CYBERHOTEN

Så ser hotbilden och attackerna ut
mot svenska teknikföretag

Teknikföretagen

Innehåll

Dataintrången ökar mot svenska underleverantörer och mindre teknikföretag

Sveriges konkurrenskraft bygger på ett kunskapsintensivt näringsliv med kvalificerade teknikföretag och industriella produkter. Sverige gynnas av ett öppet utbyte med andra länder, men många företag har sina servrar fulla med forskningsresultat, utvecklingsprojekt och patentansökningar. Dessa representerar enorma värden för den stat som vill gå genvägar i sin egen näringslivs- och teknikutveckling. I praktiken kan det innebära att de företag som utvecklat ny teknik konkurreras ut av sina egna lösningar, realiserade av statsunderstödda företag i andra länder. Detta hotar på sikt Sveriges innovationsförmåga.[1]

Under senare år har frekvensen av digitala intrång ökat markant och används nu systematiskt för industrispionage. De statsunderstödda cyberattackerna blir också gradvis allt mer avancerade och innebär bland annat att svagheter i system hos underleverantörer utnyttjas för att komma åt konfidentiell information, inte minst med koppling till storföretag. Det behövs en ökad kunskap om hotbilden mot mindre teknikföretag* och underleverantörer samt mer stöd för ökat skydd. I denna skrift ger vi en kort introduktion till ämnet och några konkreta råd.

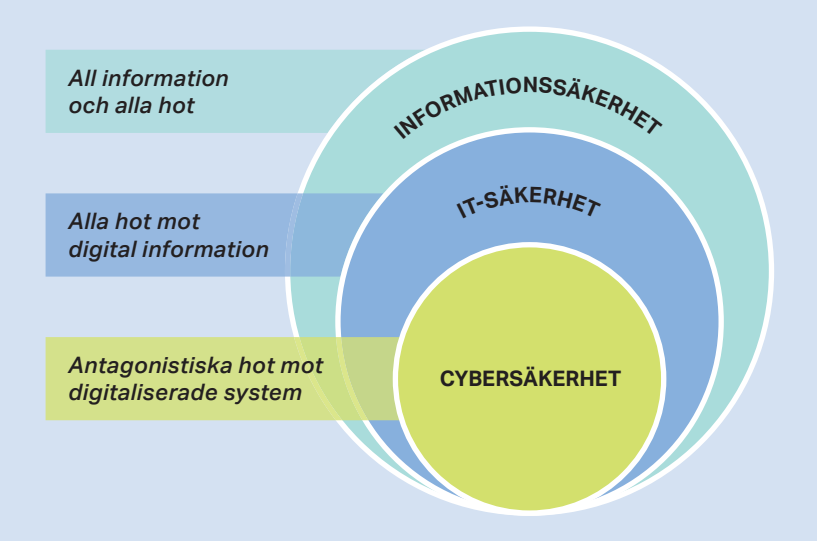
Patrik Sandgren
Expert digitalisering,
Teknikföretagen

* Begreppet mindre teknikföretag avser i denna skrift primärt företag med under 250 anställda.

Vad är cybersäkerhet?

Cybersäkerhet handlar om att skydda elektronisk utrustning exempelvis datorer, servrar, mobila enheter, digitala system, nätverk och data mot skadliga angrepp. Begreppet cybersäkerhet används även synonymt med informationssäkerhet och IT-säkerhet men har generellt en mer avgränsad betydelse och kan ses som delar av de två nämnda begreppen.[2] Primärt adresserar cybersäkerhet tre slags hot[3]:

1. **Cyberbrott**, där enstaka personer eller grupper angriper system för ekonomisk vinning.
2. **Cyberspionage**, där statsaktörer primärt angriper utländska bolag för att komma över affärshemligheter i syfte att överföra dem till inhemsk industri.
3. **Cyberterrorism**, angrepp avsedda att underminera elektroniska system och orsaka panik eller rädsla.



Industrin genomgår en omfattande digitalisering

Företag i Sverige genomgår just nu en omfattande digitalisering. Detta gäller inte minst mindre teknikföretag och underleverantörer. Genom de tekniska framstegen har priset för digitala lösningar sjunkit samtidigt som utbudet ökat exponentiellt.

