Myndigheten för samhällsskydd och beredskap

Medfinansierat av Europeiska unionens fond för ett sammanlänkat Europa

Hoten mot de digitala leveranskedjorna

50 rekommendationer för att stärka samhällssäkerheten

Hoten mot de digitala leveranskedjorna
– 50 rekommendationer för att stärka samhällssäkerheten

MSB står ensamt ansvarig för denna publikation, vars innehåll inte nödvändigtvis återspeglar Europeiska unionens hållning.

Omslag: Shutterstock
Tryck: DanagårdLiTHO
Produktion: Advant

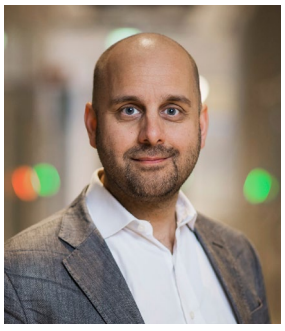
Publikationsnummer: MSB1855 - november 2021
ISBN: 978-91-7927-194-7

Förord

De senaste åren har de digitala leveranskedjorna växt i betydelse för såväl enskilda människor som för organisationer och samhället i stort. Utvecklingen sker i takt med den globala digitaliseringen och varken kan eller bör undvikas. På det hela taget, är fördelarna med utvecklingen stora, men den är inte riskfri. Det är vår uppgift att i samarbete med andra bygga och sprida mer kunskap om de digitala leveranskedjorna, hur de fungerar och kan se ut, vilka risker de medför och vad som kan göras för att öka säkerheten i dem. I delar där staten kan göra en insats på ett mer handfast sätt har vi också en roll att spela. Målet är naturligtvis att de digitala leveranskedjorna ska leva upp till samhällets behov av säkerhet och funktionalitet.

Efter ett antal uppmärksammade incidenter i eller genom digitala leveranskedjor de senaste åren har säkerhetsfrågorna aktualiserats. Det är tydligt att vi behöver stärka hela ekosystemet av producerande, transporterande och mottagande organisationer, så att vi kan stå bättre rustade mot hoten vi ser. De senaste årens säkerhetspolitiska utveckling har föranlett en omvärdering av gamla uppfattningar, och den digitala omställning som har skett under pandemin har aktualiserat att vi behöver tänka nytt även på det digitala området.

Min förhoppning är att den här rapportens redogörelse för riskbilden och dess konsekvenser, både det analytiska ramverket och rekommendationerna, ska bidra till att öka säkerheten i de digitala leveranskedjorna. Det vi behandlar här är, i slutändan, en delmängd av de utmaningar som det systematiska och riskbaserade informationssäkerhetsarbetet ska kunna – och kan – bemöta. Det är min fasta övertygelse att det är genom att vi blir mer systematiska och grundade i riskerna som vi på allvar kan tillvarata digitaliseringens fördelar utan att äventyra samhällssäkerheten. Vi på MSB kommer att fortsätta göra vår del, både genom den här rapporten och kommande produkter och satsningar.



Stockholm, 2021-11-10

Åke Holmgren

Avdelningschef, Avdelningen för cybersäkerhet och säkra kommunikationer
Myndigheten för samhällsskydd och beredskap

Innehåll

Begreppsförteckning

Detta kapitel innehåller de begrepp, med tillhörande beskrivningar, som är centrala för rapporten.

Aktör: Används i rapporten som synonymt med ”organisation”.

Baklängeskonstruktion: Ett förfarande där en produkt demonteras och dess respektive delar analyseras för att man därigenom ska kunna sluta sig till hur produkten fungerar.

Digital leveranskedja: De tjänster och infrastrukturer som levererar eller möjliggör leverans av digitala produkter vilka används för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem.

Digital produkt: En informationsmängd (som kan upprättas, lagras och bearbetas i informationssystem), mjukvara, hårdvara eller en tjänst (som upprätthålls, utvecklas och tillhandahålls via informationssystem).

Förtroendebaserad: Ett förhållande mellan aktörer som baseras på tillit och där man därför i mindre utsträckning kontrollerar och granskar produkter och tjänster som man mottar.

Halvledare: Halvledare utgörs av material vars elektriska ledningsförmåga är mellan ledares och isolatorers. På grund av detta kan de användas som små strömbrytare i datorchipp – och är därför fundamentala för modern elektronik.

Incident i digital leveranskedja:

1. En händelse där något som:
    a. ska levereras i den digitala leveranskedjan (en framgångsfaktor eller ett skydd) inte levereras, eller
    b. inte ska levereras i den digitala leveranskedjan (ett hot eller ett hinder) ändå levereras, och
2. där händelsen resulterar i antingen en oplanerad negativ påverkan[1] eller en oönskad avsaknad av positiv påverkan[2] på informationssystems, eller informationen i informationssystems, konfidentialitet, riktighet eller tillgänglighet.

Levererande organisation: En organisation som levererar, det vill säga producerar och skickar eller transporterar digitala produkter vidare i en digital leveranskedja.

Monoberoende: En organisation har ett monoberoende av (exempelvis) en tjänst när den är beroende av den tjänsten och det inte finns några alternativa tjänster att använda ifall den tjänst man redan använder upphör.

Mottagande organisation: En organisation som mottar digitala produkter i en digital leveranskedja.

Noder: Organisationer som utgör en startpunkt för många digitala leveranskedjor, eller genom vilka många digitala leveranskedjor passerar.

Underleverantör: Används i rapporten som synonymt med levererande organisation.

---

1. Såsom när skadlig kod installeras i ett informationssystem p.g.a. en mjukvaruuppdatering som skickats ut inom ramen för en digital leveranskedja.

2. Såsom när en ny komponent som behövs för att reparera ett trasigt informationssystem inte levereras trots att det är beställt.

Sammanfattning

Sammanfattning

Digitala leveranskedjor möjliggör de flesta samhällsviktiga tjänster som vi använder dagligen och är beroende av. Incidenter i leveranskedjorna kan leda till omfattande konsekvenser och kommer sannolikt, i takt med den fortsatta digitaliseringen, att bli allt vanligare.

Den moderna ekonomin präglas av att många organisationer fokuserar på sin mest centrala verksamhet. Man specialiserar sig på det man är, och ska vara, bra på. För att kunna göra det utkontrakterar många organisationer verksamhet och stödfunktioner, som inte hör till kärnverksamheten, till andra organisationer. Detta gäller i synnerhet informationsflöden, mjuk- och hårdvara, samt digitala tjänster – så kallade digitala produkter. På motsvarande sätt väljer många organisationer att fokusera på en egen, specifik och avgränsad nisch i värdekedjan. När den egna nischen blir snävare så ökar organisationens behov av leveranser av komponenter. Då detta är en utveckling som många organisationer genomgår uppstår ett läge där organisationer blir beroende av allt fler underleverantörer, som i sin tur blir beroende av ytterligare fler underleverantörer. Kedjorna blir mer komplexa, och involverar allt fler organisationer. När organisationer blir nischade blir också deras produkter mer särpräglade – och när det händer kan det uppstå ett läge där en organisation blir helt, eller nästintill, ensam om att leverera en viss typ av produkt. Organisationer som är beroende av sådana produkter har monoberoenden.

Antalet monoberoenden till specifika digitala leveranskedjor, och antalet organisationer som har samma monoberoende, verkar öka över tid – och det medför två växande risker. Den ena är att avbrott i leveranserna av en viss digital produkt leder till avstannad verksamhet hos allt fler. Den andra är att behovet av att fort installera, aktivera eller använda den digitala produkt som levereras för att snabbt kunna dra nytta av den gör att organisationer undviker att testa och granska leveransen för att slippa förlora tid. Följden blir att skadlig kod eller annat som inte ska följa med i leveransen installeras, aktiveras eller används hos många på en och samma gång. De båda riskernas omfattning börjar nu bli påtagliga på samhällsnivå.

De båda riskerna kan realiseras och bli till incidenter på ett antal olika sätt. Vi har därför utgått ifrån allriskperspektivet i arbetet med denna rapport. Vi har delat in hoten som orsakar incidenter i digitala leveranskedjor i fyra övergripande kategorier; misstag, angrepp, systemfel och naturhändelser. Vi har bedömt att det är viktigt att ge en bred bild av incidenter i digitala leveranskedjor. Bedömningen grundar sig dels i att ett antal incidenter i digitala leveranskedjor som har orsakats av angrepp har uppmärksammats under det senaste året. Samtidigt visar incidentrapporteringen som myndigheten mottar att:

- Det är mycket vanligt med incidenter i digitala leveranskedjor.
- Den stora majoriteten av sådana incidenter orsakas av misstag, systemfel och naturhändelser.
- Incidenter i digitala leveranskedjor som orsakas av icke-antagonistiska hot kan leda till konsekvenser som är lika allvarliga som de som följer av angrepp.

Vi har också funnit att informationsdelningen i de digitala leveranskedjorna ofta brister, att det gör att många organisationer kan vara omedvetna om hur deras säkerhetssituation ser ut och att det kan vara svårt att veta vad man ska göra när en incident sker i någon av ens digitala leveranskedjor. Det finns även en risk att man får felaktig eller missvisande information som kan leda till att man fattar dåliga eller ineffektiva beslut.

Vi har utfört analysen av riskerna på tre nivåer; organisationsnivån, den nationella nivån och den internationella nivån. Resultatet har gjort det tydligt att den samhällsutmaning som riskerna med koppling till monoberoenden i digitala leveranskedjor medför behöver hanteras i samverkan mellan de olika nivåerna. Rapporten innehåller därför rekommendationer till aktörer på alla de tre nivåerna; till levererande och mottagande organisationer på organisationsnivån, till organisationer som stöttar, reglerar och utför tillsyn över organisationer i digitala leveranskedjor på den nationella nivån och till stater och statliga organ på den internationella nivån.

Kärnan i rekommendationerna är att:

1. Bryta monoberoenden där det är möjligt.
2. Hitta sätt att hantera nya problem och utmaningar utan att upprätta nya eller befästa befintliga monoberoenden.
3. Bygga in mer säkerhet i de digitala leveranskedjorna så att den destruktiva potentialen de medför minskar.
4. Stärka informationsdelningen så att incidenter kan hanteras mer samordnat mellan de ingående organisationerna i en digital leveranskedja.

Slutsatser och rekommendationer

Slutsatser och rekommendationer

Den stegvisa specialiseringen och digitaliseringen leder till att allt fler digitala leveranskedjor upprättas, och att även av olika och sammanlänkade aktörer som är beroende av varandra blir allt tätare. Utvecklingen gör att incidenter i digitala leveranskedjor sannolikt kommer att bli allt vanligare, och effekterna av sådana incidenter kommer att fortsätta slå brett om inte exempelvis monoberoendena kan brytas.

I det här kapitlet presenterar vi övergripande slutsatser och rekommendationer utifrån MSB:s arbete med att analysera hoten mot, och sårbarheterna i, de digitala leveranskedjorna. Hoten kan resultera i två typer av incidenter, dels i form av incidenter där sådant som inte ska levereras ändå levereras[3], dels i form av incidenter där sådant som ska levereras inte levereras.[4] Vi har delat upp slutsatserna och rekommendationerna i varsitt avsnitt utifrån rapportens huvudsakliga målgrupper.

Det finns olika typer av hot mot digitala leveranskedjor, men de kan övergripande delas in i:

1. Mänskliga hot (både antagonistiska hot i form av angrepp och icke-antagonistiska hot i form av misstag).
2. Tekniska hot (i form av systemfel).
3. Naturhot (såsom väderfenomen, jordbävningar, etc.).

Vi har efter en genomgång av data från incidentrapporteringen och händelser i omvärlden bedömt den vanligaste källan till incidenter i digitala leveranskedjor med mottagande organisationer i Sverige är misstag och systemfel i samband med att aktörer levererar digitala produkter. Samtidigt har hotaktörer ett särskilt incitament att angripa via de digitala leveranskedjorna eftersom de kan användas för att få åtkomst till känsliga system hos de som använder dessa. Utöver pandemins påverkan på produktion och transport av digitala produkter utgör många naturhot ett växande problem för de digitala leveranskedjorna, det gäller inte minst klimatförändringarna.

3. Såsom skadlig kod och andra hot som av misstag eller avsiktligen byggs in i den digitala produkt som ska levereras, med eller utan tillverkarens vetskap.

4. Såsom misstag och sabotage i produktionen eller transporten, handelshinder eller naturfenomen.

Slutligen måste vi betona att det mest centrala för att organisationer ska kunna uppnå och bibehålla en lämplig nivå för sin informations- och cybersäkerhet är att de bedriver ett systematiskt och riskbaserat informationssäkerhetsarbete. Hoten mot leveranskedjorna bör identifieras och hanteras inom organisationens informationssäkerhetsarbete som ska klargöra ansvarsförhållanden och arbetssätt för att skydda organisationens information och informationssystem. Det innebär bland annat att värdera hur viktig information och informationssystem är för organisationen och bedöma riskerna vad gäller tillgänglighet, riktighet och konfidentialitet när information och system behövs. Utifrån resultatet av riskbedömningen kan organisationen prioritera vilka åtgärder (tekniska och administrativa) som kan införas för att säkerställa ett ändamålsenligt skydd.

