Policy för stärkt säkerhet i digitala leveranskedjor

Nulägesbeskrivning och analys sammanställdes i oktober 2025. Dessa kommer att uppdateras i det vidare arbetet med policyn.

Nulägesbild för policyområdet

It-tjänstekoncentrationen i Sverige är hög. Många organisationer använder sig av samma, eller endast ett litet antal leverantörer, för samma slags tjänster. Många organisationer ingår därmed i samma digitala leveranskedjor, och det leder i vissa fall till att monoberoenden etableras som en följd av nätverkseffekter. Ofta uppstår också inlåsningseffekter, d.v.s. omständigheter som gör det praktiskt mycket svårt att byta leverantör. När allt fler väljer en och samma tjänsteleverantör ges den tjänsteleverantören ekonomiska förutsättningar att stärka sitt erbjudande, vilket i sin tur gör att fler organisationer blir kunder till tjänsteleverantören, och ju mer utvecklad tjänsten som erbjuds är – desto svårare blir det att hitta en annan tjänst att byta till om en organisation skulle önska det.

Ett högt antal kunder hos en och samma tjänsteleverantör innebär också att den tjänsteleverantören får ekonomiska förutsättningar att finansiera en högre grad av säkerhet i sina system och tjänster. Samtidigt innebär det höga antalet kunder hos en och samma leverantör leda till att en incident hos den leverantören kan medföra bred påverkan i samhället. Samma omständigheter som gör att det finns goda möjligheter till hög robusthet har alltså samtidigt inneburit att incidenter, när de trots robustheten ändå inträffar, kan få större samhällspåverkan.

Detta återspeglas tydligt i den nationella statistiken för it-incidentrapporteringen. I rapporten Hoten mot de digitala leveranskedjorna[1] rapporterade MSB år 2021 att:

Sedan början på 2020 och fram till slutet på juni 2021 har två tredjedelar av alla inrapporterade incidenter hos leverantörer av samhällsviktiga eller digitala tjänster haft sitt ursprung i en leveranskedja.

[1] https://www.msb.se/sv/publikationer/hoten-mot-de-digitala-leveranskedjorna--50-rekommendationer-for-att-starka-samhallssakerheten/

MSB:s årsrapporter för it-incidentrapporteringen[2] har därefter årligen visat att en hög andel av de rapporterade incidenterna inte har inträffat hos den rapporterande organisationen själv, utan hos en leverantör av en tjänst som den använder sig av.

De vanligaste kända orsakerna till leveranskedjeincidenter i Sverige har, i likhet med andra kategorier av incidenter, varit misstag och systemfel. Naturhändelser som bakomliggande orsak är mer sällsynta i rapporteringen, men har globalt resulterat i bl.a. avbrott i tillverkning av fysiska komponenter (exempelvis i samband med en snöstorm och extrem kyla i Texas under februari 2021[3]) som behövs för upprättande, återställning respektive utveckling av informationssystem. Samtidigt har de leveranskedjeincidenter som har haft de mest allvarliga konsekvenserna i Sverige (Kaseya-incidenten[4], TietoEvry-incidenten[5] och Miljödata-incidenten[6,7]) de senaste åren alla orsakats av angrepp. Då de rapporterande organisationerna ofta har haft begränsad insyn i vad som har hänt hos deras leverantörer (och i de flesta *ingen* direkt insyn i vad som har hänt hos deras leverantörers leverantörer) så har det årligen också varit en hög andel rapporter som beskriver leveranskedjeincidenter och där det anges att orsaken till incidenten är okänd.

Ett relaterat fenomen som bl.a. beror på den bristande insynen hos leverantörer är s.k. *visklekproblematik*. Det betyder att information som upprättas och skickas vidare av en organisation långt ”uppströms” i kedjan, successivt tolkas och i tolkat format adderas till, reduceras från och vidarebefordras till organisationer nedströms. Det kan ofta ske på ett sätt som gör att den information som ursprungligen förmedlades inte är densamma som den information som når organisationer några steg längre ned i kedjan. Det leder till att organisationer får svårt att ta välgrundade beslut om hur de ska agera när incidenter sker, eller att de får en felaktig bild av vad som behöver göras och därför fattar olämpliga beslut.