Detta märks på flera sätt inte minst genom att:

- **Datorkapaciteten** har ökat vilket erbjuder högre prestanda till samma pris
- **Sensorer** har krympt i storlek och designats för förenklad integration
- **Digital lagring** har underlättats genom molntjänster
- **Trådlös teknik** har förbättrats genom mindre och effektivare antenner
- **Optisk fiber** har möjliggjort robust överföring av data
- **Mjukvara** har utvecklats för informationssystem, maskininlärning och dataanalys

Utvecklingen innebär att utrustning och verktyg både kan kopplas upp och kopplas ihop till en rimlig kostnad, samt att data som skapas i olika processer kan fångas upp och användas. Detta ger möjlighet till ökad produktivitet, nya affärsmöjligheter och en ökad miljömässig hållbarhet.[4] Parallellt med dessa möjligheter så har också förväntningarna och kraven ökat från kunder och leverantörer att tjänster ska finnas att tillgå digitalt. Det gäller alla företag, oavsett storlek.

Med digitaliseringen kommer en ökad sårbarhet

Baksidan av digitaliseringen är att den ger upphov till stora risker som måste hanteras. För mindre teknikföretag och underleverantörer är det tre faktorer som är särskilt utmanande:

För det första är den generella säkerheten vid uppkoppling av utrustning bristfällig. För många produkter och lösningar har exempelvis användbarhet prioriterats medan säkerhet setts som en sekundär fråga. Detta har inneburit att produkter inte designas säkert och att sårbarheter som identifieras ignoreras.

För det andra har mindre företag relativt sett mindre resurser att allokera till cybersäkerhetsområdet. Det innebär att de har svårare att upptäcka svagheter och även att kunna hantera dem på ett kostnadseffektivt sätt. Resultatet är bland annat att de i stor utsträckning är beroende av att leverantörer av digitaliseringslösningar hanterar och beaktar säkerheten.

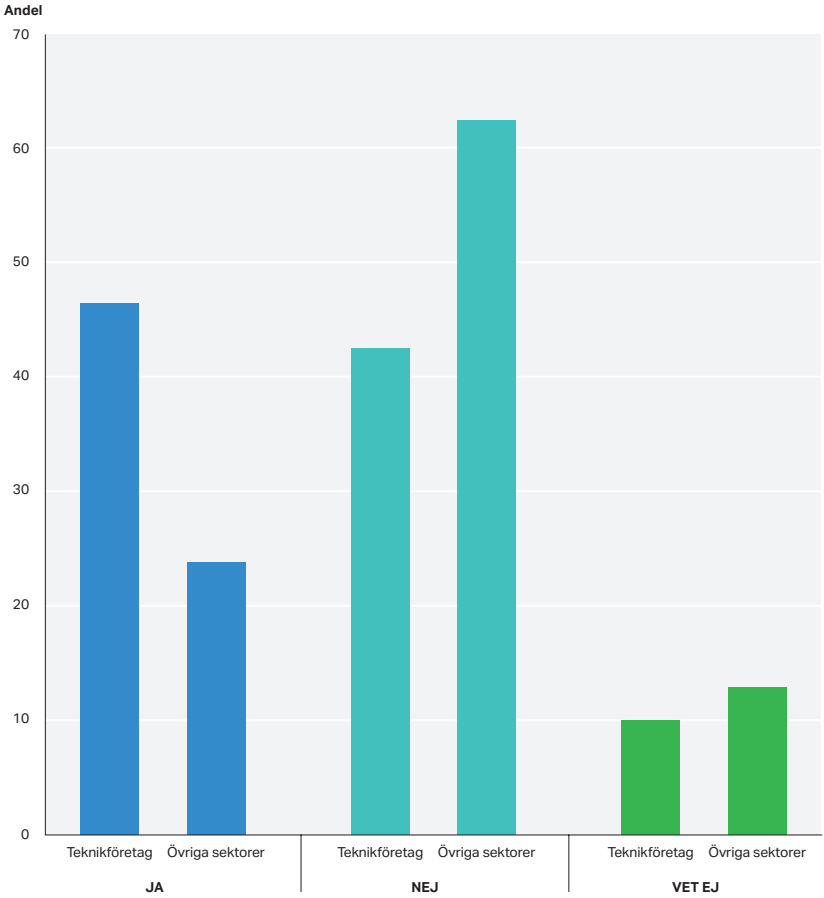
För det tredje har frekvensen, såväl som konsekvensen, av cyberattacker ökat. Attackerna har därtill blivit diversifierade, mer sofistikerade och riktade mot specifika sektorer. Mindre teknikföretag och underleverantörer är numera primära måltavlor.

