVERIGES FÖRETAGARE

En överlägsen majoritet (84 procent) av de företagare som i årets undersökning uppgav att de hade blivit utsatta för någon form av it-relaterad brottslighet under det senaste året valde att inte polisanmäla händelsen/händelserna (se figur 4). Detta är en bekymmersam siffra som har legat på en hög nivå även under tidigare år i fråga om företagares anmälningsbenägenhet. Det bör dock noteras att det i tidigare undersökningar ställdes frågor som gällde alla typer av brott, och inte enbart it-relaterade sådana.

Figur 4 ”Polisanmälde du händelsen/händelserna?”

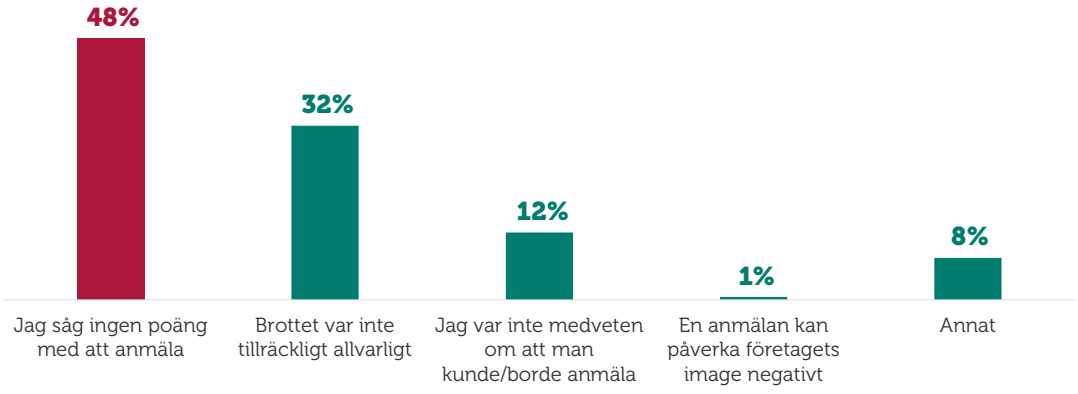


Bas: Företagare utsatte för it-brott, n=966

Varför anmäls inte brotten?

48 procent av de företagare som avstått från att polisanmäla svarar att den främsta anledningen var att man inte ser någon poäng med det. Som visas i figur 5 var det också drygt en tredjedel av respondenterna (32 procent) som inte uppfattade det it-brott som de blivit utsatta för som tillräckligt allvarligt för att anmäla, medan tolv procent uppgav att de inte var medvetna om att brottet var något som kunde och/eller borde anmälas.

Figur 5 Anledningar till att inte göra en polisanmälan efter att ha blivit utsatt för it-brott



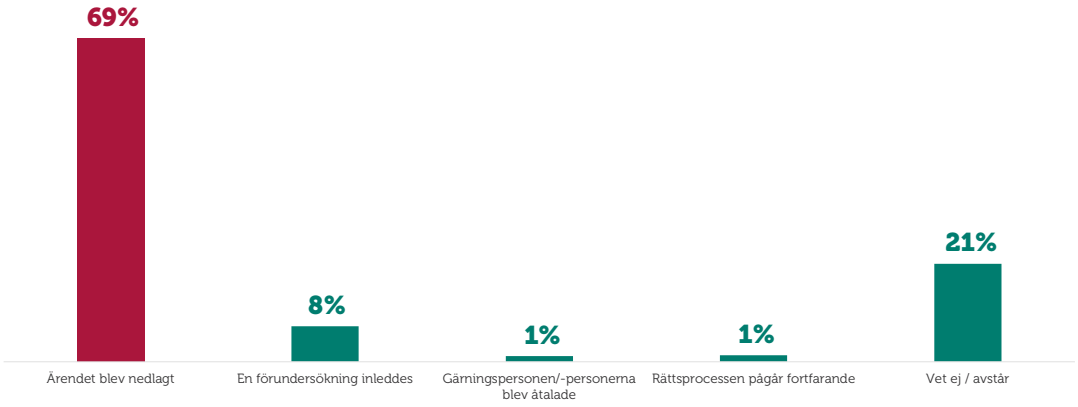
Bas: Företagare utsatta för it-brott, men som inte anmält brottet till polisen, n=785

Att processen att polisanmäla brott ofta upplevs som meningslös framgår tydligt, vilket också nämns av ett flertal av de respondenter som angav egna svar på varför någon polisanmälan inte gjordes. Av de åtta procent som svarade ”Annat” var det många som nämnde hur tidskrävande det kan vara, bland annat då det nästan alltid innebär att stå i långa telefonköer till 114 14 eftersom det inte går att anmäla it-brott på något annat sätt. Detta gäller särskilt i de fall då det rör sig om misslyckade försök till brott där ingen allvarlig skada hunnit ske, det vill säga efter att exempelvis ha utsatts för phishingförsök.