Till levererande organisationer i digitala leveranskedjor

MSB:s genomgång av incidentrapporteringsdata och andra källor visar att det är vanligt att organisationer drabbas av incidenter som uppstått hos andra organisationer som levererar information, mjukvara, hårdvara eller tjänster. Enligt MSB:s incidentrapporteringsstatistik[5] har systemfel och misstag hittills varit de vanligaste kända orsakerna till incidenter men bland annat sommarens angrepp mot Kaseya (som i Sverige bl.a. drabbade Coop) visar att även angrepp genom digitala leveranskedjor kan få allvarliga konsekvenser.

Organisationer fortsätter att specialisera sig inom de flesta samhällssektorer. För att kunna göra det lägger de ut viss verksamhet och stödfunktioner på andra organisationer. Följden blir att fler och fler digitala leveranskedjor upprättas, och att vissa organisationer som exempelvis tillhandahåller stödfunktioner tillhandahåller de funktionerna till allt fler. Därmed bildas så kallade noder, och i vissa fall monoberoenden. När incidenter inträffar hos noder får de konsekvenser för många eller alla som använder nodens tjänst. Två tredjedelar av rapporterna som inkommer till MSB med anledning av NIS-regleringen[6] beskriver incidenter som har inträffat hos en aktör som tillhandahåller en tjänst till NIS-leverantören. Rapporterna MSB mottar visar att NIS-leverantörerna ofta har en begränsad insyn i vad som har hänt hos deras underleverantör, bland annat avseende vad som har orsakat incidenten. I de fall där NIS-leverantören har kunnat redogöra för orsaken handlar det nästan uteslutande om systemfel eller misstag.

Den successiva utkontrakteringen till organisationer som specialiserar sig på att tillhandahålla it-tjänster leder till att allt fler blir beroende av ett relativt begränsat antal underleverantörer. När sådana leverantörer konfigurerar om system, lägger till eller tar bort komponenter eller adderar nya tjänster utan att tillräckligt kontrollera att den samlade infrastrukturen eller tjänsterna är kompatibla och fungerar, uppstår ofta incidenter. När sådana incidenter består av avbrott eller förändringar i funktionaliteten i tjänster som deras kunder redan använder får incidenten konsekvenser för många på samma gång.

5. Se exempelvis Årsrapport: *NIS-leverantörers it-incidentrapportering 2020,* MSB1695 - februari 2021 (2021), länk: https://rib.msb.se/filer/pdf/29491.pdf, och Årsrapport statliga myndigheters it-incidentrapportering 2020 : Utmaningar för en säker och robust informationshantering, MSB1692 - februari 2021 (2021), länk: https://rib.msb.se/filer/pdf/29488.pdf.

6. Lagen (2018:1174) om informationssäkerhet för samhällsviktiga och digitala tjänster riktar sig till leverantörer av samhällsviktiga och digitala tjänster och ställer krav på bland annat systematiskt informationssäkerhetsarbete, riskanalyser, säkerhetsåtgärder och incidentrapportering.

Sådana scenarier är troligen den vanligaste orsaken till de misstag och systemfel som sker i digitala leveranskedjor i Sverige. Även om det inte verkar vara lika vanligt förekommer det också att underleverantörer (oavsiktligt) levererar produkter med inbyggda fel som leder till negativa konsekvenser. Exempel på det kan vara att informationssystem slutar att fungera, eller att de levererade produkterna saknar inbyggda skydd som den mottagande parten räknar med att de har, vilket kan leda till att den mottagande organisationen kan drabbas av incidenter som den räknar med att vara skyddad mot.

Även om det saknas god och kvalitetssäkrad statistik tyder uppmärksammade händelser de två senaste åren på att angrepp genom digitala leveranskedjor blir vanligare.[7] En orsak är att hotaktörer kan angripa många organisationer på en och samma gång via en digital leveranskedja, en annan är att hotaktörer som önskar komma åt specifika organisationers interna miljöer kan bedöma att ett angrepp som tar ”omvägen” via en digital leveranskedja kan ha större chans att lyckas. Hotaktörer kan också göra bedömningen att ett angrepp genom en digital leveranskedja innebär en mer effektiv satsning om det är flera specifika mål som ska angripas och alla eller flera av dem går att nå via en och samma digitala leveranskedja. Sammantaget bör organisationer som levererar inom ramen för en digital leveranskedja förvänta sig fler och mer frekvent förekommande angrepp i framtiden. Det gäller i synnerhet om de har många kunder, kunder som är ekonomiskt starka eller strategiskt intressanta, eller om deras kunder i sin tur levererar i digitala leveranskedjor och har många kunder eller kunder som är ekonomiskt starka eller strategiskt intressanta.

Rekommendationer

Med anledning av utvecklingen bör levererande organisationer framöver förvänta sig högre och nya säkerhetskrav, bland annat de nedanstående. Skälet till det är att incidenter hos levererande organisationer som får återverkningar på, eller igenom, digitala leveranskedjor, alltmer leder till allvarliga konsekvenser för såväl enskilda mottagande organisationer som för samhällen. MSB rekommenderar därför levererande organisationer att:

1. Säkerställa att ni har skydd mot såväl externa som interna hot, såväl antagonistiska som icke-antagonistiska.
2. Säkerställa att ni har insyn i och kontroll över era egna digitala leveranskedjor.
3. Säkerställa att ni har kontinuitetshantering för och redundans i era egna digitala leveranskedjor.
4. Säkerställa att ni har beaktat säkerhetsfrågorna i hela designfasen av det som ska levereras.
5. Säkerställa att ni har en hög grad av transparens och snabb och detaljerad informationsdelning vad gäller kvalitetssäkring, säkerhetsarbete, incidenter, risker, hot och sårbarheter.

7. På internationell nivå genom att störa eller blockera leveranser av sådant som ska levereras, och därutöver mer allmänt genom att hotaktörer använder de digitala leveranskedjorna för att leverera sådant som inte ska levereras, såsom skadlig kod i form av ransomware eller spionprogramvara.

6. Säkerställa att ni har frekventa granskningar av såväl kvalitetsarbete som säkerhet, samt krav på åtgärder och förbättringar när sårbarheter och brister upptäcks.
7. Säkerställa att ni har garanterad leverans inom överenskomna parametrar (såsom leveranstid) om det som ska levereras utgör en nödvändig komponent i det som ska produceras av mottagaren, eller om det som ska levereras anses vara en strategisk produkt.
8. Säkerställa att ni kan lämna garanti till mottagande organisationer om att det och endast det som har beställts också levereras.
9. Säkerställa att ni kan lämna garanti till mottagande organisationer om att det som levereras har lämpliga skydd inkluderade.

Vissa organisationer som utgör leverantörer inom ramen för digitala leveranskedjor bör dessutom räkna med att vissa av ovan rekommendationer framöver kan komma att även ställas i form av rättsliga krav, exempelvis i samband med att NIS 2-direktivet implementeras i svensk rätt.

Till mottagande organisationer i digitala leveranskedjor

Som vi noterat i föregående avsnitt medför den successiva specialiseringen inom olika sektorer att allt fler digitala leveranskedjor upprättas, och att vissa aktörer i allt större utsträckning får roller som noder.

Effekten av utvecklingen blir att (mottagande) organisationer blir mer och mer beroende av att allt fungerar som det ska hos deras leverantörer för att de själva ska kunna bedriva sin egen verksamhet eller producera sina egna tjänster och produkter. Om de inte vidtar extra skyddsåtgärder blir de mer och mer sårbara inför bristande kvalitetssäkring och säkerhetsarbete hos sina underleverantörer. För att kunna förbereda sig på driftstörningar och säkerställa att de kan bedriva verksamhet under andra former, om störningar ändå skulle ske blir de därmed också beroende av att få förhandsinformation om väntande förändringar och ingrepp i underleverantörernas system och tjänster.

Utvecklingen innebär också att mottagande organisationer måste räkna med att hotaktörer kan komma att angripa deras leverantörer för att komma åt dem själva.[8] Det gäller i synnerhet ekonomiskt starka eller strategiskt intressanta aktörer och särskilt om de i övrigt har en god informations- och cybersäkerhet. Utvecklingen innebär även att mottagande organisationer måste räkna med att ju fler och mer ekonomiskt starka eller strategiskt intressanta kunder deras leverantör har, desto mer intressant kan leverantören bli för hotaktörer. Ju mer intressant ens leverantör kan bli för hotaktörer, desto mer kan man komma att drabbas av angrepp som antingen avsiktligen slår mot alla leverantörens kunder, eller som drabbar en själv men där angriparens avsikt var att komma åt någon annan.

8. Både genom att störa eller blockera leveranser av sådant som ska levereras, och genom att använda de digitala leveranskedjorna för att leverera sådant som inte ska levereras, såsom skadlig kod i form av ransomware eller spionprogramvara.

Rekommendationer

För mottagande organisationer är det både viktigt att få de leveranser man behöver, när man behöver dem – och att det inte i leveranserna ingår sådant som den mottagande organisationen inte ska ha (såsom inbyggd skadlig kod). För att säkerställa att man får det man behöver, när man behöver det, rekommenderar MSB mottagande organisationer att:

10. Kontrollera huruvida digitala produkter ni använder eller är beroende[9] av endast kan levereras av enstaka aktörer. Överväg om det finns sätt att justera er egen produktion så att ni kan använda digitala produkter från andra leverantörer än de som ni använder nu.
11. Kontrollera huruvida digitala produkter ni använder eller är beroende av kommer från aktörer som endast kan leverera till er om de själva först får information, mjukvara eller hårdvara som i sin tur endast kan levereras av enstaka aktörer. Diskutera med era leverantörer om det finns sätt att justera deras produktion så att de kan använda digitala produkter från andra leverantörer än de som de använder nu.
12. Kontrollera huruvida digitala produkter ni använder eller är beroende av tillhandahålls av aktörer som inte har ett systematiskt säkerhetsarbete som förebygger såväl interna och externa som antagonistiska och icke-antagonistiska hot. Se över er kravställning gentemot de aktuella leverantörerna och se även över om det finns andra möjliga leverantörer som har ett mer systematiskt säkerhetsarbete. Överväg om det är bäst att fortsätta det befintliga samarbetet eller att påbörja ett nytt med en annan leverantör.
13. Kontrollera huruvida digitala produkter ni använder eller är beroende av tillhandahålls av aktörer som verkar inom jurisdiktioner som kan komma att vidta åtgärder som negativt inverkar på leveranserna till er. Diskutera med era leverantörer om det finns möjligheter att etablera produktion i andra jurisdiktioner.
14. Kontrollera huruvida digitala produkter ni använder eller är beroende av Tillhandahålls av aktörer som verkar på platser som är känsliga för naturhot eller kan komma att bli negativt påverkade av klimatförändringar. Diskutera beredskapen mot naturhot hos era leverantörer, och se över er kravställning gällande deras förebyggande och hanterande arbete.

För att säkerställa att man inte får sådant levererat som man inte ska ha rekommenderar MSB mottagande organisationer att:

15. Säkerställa att ni inom ramen för ert kvalitets- säkerhetsarbete återkommande inventerar vilka digitala leveranskedjor ni använder och är beroende av, samt i vilken utsträckning de är förtroendebaserade.
16. Säkerställa att ni inom ramen för ert kvalitets- säkerhetsarbete i mesta möjliga mån granskar det som mottas inom ramen för digitala leveranskedjor, innan det installeras, aktiveras eller används – för att kontrollera att allt och endast det som ska vara med är med.

9. Med beroende avses här tre saker: Att organisationen använder något som levereras av någon annan i sin produktion, att sådana komponenter som levereras är nödvändiga för den mottagande organisationens produktion och att den mottagande organisationen inte själv kan producera det som levereras.

17. Säkerställa att ni inom ramen för ert kvalitets- säkerhetsarbete har kontinuitetshantering och redundans avseende era leverantörer av nödvändiga komponenter där alternativa leverantörer är oberoende av varandra samt geografiskt, jurisdiktionellt och på andra sätt åtskilda så att naturhändelser, handelshinder och andra hot mot den ena leverantören inte också påverkar den andra.
18. Säkerställa att ni inom ramen för ert kvalitets- säkerhetsarbete har en plan för att på ett ordnat sätt hantera avbrott i leveranserna av vissa nödvändiga komponenter, så att övriga leveranskedjor inte drabbas av skada om den egna produktionen måste dras ned eller avbrytas.