Hälften av teknikföretagen har angripits det senaste året

Angreppen mot företagen sker i olika former. I början av 2020 var över 17 000 datorer infekterade i Sverige, det vill säga att de var exempelvis angripna av virus eller utgjorde delar av ett botnät.[5] Motsvarande siffra för mobila enheter uppskattas till ca 400 000 st.[6] Denna stora mängd datorer och mobiler kan användas för koordinerade attacker mot enskilda företag eller specifika branscher och riskerar då att slå ut exempelvis kritiska produktionssystem.

Den mest frekventa formen av angrepp som företagen identifierat sker genom elakartad programvara som virus och trojaner samt genom att sårbarheter i de digitala systemen utnyttjas för intrång.[7] Bland Teknikföretagens medlemmar, det vill säga tillverkande företag och industrinära tjänsteföretag, uppger nära hälften att de under år 2018–2019 blivit utsatta för cyberangrepp. Andelen för företag i övriga sektorer i näringslivet är knappt 25 procent.[8] En särskild utmaning är att cyberattackerna som riktas mot företagen bedrivs långsiktigt och systematiskt där bitar av information pusslas samman.[9] I detta perspektiv är mindre teknikföretag och underleverantörer nyckelkomponenter för att komma över uppgifter.

Diagrammet visar hur stor andel företag som utsatts för cyberangrepp 2018/2019. Teknikföretag är betydligt mer utsatta för cyberangrepp än företag i andra sektorer.



Källa: Svenskt Näringslivs företagspanel i samarbete med Teknikföretagen, 2019.

Fem industrisektorer där företag är i riskzonen att drabbas av cyberangrepp[10]

1. **Industriella produkter**
2. **Industriella maskiner**
3. **Fordon**
4. **Informationsteknik**
5. **Energiteknik**

Olika aktörer utför olika typer av angrepp

Antalet identifierade cyberattacker mot olika företag och myndigheter i Sverige har trendmässigt ökat och uppgår nu till över 100 000 per år.[11] Sedan ett antal år tillbaka kommer emellertid cyberhoten som möter industrin i Sverige, i påfallande stor utsträckning, från främmande makter.[12] Dessa stater utför själva attackerna eller ger direkt stöd åt kriminella grupperingar för riktade intrångsförsök.[13] Sammantaget är det ett femtontal länder som aktivt opererar med sikte på svenska företag.[14]