Flera av respondenterna menar också att det många gånger känns som ett slöseri med både tid och resurser eftersom en polisanmälan sällan leder till åtal.

Av samtliga respondenter som någon gång under det senaste året blivit utsatta för it-relaterad brottslighet var det, som framgår av figur 4, enbart 13 procent av dem som valde att anmäla det till polisen. Av dessa svarar 7 av 10 att ärendet blev nedlagt. Endast 1 procent svarar att kontakterna med polisen ledde till att gärningspersonen blev åtalad (se figur 6).

Figur 6 ”Vad hände med din polisanmälan?”

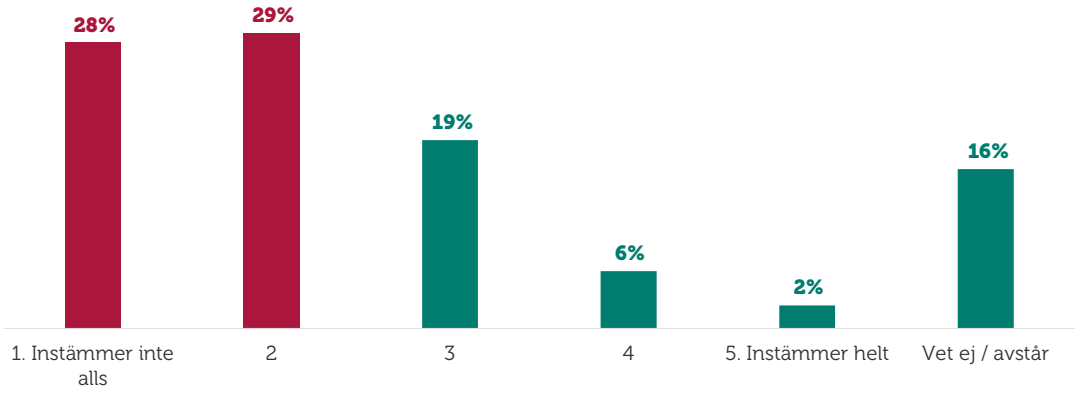


Bas: Företagare utsatta för it-brott och som gjort en polisanmälan, n=154

Stort mörkertal

Endast 13 procent av de företagare som under det senaste året har blivit utsatta för it-relaterad brottslighet valde att göra en polisanmälan, vilket tyder på att det finns ett enormt mörkertal i statistiken över it-brott. I årets enkät framgår det att närmare 70 procent av respondenterna helt eller till stor del instämmer i påståendet att det är viktigt att polisanmäla it-brott, vilket går att tolka som att mörkertalet inte nödvändigtvis grundar sig i en bristande kunskap kring vikten av att göra en polisanmälan. Det största problemet i fråga om det stora mörkertalet verkar snarare vara en bristande tilltro till polisen och rättsväsendet. När de tillfrågade i årets undersökning ombads ta ställning till huruvida de känner ett starkt förtroende för polisens förmåga att utreda och lösa it-relaterade brott svarade 57 procent att de inte alls eller endast till viss del instämmer i påståendet (se figur 7).

Figur 7 I vilken utsträckning respondenterna instämde i påståendet ”Jag känner ett starkt förtroende för polisens förmåga att utreda och lösa it-relaterade brott”



