Techbranschens förslag för att möta cyberhoten

TechSverige

TechSverige

Techbranschens förslag för att möta cyberhoten

TechSverige maj 2023

TechSverige

Techbranschens förslag för att möta cyberhoten

Techbranschen med de digitala lösningar den erbjuder är av avgörande betydelse för Sveriges ekonomiska tillväxt, för produktiviteten och innovationskraften i hela näringslivet och i all offentlig verksamhet samt för en hållbar samhällsutveckling. Digitaliseringen erbjuder många möjligheter, men allvarliga baksidor behöver också uppmärksammas. Även om säkerhetsinvesteringarna har släpat efter så finns det redan i dag lösningar som kan användas för att öka informationssäkerheten och motverka cyberbrottslighet.

Det fortsatta arbetet med informations- och cybersäkerhet behöver också diskuteras på samhällsnivå. I denna rapport utvecklar TechSverige de övergripande förslagen från rapporten En techagenda för Sverige som var inspelet till politiken inför valet och mandatperioden.

Det har blivit vanligare, farligare och dyrare med cyberbrott

Driftstörningar och andra problem sker ofta utan att det finns en brottslig gärning bakom. Tidigare var fel i utrustningen den vanligaste källan, i dag är det programmen som ger upphov till problemen. Det kan vara när en tjänst slutar fungera för att en annan tjänst har uppdaterats och därmed förändrats. Ett annat exempel är när ett nytt program inte är tillräckligt testat innan det tas i drift. Brister i it-administrationen, som kravställning, testning och driftövervakning, kan också ge upphov till avbrott.[1]

I dag drivs dock diskussionen om informations- och cybersäkerhet av de ökande cyberattackerna och cyberbrottsligheten – det vill säga när en antagonistisk aktör står bakom attackerna. Det kan vara brottslingar eller främmande makt.

Dataintrång var ett av de brott där polisanmälningarna ökade mest under 2021. Hela 11 531 anmälningar gjordes under året, vilket motsvarar en ökning med 2 617 anmälningar eller 29 procent jämfört med 2020.[2] Dataintrången och cyberbrotten sker i användarnas vardag och den största andelen av dataintrången, 5 500 anmälningar (48 procent), var i sociala medier eller e-tjänster.[3] Hela 6 av 10 internetanvändare har blivit utsatta för bedrägeriförsök på nätet under det senaste året.[4]

Ett stort mörkertal

Cyberattacker ökade globalt under 2022 med 38 procent jämfört med 2021. I Sverige var ökningen dock mindre, 8 procent. En förklaring till ökningen är ett ökat antal små, mer snabbfotade hackargrupper som fokuserat på samarbetsverktyg för distansarbete och distansundervisning. Bakom de svenska brottsanmälningarna döljer sig förmodligen ett mycket stort mörkertal. Under 2022 var statliga och militära mål de mest utsatta i Sverige, med ett genomsnitt på 1 440 attacker per verksamhet och vecka.[5]

---

[1] MSB (2018), s. 5–7.
[2] Brottsförebyggande rådet (2022).
[3] Svenska stöldskyddsföreningen (2022).
[4] Internetstiftelsen (2022), s. 89.
[5] Check Point Research (2022).

Farligare med nya hot

Utpressningsangrepp med gisslanprogram fortsätter att stå för de allvarligaste incidenterna.[6] Användningen av gisslanprogram ökade med 25 procent mellan 2021 och 2022.[7] Fler brottslingar experimenterar nu med olika typer av utpressning, utöver gisslanprogram. Det förekommer också att data stjäls, till exempel känsliga kunddata som förbrytarna hotar att publicera om brottsoffret inte betalar en lösensumma. En del brottslingar kopierar data och förstör originalen, bara för att sedan erbjuda offret att köpa tillbaka sina egna data.[8]