Samhällskonsekvenser av incidenter i digitala leveranskedjor

Incidenter i digitala leveranskedjor får olika grad av samhällspåverkan i olika delar av landet beroende på huruvida boende och organisationer i lokalområdet har monoberoenden till någon eller några organisationer som drabbats av en sådan incident. Kaseya-incidenten drabbade organisationer inom bl.a. dagligvaruhandel (Coop) och apoteksverksamhet (Apoteket Hjärtat).[8] Konsekvenserna av incidenten varierade över landet. I områden där det finns flera apotekskedjor var det fortfarande möjligt att hämta ut medicin hos kedjor som inte nyttjade betalsystemet som hade infekterats med

[2] https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/hantera-och-rapportera-it-incidenter-och-cyberangrepp/arsrapporter-om-it-incidenter-och-cyberangrepp/
[3] https://www.bbc.com/news/technology-56114503
[4] https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack
[5] https://www.svt.se/nyheter/inrikes/120-myndigheter-drabbade-av-it-attack-tiotusentals-anstallda
[6] https://www.svt.se/nyheter/inrikes/miljodata-aterstallningen-ar-snart-klar
[7] https://www.svt.se/nyheter/inrikes/experten-en-miljon-svenskars-personuppgifter-publicerade-pa-darknet
[8] https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant

ransomware. På vissa platser i Norrland, där det exempelvis endast fanns en Coop-butik, innebar incidenten att boende fick resa långa avstånd för att få tag i dagligvaror.

Incidenter hos mycket stora it-tjänsteleverantörer kan också få *icke-linjära konsekvenser* för mottagare av den drabbade tjänsten. I samband med TietoEvry-incidenten förlorade först vissa regioner åtkomst till information och tjänster som de hyrde från TietoEvry. Därefter upptäckte de också att deras leverantörer av vissa typer av varor och artiklar också nyttjade tjänster från TietoEvry, varför det ett tag såg ut som att det kunde bli problem med att få även sådana leveranser.[9]

Ökad medvetenhet om risker med digitala leveranskedjor

De påtagliga konsekvenser som vissa leveranskedjeincidenter har haft har de senaste åren lett till en ökad medvetenhet bland såväl allmänheten som hos organisationer om vikten av att stärka säkerheten i de digitala leveranskedjor man nyttjar. Det finns dock en viss variation. Hos små och medelstora företag har utvecklingen inte varit lika påtaglig. Samtidigt har nya incidenter fortsatt att inträffa. Det är oklart om den ökade medvetenheten har lett till ett förstärkt cybersäkerhetsarbete hos leverantörer generellt.

Initiativ som syftar till att stärka säkerheten i digitala leveranskedjor

Den ökade medvetenheten om risker kopplade till digitala leveranskedjor har resulterat i att nya tjänster för att hantera sådana risker har utvecklats på olika nivåer och inom såväl staten som det privata näringslivet.

På EU-nivå är arbetet med att ta fram en verktygslåda för att stärka säkerheten i digitala leveranskedjor nu i sin slutfas.[10] Ett antal olika områden är också föremål för analys i enlighet med NIS2-direktivets artikel 22. Sverige, genom MSB, har, som ett av ordförandeländerna i arbetsgruppen som driver arbetet, en ledande roll.

I Sverige har regeringen gett MSB i uppdrag att genomföra en kartläggning av digitala leveranskedjor och ta fram en modell för uppföljning av digitala leveranskedjor.[11] Uppdraget har resulterat i att MSB:s verktyg Cybersäkerhetskollen numera inkluderar verktyget Leveranskedjekollen. Leveranskedjekollen har under 2025 för första gången tillhandahållits till svenska organisationer. MSB har också etablerat möjligheter för svenska organisationer att vända sig till myndighetens tjänst Cybersäkerhetsrådgivningen för att ställa frågor om säkerhet i digitala leveranskedjor. Ett arbete har också inletts på myndigheten för att utvidga tjänsten Metodstödet, så att organisationer ska ha ett mer fullödigt material om säkerhet i digitala leveranskedjor att nyttja för självstudier. Även andra myndigheter har tagit fram stöd. Exempelvis har Upphandlingsmyndigheten tagit fram stöd för utarbetandet av krav på bl.a. säkerhet vid upphandling[12] och Tillväxtverket

[9] https://lakartidningen.se/nyheter/hackerattacken-som-skakade-samhallet/
[10] https://www.mlex.com/mlex/technology/articles/2392767/eu-toolbox-for-managing-blocking-high-risk-digital-suppliers-almost-ready
[11] Fö2025/00390
[12] https://www.upphandlingsmyndigheten.se/om-hallbar-upphandling/socialt-hallbar-upphandling/arbetsrattsliga-villkor/ansvarsfulla-leveranskedjor/

kartlagt små och medelstora företags förutsättningar att arbeta med bl.a. säkerhet i digitala leveranskedjor[13].