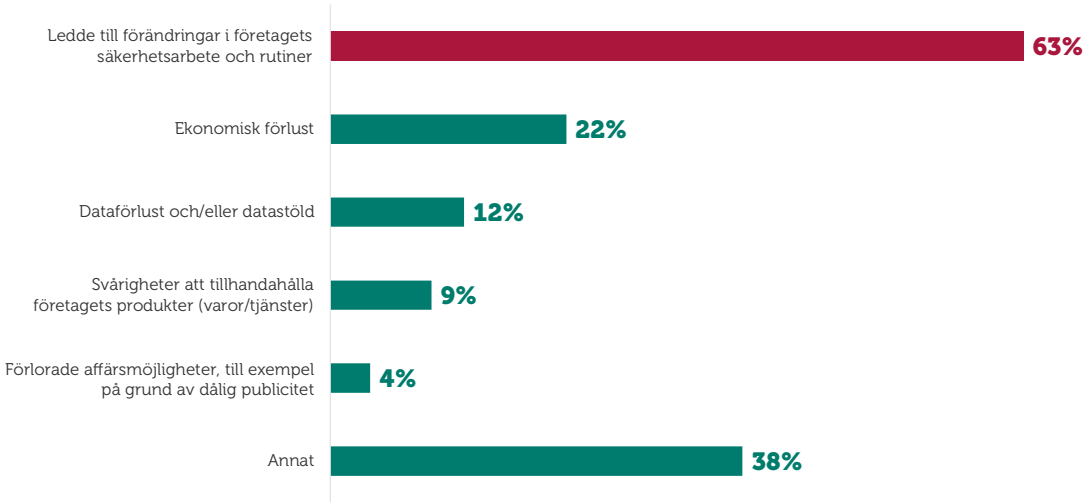
Bas: Samtliga företag, n=1216

Detta skulle delvis kunna kopplas till hur, som framgår av figur 6, en överlägsen majoritet av de polisanmälningar som den här enkätens respondenter har gjort resulterade i nedlagda ärenden. Utifrån detta riskerar nämligen inledningen av en sådan process att bli dyrare än konsekvenserna av själva it-brottet i fråga, speciellt i de fall där utsattheten inte har inneburit några konsekvenser för företaget. Att en stor andel av företagarna låter bli att polisanmäla de it-brott som de utsätts för kan därför inte påstås vara något konstigt, för även om det råder en medvetenhet kring vikten av att göra en polisanmälan om så enbart för statistikens skull, så är det inte alltid den tid och de resurser som krävs kan rättfärdigas.

DEN IT-RELATERADE BROTTSLIGHETENS KONSEKVENSER

Av de företagare som drabbats av ett it-relaterat brott under det senaste året var det en tredjedel som uppgav att brotten fått konsekvenser. Den vanligaste konsekvensen var förändringar i företagets säkerhetsarbete och rutiner, vilket 6 av 10 svarade (se figur 8). Bland de möjliga svarsalternativen på denna fråga kan detta ses som en av de mer positiva följderna av it-brott, då det indikerar att vissa sårbarheter i företagens it-säkerhet har upptäckts och därefter också åtgärdats för att minska risken för upprepad utsatthet.

Figur 8 ”På vilket sätt påverkade brottet dig och ditt företag?”, exklusive svarsalternativen ”ingen påverkan” och ”vet ej/avstår”



Bas: Företagare utsatta för it-brott, exklusive svarsalternativen ”ingen påverkan” och ”vet ej/avstår”, n=387

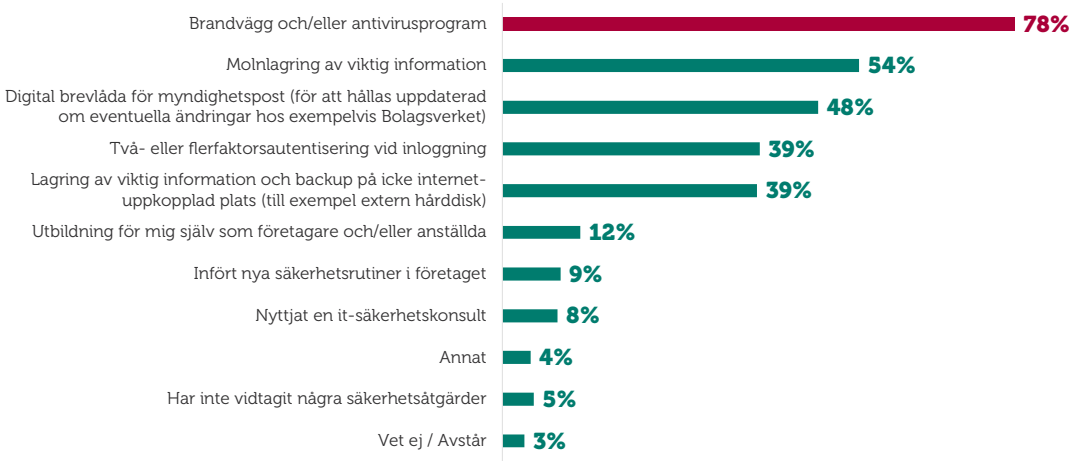
Av de 38 procent som angav ”Annat” som svar på hur deras företag påverkades efter att ha blivit utsatt för någon form av it-brottslighet, var det ett flertal av dem som nämnde onödiga kostnader i form av just tid och resurser. Många av fritextssvaren betonade det extraarbete som denna utsatthet tenderar att innebära, exempelvis genom att ständigt behöva kontrollera och försäkra sig om att den e-post och de samtal, sms och fakturor som tas emot är äkta, såväl som att i vissa fall behöva kontakta sin bank eller på andra sätt behöva åtgärda eventuella problem som kan ha uppstått till följd av att ha blivit utsatt för (försök till) it-brott. Andra respondenter beskrev istället en mer personlig och känslomässig påverkan av att utsättas för it-brott, och då bland annat i form av negativa känslor som oro, irritation och ilska. Bland fritextssvaren framgick det också att den i vissa fall dagliga utsattheten av digitala brott och bedrägeriförsök kan leda till en förlust av motivation och engagemang, något som kan medföra stora konsekvenser för samhället på längre sikt om det skulle leda till att företagare av den anledningen inte längre vill fortsätta driva sin verksamhet.