Cyberbrottsligheten riktar också in sig mot känslig verksamhet. En av 42 organisationer inom sjukvården utsattes för attacker med gisslanprogram under tredje kvartalet 2022.[9]

Dyrare att skydda sig

Kostnaderna för it-avbrott varierar förstås stort. I en undersökning från 2018 finns exempel från transportföretag, livsmedelsföretag och statliga myndigheter där kostnaderna varierade från tiotusentals kronor till tiotals miljoner på ett år. Avbrotten kunde vara från några timmar till hundratals timmar i enstaka fall.[10]

Den ökande brottsutvecklingen på området driver på kostnaderna. Det blir dyrare att skydda sig och kostnaderna för att återställa efter attacker kan bli stora. Under de senaste åren har premierna för cyberförsäkringar ökat kraftigt med en fördubbling 2019 och tredubblats sedan 2014.[11] Den totala skadekostnaden orsakad av cyberangrepp för bara svenska företag beräknades uppgå till cirka 30 miljarder kronor under 2021. Detta var en fördubbling sedan 2019 och motsvarade ungefär 80 000 svenska medianårslöner.[12]

Över tid har inte heller investeringarna i digitalisering åtföljts av investeringar i informationssäkerhet. Trots växande kostnader och betydelsen av cybersäkerhet anser 44 procent av svenska it-beslutsfattare att deras organisation inte har investerat tillräckligt i cybersäkerhet.[13]

Informations- och cybersäkerheten behöver höjas

Det finns många typer av hot och sårbarheter som behöver hanteras för att skydda verksamhets- och affärsnytta, personlig integritet, tillit och trygghet. En hög informations- och cybersäkerhet är en förutsättning för att maximera digitaliseringens möjligheter och samtidigt höja förtroendet för den digitala utvecklingen i samhället.

Säkerheten börjar i vardagen. Arbetet med informations- och cybersäkerhet måste följa med i samhällets digitalisering. En hög säkerhet för vardaglig drift och it-användning är grunden för skydd mot avancerade hot, inklusive från brottslighet och främmande makt.

Techbranschen kan bidra med produkter och tjänster som höjer säkerheten. Det kan röra sig om säkerhetsprogram, driftentreprenad eller stöd under och efter en attack eller störning. Det finns också tjänster som stöder till exempel informationsklassning, annat administrativt säkerhetsarbete och utbildning av användare. Det gäller också stöd i arbetet med informationssäkerhet som riskhantering – inte bara som en teknikfråga.

I vad som ibland kallas cyberdomänen, till skillnad från land, luft och hav, så har techbranschen en unik position för informationsinhämtning och försvarsförmåga. Därför behö-

---

[6] Truesec (2022).
[7] Truesec (2023), s. 4.
[8] Svensk Handel (2022).
[9] Check Point Research (2023).
[10] MSB (2018), s. 9–10.
[11] Stockholms Handelskammare (2022), s. 29.
[12] Stockholms Handelskammare (2022) s. 10.
[13] Radar Ecosystem Specialists (2021) s. 7.

ver branschen beaktas på ett annat sätt än vad som traditionellt gäller mellan å ena sidan brottsbekämpande myndigheter och försvarsmyndigheter och privata aktörer å andra sidan.

Det offentliga och näringslivet behöver varandra och måste samarbeta för att möta hoten. Techbranschen har kunskap, teknik och möjligheter att höja informationssäkerheten för många. Inom några områden har dock staten tillgång till resurser och möjligheter som måste komma näringslivet till del för att höja informations- och cybersäkerheten. Det gäller till exempel information om hot och aktörer som polis- och underrättelsemyndigheter har. I vissa fall upplever svenska företag att de får bättre stöd av andra länders myndigheter. Staten behöver också verka för att säkra kompetensförsörjningen inom informations- och cybersäkerhet.