Parallellt med utvecklingen av de ovan nämnda stödtjänsterna utvecklar MSB, i nära samarbete med de myndigheter som har föreslagits bli tillsynsmyndigheter utifrån Cybersäkerhetslagen, nya föreskrifter som bl.a. konkretiserar kraven i NIS2-direktivets artikel 21 p 2d om stärkt säkerhet i digitala leveranskedjor.

Samtidigt som myndigheterna har stärkt sitt arbete på området så har också det privata näringslivet utvecklat nya tjänster. Det finns idag ett brett utbud av såväl tekniska tjänster som olika utbildningar, rådgivningstjänster, stöd i utarbetandet av krav och andra delar.

För att ytterligare stärka det privata näringslivets tjänsteutbud avseende hantering av säkerhet i digitala leveranskedjor genomförde Sveriges nationella samordningscenter för forskning och innovation inom cybersäkerhet, NCC-SE (en del av MSB) också under 2025 en utlysning om finansiellt stöd till tredje part. Utlysningen utmynnade i att myndigheten beslutade om att stödja 25 nya projekt med ett samlat värde motsvarande totalt 34 miljoner kronor.[14]

Digital suveränitet

Digitala leveranskedjor utnyttjas också för problematisk eller antagonistisk aktivitet på andra sätt än genom cyberangrepp. Monoberoenden till digitala leveranskedjor som står under andra jurisdiktioners kontroll har utnyttjats, och fortsätter att utnyttjas, av andra stater utifrån säkerhets- och/eller geopolitiska intressen. Hot om att stänga av leveranser som samhällen har monoberoenden till används för att sätta press i syfte att få stater, eller organisationer i stater, att agera respektive avstå från att agera på vissa sätt. I vissa fall genomförs också det som man har hotat om att man skulle göra, exempelvis för att hämma eller sabotera aktivitet som man anser går emot de egna intressena.

Stater som har inflytande över leverantörer använder sådant inflytande för att driva egna intressen även när organisationer har egna, fristående och lokalt installerade digitala produkter, exempelvis genom att förhindra försörjning av komponenter, eller av säkerhetsuppdateringar som behövs för att hantera upptäckta sårbarheter. Det omvända förekommer också – stater utnyttjar sin kontroll för att antingen (i skymundan och utan leverantörens vetskap) introducera cyberhot i leverantörens digitala produkter, eller för att tvinga leverantören att själv introducera cyberhot i sina digitala produkter.

Jurisdiktionell kontroll används därutöver för att tilltvinga sig tillgång till information som flödar fram och tillbaka genom digitala leveranskedjor inom allt ifrån telekominfrastruktur till uppkopplade fordon.

---

13 https://tillvaxtverket.se/tillvaxtverket/publikationer/publikationer2021/sakerdigitaliseringismaochmedelstoraforetag.1427.html

14 https://ncc-se.msb.se/sv/nyheter/msb-beviljar-stod-till-25-nya-cybersakerhetsprojekt-for-att-starka-sveriges-digitala-leveranskedjor/

Den legala utvecklingen inom EU

För att hantera de komplexa säkerhetsutmaningarna kopplat till säkerhet i digitala leveranskedjor, inklusive den växande problematiken med statlig inblandning och statliga ingripanden i sådana leveranskedjor, har det införts, och fortsätter att införas, ny lagstiftning för att öka säkerheten. Den legala utvecklingen kan delas in i tre kategorier, reglering av säkerhet i digitala leveranskedjor där:

1. både leverantör och mottagare, respektive deras ägare, finns inom EU,
2. leverantören eller dess ägare finns utanför EU och mottagaren och dess ägare finns inom EU,
3. leverantören och dess ägare finns inom EU och mottagaren eller dess ägare finns utanför EU.