MSB rekommenderar därutöver att ni ser över er kravställning på leverantörer och transportörer i era digitala leveranskedjor. Mottagande organisationer bör:

19. Ställa krav på skydd mot såväl externa och interna hot, som antagonistiska och icke-antagonistiska.
20. Ställa krav på insyn i och kontroll över deras egna digitala leveranskedjor.
21. Ställa krav på kontinuitetshantering för och redundans i deras egna digitala leveranskedjor.
22. Ställa krav på att leverantören har beaktat säkerhetsfrågorna i hela designfasen av det som ska levereras.
23. Ställa krav på att leverantören är transparent och delar information transparens och informationsdelning avseende kvalitetssäkring, säkerhetsarbete, incidenter, risker, hot och sårbarheter.
24. Ställa krav på att leverantören genomför frekventa granskningar av såväl kvalitetsarbete som säkerhet, samt på åtgärder och förbättringar när sårbarheter och brister upptäcks.
25. Ställa krav på att leverantören har garanterad leverans inom överenskomna parametrar (såsom leveranstid) om det som ska levereras utgör en nödvändig eller strategiskt viktig komponent för mottagaren.
26. Ställa krav på att leverantören har garanti om att det och endast det som har beställts också levereras.
27. Ställa krav på att leverantören har garanti om att det som levereras har lämpliga skydd inkluderade.

Vissa organisationer som utgör mottagare inom ramen för digitala leveranskedjor bör dessutom räkna med att NIS 2 direktivet kan komma att medföra högre krav på säkerhet i leveranskedjan, bland annat i enlighet med kraven i punkt 19 till 27.

Till organisationer som stödjer, reglerar eller genomför tillsyn av aktörer som levererar eller mottar inom digitala leveranskedjor

Regleringens och tillsynens roll i att stärka säkerheten i digitala leveranskedjor handlar i stort om att minimera risk för samhället Det kan göras inom fyra övergripande områden. Det handlar om att förmå levererande organisationer att ha en god kontinuitetshanteringsförmåga så att de i mesta möjliga mån undviker att

drabbas av avbrott i sin produktion eller transport av det som ska levereras. Det handlar också om att förmå levererande organisationer att ha en god kvalitetskontroll och säkerhet i samband med att de upprättar, skickar och transporterar de digitala produkter som ska levereras så att det som levereras inte innehåller hot eller saknar funktionalitet eller skydd.[10] Det handlar även om att förmå mottagande organisationer att även ha en god förmåga till kontinuitetshantering, inklusive redundanta uppsättningar leverantörer av nödvändiga digitala produkter, så att avbrott i produktion eller transport från en leverantör kan kompenseras genom att det som behövs tillhandahålls av en annan leverantör. Slutligen handlar det om att förmå mottagande organisationer att ha en god kvalitetskontroll och säkerhet, samt granskning av det som mottas, innan det som mottagits installeras, aktiveras eller används.

Rekommendationer

Stötta, reglera och genomför tillsyn av levererande och mottagande organisationers arbete med digitala leveranskedjor så att de har incitament att:

28. Stötta och reglera så att organisationer får incitament att beställa digitala produkter som har den, och endast den, funktionalitet och de skydd som de behöver.
29. Stötta och reglera så att organisationer får incitament att analysera, förebygga och ha förmåga att hantera riskerna både när sådant som inte ska levereras ändå levereras och när sådant som ska levereras inte levereras.
30. Stötta och reglera så att organisationer får incitament kravställa om lämpliga kvalitetssäkrings- och säkerhetsåtgärder, *security by design*, återkommande granskningar[11] samt transparens och informationsdelning hos de underleverantörer som utgör deras digitala leveranskedjor.[12]
31. Stötta och reglera så att organisationer får incitament att undvika monoberoenden och inlåsningseffekter.
32. Stötta och reglera så att organisationer får incitament att etablera redundanta och diversifierade digitala leveranskedjor.
33. Stötta och reglera så att organisationer får incitament att verka för interoperabilitet mellan olika tillhandahållare av information, mjukvara, hårdvara och tjänster.
34. Stötta och reglera så att organisationer får incitament att upprätthålla en god informations- och cybersäkerhet i allmänhet, och gällande hanteringen av information, mjukvara, hårdvara och tjänster som levereras inom ramen för digitala leveranskedjor i synnerhet.[13]
35. Undvika att stötta och reglera så att monoberoenden uppstår genom direkt eller indirekt tvång eller starka incitament.

10. För användning av begreppen se bilaga *Om analys av incidenter i digitala leveranskedjor.*

11. Samt löpande arbete med säkerhetsåtgärder som granskningarna visar att aktören behöver.

12. En del sådant arbete kommer bedrivas inom ramen för EU:s Cybersäkerhetsakt. Att tillgängliggöra en förteckning (*Software Bill of Materials)* över innehållet i produkter är också något som aktualiserats i exempelvis USA och Storbritannien under det senaste året.

13. Ett möjligt sätt att åstadkomma detta skulle kunna vara att inspireras av principerna för *zero trust*.

36. Undvika att stötta och reglera så att redan existerande mono-beroenden befästs.
37. Samarbeta med levererande och mottagande organisationer för att öka informationsdelning och sprida erfarenheter kring såväl incidenter som *best practices*.
38. Samarbeta med levererande och mottagande organisationer för att stärka kunskapen och kompetensen kring hur man kan utforma kravställning för hög digital leveranskedjesäkerhet.
39. Samarbeta med levererande och mottagande organisationer för att stärka kunskapen kring vilka beroenden till digitala leveranskedjor som finns, vilka underleverantörer som utgör noder och vilka alternativ det finns för den som vill välja en leverantör som är mindre intressant för hotaktörer.
40. Samarbeta med levererande och mottagande organisationer för att utveckla modeller[14] som kan användas för den som vill upprätta ett systematiskt arbete med säkerheten i sina digitala leveranskedjor.
41. Samarbeta med levererande och mottagande organisationer för att dela på kostnaderna för att granska säkerheten i vissa brett använda digitala leveranskedjor och deras tillhörande produkter.[15]
42. Samarbeta med levererande och mottagande organisationer för att med samlade resurser bedriva forskning och utveckling i syfte att skapa nya lösningar som möjliggör för mottagande organisationer att med högre säkerhet installera, aktivera eller använda digitala produkter utan att signifikant öka kostnaderna eller minska effektiviteten.

Till stater och statliga organ som verkar för stärkt samhällssäkerhet

Stater kan göra mycket för att säkra digitala leveranskedjor. De kan ge lämpliga mandat, resurser och uppgifter till myndigheter som ska stödja, reglera och genomföra tillsyn över organisationer inom det egna landet som levererar eller mottar inom ramen för digitala leveranskedjor. De kan även ge mandat, resurser och uppgifter till myndigheter för att upprätta en samlad kunskapsgrund om vilka de för landet avgörande digitala leveranskedjorna är och hur starkt beroendet till sådana digitala leveranskedjor är samt vilken systemisk risk det medför och vad som kan göras åt det. Detta är särskilt viktigt i fria samhällen som det svenska eftersom det kan vara svårt för staten att skaffa sig en ingående bild av hur beroendena ser ut. Stater kan därutöver utveckla sina relationer med andra stater för att dels förebygga incidenter och bygga gemensam hanteringsförmåga, dels lagföra och avskräcka såväl hotaktörer som opererar åt andra stater som hotaktörer som opererar från andra stater.

14. Exempelvis i stil med MSB:s Infosäkkollen.
15. Såsom kodbibliotek.

Rekommendationer

MSB rekommenderar stater och statliga organ att:

43. Arbeta förebyggande genom att etablera goda relationer med andra stater genom vilka särskilt viktiga digitala leveranskedjor passerar så att kanaler redan är upprättade om en incident inträffar – och så att incidenter kan förebyggas.
44. Upprätta, enskilt eller i samarbete med andra stater, egen produktion av särskilt strategiskt viktiga produkter, om det finns välgrundade förväntningar på att sådana satsningar framöver kommer att kunna bära sig.
45. Undvik att stifta lagar eller på annat sätt besluta om regler som upprättar eller befäster monoberoenden. Skapa incitament att bryta existerande monoberoenden och att verka för ökad diversitet.
46. Inför krav på att olika tillverkare av liknande digitala produkter följer samma standarder och att deras produkter, som huvudregel, är interoperabla.
47. Ställ ändamålsenliga krav på säkerhet och kvalitet i digitala leveranskedjor vid statlig upphandling, för att genom detta skapa förutsättningar för att aktörer och dess produkter alltid håller en hög lägstanivå när det gäller säkerheten i digitala leveranskedjor.
48. Verka för att digitala leveranskedjor som används av samhällsviktiga tjänster inte ska angripas av statsunderstödda aktörer genom att skapa incitament för aktörer att välja bort digitala leveranskedjor som utgör särskilt troliga mål för angripare.[16]
49. Verka för att hotaktörer som angriper digitala leveranskedjor lagförs.
50. Verka för att skapa internationella verktyg för att avskräcka och svara på angrepp mot digitala leveranskedjor.

16. Rekommendationen gäller i synnerhet leveranskedjor inom vilka särskilt viktiga produkter levereras och där det saknas alternativa leveranskedjor att tillgå, varför ett avbrott skulle kunna medföra stor påverkan. Rekommendationen gäller också i synnerhet sådana leveranskedjor som baseras på en djup åtkomst till mottagarens system, varför ett angrepp genom leveranskedjan skulle kunna orsaka särskilt stor skada.

Om rapporten

Om rapporten

Denna rapport ger en bild av vilka hot som digitala leveranskedjor står inför och hur de är sårbara för angrepp, misstag, systemfel och naturhändelser. Rapporten har sin grund i den it-incidentrapportering MSB tar emot från leverantörer av samhällsviktiga och digitala tjänster.[17]

Rapporten syftar till att ge en övergripande bild av de digitala leveranskedjorna och utmaningarna de medför utifrån individuella organisationers perspektiv, samt tillhandahålla rekommendationer för hur de utmaningarna kan mötas. Vi utgår dels från organisationer som levererar hård- eller mjukvara, information eller tjänster till andra organisationer (”levererande organisationer”), dels från organisationer som mottar sådan hård- eller mjukvara, information eller tjänster – antingen för eget bruk eller för behandling och förädling av det som har levererats för att därefter förmedla en egen produkt vidare i leveranskedjan (”mottagande organisationer”). Rapporten syftar också till att beskriva utmaningarna utifrån myndigheters perspektiv, i synnerhet sådana myndigheter som på nationell nivå stödjer, reglerar eller utövar tillsyn över levererande och mottagande organisationer i digitala leveranskedjor. Slutligen syftar rapporten till att beskriva några av utmaningarna som kan uppstå på nationell politisk nivå, samt några av utmaningarna med digitala leveranskedjor som uppstår internationellt mellan stater.

17. Enligt lagen om informationssäkerhet för samhällsviktiga och digitala tjänster (2018:1174) som berör både privata och offentliga aktörer inom sektorerna bankverksamhet, finansmarknadsinfrastruktur, transport, leverans och distribution av dricksvatten, digital infrastruktur, hälso- och sjukvård, energi samt vissa digitala tjänster. För mer information se Årsrapport: *NIS-leverantörers it-incidentrapportering 2020,* MSB1695 - februari 2021 (2021), länk: https://rib.msb.se/filer/pdf/29491.pdf (hämtad 2021-07-08)

Rapportens målgrupper är:

1. Anställda inom levererande och mottagande organisationer i säkerhetsansvariga, omvärldsbevakande, analyserande eller beslutsfattande roller.
2. Anställda inom organisationer som bistår, stöttar eller sköter säkerhetsarbete eller arbete med digitala leveranskedjor hos levererande eller mottagande organisationer.
3. Anställda i säkerhetsansvariga, omvärldsbevakande, analyserande eller beslutsfattande roller inom myndigheter som på nationell nivå stödjer, reglerar eller utövar tillsyn över levererande och mottagande organisationer i digitala leveranskedjor.
4. Anställda inom departement och parlamentariska organ som arbetar med statens internationella relationer eller med framtagandet av ny lagstiftning.
5. Politiska beslutsfattare som är verksamma inom områden som säkerhetspolitik och internationella relationer.

MSB har bedömt att en övergripande sammanställning och analys av utmaningarna med koppling till digitala leveranskedjor utgör ett angeläget område. En anledning till det är att incidentrapporteringen visar att en majoritet av de rapporterade incidenterna har sitt ursprung utanför den rapporterande organisationen. Det innebär att de har inträffat hos en annan organisation som tillhandahåller informationsmängder, mjukvara, hårdvara eller tjänster. En annan anledning är att ett antal storskaliga incidenter i digitala leveranskedjor upptäckts på senare tid, vilket har aktualiserat frågorna och ökat behovet av en kunskapsöversikt.