Informations- och cybersäkerhet är ett komplext problem och det finns ingen snabb eller enkel lösning. Ingen aktör kan på egen hand lösa problemen inom informations- och cybersäkerhet. Utformningen av lagar och förordningar, liksom annat stöd måste i större utsträckning bygga på kunskap och förståelse för hur företagen verkar och den konkurrens svenska företag möter varje dag.

Nedan utvecklar TechSverige de förslag om informations- och cybersäkerhet som vi 2022 lanserade i En techagenda för Sverige.

Förslag för ökad säkerhet

Företag, offentlig sektor och medborgare måste känna trygghet, även i den digitala verkligheten. Hög informations- och cybersäkerhet är en förutsättning för sådan trygghet och därmed för att vi fullt ut ska kunna tillvarata digitaliseringens möjligheter.

Tilliten och förtroendet till den digitala utvecklingen riskerar att skadas om inte säkerhetsbrister och cyberattacker kan hanteras på ett rimligt sätt. Det gäller för den vardagliga driften, för hot från kriminella och i ett försämrat säkerhetsläge för Sverige.

Näringslivet tar i dag ett stort ansvar och arbetar för att öka informations- och cybersäkerheten – ett arbete som hela tiden behöver pågå. Det finns ett stort behov av att samarbeta i dessa frågor för att öka säkerheten för företag och andra organisationer. Ingen aktör kan själv lösa informations- och cybersäkerhetsproblemen, och för att stärka säkerheten behövs högre medvetenhet om hoten, mer samverkan, mer kompetens och bättre förmåga att bekämpa it-brottsligheten.

I TechSveriges rapport En techagenda för Sverige är informations- och cybersäkerhet framträdande. I avsnittet Stärk informations- och cybersäkerheten framförs förslag inom fyra områden.[14]

1. Öka medvetenheten om informations- och cybersäkerhetshoten.
2. Höj förtroendet och intensifiera samarbetet mellan myndigheter och företag.
3. Stärk kompetenstillgången inom informationssäkerhet.
4. Utveckla förmågan att möta nätbrottsligheten och cybersäkerhetshoten.[15]

[14] TechSverige (2022), s. 47.
[15] I techagendan: Utveckla polisens, åklagarnas och domstolarnas kompetens, förmåga och resurser att möta nätbrottslighet och cybersäkerhetshoten.

1. Öka medvetenheten om informations- och cybersäkerhetshoten

Det kan tyckas att utvecklingen går åt fel håll och är svår att bemästra. En bieffekt av några av de senaste årens incidenter som till exempel hanteringen av data på Transportstyrelsen, attackerna mot Coop och Kalix kommun – listan kan göras lång – är att medvetenheten har ökat. Det finns också hjälp att få; it- och säkerhetsföretag utbildar, ger råd och bidrar till sina kunders säkerhet.

Den förra regeringen vidtog sent i mandatperioden några åtgärder för att öka medvetenheten om informationssäkerhet med ett uppdrag till Myndigheten för samhällsskydd och beredskap (MSB) om att genomföra en informationskampanj riktad till allmänheten och till företag i syfte att öka medvetenheten och kunskapen om informations- och cybersäkerhet. Regeringen gav i april 2023 FRA ansvar för Nationellt cybersäkerhetscentrum och där arbetet har kommit i gång. Några myndigheter fick förstärkta resurser i budgetpropositionen för 2023 för att arbeta med informationssäkerhet. Trots det behöver medvetenheten höjas ytterligare på alla nivåer i samhället. Informationssäkerheten kan dock inte på sikt höjas med bara punktinsatser.

TechSveriges förslag:

- Utveckla myndigheternas arbete med att höja medvetenheten om informations- och cybersäkerhet, särskilt inom de områden där statliga myndigheter har unik information eller viktiga kommunikationskanaler.
- Punktinsatser och kampanjer räcker inte. Inled ett långsiktigt arbete för att höja medvetenheten och kompetensen i kommuner, regioner och statliga myndigheter samt i till exempel tillsyns-, beredskaps- och sektorsmyndigheter som riktar sig till privata aktörer.