I den första kategorin ingår krav på organisationer, både leverantörer och mottagare, att stärka sin insyn i, kontroll över och säkerhet i digitala leveranskedjor (exempelvis med stöd av NIS2-direktivets artikel 21 p 2d), särskilda insatser för att öka säkerheten vissa särskilt viktiga digitala leveranskedjor (i EU med stöd av NIS2-direktivets artikel 22) och krav på att utveckla och tillhandahålla produkter som har tagits fram enligt *security by design*-principer (med stöd av Cyberresiliensförordningen). Det ingår också i regleringarna att tillsyn ska utövas av ansvariga myndigheter för att säkerställa att regelverket efterlevs, och tillsynsmyndigheterna har relativt kraftfulla verktyg för att sanktionera bristande regelefterlevnad.

I den andra kategorin har det införts legala ramverk för att kunna besluta om såväl handelshinder och som begränsningar av utom-jurisdiktionellt ägande i vissa industrier och teknologier (såsom Europaparlamentets och rådets förordning (EU) 2019/452 av den 19 mars 2019 om upprättande av en ram för granskning av utländska direktinvesteringar i unionen). EU-kommissionen har också tagit initiativ till att uppdatera EU:s Cybersäkerhetsförordning, och har i anslutning till det öppnat för att införa ett legalt ramverk för att hantera icke-tekniska aspekter på säkerhet i digitala leveranskedjor.[15]

Befintligt lagrum nyttjas också för att begränsa utom-jurisdiktionellt inflytande över upphandlade tjänster, såsom i fallet där Arbetsförmedlingen uteslöt anbudsgivare med ägaranknytning till länder som Säkerhetspolisen har pekat ut som hot mot Sverige.[16]

I den tredje kategorin kan exempelvis inräknas EU-förordningen 2021/821 om upprättande av en unionsordning för kontroll av export, förmedling, transitering och överföring av samt tekniskt bistånd för produkter med dubbla användningsområden.[17]

En konsekvens av den ökade styrningen, och den tillkommande komplexiteten som kommer genom nya lagkrav, är att det blir dyrare och svårare att göra affärer inom berörda

[15] https://digital-strategy.ec.europa.eu/en/news/commission-opens-consultation-revising-eu-cybersecurity-act
[16] https://www.dagensjuridik.se/nyheter/domstol-kinesiskt-agande-kan-utesluta-bolag-fran-upphandling/
[17] https://isp.se/produkter-med-dubbla-anvandningsomraden/introduktion-till-pda/

sektorer. Många organisationer upplever att den stora mängden krav som följer av ett stort antal olika lagar som organisationer måste följa samtidigt innebär att stora resurser måste läggas på att identifiera den samlade kravbilden och regelefterlevnad.[18]

När sådant som inte ska levereras ändå levereras

Det finns två typer av risk i digitala leveranskedjor. Den första sortens risk handlar om att mottagande organisationer *får* något skickat till sig som de *inte ska* ha och behandlas i detta avsnitt. Den andra risken behandlas i nästföljande avsnitt.

En drivande faktor i nyttjandet av digitala leveranskedjor är att mottagande organisationer i allmänhet försöker uppnå maximal effektivitet i hanteringen av det som levereras genom att endast i begränsad omfattning granska och testa det som skickas till dem inom ramen för den digitala leveranskedjan. Ofta finns det en förberedd kanal in i organisationen som ska minimera tiden mellan mottagande och installation och tillämpning. Detta gäller i synnerhet mjukvaruuppdateringar. Mottagande organisationer upprättar en sådan kanal när de har förtroende för avsändaren och när de har stor nytta av att uppdateringen installeras snabbt och i alla relevanta delar av organisationens it-miljö. Om det som har levererats då är skadlig kod, eller skadlig kod ingår som en komponent i en uppdatering, kan stor skada uppkomma innan organisationen inser vad som har hänt eller kan göra något för att stoppa den skadliga utvecklingen. Även om det är ovanligt så förekommer det att motsvarande händer med fysiska komponenter. Det blev inte minst blev tydligt i samband med att personsökare som hade levererats till den libanesiska organisationen Hizbollah i september 2024 exploderade efter att en i hemlighet inbyggd spränganordning i personsökarna nåddes av en given signal – något som ledde till flera dödsfall och många skadade.[19]