MSB har därför sammanställt data från den incidentrapportering som myndigheten mottar och dessutom genomfört en internationell utblick för att därigenom både ge en bild av situationen i Sverige, och redogöra för skeenden utomlands som är av vikt för den som vill få en samlad bild över området. Beskrivningarna av digitala leveranskedjor som presenteras samt hot, sårbarheter och risker kopplade till dem är dock inte unika för leverantörer av samhällsviktiga och digitala tjänster utan kan vara värdefulla för många olika typer av organisationer och i många olika situationer.[18]

Vårt arbete med rapporten har genomsyrats av allriskperspektivet, vilket bland annat återspeglas i redogörelserna för hotbilden mot digitala leveranskedjor som vi presenterar i kommande kapitel. Vi har också inkluderat delar av MSB:s analysmetodik, för att därigenom möjliggöra för andra att genomföra sina egna analyser av digitala leveranskedjor och tillhörande utmaningar.

Rapporten innehåller även konsekvensbeskrivningar, slutsatser och ett antal rekommendationer om vad som kan och bör göras på både organisations- och samhällsnivå för att stärka motståndskraften och säkerheten rörande de digitala leveranskedjor som vi är beroende av.

Rapporten är framtagen med stöd av medel från EU:s Connecting Europe Facility-fond.

18. Exempelvis måste vi i takt med att Sverige utvecklar totalförsvarsförmågan uppmärksamma vårt beroende av leveranser av mjuk- och hårdvarukomponenter och digitala tjänster inom ramen för försörjningsberedskapen. Hoten och sårbarheterna som presenteras i rapporten är därmed viktiga att uppmärksamma i såväl ordinarie verksamhetsplanering och krisberedskap som i totalförsvarsplaneringen.

Om digitala leveranskedjor

Om digitala leveranskedjor

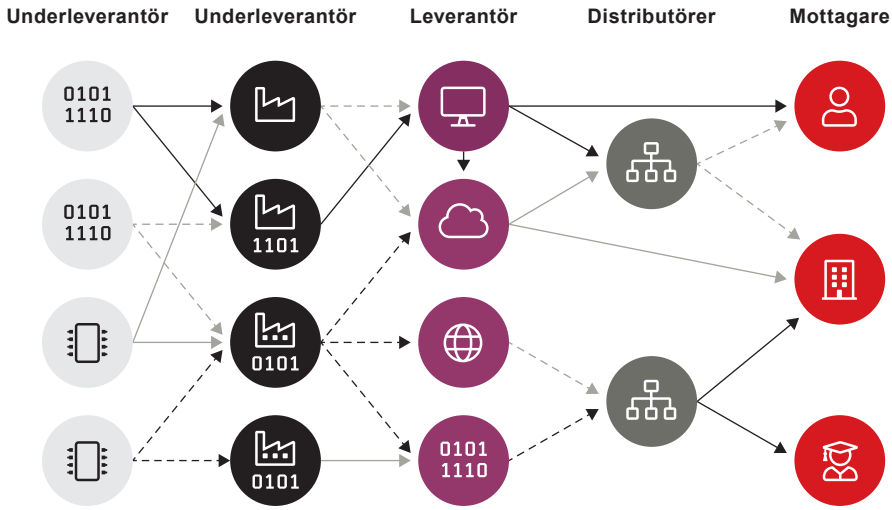
Digitala leveranskedjor utgör en livsnerv i samhället. Bakom nästan alla varor och tjänster finns i dag digitala leveranskedjor. De digitala leveranskedjorna är därmed en förutsättning för att våra mest grundläggande och samhällsviktiga funktioner och verksamheter ska fungera. Utan en säker och kontinuerlig leverans av informationsmängder, försörjning av hårdvarukomponenter, uppdateringar av mjukvara eller åtkomst till tjänster och lagring via internet stannar mycket av vår moderna kommunikation och informationshantering av.

Med en *digital leveranskedja* menar MSB följande:

De tjänster och infrastrukturer som levererar eller möjliggör leverans av digitala produkter vilka används för att upprätta, upprätthålla, utveckla eller återställa en verksamhets informationshantering och informationssystem.[19]

Den digitala leveranskedjan består ofta av många delar vilka i sig tillhandahålls av många olika aktörer såsom tillverkare, leverantörer och underleverantörer, transportörer, distributörer och slutkundsförsäljning.

Figur 1. Visar en förenklad representation av olika nivåer av aktörer i en digital leveranskedja och hur det redan vid några få nivåer kan uppstå många och komplexa beroenden.



19. Detta kan genomföras antingen enskilt eller tillsammans och ibland även i serie där delar från flera olika källor kombineras.

En digital leveranskedja är en typ av leveranskedja som utmärks av att den i stor utsträckning baseras på, inkluderar eller bidrar till digitala produkter. Det finns många likheter med andra typer av leveranskedjor, men det finns också några utmärkande drag som särskiljer dem från många andra leveranskedjor, såsom att de i stor omfattning inkluderar produktion av digitala produkter som:

- När de en gång har upprättats, normalt sett kan kopieras och transporteras utan substantiella extra kostnader (såsom en mjukvaruuppdatering som laddas ned direkt över internet).
- I realtid levereras till mottagaren och där mottagaren i realtid interagerar med det som levereras (såsom sensordata som används för att bevaka och kontrollera ett dricksvattenverk).
- Används i nästan alla verksamheter, inklusive bland samhällsviktiga tjänster, och som många är beroende av.
- På grund av sin komplexa och uppkopplade natur är både bräckliga och lätta att nå på sätt som orsakar skada.

Utöver att de digitala leveranskedjorna har vissa särdrag är de också värda att särskilt studera eftersom de spelar en helt avgörande roll i säkerställandet av kontinuerlig funktion, utveckling samt återställning efter incidenter, för informationssystem. Eftersom informationssystem i sin tur upprätthåller merparten av såväl den samhällsviktiga som den ekonomiska verksamheten i digitaliserade samhällen så är de digitala leveranskedjorna av ett högt strategiskt värde för ett land som Sverige.

Några exempel på digitala produkter som levereras inom ramen för digitala leveranskedjor är:

1. **Mjukvara och uppdateringar av mjukvara:** Modern programvara, såsom administrativa stöd, säkerhetsprogramvaror, spel och annat levereras i sina grundutföranden och försörjs med uppdateringar över internet.
2. **Externt tillhandahållna programbibliotek:** I modern mjukvaruutveckling är det vanligt att försöka undvika att utveckla alla funktioner som programmet man ska utveckla behöver. Istället hämtar man funktioner från externt tillhandahållna tjänster.[20]
3. **Säkerhetsprogramvaror:** Moderna säkerhetsprogramvaror bygger oftast på en fortsatt kontinuerlig försörjning av uppdateringar även efter inköpstillfället. Denna kontinuerliga försörjning är en förutsättning för att slutkunden bland annat ska ha tillgång till de senaste virusdefinitionerna.
4. **Halvledare:** Tillgången till halvledare är en förutsättning för merparten av alla hårdvarukomponenter som i sin tur krävs för att upprätta, upprätthålla eller utveckla digital infrastruktur.
5. **Molntjänster:** Molntjänster används idag till allt från specifika programvaror till hela informationssystem. Tillhandahållare av sådana tjänster eller underliggande infrastrukturer är en förutsättning för många it-miljöer.

20. Tjänsten som tillhandahåller koden behöver inte vara densamma som den som upprättat koden. Ett exempel på detta är nättjänsten GitHub som fungerar som en plattform för en global gemenskap av utvecklare. Enskilda utvecklare lägger egen kod som löser särskilda uppgifter på GitHub, varpå andra använder den koden.

En komponents eller en bit av informations resa genom en digital leveranskedja kan initieras dels genom att en aktör beställer eller hämtar hem något genom kedjan (såsom när ett företag beställer halvledare de behöver som en komponent till något de tillverkar), dels genom att en aktör skickar ut något (såsom när ett mjukvaruföretag skickar ut en säkerhetsuppdatering av sin produkt). Digitala leveranskedjor kan dels tillhandahålla löpande försörjning av något (såsom olika former av realtidsuppdaterad statistik), dels tillhandahålla avgränsade leveranser (såsom en viss mängd halvledare eller ett visst antal programlicenser).

Digitala leveranskedjor är helt avgörande för digitaliseringen, och för digitaliserade samhällen. Incidenter i sådana leveranskedjor kan resultera i både allvarliga konsekvenser för enskilda aktörer och i konsekvenser för många aktörer antingen samtidigt eller efter varandra. Ytterst riskerar inträffade incidenter och de bakomliggande hoten att påverka samhällets säkerhet.

Med incident i digital leveranskedja menar MSB:

1. En händelse där något som:
    a. ska levereras i den digitala leveranskedjan (en framgångsfaktor eller ett skydd) inte levereras, eller
    b. inte ska levereras i den digitala leveranskedjan (ett hot eller ett hinder) ändå levereras, och
2. Där händelsen resulterar i antingen en oplanerad negativ påverkan[21] eller en oönskad avsaknad av positiv påverkan[22] på informationssystems, eller informationen i informationssystems, konfidentialitet, riktighet eller tillgänglighet.

21. Såsom när skadlig kod installeras i ett informationssystem p.g.a. av en mjukvaruuppdatering som skickats ut inom ramen för en digital leveranskedja.

22. Såsom när en ny komponent som behövs för att reparera ett trasigt informationssystem inte levereras trots att det är beställt.

Exempel: En digital leveranskedja för en NIS-leverantör

Inom såväl äldrevården som vissa andra vårdformer använder man trygghetslarm för att snabbt kunna upptäcka om när någon drabbas av ett problem eller en olycka. Trygghetslarmen består av små dosor som ofta bärs antingen i ett halsband eller som en klocka kring handleden.

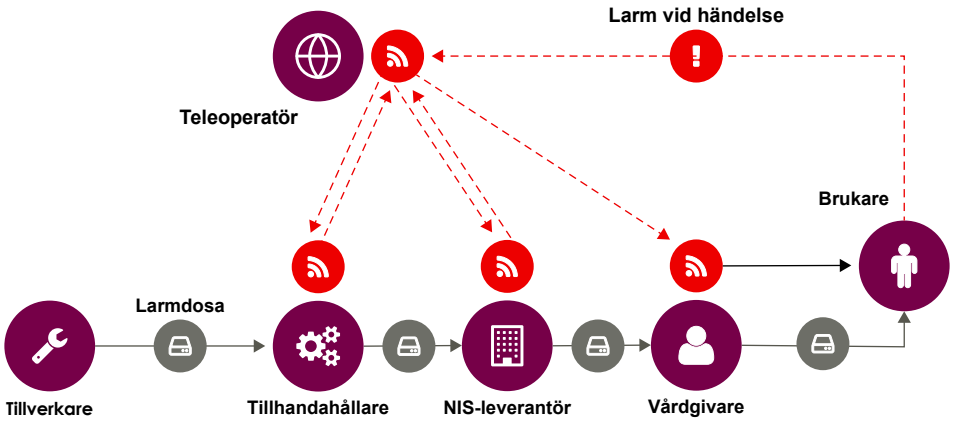
Sådana larm tillverkas i allmänhet inte av leverantören av den samhällsviktiga tjänsten (d.v.s. vårdgivaren), utan larmen köps eller hyrs ofta in av en annan aktör (”larmtillhandahållaren”). Larmtillhandahållaren köper i sin tur in larmen ifrån en tillverkare, och integrerar dem i en egen informationsinfrastruktur. Affärsidén går ut på hyra ut larmen inom ramen för ett slags abonnemang, där underhåll och successiv försörjning av nya larm och ersättning av gamla larm ingår.

Rent tekniskt ansluter enskilda larm till larmtillhandahållarens it-miljö genom att signaler skickas över telenätet, varpå de antingen skickas vidare till vårdgivarens egen it-miljö, eller direkt till vårdgivarens personals mobiltelefoner, eller annan teknisk utrustning.

Så, för att vårdpersonalen snabbt ska kunna upptäcka om någon har farit illa använder de en digital leveranskedja i form larmtillhandahållarens larmtjänst. Larmtillhandahållaren i sin tur använder sig av två digitala leveranskedjor, en signalöverföringstjänst som tillhandahålls av en teleoperatör, och en hård- och mjukvaruförsörjningstjänst som tillhandahålls av en larmtillverkare. Alla dessa aktörer är dessutom ofta i sin tur beroende av ytterligare digitala leveranskedjor för att kunna bedriva sin verksamhet.

En störning i den samhällsviktiga tjänsten kan därmed uppstå om larmtillhandahållaren har en incident i sin informationsinfrastruktur (så att inkommande larm inte skickas till vårdpersonalens mobiltelefoner), om teleoperatören har ett problem i sitt nät (så att larmsignaler inte når larmtillhandahållarens informationsinfrastruktur) eller om larmen innehåller hård- eller mjukvarufel (som gör att de inte fungerar som de ska när en vårdtagare trycker på larmknappen).

Figur 2. Visar hur en larmdosa som används inom exempelvis äldrevården går från en aktör till annan (och under tiden eventuellt konfigureras och justeras), tills den når brukaren. Ovantill visar bilden hur ett larm från brukaren, som skickas från larmdosan, först går till en teleoperatör som för det vidare till tillhandahållaren av larmdosan (om NIS-leverantören hyr en sådan tjänst) eller till NIS-leverantören (om NIS-leverantören har en egen sådan tjänst) och hur en signal därefter går tillbaka till teleoperatören som i sin tur skickar den vidare till vårdgivaren.