2. Höj förtroendet och intensifiera samarbetet mellan myndigheter och företag

Med FRA:s ansvar för Nationellt cybersäkerhetscentrum följde bland annat uppdrag om att utveckla samarbetet med näringslivet. Frågan är om en underrättelsemyndighet med lätthet kan utveckla förmågan att leda och bistå i ett brett arbete med informations- och cybersäkerhet. Det är ett komplext samspel mellan bland annat teknik, organisation och verksamhet. Till detta kommer förutsättningar och regler till exempel tillsynsmyndigheter inom olika områden där statens ansvar skiftar. Flera myndigheters ansvar för viktiga informations- och cybersäkerhetsfrågor kvarstår också. Ett företags verksamhet kan falla under flera lagar och tillsynsmyndigheter i fråga om säkerheten. Det har också kommit både svensk lagstiftning och EU-lagstiftning som påverkar informationssäkerhetsarbetet i många branscher.

En undersökning från Almega visar att tjänsteföretag vill öka utbytet och samarbetet med myndigheter. Dessvärre tyder mycket lite på att ett sådant utbyte sker. En av anledningarna till detta var att flera myndigheter ansvarar för olika aspekter av cybersäkerhet, såsom myndigheter med ansvar inom en särskild sektor eller aspekt inom cybersäkerhet (till exempel MSB, Säkerhetspolisen och Polisen) eller myndigheter med samverkans- eller tillsynsansvar. Detta leder till osäkerhet vilken myndighet man kan och bör samverka med eller söka stöd från. En stor andel av de som faktiskt samarbetar med myndigheter anser dock att det fungerar bra.[16]

Formerna för hur myndigheterna, privata företag och organisationer samverkar och delar information om säkerhetshot behöver fortsätta att utvecklas. Relevanta myndigheter behöver bli bättre på att dela sådan information. I många fall har näringslivet information och kunskap som skulle öka säkerheten för flera aktörer om rätta förutsättningar kom på plats för att dela denna information under trygga former som till exempel sekretess när företagen delar information med myndigheter.

TechSveriges förslag:

- Den nya nationella informations- och cybersäkerhetsstrategin behöver ta större hänsyn till näringslivets behov och vad branschen kan bidra med.
- Samordna staten inom informations- och cybersäkerhet för att undvika att företagen ska rapportera till exempel incidenter eller vidtagna åtgärder till flera myndigheter.
- Se över befintliga nätverk och utveckla fler nätverk för samverkan mellan företag och offentlig sektor. Arbetet behöver inkludera fler branscher.
- Det behövs fler forum där företag kan rapportera och ta del av relevant information samt sprida goda exempel på hur de kan arbeta förebyggande med cybersäkerhet.
- Ersätt företagen för kostnader för statliga informationssäkerhetskrav som går utöver de som kan motiveras kommersiellt inom till exempel totalförsvar.
- Natomedlemskapet kommer att ställa större krav till exempel inom området resilienta civila kommunikationssystem. Ta med näringslivet direkt från start.
- Säkerställ att myndigheter inte konkurrerar med privata aktörer inom informations- och cybersäkerhet.
- Stärk förmågan hos statliga, kommunala och regionala myndigheter inom informations- och cybersäkerhet, bland annat i offentliga upphandlingar och i övrigt samarbete med den privata sektorn med offentlig it-drift.

[16] Almega (2022), s. 16–17.

3. Stärk kompetenstillgången inom informationssäkerhet

För att minska risken för och konsekvenser av cyberattacker behövs kompetens på alla nivåer. TechSveriges undersökningar visar att säkerhetsfrågorna är bland de viktigaste, både som drivkraft i kompetensbehovet och i efterfrågetillväxt. Efterfrågan på kunskap om informations- och cybersäkerhet måste få större genomslag i utbildningssystemet och på arbetsmarknaden.