Ett specialfall av den här problematiken rör säkerhetsuppdateringar. Generellt är rådet som ges till organisationer att de ska installera säkerhetsuppdateringar så fort och så brett som möjligt. Genom att göra det så förebyggs angripares möjligheter att genomföra angrepp med hjälp av sårbarheten som säkerhetsuppdateringen åtgärdat. Det är vanligt att säkerhetsuppdateringar släpps precis innan, och ibland samtidigt, som angrepp som bygger på sårbarheten genomförs. Men om säkerhetsuppdateringen i sig innehåller skadlig kod så kan ambitionen att snabbt säkerställa att organisationen har ändamålsenligt it-skydd innebära att desto mer skada orsakas istället.

En ytterligare problematik kopplat till uppdateringar består i att tjänster som upprätthåller säkerheten i it-miljöer oftast har (för att de behöver ha) djupgående tillgång och rättigheter till konfigurationer och kärnsystem för att dels kunna upptäcka, och dels (genom att ha ändringsrättigheter) kunna bekämpa antagonistisk aktivitet. Skadlig kod som ingår i uppdateringar till sådana tjänster får därför direkt möjlighet att orsaka skada på djupare

[18] https://www.svensktnaringsliv.se/english/simplifying-the-eus-digital-regulatory-framework_1233384.html
[19] https://en.wikipedia.org/wiki/2024_Lebanon_electronic_device_attacks

nivåer eller i mer skyddsvärda miljöer än skadlig kod som kommer in i miljön på andra sätt. Ett globalt uppmärksammat exempel på det var Crowdstrike-incidenten 2024.[20]

Utveckling av programvara är en komplex process som ofta innebär att kod som redan har tagits fram i andra sammanhang, och som utför en viss sorts funktion, introduceras i en större uppsättning kod för att skapa en komplex produkt med många olika funktioner. Koden som återanvänds hämtas ifrån kodbibliotek och koden som finns i sådana bibliotek underhålls och utvecklas av organisationer och individer som organisationen som ska använda koden kanske aldrig har haft kontakt med, eller vet vilka de är. Den här omständigheten resulterar i att organisationer inte alltid vet vad koden de har i sina egna produkter kommer att göra givet olika typer av inputs, eller givet vilken miljö koden introduceras i. För att hantera den här utmaningen har olika initiativ om programvaruförteckningar (*Software Bill of Materials*, SBOM[21]) växt fram. Att underhålla sådana förteckningar är dock resurskrävande och initiativen har fått begränsat genomslag.

Det höga antalet kunder, den snabba och förtroendebaserade process som organisationer följer när de installerar i synnerhet mjukvara som de mottar och den djupa tillgången till system och tjänster som i synnerhet it-säkerhetstjänster måste ha gör att leverantörer av it-tjänster i allmänhet, och leverantörer av it-säkerhetstjänster i synnerhet, utgör lockande mål för hotaktörer som önskar sprida skadlig kod till många, eller till mål som i övrigt är väl skyddade. Intresset för leverantörer tar sig båda i uttryck genom cyberangrepp, men också genom att stater utövar juridiskt och annat inflytande över sådana leverantörer på sådana sätt som har beskrivits ovan.

När sådant som ska levereras inte levereras

Det finns två typer av risk i digitala leveranskedjor. Den andra sortens risk handlar om att mottagande organisationer *inte får* något skickat till sig som de *ska* ha och behandlas i detta avsnitt. Den andra risken behandlas i föregående avsnitt.

Den vanligaste formen av digital leveranskedjeincident är avbrott i en sådan tjänst som en tjänsteleverantör tillhandahåller till andra.

Det är vanligt att organisationer saknar redundans i sina tjänster, varför uteblivna leveranser av digitala produkter från en leverantör innebär att produktion eller verksamhet avstannar, eller åtminstone tappar påtagligt i effektivitet och takt.