En väv av nischaktörer

Organisationer som på olika sätt försöker effektivisera sin verksamhet har ett löpande behov av högre och mer specialiserad prestanda. Eftersom utvecklingen av de komponenter som den prestandan förutsätter är dyr, utmanande och kräver en stor koncentration av nischad expertis, har digitaliseringens industrier därför alltmer opererat på en global marknad. Trots detta har antalet aktörer som klarar av och har råd att hålla sig i teknikens och forskningens framkant successivt blivit lägre inom vissa områden (såsom avancerad halvledardesign och tillverkning). Kluster av företag som står för olika delar av den samlade försörjningen till vår digitala infrastruktur har uppstått på olika håll världen över. Följden har blivit att produkter och tjänster som består av många olika delar succesivt har kommit att behöva försörjning från allt fler organisationer i kedjor där olika komponenter upprättas, förädlas, kombineras och förs vidare i en ständig rörelse mellan olika delar av världen.

Vår digitala infrastruktur består av hård- och mjukvara, vars respektive komponenter i allmänhet tillverkas, kombineras, integreras och transporteras vidare mellan olika organisationer som befinner sig i olika delar av världen. Exempelvis består en dator av en rad komponenter, såsom moderkort, hårddisk, grafikkort, RAM-minnen och nätverkskort. Dessa är ofta tillverkade av flera olika leverantörer i olika delar av världen. Komponenterna består i sig av en rad olika delkomponenter där exempelvis datorchipp med mikroprocessorer och minnen är några av de mindre beståndsdelarna. Dessa kan i sin tur vara tillverkade hos ytterligare led av underleverantörer. Bland de minsta elektronikkomponenterna återfinns halvledare. Dessutom har de flesta hårdvarukomponenter tillhörande mjukvara, för att inte tala om att slutprodukten, själva datorn, har många olika mjukvaror (varav vissa är helt nödvändiga för att datorn ska fungera) som ofta också kommer från olika tillverkare och olika platser.

I uppbyggnaden och försörjningen till datorers mjukvara finns ett liknande komplext upplägg, men ”tillverkningsprocessen” kan vara än mer distribuerad. Olika leverantörer, med sina programmerare, står bakom operativsystem, nätverksprotokoll och en rad olika applikationer som måste kunna kommunicera med varandra på ett korrekt sätt. Applikationer och protokoll bygger i sin tur på olika bitar av källkod eller programtext. Källkoden kan ofta vara en blandning av olika bitar kod som olika programmerare skrivit, ibland över lång tid och i flera organisationer eller av privatpersoner. Inte sällan utgörs olika mjukvaror av färdig kod där utvecklaren utnyttjat befintliga kodbibliotek i utvecklingsprocessen. Det finns ofta en brist på dokumentation om vilka kodbibliotek eller versioner som ingår i den färdiga produkten. Den färdiga koden och mjukvaran ska i sin tur kunna kompileras[23] och köras för att olika program ska kunna göra det de är tänkta att göra. Dessa faktorer skapar tillsammans en komplex kedja av aktörer och källor bakom nästintill all mjukvara på dagens marknad.[24]

23. Översättning av kod från programspråk till maskinkod.

24. För en genomgång av uppbyggnaden av och komplexiteten i informationssystem se FOI:s rapport *Säkra leveranskedjor för Informationssystem*, FOI-R--4851--SE (2019), länk: https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--4851--SE (hämtad 2021-04-16).

Fortlöpande förtroende är en nödvändig förutsättning

Digitala leveranskedjor innefattar i regel inte bara att en produkt produceras och skickas till en mottagare. När produkten har levererats ingår det också ofta stöd för installation, aktivering eller användande samt såväl uppdateringar som olika former av underhåll om produkten inte fungerar som den ska. Organisationer har i allmänhet ett behov av ett kontinuerligt inflöde av tekniska komponenter som datorer, mobiler, servrar, routrar och annat. För varje teknisk komponent behövs i allmänhet en egen mjukvara. Nya funktioner tillkommer ofta regelbundet genom uppdateringar, och sårbarheter upptäckts och måste åtgärdas genom säkerhetsuppdateringar. Mjukvaror är ofta beroende av andra mjukvaror som i sin tur kan förändras på ett lika dynamiskt sätt. Även om det är ovanligt kan själva uppdateringen av en mjukvara i sig dessutom resultera i att mjukvaran blir sårbar, eller att nya hot uppstår. Ett problem som är vanligare för många organisationer är att leverantören av en digital produkt efter ett tag väljer att stänga ner sin digitala leveranskedja till just den produkten, varpå produkten inte utvecklas med nya funktioner eller får nya skydd i takt med att nya sätt att felaktigt använda eller angripa produkten upptäcks. Ofta tar leverantören ett beslut om att stänga ner den digitala leveranskedjan för en viss produkt när leverantören har lanserat en ny produkt i samma kategori.[25]

Det kontinuerliga behovet av underhåll och kompletteringar innebär att den digitala leveranskedjan förutsätter en hög grad av förtroende till en rad inblandade parter. Ett exempel är hanteringen av säkerhetsuppdateringar från leverantörer av mjukvarutjänster. Innehållet i det ständiga inflödet av uppdateringar och säkerhetsuppdateringar är närmast omöjligt att granska och man rekommenderas ofta att implementera dem så snart som möjligt av säkerhetsskäl. På motsvarande sätt förutsätter användandet av exempelvis driftentreprenad, antivirusskydd eller andra säkerhetslösningar en hög nivå av förtroende eftersom dessa dessutom ofta behöver priviligierad åtkomst till sina kunders system och nätverk. Detta gör att grunderna för förtroende till mjukvaruprodukter eller leverantörer inte enbart gäller vid inköpstillfället. Vid inköp och användning av mjukvara förbinder sig organisationer till ett långvarigt förtroendebaserat beroende till sin leverantör, och i förlängningen dennes underleverantörer och alla inblandade mjukvaror och de beroenden som dessa har. Förtroendet vilar förhoppningsvis på att leverantören och underleverantörerna bedriver ett kravställt och kontinuerligt verifierat systematiskt säkerhetsarbete under kontraktstiden med möjlighet till uppföljning, kontroll och åtgärder från kundens sida.

25. Såsom när tillverkare av operativsystem släpper en ny version av sitt operativsystem och vill skapa incitament att köpa in det nya operativsystemet, i stället för att behålla det andra. Eller när en tillverkare av mobiltelefoner släpper en ny mobiltelefon och vill att man ska investera i den.

Exempel: Uppdateringar av antivirus-programvara

Ett exempel på ett förtroendebaserat beroende är det mellan informationssystem som har antivirus-programvara installerad och informationssystem hos tillverkaren av antivirusprogramvaran. Antivirusprogramvaran fungerar på så sätt att nyligen upptäckta hot i form av exempelvis skadlig kod beskrivs i en så kallad signatur. För att antivirusprogramvaran ska kunna upptäcka och hantera ny skadlig kod behöver den en kontinuerlig försörjning av nya signaturer för att kunna hantera den ständiga strömmen av ny skadlig kod.

Antivirusprogramvaror kräver ofta en hög nivå av behörighet i de system och klienter som de ska skydda, ofta ända in i de djupaste delarna av operativsystemet. Detta är nödvändigt för att skyddet mot skadlig kod ska kunna ske på alla nivåer i mjukvaran. Detta gör att förtroende till leverantören av antivirusprogramvaran är kritisk för organisationen som använder den.

För att antivirusprogramvaran ska kunna hantera nya hot effektivt krävs det att den så snabbt som möjligt kan installera nya signaturer efter att de släppts av antivirusprogramvarans tillverkare. För att det ska vara möjligt måste överföringen mellan tillverkarens och användarnas informationssystem gå så snabbt som möjligt. Av det skälet kommer sådana produkter i regel med en färdig lösning som använder en förtroendebaserad nätverkskoppling till tillverkarens informationssystem. Denna möjliggör automatiserad överföring och installation utan att kunden granskar varje inkommande signatur och kod. Detta är ytterligare en faktor som gör att grunden för förtroende till leveranskedjan och leverantören är kritisk.

Kombinationen av djupgående tillgång och ändringsrättigheter (som kan användas för att styra och sabotera) å ena sidan och å andra sidan den låga graden av granskning och kontroll som många som använder sådana programvaror har över sådana programvaror gör det lockande för hotaktörer att använda dem.

Lägesbild över säkerheten i digitala leveranskedjor

Lägesbild över säkerheten i digitala leveranskedjor

De senaste åren har det skett en rad olika störningar i digitala leveranskedjor på grund av både angrepp, misstag och naturhändelser. I det här kapitlet redogör vi dels för vad incidentrapporteringen har visat, dels för hur den övergripande hotbilden ser ut och exempel på incidenter som den har resulterat i.

Lägesbild från NIS-rapporteringen

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. Detta är talande för den relativt höga andel hot, sårbarheter och risker som handlar om externa parters resurser och komponenter, men som ändå påverkar säkerheten och kontinuiteten i den egna verksamheten. Det säger också något om hur pass vanligt det är för verksamheterna bakom samhällsviktiga tjänster att idag ha starka beroenden till olika typer av digitala leveranskedjor och deras tillhörande leverantörer. Rapporteringen visar att det vanligaste är att det har rört sig om system eller nätverk för kommunikation men att det även är vanligt med incidenter i system för processtyrning eller kontroll samt administrativa system.

De rapporterade incidenterna pågår oftast ett fåtal timmar, även om spannet sträcker sig från minuter till månader. Tiden inkluderar perioden från när incidenten inträffade till när den upptäcktes, hanterades och slutligen upphörde. Ofta upptäcks incidenterna direkt och i de flesta fall av egen personal genom att en tjänst de använder inte är tillgänglig eller inte fungerar som vanligt. I vissa fall har dock incidenten uppmärksammats genom att underleverantören hört av sig. I andra fall, särskilt inom bankverksamhet och dricksvattenförsörjning, har incidenten upptäckts av interna detekteringssystem. I några få fall har det rapporterats att incidenten upptäckts av externa detekteringssystem. Så även om incidenten inträffar i leveranskedjan är det vanligast att det är påverkan internt inom en organisation som är det första tecknet på att en incident har inträffat.

Exempel från rapporteringen

En leverantör av dricksvatten fick problem med sina processtyrningssystem när VPN-servern hos deras systemleverantör drabbades av en incident. Flera funktioner påverkades, exempelvis bröts informationsflödet från fjärr-anläggningar (t.ex. vattentorn) under cirka fem timmar. Enligt leverantören förelåg det ingen risk för människors hälsa under tiden för avbrottet.

Bakomliggande hot och sårbarheter

Baserat på informationen i de mottagna rapporterna är det endast några få procent av incidenterna som har sitt ursprung i antagonistiska handlingar som exempelvis intrång, ransomware[26] eller DDoS[27]-angrepp. Detta kan jämföras med den omfattande internationella mediala rapporteringen om angrepp mot digitala leveranskedjor under samma period. Denna skillnad kan bero på dels att Sverige jämfört med vissa andra länder klarat sig förhållandevis lindrigt undan de stora internationella angreppen[28] under tidsperioden, dels att nyhetsmedia oftare fokuserar på avsiktliga hot som angrepp än oavsiktliga hot som misstag och olyckor.[29] I stället har det varit systemfel och misstag som varit de vanligaste kända orsakerna till incidenterna, och då ofta i samband med förändrings- eller uppgraderingsarbete. I takt med att system blir allt mer komplexa och svåröverskådliga blir det än mer viktigt att säkerställa både processer och kompetens som kan omhänderta dessa arbeten med så minimal risk för incidenter som möjligt.

För mer än 60 procent av de inrapporterade incidenterna som har haft sitt ursprung i en digital leveranskedja har orsaken bakom varit okänd för NIS-leverantören.[30] Denna höga andel kan jämföras med att motsvarande andel incidenter med okänt ursprung i de fall där incidenten sker hos den rapporterade organisationen är drygt 20 procent, det vill säga endast en tredjedel så många. Detta visar på problematiken kring insyn i och information om incidenter som sker i de digitala leveranskedjorna. Det visar också på att hoten och sårbarheterna i de digitala leveranskedjorna i de allra flesta fall är okända för leverantörerna av de samhällsviktiga och digitala tjänsterna. Att så är fallet är oroande på flera sätt, inte minst på grund av svårigheten med att bygga skyddsåtgärder för att bemöta

26. Ransomware kommer från engelskans ”ransom” (lösensumma) och ”software” (mjukvara). Ett angrepp av ransomware, kan innebära att hela eller delar av en verksamhets informationssystem med dess information blir krypterad och inte är tillgänglig för personalen. Genom att kryptera informationen hoppas angriparna på att den utsatta organisationen ska betala en lösensumma för att få tillgång till dekrypteringsnyckeln och få tillbaka den förlorade informationen.