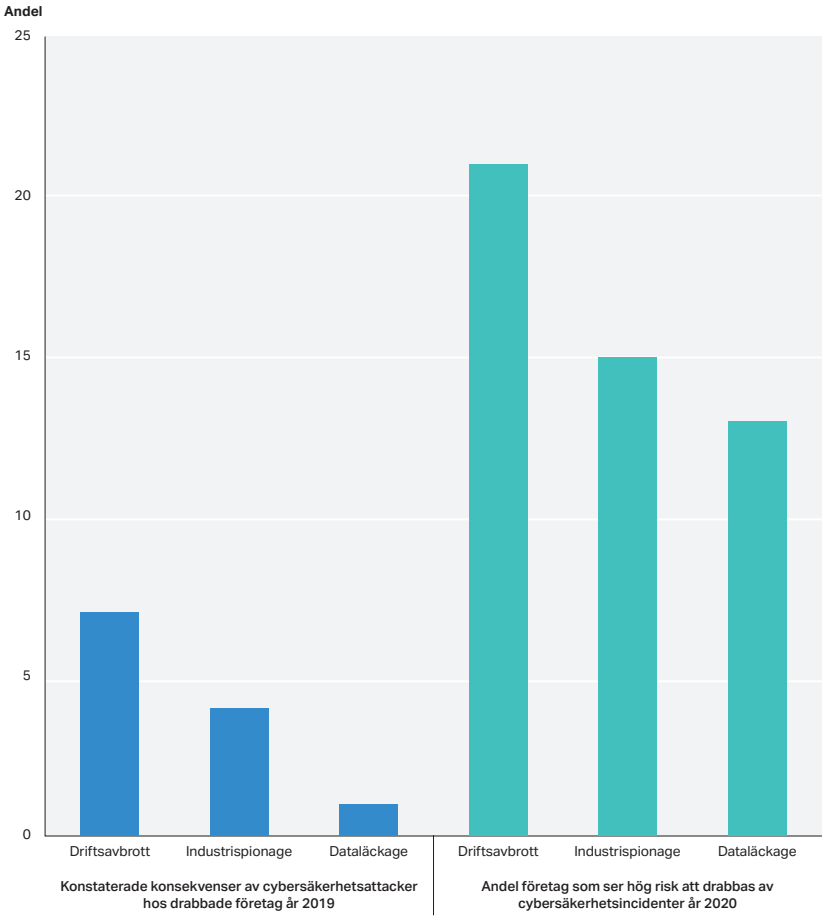
Att industrin är särskilt utsatt blir också tydligt när cyberattacker mot företag ses i ett holistiskt perspektiv. Attackerna kombineras nämligen med *”påverkansoperationer, traditionella underrättelseaktiviteter* och *strategiska uppköp”*[15] vilket riktas mot bland annat företag inom elektronik, kommunikationsteknik samt industriella produkter.[16] Det är värt att notera att en del av de företag som är måltavlor, tillhandahåller civila komponenter och produkter, (exempelvis vakuumpumpar) som har dubbla användningsområden. Genom att produkterna även kan användas för militära ändamål är de av särskilt intresse för främmande makter.[17]

Angrepp för miljarder och stort mörkertal

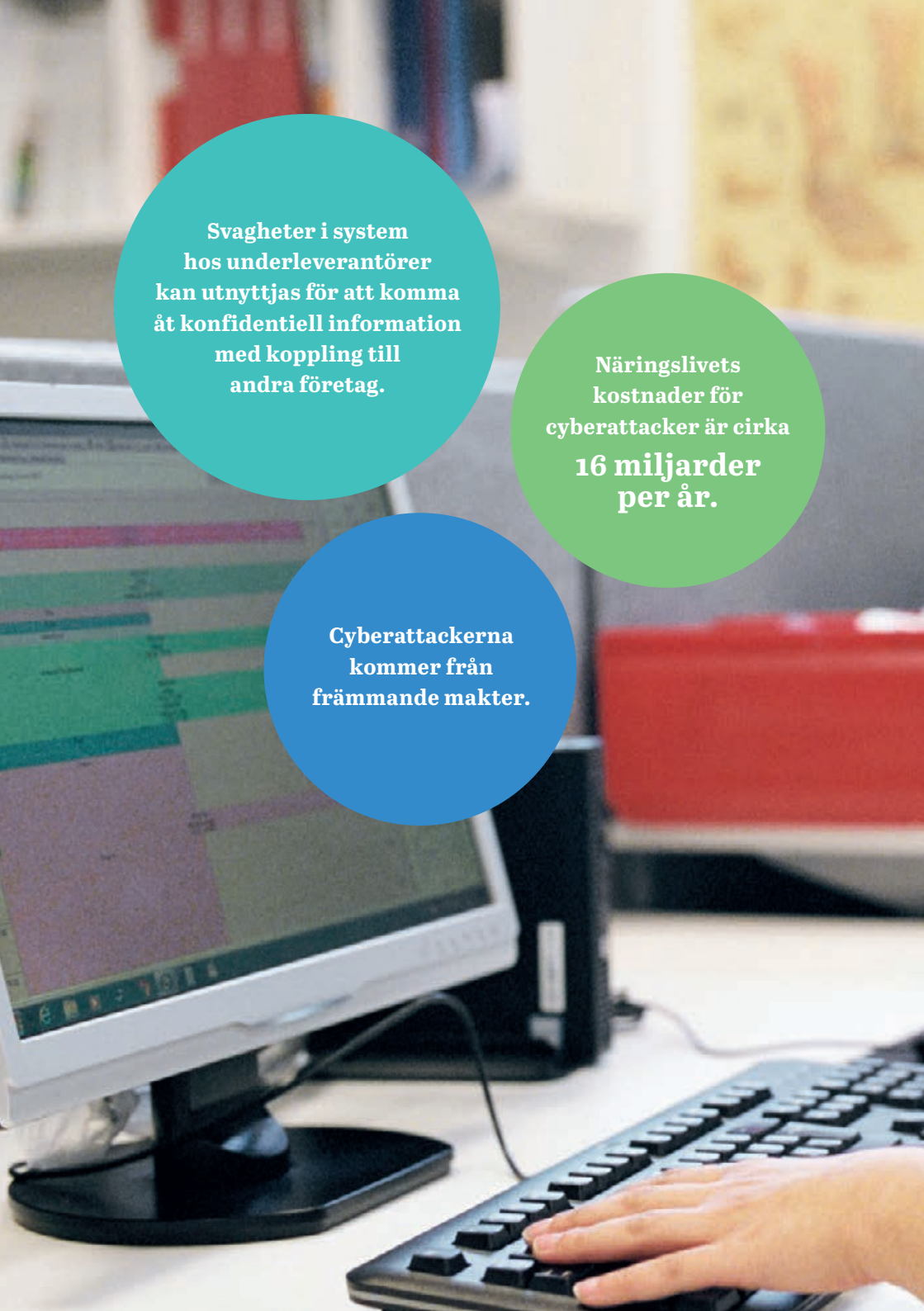
På samma sätt som attackerna varierar, på samma sätt skiftar konsekvenserna. För Teknikföretagens medlemmar har cyberattackerna, under 2019, gett upphov till att system blivit otillgängliga samt data blivit publikt eller att affärshemligheter stulits. Bedömningen är att denna utveckling kommer att fortsätta med ökande styrka under år 2020.[18]