22 procent svarade att deras utsatthet för it-brott innebar någon form av ekonomisk förlust för företaget. Detta är en överraskande siffra med tanke på hur många företagare som faktiskt har blivit utsatta, och detsamma gäller för den andel som uppgav att deras utsatthet inte medförde några konsekvenser för det egna företaget. Att det för två tredjedelar av samtliga respondenter som någon gång blivit utsatta för it-brott under det senaste året inte hade någon direkt påverkan är självklart något positivt med tanke på de förödande konsekvenser som det riskerar att innebära för både företag och privatpersoner. En möjlig förklaring till att denna siffra är så pass hög är att enkätens svarsalternativ är formulerade så att de även fångar upp incidenter där brott har hunnit upptäckas och stoppats innan någon större skada har kunnat äga rum. Detta kan därför tolkas som att den utbredda utsattheten för it-brott bland Sveriges företagare inte enbart utgör ett stort irritationsmoment där man ständigt behöver vara på sin vakt, utan att det också tar väldigt mycket tid och resurser från företagets verksamhet som egentligen skulle kunna läggas på något annat.

FÖRETAGENS IT-SÄKERHET

För att skydda det egna företaget mot it-relaterad brottslighet finns det en mängd olika säkerhetsåtgärder som kan vidtas. Enligt årets enkätresultat är det, som framgår av figur 9, en användning av antivirusprogram och/eller brandväggar som utgör den överlägset vanligaste säkerhetsåtgärden bland svenska företagare (78 procent).

Figur 9 ”Vilka åtgärder har ditt företag vidtagit för att motverka it-brottslighet?”

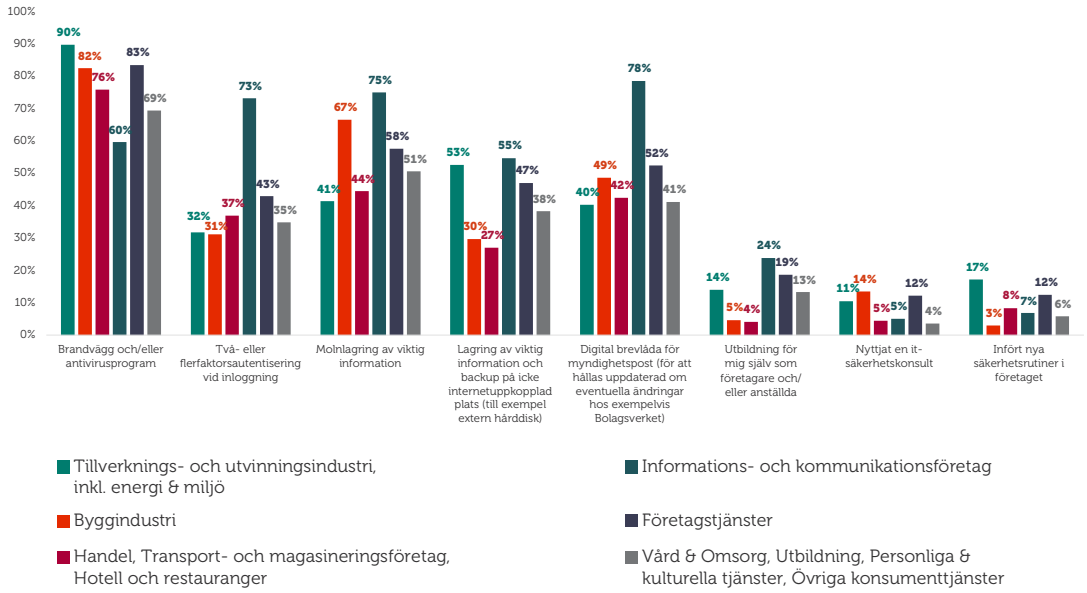


Bas: Samtliga företag, n=1216

54 procent av respondenterna uppger också att de använder molntjänster till att lagra viktig information. Nästan hälften av de tillfrågade (48 procent) använder dessutom en digital brevlåda för myndighetspost, genom vilken det går att hålla sig uppdaterad om eventuella ändringar hos exempelvis Bolagsverket. Två- eller flerfaktorsautentisering vid inloggning är något som 39 procent av företagarna uppger sig använda, där en lika stor andel av de tillfrågade också lagrar viktig information och backup på en icke internetuppkopplad plats som exempelvis en extern hårddisk. Bland de mindre vanliga säkerhetsåtgärderna är att gå en utbildning kring it-säkerhet (9 procent), att införa nya säkerhetsrutiner (9 procent), samt att nyttja en it-säkerhetskonsult (8 procent).

Enkätresultaten visar också att det är företag inom informations- och kommunikationsbranschen som i högst utsträckning använder sig av olika slags säkerhetsåtgärder för att motverka it-brott, där bland annat åtgärder som två- eller flerfaktorautentisering vid inloggning, digital brevlåda och utbildningar för anställda är betydligt vanligare än hos företag som är verksamma inom andra branscher (se figur 10).