27. Distribuerade överbelastningsattacker efter engelskans Distributed Denial of Service. Ett DDoS-angrepp kan innebära att hela eller delar av en verksamhets internetanslutna system belastas med mer trafik än de kan hantera och då blir otillgängliga.

28. Angreppet mot Kaseya fick dock påverkan på flera stora svenska organisationer. För mer information om angreppet, se kapitel *Avsiktliga hot mot digitala leveranskedjor (angrepp)*.

29. För en mer detaljerad genomgång av den publika diskursen om informationssäkerhet se MSB:s rapport *Is IT safe? En studie av den publika diskursen av informationssäkerhet i Sverige.* MSB1802 – juli 2021 (2021), länk: https://rib.msb.se/filer/pdf/29705.pdf (hämtad 2021-09-21). För en vidare diskussion om hur diskursen och fokus på vissa, snarare än andra, problemområden successivt formas på informations- och cybersäkerhetsområdet, se MSB:s och SIPRI:s rapport *Cyber-incident Management: Identifying and Dealing with the Risk of Escalation*.SIPRI Policy Paper 55 – september 2020 (2020), länk: https://www.sipri.org/publications/2020/sipri-policy-papers/cyber-incident-management-identifying-and-dealing-risk-escalation (hämtad 2021-09-28).

30. Baserat på övrig information i rapporterna finns det inget som tyder på att orsakerna till dessa incidenter inte skulle vara normalfördelade mellan övriga orsakskategorier

ett okänt hot eller att avhjälpa en okänd sårbarhet. Att ta fram avtal med sina leverantörer för att säkerställa både att ett tillräckligt säkerhetsarbete genomförs och att man har tillräcklig insyn i detta blir därför viktiga åtgärder tillsammans med att se över hur man säkerställer redundans för de mest kritiska resurserna när en incident ändå inträffar.

Störningar som incidenterna har orsakat

Även om incidenterna orsakats i leveranskedjan till en leverantör av samhällsviktiga eller digitala tjänster anger de flesta att incidenten inte orsakar störning för andra aktörer i sin tur. Ingen av de incidenterna bedöms heller ha orsakat en störning som inneburit konsekvenser för en annan medlemsstat. Detta kan tyda på att det sker få incidenter med gränsöverskridande konsekvenser men det kan även visa på svårigheten att överblicka vilka beroenden aktörer i andra länder har till en viss tjänst.[31] Leverantörerna bedömer vidare att negativ påverkan av störningarna främst gäller privatpersoners hälsa, men i liten eller begränsad omfattning, vilket delvis kan förklaras av att hälso- och sjukvårdssektorn står för en stor del av rapporteringen och att man i den sektorn är förhållandevis väl förberedd på och van vid att arbeta under andra former när situationen kräver det. Framför allt bedöms det i stället att det är användarnas förtroende för den samhällsviktiga tjänsten som påverkas mest av störningen.

Över 40 procent av leverantörerna bedömer att incidenterna som hade sitt ursprung i den digitala leveranskedjan orsakade stora störningar på tjänsten vilket innebar att hela eller flera funktioner av tjänsten inte kunde tillhandahållas. Ytterligare en tredjedel av leverantörerna rapporterade att endast vissa funktioner påverkades medan andra var tillgängliga. De resterande uppgav att störningen endast påverkade tjänsten i begränsad utsträckning och att den samhällsviktiga tjänsten helt kunde tillhandahållas under tiden, vilket i flera fall beror på alternativa manuella rutiner. Användandet av sådana alternativa rutiner innebär dock i regel en ökad arbetsbelastning för organisationen, och ett tapp i effektivitet.

31. Eftersom det är leverantören av den samhällsviktiga tjänsten som rapporterar, men det är hos dess underleverantör som incidenten har inträffat, är det troligen svårt för leverantören av den samhällsviktiga tjänsten att överblicka vilka som påverkas av incidenten, oavsett om det handlar om organisationer i Sverige eller utomlands.

Hantering av incidenterna och förebyggande åtgärder

I nästan hälften av rapporterna som handlar om incidenter som har inträffat hos en underleverantör till leverantörer av samhällsviktiga eller digitala tjänster uppger rapportörerna att de vid tidigare tillfällen har drabbats av liknande incidenter och störningar. Det är dock skillnad på hur leverantörerna hanterar incidenter som har sitt ursprung hos en underleverantör. När det gäller att beskriva vad orsaken till incidenten var, framträder en skillnad mellan incidenter som skett inom den egna organisationen och incidenter som har ursprung hos en underleverantör. I majoriteten av fallen när incidenten skett i en digital leveranskedja vet den rapporterande organisationen vid rapporteringstillfället inte alls vad incidenten beror på utan inväntar incidentrapport från underleverantören. Det finns beskrivet att det i vissa fall varit så att underleverantören inte haft helgbemanning, vilket lett till långa svarstider på vad felet är och hur länge det kan komma att pågå. I andra fall har hanteringen behövts anpassats till servicefönster i andra länder vilket försvårat och försenat hanteringen.

När det kommer till hur de ska förebygga liknande incidenter är det många som främst planerar att se över sina egna rutiner, eller att köpa in ny hårdvara. Det handlar även ofta om att man ska se över kommunikationen med underleverantören. I enstaka fall meddelar leverantören att de ska se över sina Service Level Agreements (SLA) med underleverantören och i ett fåtal fall går det så långt att leverantören säger att det kommer ske ett byte av underleverantör. Generellt är det tydligt att flera leverantörer inte bara utkontrakterar sin tjänst, utan även kunskap om tjänsten, och utan information från underleverantörer står de ibland handfallna inför att beskriva vad det är som inträffat.

Hot mot digitala leveranskedjor

I det här avsnittet behandlar vi hot mot digitala leveranskedjor inom fyra övergripande kategorier; angrepp, misstag, systemfel och naturhändelser. Med hot[32] menar vi något som orsakar, eller kan orsaka, en incident i en digital leveranskedja.

32. Se bilagan *Om analys av hot, sårbarheter och risker i digitala leveranskedjor*.

Avsiktliga hot mot digitala leveranskedjor (angrepp)

I det här avsnittet delar vi in antagonistiska hot i fyra motivbaserade kategorier och behandlar dem i varsitt underavsnitt.[33] Vi presenterar troliga val av strategier och eftersökta utfall och effekter till respektive övergripande motiv. I respektive underavsnitt ger vi också en redogörelse för och klassificering av ett samtida angrepp som involverar digitala leveranskedjor.[34]

Det är viktigt att komma ihåg att en antagonist kan ha flera olika motiv samtidigt, och att det är möjligt att kortsiktigt ha ett motiv och långsiktigt ett annat. Hur en antagonist förhåller sig kommer naturligtvis också att bestämmas av andra faktorer än det motiv som driver antagonisten, exempelvis kommer det kanske att spela roll vad det är för slags aktör och hur riskbenägen antagonisten är, vilka resurser och förmågor den har tillgång till etc.

När antagonistens avsikt är att orsaka skada

Det här motivet kan handla om att orsaka skada hos den som angrips, eller hos andra, via den som angrips. Antagonister som är ute efter att skada en aktör kan välja att försöka angripa aktören genom att dra nytta av de förtroendebaserade kanaler som aktören har till leverantörer i sina digitala leveranskedjor. Därigenom kan angriparen få åtkomst till skyddade miljöer hos aktören och därefter använda åtkomsten för att orsaka skada. Skälen till att en angripare väljer att ta en sådan ”omväg” för att få tillträde till skyddade miljöer och system kan dels vara att angriparen också har andra tilltänkta mål, som den också kan få åtkomst till via leverantören, dels att angriparen bedömer att det är lättare att få åtkomst till leverantören och därefter till det egentliga målet än vad det är att direkt försöka ta sig förbi det tilltänkta målets egna skydd.

Antagonisten kan också angripa någon av det egentliga målets leverantörer, skaffa sig åtkomst till leverantörens system och därigenom introducera hot eller ta bort skydd i de digitala produkter som leverantören tillhandahåller till det egentliga målet. Det introducerade hotet kan därefter orsaka skada när hårdvaran eller mjukvaran installeras, eller när angriparen utnyttjar att ett skydd har tagits bort för att få en väg in i det egentliga målets system. En strategi som bygger på att introducera hot i leverantörens tjänster eller produkter är dock riskabel för angriparen av två skäl. Det kan vara så att hotet kan orsakar en incident hos någon annan som installerar tjänsten eller produkten tidigare än det egentliga målet, varpå det egentliga målet får en chans att bli varse hotet och undvika att installera produkten eller tjänsten. Det kan även vara för att den skada som hotet orsakar också kommer att drabba många andra som installerar produkten eller tjänsten, varpå motreaktionen på angreppet kan bli mycket stor. Om det introducerade hotet dessutom har en förmåga att sprida sig själv vidare så finns ytterst risken att angriparen själv, eller andra som angriparen måste förhålla sig till, drabbas av incidenter.

---

33. Motiven utgör samlat ett sätt att på en övergripande nivå samla alla de drivkrafter som en antagonist kan ha. De är att: (1) Orsaka skada hos den som angrips, eller hos andra, via den som angrips, (2) Orsaka nytta för den som angriper, eller för andra, för vilkas räkning antagonisten genomför angreppet, (3) Förhindra skada för den som angriper, eller för andra, för vilkas räkning antagonisten genomför angreppet (preemptiva angrepp) och (4) Förhindra nytta hos den som angrips, eller hos andra, via den som angrips.

34. Se analysramverket i bilagan *Om analys av hot, sårbarheter och risker* för mer information om hur incidenter i och angrepp mot digitala leveranskedjor kan analyseras.

Angreppet mot Intellect-Service's digitala leveranskedja (NotPetya)

Typ av incident i digital leveranskedja: Leverans av något (ett hot och ett hinder) som inte ska levereras.

Någon gång innan den 22 juni 2017 lyckades angripare, med hjälp av stulna användaruppgifter, skaffa tillgång till företaget Intellect-Service's (numera kallat Linkos Group) utvecklingsmiljö. Företaget låg bakom programvaran M.E.Doc som användes av de flesta som behövde sköta skatteärenden eller hade affärer i Ukraina. Programmet användes därför av en stor del av landets samhällsviktiga verksamheter men även av internationella bolag som verkade i landet.

När angriparna hade säkerställt sin tillgång till utvecklingsmiljön och försäkrat sig om att de inte var upptäckta så la de till skadlig kod i en uppdatering till M.E.Doc som därefter sändes ut till Intellect-Services kunder. Den skadliga koden kom att kallas NotPetya[35], och har kallats för världens mest destruktiva cybervapen. NotPetya var utrustat med ett antal programfunktioner, bland annat penetrationsverktyget *EternalBlue* som ska ha stulits från amerikanska National Security Agency, och en sen tidigare känd metod för att utnyttja Windows-sårbarheten *Mimikatz*. Detta gjorde att NotPetya, när det väl fått fotfäste i en organisations system, snabbt kunde sprida sig vidare. NotPetya var även utrustat med funktioner som krypterade såväl datorers huvudstartsektor[36], varpå de inte kunde startas, som deras filer. Krypteringen var dessutom irreversibel, vilket ledde till att all data som NotPetya kom över gick förlorad.

NotPetya blev ett av de dyraste cyberangreppen i historien. Kostnaderna uppkom på grund av de stora störningar som uppkom under angreppet, all information som gick förlorad och all hårdvara som förstördes och behövde bytas ut. Stora delar av Ukrainas informationssystemsunderstödda infrastruktur drabbades och gjordes otillgänglig – däribland banker, elproducenter, sjukhus och flygplatser. Det uppskattas att 10 procent av Ukrainas datorer förstördes som en konsekvens av angreppet. Effekterna stannade dock inte vid Ukrainas gränser. Det danska logistikföretaget Maersk var en av de hårdast drabbade aktörerna globalt – bland annat påverkades transportflödena i flera hamnar där stora laster med containrar blev stående. NotPetya tros ha kommit in i Maersks nätverk via en enda dator på ett kontor i Ukraina som hade M.E. Doc-mjukvaran installerad. Därifrån spred sig sedan den skadliga koden inom företagets nätverk till andra system över hela världen.

35. Den skadliga koden som kom att kallas NotPetya för att signalerar likheten (men samtidigt stora skillnader) med utpressningsviruset känt som Petya, vilket upptäcktes 2016.

36. På engelska kallad *Master Boot Record* (MBR).

När antagonistens avsikt är att vinna fördelar

Det här motivet kan handla om att orsaka nytta för den som angriper, eller för andra, för vilkas räkning antagonisten genomför angreppet. Antagonister som önskar vinna otillbörlig nytta för sig själva, exempelvis genom att stjäla känslig information, kan i likhet med den föregående typen av motiv använda sig av angrepp mot eller genom digitala leveranskedjor. Genom att tillskansa sig åtkomst till leverantörens system kan angriparen använda den förtroendebaserade kanalen in hos det egentliga målet för att därigenom antingen skaffa sig direkt åtkomst, eller manipulera leverantörens produkter eller tjänster så att de innehåller hot eller saknar skydd. När produkterna eller tjänsterna installeras eller börjar användas kan hotet ta bort, deaktivera eller blockera skydd hos det egentliga målet, ta kontroll över drabbade system eller exempelvis direkt skicka information till angriparen. Alternativt kan bristen på skydd i det som levereras användas för att ta sig in i systemen och därefter stjäla information.