Det bör noteras att företag ogärna offentliggör när de blivit attackerade varför redovisade uppgifter sannolikt döljer ett stort mörkertal. Dessutom förblir många företag ovetandes om att de överhuvudtaget har blivit utsatta för angrepp.[19] En rimlig uppskattning är att de samlade direkta kostnaderna uppgår till ca 16 miljarder kr för svenska företag, vilket främst drabbar de forskningsintensiva industriföretagen och företag som arbetar med dem, exempelvis underleverantörer.[20] Även störningar och avbrott som följer av cyberattacker är riskabla och kan bli kostsamma. Under 2019 rapporterades exempelvis 50 allvarliga och betydande incidenter.[21] Prislappen för dessa har inte uppskattats, men totalt beräknas en nedstängning eller blockering av datatrafiken i Sverige generera en kostnad för samhället på i storleksordningen 6 miljarder kr om dagen.[22]

Diagrammet visar de vanligaste konsekvenserna av cyberattackerna samt estimerade konsekvenser framåt. Driftsavbrott är den vanligaste konsekvensen bland Teknikföretagens medlemmar.



Källa: Teknikföretagen, ”Digitaliseringsundersökning”, 2019


Svagheter i system hos underleverantörer kan utnyttjas för att komma åt konfidentiell information med koppling till andra företag.
Näringslivets kostnader för cyberattacker är cirka 16 miljarder per år.
Cyberattackerna kommer från främmande makter.

Säkerhetsmedvetandet behöver genomsyra både den fysiska och digitala miljön

Medan det länge varit givet att ha lås och larm på byggnader så har cybersäkerhet i många företag, fram tills nu, inte bedömts som prioriterat. Bakom det fysiska skalskyddet har också uppkopplad utrustning lämnats öppen, obevakad och placerad på exempelvis undanskymda ställen – vilket ger enkel access om någon kommer in i lokalerna under förespegling att utföra exempelvis service eller reparationer. Det fysiska och digitala skyddet måste därför hänga ihop för att vara effektivt, och detta bör återspeglas i de regler som sätts upp.