TechSveriges rapport IT-kompetensbristen från år 2020 visar att it-säkerhet är den tredje viktigaste drivkraften i efterfrågan på kompetens.[17] Att stärka kompetenstillgången inom informationssäkerhet är något av det viktigaste staten kan göra. Fokus i debatten har varit på hur några statliga myndigheter (förvisso viktiga) som FRA, Must, MSB och Säkerhetspolisen kan stärka informationssäkerheten. Till slut är det ändå någons medarbetare som ska göra jobbet. Både privata och offentliga organisationer har behov av kompetens inom informationssäkerhet.

En av de viktigaste sakerna staten kan göra är att bidra till att lösa kompetensbrister inom informationssäkerhet. Staten är en stor utbildningsaktör och påverkar ramarna för många andra.

I dag saknas både en enhetlig bild av efterfrågan på olika säkerhetskompetenser och tillgång till ett utbildningsutbud som möter efterfrågan. Ett första steg skulle kunna vara att samla aktörer inom området för att analysera och identifiera kompetensbehoven. Sedan kan utbildningsanordnare på olika nivåer och i olika former ges förutsättningar att börja möta behoven av utbildningar.

TechSveriges förslag:

- Ta fram en lägesbild över kompetensbehoven. Det kan ske med hjälp av branschen i ett samverkansråd för området.
- Regeringen och utbildningsanordnare måste säkerställa att det finns informationssäkerhetsutbildningar på eftergymnasial nivå som svarar mot efterfrågan. Utbudet behöver tas fram i samverkan med näringslivet.
- Regeringen måste prioritera forskning och utbildning på högre nivå då dagens utbud är begränsat.

[17] TechSverige (2020), s. 15 och 18.

4. Utveckla förmågan att möta nätbrottsligheten och cybersäkerhetshoten

Företag och medborgare utsätts allt oftare för brott på nätet. Flera aktörer inom rättsväsende och stödmyndigheter behöver bli bättre på att förhindra, utreda och lagföra brott som begås på nätet. Det behövs både ändamålsenlig lagstiftning och resurser för att följa med i den snabba teknik- och brottsutvecklingen. Det ställer också stora krav på internationellt samarbete, både vad gäller normgivning och brottsbekämpning.

Informations- och cybersäkerhet är ett område som utvecklas snabbt och stiger på den internationella dagordningen. Sverige måste vara en stabil och kunnig aktör inom brottsbekämpning, nationellt som internationellt. Senfärdigheten har ibland varit skrämmande – det tog närmare tjugo år för Sverige att tillträda Europarådets konvention om it-relaterad brottslighet (Budapestkonventionen). Detta när det redan från början stod klart att frågorna var angelägna och behövde kontinuerlig uppmärksamhet.

Ett mer praktiskt exempel är att förundersökningen av attacken mot Kalix kommun lades ner på grund av bristande bevisning. Attacken som stängde alla it-system i kommunen och kostade tre miljoner kronor bara i konsultkostnader när man tvingades göra tre års utveckling på en månad.[18]

Det finns flera områden som behöver ses över för att bekämpa cyberbrott. Det krävs en mer utvecklad, ändamålsenlig och mindre sårbar polisiär organisation. Framgångsrikt brottsbekämpningsarbete mot den organiserade cyberbrottsligheten kräver ett polisiärt samarbete på internationell nivå. Polisens möjligheter att utreda komplexa dataintrång och delta i internationella sammanhang är beroende av en ändamålsenlig lagstiftning.[19] Det är angeläget att Sverige deltar i internationella samarbeten som till exempel International Counter Ransomware Initiative och arbetet inom EU.