Det förekommer också att digitala produkter levereras, men saknar sådana komponenter (i form av funktionalitet eller skydd) som den mottagande organisationen förväntar sig, eller har uppfattat, ska ingå i den digitala produkten. När sådan hård- eller mjukvara installeras och används uppstår problem när förväntade funktioner eller effekter visar sig saknas eller inte uppstå. På motsvarande sätt exponerar organisationer som installerar nya digitala produkter som de tror har ett adekvat skydd, men som i själva verket inte har det, sig för angrepp eller misstag som de inte förväntar sig ska kunna vara skadliga för dem.

[20] https://en.wikipedia.org/wiki/2024_CrowdStrike-related_IT_outages
[21] https://about.gitlab.com/blog/the-ultimate-guide-to-sboms/

Ett vanligt fenomen är att en tjänsteleverantör, för att kunna leverera en viss tjänst, samtidigt också måste vara mottagare av stora mängder information ifrån de som tjänsten ska levereras till. Exempelvis kan lagrings- respektive bearbetningstjänster endast göra nytta om de ges information att lagra eller bearbeta. När många organisationer lagrar eller bearbetar sin information hos samma leverantör kan det därför, om det uppstår en incident hos leverantören, bli så att de organisationernas information raderas eller otillbörligen tillgängliggörs. Detta blev i Sverige påtagligt i samband med Miljödata-incidenten 2025, under vilken bl.a. HR-tjänsterna Miljödata tillhandahåller angreps, varpå informationen som hade lagrats däri sedermera publicerades på Darknet.

Analys av nuläget

Det är positivt att medvetenheten om riskerna kopplat till digitala leveranskedjor har ökat, och att det har resulterat i att såväl staten som det privata näringslivet har utvecklat nya tjänster för att underlätta arbetet med att stärka säkerheten. Det är också positivt att ny lagstiftning, såsom NIS2-direktivet, DORA-förordningen och Cyberresiliensförordningen, har tillkommit och ställer krav på ökad säkerhet i digitala leveranskedjor. Därtill är det positivt att individer och organisationer i medelstora och större orter i landet, där det finns fler än en leverantör av viktiga samhällsfunktioner som var för sig har olika digitala leveranskedjor, (åtminstone i viss utsträckning) kan kompensera för bortfallet av en viss leverantörs samhällsviktiga funktion (såsom telenät, dagligvaruhandel, etc.) genom att vända sig till en annan.

Samtidigt finns ett antal utmaningar inom området:

- Incidenter i digitala leveranskedjor fortsätter att inträffa i oförminskad årlig frekvens. Incidenter som inträffar hos leverantörer av digitala produkter får ofta inverkan på många andra organisationer som drabbas i förlängningen. Incidenterna orsakas av såväl misstag och systemfel som av angrepp.
- Förekomsten av monoberoenden och inlåsningseffekter. När incidenter inträffar hos leverantörer som det finns ett monoberoende till så uppstår en ofta påtagligt högre samhällspåverkan än när samma slags incidenter inträffar hos andra organisationer. Monoberoenden uppstår som en följd av nätverkseffekter.
- Stater utnyttjar att monoberoenden har uppstått i förhållande till leverantörer som de kan utöva inflytande över, eller ingripa hos, som ett sätt att hota eller påverka andra stater och i syfte att uppnå säkerhets- eller geopolitiska mål. Sådant inflytande orsakas av att vissa tjänsteleverantörer har ett tekniskt och tjänstemässigt försprång gentemot lokala alternativ, och det försprånget innebär att nätverkseffekter uppstår, varpå monoberoenden resulterar.
- Incidenter (i form av att sådant som ska levereras inte levereras) som inträffar hos tjänsteleverantörer som har många kunder resulterar ibland i icke-linjära konsekvenser för mottagare av den eller de drabbade tjänsterna. När mottagare av den drabbade tjänsten också nyttjar tjänster ifrån andra organisationer som också nyttjar den drabbade tjänsten kan de drabbas dubbelt. Först genom att de förlorar åtkomst till sin information och tjänsterna de använder, och därefter genom att

andra leveranser som de också ska ha uteblir eftersom leverantören av de leveranserna också har förlorat åtkomst till tjänster de är beroende av för att kunna genomföra sin verksamhet. Sådana icke-linjära konsekvenser orsakas också av nätverkseffekter.