Att ha policies kring vem som har tillgång till vilka system, vem som släpps in var och hur utrustning ska lokaliseras hjälper dock inte tillräckligt om de riktlinjer som bestämts ignoreras. Bland Teknikföretagens medlemmar rapporterar ca 25 procent av företagen att de har återkommande incidenter där anställda åsidosätter cybersäkerhetsföreskrifter genom att exempelvis använda egen it-utrustning[23], ladda ner icke-auktoriserad programvara eller dela lösenord. Säkerhetsmedvetandet behöver genomsyra hela verksamheten.

Dessa skyddsåtgärder bör prioriteras för en grundläggande säkerhetsnivå

Hoten mot företagen tar sig kontinuerligt nya former, vilket gör det svårt att bibehålla ett adekvat skydd. Att involvera professionella cybersäkerhetskonsulter som kan bistå med riskanalys, ge vägledning och implementera lösningar är därför rekommenderat.

För att nå en grundläggande säkerhetsnivå och börja cybersäkerhetsarbetet är dock fem åtgärder prioriterade:[24]

1. **Installera och uppdatera virusskydd och brandväggar** – Ett grundläggande skydd i form av digitalt lås och övervakning kan bidra till att angrepp upptäcks snabbare och att omfattningen begränsas.

2. **Kontrollera att utrustning är uppkopplad på ett säkert sätt** – Användarvänligheten gör ibland att produkter inte är konfigurerade eller designade med säkerhet som utgångspunkt. Det går därför inte att förutsätta att utrustning som kopplas upp per definition är säker.

3. **Lösenordsskydda, med starka lösenord, utrustning och information** – Produkter och utrustning kommer ofta med förutbestämda lösenord som är lätta att forcera. Säkerställ därför att lösenorden byts ut med jämna mellanrum och att de klassas som starka.[25]

4. **Ta fram riktlinjer för företaget och personalen och förklara vikten av att de efterlevs** – Sätt upp regler för hur elektronisk utrustning ska hanteras och vilka försiktighetsåtgärder som behöver vidtas för att upprätthålla ett adekvat skydd. Här bör den digitala och fysiska säkerheten kopplas ihop och att ett säkerhetsmedvetande genomsyrar alla på företaget.

5. **Identifiera företagskritisk information, var den lagras och gör regelbunden backup** – All information är inte lika viktig. För att kunna prioritera rätt bör därför företagsinformation värderas och klassificeras. På så sätt kan det tydliggöras var skyddsvärdet ligger, och var resurser till skydd bör allokeras. Den information som klassas som känslig information bör ges adekvat skydd, säkerhetskopieras och lagras säkert.

Slutnoter

[1] FRA, "Årsbok 2018", https://www.fra.se/download/18.69cf97cd-167832fc038250/1548773731405/FRA-arsrapport-2018.pdf

[2] IVA, "Digitalisering för ökad konkurrens", https://www.iva.se/globalassets/projekt/201902-iva-digitalisering-slutrapport-l.pdf

[3] Kaspersky, "Vad är cybersäkerhet?", https://www.kaspersky.se/resource-center/definitions/what-is-cyber-security

[4] Teknikföretagen, "Digitaliseringsundersökning", 2019

[5] Cert.se, "Infekterade datorer i Sverige", https://www.cert.se/megamap/

[6] Estimering baserat på att antalet mobilabonnemang totalt uppgick till 14,2 miljoner i Sverige och att ca 3 procent av dessa vara infekterade med skadlig kod. Comparitech," Which countries have the worst (and best) cybersecurity?", https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/, Kaspersky, "IT threat evolution Q2 2019. Statistics", https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/ samt PTS, "Svensk telemarknad", www.pts.se

[7] Företagarna, "Cyberattacker mot företag 2019", 2019

[8] Svenskt Näringslivs företagspanel i samarbete med Teknikföretagen, november 2019.

[9] PWC, "Operation Cloud Hopper", https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/operation-cloud-hopper.html

[10] Totalförsvarets forskningsinstitut, "Kinesiska bolagsförvärv i Sverige: en kartläggning – FOI", https://www.foi.se/rest-api/report/FOI%20Memo%206903

[11] Totalförsvarets Forskningsinstitut, "Årsrapport 2019", https://fra.se/download/18.6cf5edb9170382a0ad51c/1581950150002/FRA-arsrapport-2019.pdf samt SVT, "Cyberangreppen mot Sverige ökar", www.svt.se

[12] Denna typ av attacker kan benämnas med akronymen APT – "Advanced Persistent Threats".