TechSveriges förslag:

- Stärk Polismyndighetens avdelning nationellt forensiskt center (NFC) för att korta ledtiderna i brottsutredningar och gör det möjligt för privata it-forensiker att bistå myndigheterna.
- Stärk det internationella samarbetet mot cyberbrott och verka för att Sverige deltar med kraft fullt i det, både på politisk nivå och myndighetsnivå.
- Regeringen bör prioritera utvecklingen av lagstiftningen mot cyberbrott.
- Metoderna att bekämpa gisslanprogram bör vara i fokus för internationellt samarbete, lagstiftning och brottsbekämpning.
- Nationellt cybersäkerhetscenter bör utveckla riktlinjer och samarbetsformer att användas vid större attacker eller sårbarheter med nationell stor påverkan på både privata och statligt ägda verksamheter
- MSB (myndigheter/kommuner/regioner) bör få dela säkerhetsmeddelanden från CERT-SE även med leverantörer som har ansvar för till exempel driftentreprenad för bättre informationsdelningen.

[18] CIO (2022) och SVT (20022b).
[19] Brå (2022).

Källor

Almega (2022), Tjänsteföretagen och stärkt cybersäkerhet i Sverige, <https://www.almega.se/app/uploads/2022/06/cybersakerhet.pdf>.

Brottsförebyggande rådet (2022), pressmeddelande 2022-01-20, Anmälda brott 2021 – Preliminär statistik, <https://via.tt.se/pressmeddelande/anmalda-brott-2021-preliminar-statistik?publisherId=1026483&releaseId=3314612>.

Brå (2022), Polisanmälda dataintrång, <https://bra.se/publikationer/arkiv/publikationer/2022-10-31-polisanmalda-dataintrang.html>.

Check Point Research (2023), pressmeddelande 2023-01-11, Stor ökning av cyberattacker under 2022, <https://www.mynewsdesk.com/se/checkpoint/pressreleases/stor-oekning-av-cyberattacker-under-2022-3227008>

CIO (2022), Kalix it-chef efter attacken: ”Vi har gjort tre års utvecklingsarbete på en månad”, <https://cio.idg.se/2.1782/1.761407/kalix-efter-attacken--it-har-gjort-tre-ars-arbete-pa-en-manad>

Internetstiftelsen (2022), Svenskarna och internet 2022, <https://svenskarnaochinternet.se/app/uploads/2022/10/internetstiftelsen-svenskarna-och-internet-2022.pdf>.

MSB (2018), Driftavbrott i samhällsviktiga it-tjänster.

Radar Ecosystem Specialists (2021), Svensk cybersäkerhet 2021.

Stockholms Handelskammare (2022), Cyberbrott mot svenska företag, <https://stockholmshandelskammare.se/rapporter/rapport-cyberbrott-mot-svenska-foretag>.

Svensk Handel (2022), Threat Intelligence report från Truesec, <https://www.svenskhandel.se/nyhetscenter/nyheter/2022/threat-intelligence-report-fran-truesec/>.

Svenska stöldskyddsföreningen (2022), Årsstatistik dataintrång 2021, <https://sakerhetskollen.se/brottsstatistik/statistik-dataintrang-2021>.

TechSverige (2022), En techagenda för Sverige, <https://www.techsverige.se/techagenda/>.

Truesec (2022), pressmeddelande 2022-02-14, Cyberkriminella har bytt taktik, <https://press.truesec.se/posts/pressreleases/cyberkriminella-har-bytt-taktik>.

Truesec (2023), Threat Intelligence Report 2023.

EN RAPPORT FRÅN TECHSVERIGE

Techbranschens förslag för att möta cyberhoten

Version 1.1

TechSverige är en bransch- och arbetsgivarorganisation för alla företag inom techsektorn, med uppdrag att tillsammans med medlemmarna skapa bästa möjliga villkor för en världsledande techsektor i Sverige. Bland våra över 1 400 medlemsföretag – som sammantaget har närmare 100 000 medarbetare i Sverige – återfinns allt ifrån små startupbolag med få anställda, till stora, multinationella företag med tusentals anställda runtom i världen.

Besök oss gärna på techsverige.se

TechSverige