Figur 10 Åtgärder som har vidtagits för att motverka it-brottslighet, fördelat på bransch



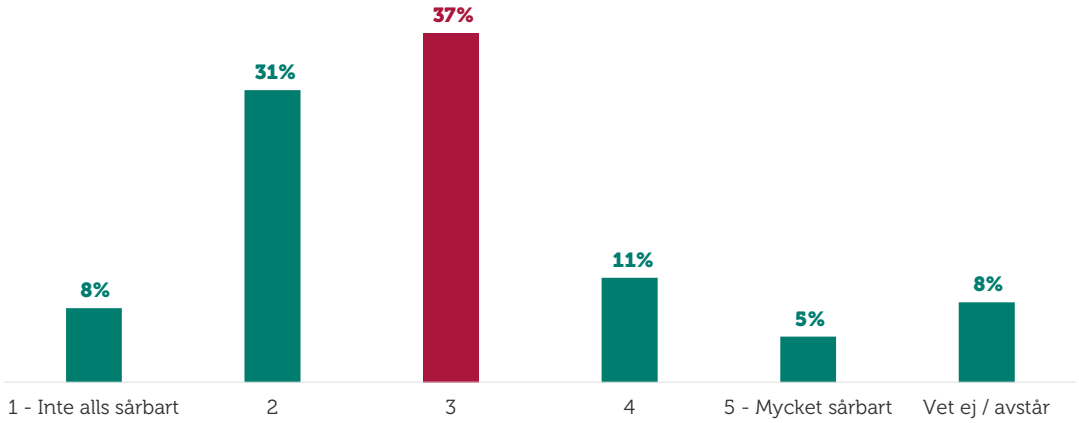
Bas: Samtliga företag, n=1216

Fem procent av de tillfrågade företagarna i årets enkät svarade att de inte hade infört några som helst brottsförebyggande åtgärder. Med andra ord har hela 95 procent gjort investeringar i säkerhetslösningar i någon utsträckning, vilket pekar på att det råder en stor medvetenhet kring it-säkerhetsfrågor bland Sveriges företagare. Dessa siffror kan dock ställas i kontrast till hur 63 procent av dem som under det senaste året har blivit utsatta för it-brott svarade att det inte hade någon påverkan på deras företag. Trots att det ofta inte innebär några allvarliga konsekvenser innebär alltså det brottsförebyggande arbetet en kostnad som både nya och erfarna företagare alltid måste ha i åtanke.

Den mänskliga faktorn

Trots den utbredda användningen av olika slags säkerhetsåtgärder är det endast 39 procent av de tillfrågade som uppskattade det egna företaget som inte alls eller enbart till viss del sårbart när det gäller it-relaterade brott (se figur 11).

Figur 11 ”Hur sårbart uppskattar du att ditt företag är när det gäller it-relaterade brott?”

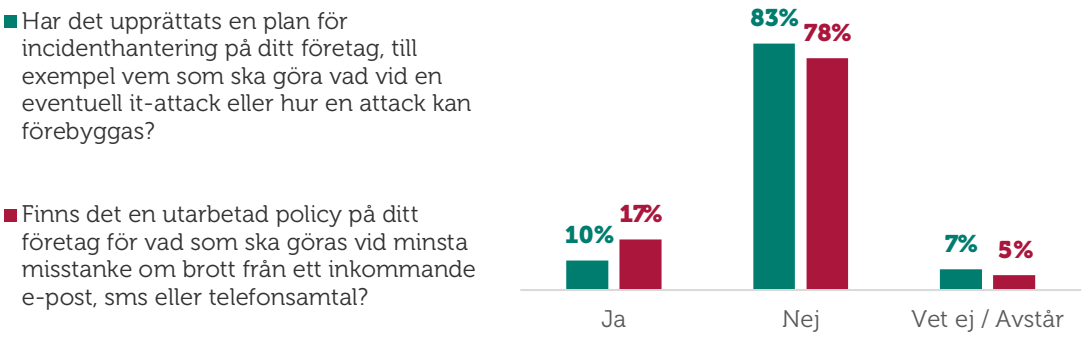


Bas: Samtliga företag, n=1216. Medelvärde = 2,7

Då majoriteten av de åtgärder som de tillfrågade uppger sig ha vidtagit är tekniska sådana, blir det därför tydligt att säkerhetstänket inom företagen måste inkludera mer än så. Säkerhetslösningar som att använda flerfaktorsautentisering och lösenordshanterare kan i många fall vara avgörande i förebyggandet av it-brott, men det är viktigt att inte enbart förlita sig på dem då en allt för vanlig orsak till att exempelvis obehöriga får tillgång till viktig data beror på den mänskliga faktorn. Därför kan det också påstås vara av stor vikt att inom det egna företaget försöka öka medvetenheten kring olika hot och risker och uppmuntra till en öppen dialog och en tillåtande kultur, vilket kan göra stor skillnad i de fall anställda känner sig osäkra på hur de ska agera om de till exempel mottar e-post med ett misstänkt innehåll.