[13] Totalförsvaret Forskningsinstitut, "Kinas industriella cyberspionage", https://www.foi.se/rest-api/report/FOI%20MEMO%206698

[14] Säkerhetspolisen, "Årsbok för 2018", https://www.sakerhetspolisen.se/download/18.6af3d1c916687131f1fae5/1552543607309/Arsbok-2018.pdf

[15] Försvarets Radioanstalt, "Årsrapport 2019", https://fra.se/download/18.6cf5edb9170382a0ad51c/1581950150002/FRA-arsrapport-2019.pdf. Se även uppgifter från Säkerhetspolisen (SÄPO) där just företagsuppköp lyfts fram som ett komplement till cyberangrepp. Säkerhetspolisen, "Årsbok för 2018", https://www.sakerhetspolisen.se/download/18.6af3d1c916687131f1fae5/1552543607309/Arsbok-2018.pdf

[16] Totalförsvarets forskningsinstitut (FOI) har kunnat identifiera 25 företag inom elektronik, kommunikationsteknik samt industriella produkter som blivit uppköpta under senare år, men uppger att det sannolikt finns fler. Totalförsvarets forskningsinstitut, "Kinesiska bolagsförvärv i Sverige: en kartläggning – FOI", https://www.foi.se/rest-api/report/FOI%20Memo%206903

[17] Dessa produkter förkortas ofta PDA – Produkter med dubbla användningsområden. Säkerhetspolisen, "Årsbok för 2018", https://www.sakerhetspolisen.se/download/18.6af3d1c916687131f1fae5/1552543607309/Arsbok-2018.pdf

[18] Teknikföretagen, "Digitaliseringsundersökning", 2019, Företagarna, "Cyberattacker mot företag 2019", 2019 samt SCB, "IT användning i företag", 2019, https://www.scb.se/hitta-statistik/statistik-efter-amne/naringsverksamhet/naringslivets-struktur/it-anvandning-i-foretag/

[19] Totalförsvarets Forskningsinstitut, "Kinas industriella cyberspionage", https://www.foi.se/rest-api/report/FOI%20MEMO%206698

[20] Estimat baserat på McAffe, "Economic impact of cybercrime", 2018 och IBM, "Cost of a Data Breach Report, 2019.

[21] Post- och Telestyrelsen, "Ökning av rapporterade incidenter", https://pts.se/sv/nyheter/internet/2020/r-arlig-granskning/

[22] ISOC, "The cost of shutdown", https://netblocks.org/cost/.

[23] Exempelvis datorer eller lagringmedia som USB-minnen.

[24] Teknikföretagen, "Skydda din IT-miljö", https://www.teknikforetagen.se/globalassets/i-debatten/publikationer/cybersakerhet/skydda-din-it-miljo---en-guide-till-medvetet-sakerhetsarbete-i-mindre-teknikforetag.pdf

[25] Med starka lösenord avses att de är exempelvis är långa, innehåller gemener och versaler samt specialtecken vilket gör dem svårare för en antagonist att gissa.

VAD GÖR TEKNIKFÖRETAGEN INOM DIGITALISERING

Teknikföretagen bevakar, driver och påverkar frågor inom digitalisering och cybersäkerhet utifrån våra medlemsföretags behov.

För mer information om cybersäkerhet för mindre företag, se Teknikföretagens guide ”Skydda din IT-miljö”. Tillgänglig på **www.teknikforetagen.se**

Har ni frågor kontakta:
Patrik Sandgren, expert digitalisering
patrik.sandgren@teknikforetagen.se, tfn 08-782 09 42

Teknikföretagen

Teknik gör världen bättre

Den svenska teknikindustrins företag står för de lösningar som tacklar vår tids stora utmaningar. Det är hos Teknikföretagen som dessa företag är medlemmar.

2020. FORM: ORDFÖRRÅDET. FOTO: 14–15 EMILIA BERGMARK-JIMÉNEZ. 17, 20 JONAS BILBERG