- Incidenter (i form av att sådant som inte ska levereras ändå levereras) sker och får allvarligare konsekvenser genom att skadliga digitala produkter levereras inom ramen för en förtroendebaserad process där endast begränsad granskning och testning sker, och målet är snabb och bred implementering. Sådana allvarligare konsekvenser möjliggörs och orsakas av att det ofta finns goda skäl för organisationer att arbeta på ett sådant sätt.
- Leverantörer av digitala produkter, framförallt it-tjänsteleverantörer, och i synnerhet it-säkerhetstjänsteleverantörer, utgör särskilt intressanta mål för hotaktörer. När cyberangreppsförsök mot sådana organisationer lyckas så får det typiskt sett följdkonsekvenser för många andra organisationer. Hotaktörers incitament att angripa sådana organisationer orsakas av att de har många kunder, att de har förtroendebaserade processer (processer där granskning och testning endast genomförs i begränsad utsträckning) för att överföra och installera sina digitala produkter hos sina kunder och för att deras produkter (i synnerhet vad gäller it-säkerhetstjänsteleverantörer) ofta måste ha djupgående tillgång och rättigheter i mottagarnas it-miljöer.
- Många organisationer har bristande insyn hos sina leverantörer, och får begränsat med information – ibland med en tidsfördröjning – vilket gör att möjligheten att mildra incidenters konsekvenser blir begränsad. Den bristande insynen är ett resultat av otillräcklig kravställning när tillhandahållandet av tjänsten har avtalats.
- Många organisationer har också begränsad insyn i vad koden de nyttjar ifrån andra källor har för funktion, eller hur dess funktion förändras när den genomgår uppdateringar. Det leder till att skadlig kod kan inkluderas i kod som i övrigt fyller en viktig funktion i olika sorters programvara, utan att den som använder koden i sin digitala produkt vet om det. Problematiken orsakas av att det är ekonomiskt mycket fördelaktigt att kunna återanvända redan producerad kod som man vet att man själv, eller andra, tidigare har sett göra sådant som man behöver ha kod för att göra. Det har därför växt fram ett förtroendebaserat system för vidareutnyttjande av kod som kan utnyttjas av hotaktörer för att introducera medvetet utvecklad skadlig kod, men som också kan resultera i att oupptäckta buggar introduceras i stora mängder kod hos olika organisationer.
- Viskleksproblematik uppkommer när incidenter i digitala leveranskedjor får konsekvenser i flera led och information inte delas transparent mellan alla led. Detta hämmar förmågan att begränsa incidenters konsekvenser hos organisationer i det andra ledet, och organisationer i ytterligare led efter dem. Viskleksproblematik blir resultatet när information om det inträffade inte delas publikt, och information om det inträffade delas typiskt sett enbart publikt om det finns tydliga lagkrav om det eller om det ligger i den drabbade organisationens eget intresse att informera om det inträffade.

- Stora mängder (ofta skyddsvärd) information koncentreras hos vissa leverantörer. För att tjänsten som en leverantör tillhandahåller ska kunna fungera krävs ofta att mottagaren av tjänsten överför sin information. Det leder till att många organisationer sparar sin (ibland känsliga) information på ett och samma ställe. Det kan i sin tur leda till att många organisationer samtidigt får sin information raderad, eller exponerad, när en incident inträffar hos leverantören. Problematiken orsakas inte av någon särskild faktor, utan är en del av själva tjänstemodellen.
- Regleringen av området är inte samlad, utan kommer ifrån ett antal olika lagar. Det får till konsekvens att det blir svårt för organisationer att överblicka vad de förväntas göra. Det förekommer också att organisationer upplever att det är svårt att sammanställa en samlad kravbild, inte minst då det är olika ansvariga myndigheter (som huvudsakligen har kunskap och kompetens inom den del av området som de har ansvar för) som måste konsulteras för att (exempelvis) förtydliga hur lagtext ska förstås. Utmaningen är orsakad av en blandning av faktorer som har att göra med att området överlappar med många andra områden som var för sig har egen reglering och att lagstiftaren de senaste åren har sett behov av att ytterligare reglera området med anledning av bl.a. hotbildsutvecklingen.

Myndigheten för samhällsskydd och beredskap

Postadress: 651 81 Karlstad
Telefon: 0771-240 240 Fax: 010-240 56 00
registrator@msb.se www.msb.se
Org.nr: 202100-5984