På frågan om huruvida det har upprättats en plan för incidenthantering hos företagen var det hela 83 procent av respondenterna som svarade ”Nej”. När det gäller att ha en utarbetad policy kring vad som ska göras vid minsta misstanke om brott från ett inkommande e-post, sms eller telefonsamtal, var motsvarande siffra 78 procent (se figur 12).

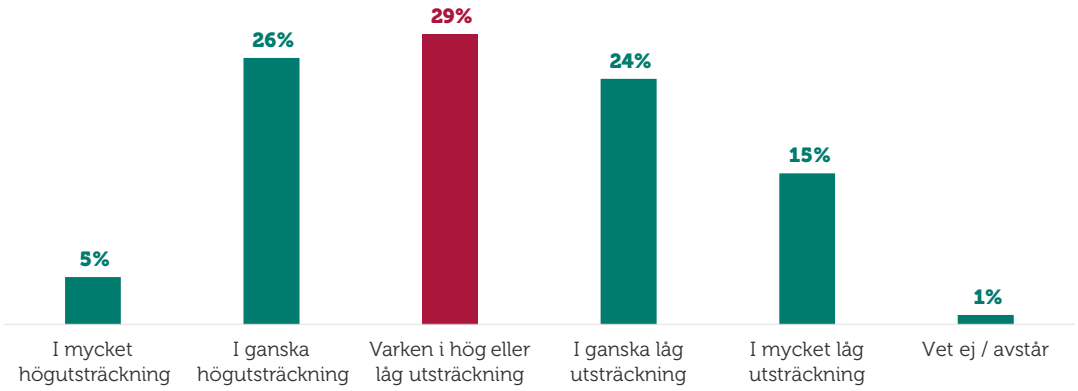
Figur 12



Att exempelvis veta vad som ska göras vid en eventuell it-attack kan göra stor skillnad när det gäller att försöka minimera dess påverkan på det egna företaget, och genom att rapportera sådana incidenter underlättas även det proaktiva arbetet då det möjliggör att potentiella sårbarheter i företaget identifieras och åtgärdas innan det är för sent. Med hjälp av denna slags brottsförebyggande arbete kan företagens it-säkerhet öka samtidigt som risken för upprepad utsatthet minskar. Då phishingförsök utgör en av de vanligaste formerna av it-brott som företagare drabbas av, skulle en ökad kunskap kring hur sådana incidenter ska hanteras också kunna vara ett effektivt sätt att minska den oro som många känner inför att själva bli utsatta.

Årets enkätresultat visar att 31 procent av företagarna i mycket eller ganska hög utsträckning oroar sig över att det egna bolaget ska bli utsatt för it-relaterade brott (se figur 13). Att en så pass stor andel av de tillfrågade känner sig oroliga över att utsättas för it-relaterad brottslighet skulle därför kunna kopplas till en brist på kunskap om hur man på bästa sätt kan skydda det egna företaget.

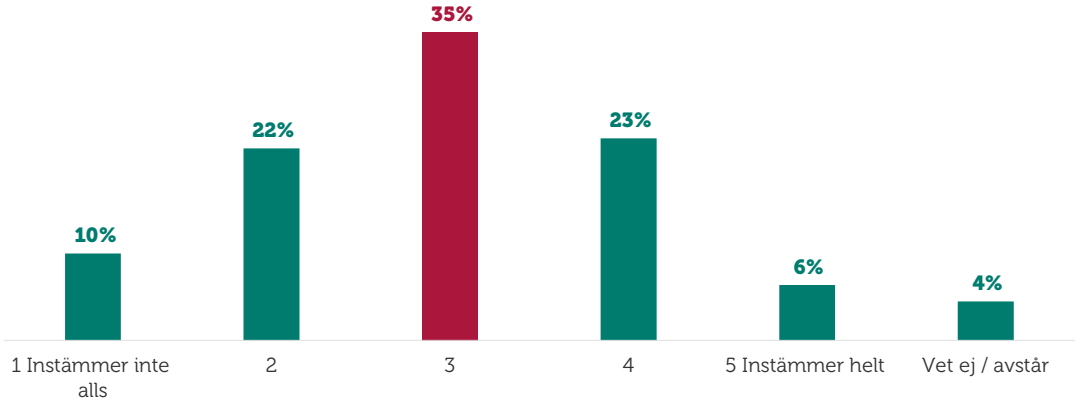
Figur 13 ”I vilken utsträckning oroar du dig över att ditt företag ska bli utsatt för it-relaterade brott?”



Bas: Samtliga företag, n=1216

När företagarna ombads ta ställning till huruvida de själva upplevde att de hade tillräckligt med information och kunskap för att kunna skydda sig från bedrägerier och digitala brott, var det bara en knapp tredjedel av dem som till stor del eller helt och hållet instämde i det påståendet (se figur 14).