Att angripa leverantörens produkter eller tjänster medför dock att alla som mottar och installerar eller använder leverantörens produkt eller tjänster kommer att installera det inlagda hotet, eller kommer att installera något som saknar ett skydd. Det ökar sannolikheten för att någon snabbt kommer att upptäcka och agera mot hotet eller bristen på skydd, vilket i sin tur äventyrar angriparens möjligheter att undgå upptäckt och komma åt de resurser som den är ute efter.

Detta, och det sista motivet, ibland i kombination, förefaller utgöra de vanligaste motiven för angripare.[37]

37. Baserat på vad vi kan se i incidentrapporteringen som MSB mottar inom området. Det förefaller också stämma väl med andra resultat från sammanställning och databaser såsom Council on Foreign Relations *Cyber Operations Tracker*, se https://www.cfr.org/cyber-operations/.

Angreppet mot SolarWinds digitala leveranskedja

Typ av incident i digital leveranskedja: Leverans av något (ett hot och ett hinder) som inte ska levereras.

Den 11 december 2020 upptäckte cybersäkerhetsföretaget FireEye att angripare hade kommit åt och manipulerat uppdateringar av företaget SolarWinds mjukvara Orion. Orion är ett verktyg för nätverksövervakning och administration med en hög behörighet och åtkomstnivå i sina kunders it-miljöer. Mjukvaran används ofta inom stora organisationer, och användes vid tiden för incidenten av hundratusentals företag och myndigheter runt om i världen. FireEyes upptäckt blev upptakten till uppdagandet av en av de hittills mest omfattande och medialt rapporterade attackerna mot digitala försörjningskedjor.

Angreppets första del bestod av att skaffa sig åtkomst till SolarWinds utvecklingsmiljö (de informationssystem och programvaror som SolarWinds anställda använder för att lägga till, ändra och ta bort kod i exempelvis Orion). Efter en del experimenterande, och utan att upptäckas, lyckades angriparen lägga in skadlig kod vars enda syfte var att, vid precis rätt tillfälle, lägga till ett specialbyggt paket av skadlig kod (som sedermera kom att kallas *Sunburst*). SolarWinds utvecklare märkte inte de förändringar i koden av deras nya uppdatering som detta medförde, så de följde sin vanliga procedur för utskick av en uppdatering – varpå deras kunder började installera densamma.

Detta innebar att cirka 18000 kunder fick uppdateringen och därmed också den skadliga koden. Angreppet var dock inte tänkt för alla de kunderna, utan det var särskilt inriktat mot amerikanska myndigheter – och det faktum att så många hade fått den skadliga koden ökade risken för upptäckt för angriparen. Sunburst var designat för att hantera den risken genom att först ligga inaktiv i två veckor från och med det att koden installerats på ett system (troligen för att därigenom inte dra uppmärksamhet till hur den skadliga koden kommit in i ett system från början), varpå den därefter försiktigt undersökte om vissa säkerhetsprogramvaror var installerade. Var de det så försökte Sunburst deaktivera eller oskadliggöra dem. Om det inte gick deaktiverade Sunburst sig själv. Om Sunburst lyckades ta sig förbi installerade skydd på det sättet så försökte koden, på ett maskerat sätt, att kontakta en utomstående server. När kontakt var upprättad skickade Sunburst information om systemet det var installerat på till servern, och därigenom kunde angriparen avgöra, eller åtminstone kvalificerat bedöma, vems system det var. Om systemet inte tillhörde något av de tilltänkta målen så kunde man skicka ett kommando till Sunburst om att avinstallera sig själv – och det ska ha hänt många gånger. Om systemet däremot var av intresse så kunde man använda Sunburst för att introducera ytterligare skadlig kod som man sedan använde för att utöva det spionage som angreppet hela tiden hade syftat till att möjliggöra.

Till skillnad från NotPetya så var inte SolarWinds-incidenten en incident som *i sig* medförde skada eller förhindrade nytta hos de som fick den skadliga koden installerad. Däremot kan den information som angriparen stal ha gett säkerhetspolitiska fördelar. Därutöver blev de drabbade organisationernas behov av incidenthantering, utredningar, utbyte av kompromitterad utrustning och andra aspekter mycket dyra.

När antagonistens avsikt är att förhindra skada

Det här motivet kan handla om att förhindra skada för den som angriper, eller för andra, för vilkas räkning antagonisten genomför angreppet. Antagonister som angriper i förebyggande syfte kan använda angrepp som orsakar båda typerna av incidenter i leveranskedjor, det vill säga både incidenter där sådant som inte ska levereras ändå levereras, och incidenter där sådant som ska levereras inte levereras.

Som vi visat i de två föregående avsnitten kan angrepp mot digitala leveranskedjor som resulterar i incidenter där sådant som inte ska levereras ändå levereras användas av angripare för att skaffa sig åtkomst eller direkt orsaka skada hos angriparens egentliga mål. Den typen av angrepp är naturliga att använda för en angripare om det egentliga målet bedöms vara väl skyddat, eller om leverantören som angreppet först riktar in sig emot har förtroendebaserade vägar in till flera måls känsliga system samt om angriparen önskar skada en redan befintlig funktion eller förmåga hos det egentliga målet.

Antagonister kan också använda sig av angrepp som orsakar den andra typen av incident i digitala leveranskedjor, det vill säga att sådant som ska levereras inte levereras, för att se till att det egentliga målet inte kan upprätthålla produktion, utveckla nya förmågor eller tjänster, eller återställa system efter incidenter. Handelshinder som gäller för strategiska produkter, såsom specialiserade mikrochipp, är exempel på insatser som innebär att produktion och innovation hos drabbade mottagande aktörer avstannar.

USA:s pre-emptiva cyberoperationer för att skydda valet 2020

Typ av incident i digital leveranskedja: Leverans av något (ett hot och ett hinder) som inte ska levereras.

Inför det amerikanska presidentvalet i november 2020 genomförde US Cyber Command ett antal operationer mot bland annat iranska, ryska och kinesiska aktörer som man misstänkte förberedde påverkansoperationer av olika slag.

Ett angrepp som har tillskrivits U.S. Cyber Commands initiativ var utslagningen av stora delar av infrastrukturen som underbyggde botnätet Trickbot[38], som hade kunnat användas för att lamslå teknisk valutrustning eller informationssystemen som upprätthåller samhällsviktiga tjänster. Botnätet styrdes från Östeuropa och hade programmerats av rysktalande personer. Något som särskilt talade för att Trickbot skulle användas för att störa valet var att botnätet hade utrustats med övervakningsfunktioner som kunde användas för att spionera på infekterade enheter och därigenom avgöra om enheten exempelvis tillhörde eller användes av någon som arbetade med valet i en officiell kapacitet.

Angreppet mot Trickbot genomfördes genom att någon tog kontroll över servrar som innehöll botnätets styr- och kontrollsystem, varpå man skickade ut en uppdatering till de uppkopplade enheter som utgjorde botnätet. Uppdateringen gjorde att den skadliga koden som installerats i enheterna omprogrammerades till att ta kommandon från enheten som den skadliga koden var installerad på, i stället för servrarna som innehöll botnätets styr- och kontrollsystem.

38. Ett nätverk av (vid tidpunkten för valet) upp till två miljoner uppkopplade enheter som kapats genom intrång och installation av skadlig kod. Den skadliga koden kunde, och hade, använts för att injicera ransomware direkt in i de enheter som kapats. Det är ett relativt vanligt förfarande bland cyberkriminella att specialisera sig inom olika områden och att dela på vinsterna av den kriminella verksamheten. Aktören eller gruppen som skapade Trickbot specialiserade sig på att genomföra intrång och upprätta kontroll på insidan. Möjligheten att använda den kontrollen kunde sedan, mot ersättning, användas av andra som exempelvis ville spionera genom att kopiera och skicka iväg information från infekterade system. Det var också möjligt att använda den kontrollen och den öppnade vägen för att infektera system med ytterligare skadlig kod, såsom ransomware.

När antagonistens avsikt är att hindra verksamhet

Det här motivet kan handla om att förhindra nytta hos den som angrips, eller hos andra, via den som angrips. Antagonister som vill försöka hindra sina mål från att generera nytta[39], exempelvis genom att stoppa en organisations produktion av viss hårdvara, kan i likhet med angripare som drivs av det föregående motivet, använda angrepp som orsakar båda typerna av incident i en digital leveranskedja.

Antagonister kan försöka orsaka incidenter där sådant som inte ska levereras ändå levereras, exempelvis för att genom inplantering av skadlig kod i en leverantörs produkt få det egentliga målet att ovetandes själv installera den skadliga koden. När den skadliga koden väl finns i det egentliga målets system så kan den aktiveras och stänga ner drabbade system.

Antagonister kan också välja att försöka orsaka incidenter där sådant som ska levereras inte levereras, med följden att det egentliga målet måste dra ner på eller stänga ner sin produktion, alternativt att nya funktioner inte kan utvecklas eller återställning i samband med en incident inte kan slutföras.

Angreppet mot Kaseyas digitala leveranskedja

Typ av incident i digital leveranskedja: Leverans av något (ett hot och ett hinder) som inte ska levereras.

Under fredagskvällen den 2 juli 2021 uppstod störningar i kassasystemen hos bland annat den svenska dagligvarukedjan Coop (det rapporterades också att liknande störningar hade uppstått bland aktörer som bedriver verksamhet inom transport, bränsleförsörjning och apoteksverksamhet). Störningarna hindrade butikerna från att kunna ta betalt av sina kunder. Snart hade runt 800 Coop-butiker fått stänga ned i stora delar av landet. Andra svenska företag skulle också visa sig ha drabbats av störningar i sina betalsystem.

Följande dag bekräftades det att störningarna orsakats av ett ransomware-angrepp. Angreppet hade inte riktats direkt mot de drabbade svenska företagen. Det var inte heller ett angrepp som riktats direkt mot leverantören av tjänsten för betalningarna – Visma Esscom. Angreppet hade i stället riktats mot det amerikanska mjukvaruföretaget Kaseya och deras programvara Virtual System Administrator (VSA), vilken används för fjärrstyrning, administration och drift av olika internetuppkopplade system. Angriparna tog sig in i Kaseyas interna nätverk och la in ransomwarekoden i en uppdatering som de därefter skickade ut. När uppdateringen installerades hos mottagarna, däribland Visma Esscom, aktiverades ransomwarekoden, varpå densamma spred sig ut till alla de enheter VSA hade kontakt med – i Coops fall deras kassasystem.

Coop-butikerna fick hålla stängt i flera dagar. Cirka 150 tekniker fick sättas in för att manuellt ominstallera kassasystemen på plats i butikerna. I media rapporterades det om miljonförluster för dagligvaruhandelskedjan till följd av nedstängningen. Precis som i fallet med NotPetya och Intellect Service visade det sig sedan att Kaseya och VSA hade ett undermåligt skydd och ett eftersatt säkerhetsarbete.

39. Motiven att vilja förhindra nytta för den man angriper och att vilja orsaka skada för den man angriper är snarlika, men skiljer sig åt i den bemärkelsen att det första motivet exempelvis kan innebära att offret går miste om inkomster (d.v.s. man får inte något önskvärt som man annars skulle ha fått) medan det senare motivet (utöver att offret kan tänkas gå miste om inkomster) innebär att offret får högre kostnader som en direkt konsekvens av angreppet (snarare än via reaktioner på angreppet, såsom återbetalnings- eller skadeståndskrav för utebliven leverans). Distinktionen är viktig i vissa sammanhang, såsom i analyser av varför vissa organisationer betalar lösensumman för att bli fria från ransomware. I många fall är det inte kostnaderna för återställning av drabbade system som gör det till en bättre ekonomisk affär att betala – utan snarare de uteblivna intäkterna under den tid som blockeringen av systemen varar. En annan viktig skillnad är att det genom angrepp går att förhindra en organisation från att generera nytta genom att angripa och skada dess leverantörer och därmed stoppa nödvändig försörjning. I det läget orsakas skadan hos någon annan, men följden blir att det egentliga målet inte kan generera nytta (såsom att exempelvis tillverka produkter).

Oavsiktliga hot mot digitala leveranskedjor (misstag)

I det här avsnittet ges exempel på hur misstag[40] och systemfel har resulterat i storskaliga incidenter i leveranskedjor. Incidentrapporteringen från NIS-leverantörer och statliga myndigheter till MSB har hittills varje år visat att misstag och systemfel orsakar fler incidenter (även allvarliga incidenter) än angrepp.