Figur 14 ”Jag har tillräckligt med information och kunskap för att kunna skydda mitt företag mot bedrägerier och digitala brott”

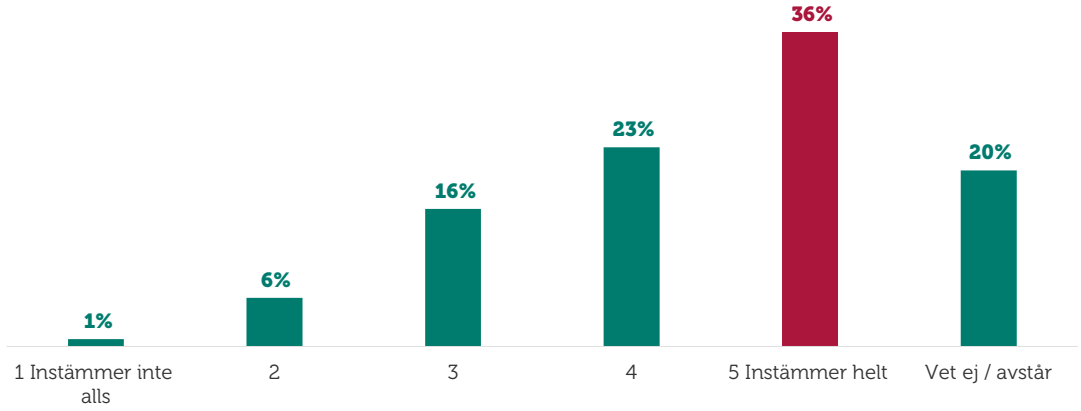


Bas: Samtliga företag, n=1216

Samarbete mellan företag och myndigheter

Privata säkerhetslösningar är effektiva till en viss grad, men om det inte förs en ständig dialog kring digital säkerhet mellan företag och brottsbekämpande myndigheter kommer det aldrig upplevas att man som företagare har bästa möjliga förmåga att effektivt skydda den egna verksamheten. 59 procent av Sveriges företagare anser att informations- och kunskapsutbytet mellan företag och myndigheter när det gäller it-säkerhet bör förbättras (se figur 15). Det som en stor andel av Sveriges företagare verkar efterfråga är därmed ett utökat samarbete.

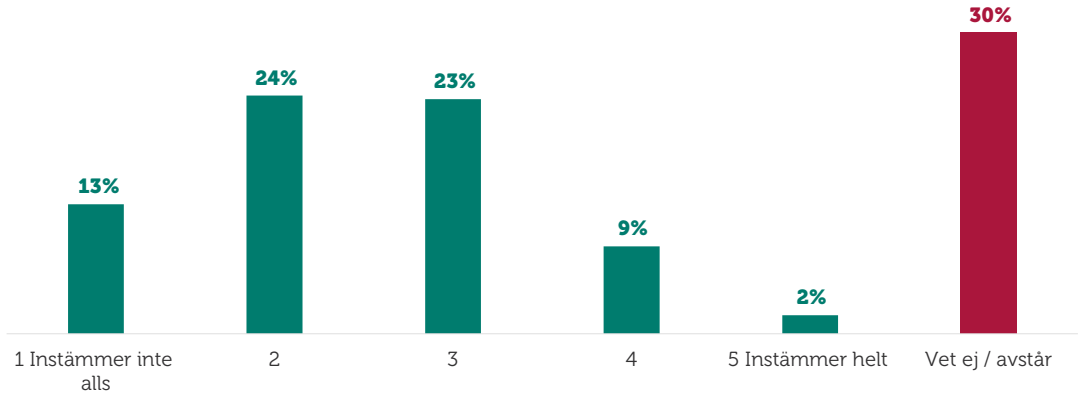
Figur 15 ”Informations- och kunskapsutbytet mellan företag och myndigheter när det gäller it-säkerhet bör förbättras”



Bas: Samtliga företag, n=1216

Att genomföra informationsinsatser i syftet att öka kunskapen kring it-säkerhet - och genom dessa samtidigt uppmana allmänheten till att tänka över sitt beteende på internet - är ett exempel på hur myndigheterna arbetar för att minska utsattheten för digitala brott och bedrägeriförsök. Som framgår av figur 16 visar enkätresultaten däremot att enbart 11 procent helt eller till stor del instämmer i påståendet att det finns god tillgång till stöd, verktyg och/eller information från myndigheters håll när det gäller it-säkerhetsfrågor, samtidigt som hela 30 procent svarade ”Vet ej / Avstår”. Att en så pass stor andel inte är säkra på huruvida så är fallet, gör detta till ett tydligt förbättringsområde.

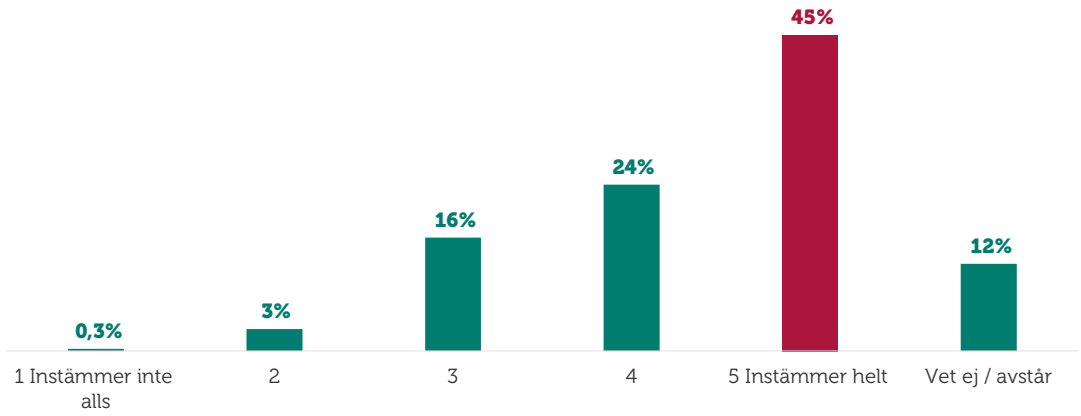
Figur 16 I vilken utsträckning respondenterna instämde i påståendet ”Det finns god tillgång till stöd, verktyg och/eller information från myndigheter när det gäller it-säkerhetsfrågor”



Bas: Samtliga företag, n=1216

Årets enkätresultat visar också att 69 procent av respondenterna helt eller till stor del instämmer i påståendet att it-säkerhet bör prioriteras högre inom politiken (se figur 17).

Figur 17 I vilken utsträckning respondenterna instämde i påståendet ”It-säkerhet bör prioriteras högre inom politiken”



Bas: Samtliga företag, n=1216

Detta försvåras dock av den låga anmälningsbenägenhet som tidigare har diskuterats, då en brist på information och statistik kring hur utbredd utsattheten faktiskt är gör en prioritering av det området betydligt svårare för både polisen och andra makthavare att motivera. Här går det att tala om en slags ond cirkel, där det låga förtroendet för polisens förmåga att utreda och lösa it-brott, i kombination med det som många företagare upplever är en tidskrävande och krånglig anmälningsprocess, bidrar till en missvisande brottsstatistik som försvårar en effektiv bekämpning av den it-relaterade brottsligheten. Då detta innebär att majoriteten av de it-brott som drabbar svenska företag inte klaras upp, påverkar det i sin tur företagarnas tilltro till polisen och rättsväsendet.

Det som skulle behövas är ett ökat samarbete, men det är något som bygger på tillit. Olika slags åtgärder och insatser som syftar till att exempelvis öka medvetenheten hos företagare kring vikten av att polisanmäla samtliga it-brott som de utsätts för, även om de sällan leder till åtal, skulle inte göra någon nytta om det inte samtidigt sker förändringar i hur polisen arbetar med de ärenden som kommer in.

STOPPA IT-BROTTEN: 10 SAKER DU SJÄLV KAN GÖRA

1. Logga aldrig in med din e-legitimation på uppmaning av någon annan om du inte själv aktivt är den som ringt upp till exempel en bank eller myndighet.
2. Installera antivirusprogram och brandvägg på företagets datorer.
3. Se till så att du regelbundet gör säkerhetskopior av innehållet i din dator.
4. Tänk efter och granska kritiskt e-post innan du klickar på en länk eller öppnar en fil, även från tillsynes kända avsändare.
5. Undvik att använda publika nät.
6. Uppdatera datorn, programvarorna, mobilen och apparna med tillverkarnas senaste säkerhetsuppdateringar.
7. Lösenordet för den e-postadress som används för att återställa övriga lösenord bör innehålla många karaktärer och ej användas i något annat sammanhang. Spara inte lösenord i datorns webbläsare.
8. Använd tvåfaktorautentisering vid inloggning om möjlighet finns. Tvåfaktorsautentisering får man genom att kombinera två säkerhetsmetoder, till exempel att samtidigt ange ett hemligt lösenord och att en pinkod skickas till mobilen.
9. Använd en digital brevlåda för myndighetspost. Alla ändringsbekräftelser eller liknande får du information om i den digitala brevlådan exempelvis om firmatecknaren ändrats hos Bolagsverket.
10. Ta reda på var företagets viktigaste information lagras. Dokumentera, om det behövs, rutiner som beskriver hur ni på företaget ska hantera er information säkert.

Häng med i debatten
och följ *@foretagarna*
på Twitter, Instagram,
LinkedIn och Facebook!

företag*arna*

Företagarna Sverige Service AB, Rådmansgatan 40, 106 67 Stockholm
foretagarna.se | info@foretagarna.se | 08 – 406 17 00