Medan antagonistiska hot med fördel kan analyseras utifrån olika motiv är det mindre lämpligt att analysera oavsiktliga mänskliga hot på samma sätt. När incidenter orsakas oavsiktligt sker det ofta för att människor försöker att göra rätt, men att de är felinformerade, eller att de fokuserar på fel saker. Exempelvis kan misstag uppstå när man fokuserar överdrivet mycket på att antingen inte göra fel (och därmed kanske inte uppnår den effekt som man avsåg att uppnå) eller när man fokuserar överdrivet mycket på att uppnå den effekt man avsåg att uppnå (och därmed missar att beakta alla de sidoeffekter som vissa ingrepp kan medföra). Oavsiktliga incidenter kan också uppstå när tid och resurser inte räcker till, och genom att ett ingrepp avbryts innan det är helt genomfört.

Haveri hos Google under covid-19-pandemin ledde till avbruten undervisning

Typ av incident i digital leveranskedja: Avsaknad av leverans av något (en framgångsfaktor eller ett skydd) som ska levereras.

Den 14 december 2020 fick Google ett internt problem med lagringskapaciteten för sina autentiseringssystem vilket resulterade i att flera av företagets tjänster som krävde inloggning från sina användare blev onåbara. Problemet orsakades av ett kompatibilitetsfel som uppstod när delar av ett system som hanterar anrop vid autentisering uppdaterades. De drabbade tjänsterna – för bland annat mejl, kalendrar, kartor och delning samt lagring av information – hade en stor användarkrets bland svenska privatpersoner och organisationer. Effekterna av störningarna, trots att de pågick mindre än en timme, blev märkbara i samhället. Bland annat avbröts undervisningen på flera gymnasieskolor, eftersom den genomfördes på distans med anledning av covid-19-pandemin och var beroende av Googles drabbade tjänster.

Därutöver finns det en gråzon mellan angrepp och misstag där aktörer kan välja att fokusera på att göra saker som gagnar dem själva, även om det innebär negativa konsekvenser för andra (men där de negativa konsekvenserna för andra inte är syftet).

Utöver incidenter som orsakas av medvetet handlande som antingen slår fel eller slår rätt för en själv men går ut över andra är det också vanligt att incidenter uppstår för att man agerar obetänksamt. Dessutom kan tekniska fel uppstå om man underlåter att, exempelvis utföra sådant underhåll som informationssystemen och deras stödsystem behöver för att inte bli utslitna i samband med användning.

40. Misslyckade ingrepp – se analysramverket i bilagan *Om analys av hot, sårbarheter och risker i digitala leveranskedjor*.

Brand i OVH Cloud:s datacenter ledde till att miljontals webbsidor blev otillgängliga

Typ av incident i digital leveranskedja: Avsaknad av leverans av något (en framgångsfaktor eller ett skydd) som ska levereras.

Onsdagen den 10 mars 2021, någon gång efter midnatt, blev plötsligt cirka två procent av alla .fr-domäner, såväl som sidor från andra domäner – inklusive hemsidor för regering och myndigheter i flera länder, otillgängliga. Totalt ska cirka. 3,6 miljoner webbsidor ha gått ned. Företaget agerade snabbt för att återupprätta drabbade webbsidor genom att tillhandahålla dem från andra datacenter men först på tisdagen den 6 april hade 80 procent av kapaciteten i den primära tjänsten som det drabbade datacentret tillhandahöll återställts. Företaget har meddelat att den slutgiltigt fastställda orsaken till branden inte kommer att meddelas förrän under 2022, men flera källor indikerar att orsaken ska ha varit ett slarvigt utfört underhållsarbete av datacentrets reservkraftsystem.

Det finns också oavsiktliga hot mot digitala leveranskedjor som uppstår som en sidoeffekt av konflikter. Exempelvis kan komplikationer i försörjningen av vissa hård- eller mjukvarukomponenter i EU uppstå som en bieffekt av de handelsrestriktioner som USA och Kina infört mot varandra.

Det är också viktigt att komma ihåg att medan digitala leveranskedjor har en viss dynamisk kapacitet att möta förändringar i efterfrågan finns det fortfarande begränsningar i hur mycket kapaciteten kan skalas upp på kort varsel. Detta har blivit tydligt under 2020-2021 då efterfrågan på vissa hårdvaruprodukter, bland annat på grund av den globala pandemin, först sjönk och därefter ökade kraftigt. Omställningssvårigheterna har drabbat såväl producenter som (globala) logistikoperatörer. I de senares fall har en slags global köbildning uppstått när hamnar inte haft kapacitet att ta emot containrar och leveranser från alla de skepp som anländer. Detta har resulterat i att producenter av produkter har fått vänta på att få sina produkter upphämtade vilket lett till att de har fått hålla produktionstakten låg eller successivt har fått betala lagerhållning av redan producerade enheter som väntar på att bli bortfraktade. Resultatet har blivit långa väntetider på vissa hårdvaruprodukter, och ökade kostnader, utöver de förseningar som incidenter av olika slag har medfört.

Hot eller sårbarheter i grundutförande eller påbyggnad

Även små misstag som sker vid produktionen av sådant som ska levereras inom ramen för en digital leveranskedja kan resultera i omfattande konsekvenser. När en felaktig konfiguration (ett hot) implementeras i en mjuk eller hårdvara som sedan massproduceras kommer effekterna av den felaktiga konfigurationen att kunna uppstå i många enheter som har den konfigurationen samtidigt. Om den felaktiga konfigurationen medför påtagliga konsekvenser i de mjuk- eller hårdvaror där den finns och om organisationer som införskaffar mjuk- eller hårdvaran inte också har tillgång till eller försörjning av annan mjuk- eller hårdvara som kan användas för samma syfte kan de få stora problem.

Cirka 1000 kraschade datorer i Västra Götalandsregionen 2019

Typ av incident i digital leveranskedja: Leverans av något (ett hot och ett hinder) som inte ska levereras.

Under hösten 2019 kraschade upp mot tusen datorers hårddiskar under några veckor i Västra Götalandsregionen. Datorerna var av samma märke och det visade sig sedan att de troligtvis hade felkonfigurerats från början så att de efter ett visst antal timmars användning skulle sluta fungera. Det resulterade i en svårhanterad situation för vårdpersonalen i delar av regionens sjukvård, exempelvis genom att det blev svårt att läsa digitala vårdjournaler och nå annan information på nätverket. På några håll fick man gå upp i stabsläge för att säkerställa att vården skulle kunna bedrivas tills problemet kunde lösas.

Samma eller liknande problematik kan uppstå när ny funktionalitet ska upprättas i redan befintliga mjuk- och hårdvaror, exempelvis i samband med uppdateringar där skadlig kod medföljer eller där nya otillräckligt skyddade (och därför sårbara) funktioner läggs till.

Sårbarheter i Microsoft Exchange-mejlservrar 2021

Typ av incident i digital leveranskedja: Avsaknad av leverans av något (en framgångsfaktor eller ett skydd) som ska levereras.

Under början av 2021 upptäcktes ett antal sen tidigare okända sårbarheter i lokalt installerade (d.v.s. inte externt och med fjärrmedel tillhandahållna) mejlservrar från Microsoft. Sårbarheterna innebar att obehöriga aktörer kunde ta kontroll över mejlservern och få höga behörigheter. Organisationer som hade upprättat egna lokala mejlservrar genom att installera Microsofts programvara hade därmed fått mejlservrar som var otillräckligt skyddade gentemot vissa former av anrop.

Kort efter att sårbarheterna upptäcktes började man också att upptäcka angrepp som utnyttjade sårbarheterna. Det bör dock noteras att medan ”introduktionen” av sårbarheter hos organisationer som upprättat lokala mejlservrar med stöd av Microsoft Exchange var en leveranskedjeincident var angreppen *inte* exempel på detta eftersom de riktades direkt mot de aktörer som hade sårbarheten, snarare än genom Microsoft och vidare genom en förtroendefull kanal till det tänkta offret.

Misslyckat förändringsarbete och systemfel i tjänster eller informationsflöden

Vid sidan av sådana incidenter i digitala leveranskedjor som uppstår i samband med försörjning av ny mjuk- eller hårdvara, eller uppdateringar, utgör oavsiktliga mänskliga hot och systemfel orsaker till incidenter i tjänster som löpande tillhandahålls inom ramen för digitala leveranskedjor. Detta är mycket vanligt bland NIS-leverantörer, exempelvis genom att man har anlitat en underleverantör som levererar journal-, larm- eller sensorsystem till många aktörer samtidigt. När saker går fel i samband med underhålls- eller utvecklingsarbete, eller när systemen inte underhålls tillräckligt (så att de slits ut, inte görs kompatibla med nya system eller överbelastas), och incidenter uppstår drabbar de många aktörer samtidigt.

Att incidenter i digitala leveranskedjor som orsakas av misstag rapporteras så ofta kan övergripande förklaras av tre faktorer: det stora antalet organisationer som anlitar underleverantörer för verksamhet och stödfunktioner, det relativt begränsade antalet underleverantörer samt underleverantörernas relativt frekvent förekommande incidenter. De tre faktorerna samverkar på så vis att de flesta underleverantörerna (eventuellt med undantag för några mindre aktörer på marknaden) var och en har många kunder, varför många organisationer drabbas samtidigt varje gång underleverantören har en incident som får återverkningar på tjänsten de tillhandahåller. Det resulterar i sin tur i att många organisationer samtidigt drabbas av en incident som de behöver rapportera. Om underleverantören då har ett antal incidenter under ett år kommer de incidenterna fort att dominera i statistiken.

Mjukvaruuppdateringar i Fastlys respektive Akamais CDN-tjänster gjorde medietjänster samt, regeringars och globala företags webbsidor otillgängliga

Typ av incident i digital leveranskedja: Avsaknad av leverans av något (en framgångsfaktor eller ett skydd) som ska levereras.

Onsdagen den 12 maj 2021 genomförde CDN[41]-tillhandahållaren Fastly en mjukvaruuppdatering i sin tjänst som innehöll en bugg som vid en särskild typ av interaktion med ett kundsystem kunde trigga ett avbrott i hela företagets tjänst. På morgonen den 8 juni inträffade just en sådan interaktion. På kvällen den 21 juni och eftermiddagen den 22 juli genomförde CDN-tillhandahållaren Akamai ett liknande arbete. Störningarna som orsakades i respektive tjänst fick globala återverkningar genom att webbsidor och tjänster som använder Fastlys respektive Akamais CDN-tjänster blev otillgängliga. Effekterna av otillgängligheten blev att företag och myndigheter som inte hade reservlösningar inte kunde tillhandahålla sina tjänster, och att exempelvis medier blev svåra att nå. Medan Fastlys incident och Akamais första incident varade i cirka ett halvt dygn varade Akamais senare avbrott betydligt kortare tid.

41. Förkortningen står för *Content Delivery Network* och avser ett geografiskt utspritt nätverk av servrar och annan informationsinfrastruktur som används för att webbtjänster som anropas från olika delar av världen samtidigt ska kunna tillhandahållas i närheten av de regioner som anropen kommer ifrån, för att därigenom korta svarstider och minska belastningen på en viss domän. CDN-tjänsten tillhandahålls i allmänhet av en aktör som samlat styr, underhåller och tillhandahåller tjänsten till ett stort antal kunder världen över. Styrningen och underhållet av hela CDN-tjänstens samlade informationsinfrastruktur hanteras centralt, varför ett fel i samband med omkonfigurationer eller uppdateringar kan slå över hela CDN-tjänsten samtidigt, och därmed också drabba alla de organisationer som använder CDN-tjänsten.

Naturhot mot digitala leveranskedjor

Vissa av de digitala leveranskedjorna bygger på löpande leveranser av exempelvis mikrochipp eller halvledare från ett begränsat antal producenter som i sin tur skapar sina produkter i ett litet antal produktionscentra. Sådana centra måste själva klara ett stort antal krav, men omgivningen måste också vara beskaffad på särskilda sätt. Vid tillverkning av många hårdvarukomponenter krävs exempelvis att luftfuktighet, temperatur och andra faktorer är mycket stabila. Dessutom kräver produktionen stora mängder el och vatten, vilka i sin tur hämtas från resurser i omgivningarna. Vattnet som används måste dessutom vara mycket rent eftersom förekomst av exempelvis radioaktiva partiklar, även i mycket små mängder, kan påverka den känsliga kiselstrukturen i en halvledare. Eftersom tillverkningen måste ske på ett mycket precist sätt för att bli rätt blir produktionen känslig för exempelvis jordbävningar. Det medför att många naturliga fenomen också hotar de digitala leveranskedjorna.

Jordbävning i Ibaraki, Japan, stoppade Renesas chipproduktion

Typ av incident i digital leveranskedja: Avsaknad av leverans av något (en framgångsfaktor eller ett skydd) som ska levereras.

Lördagen den 13 februari 2021 inträffade en jordbävning i Ibaraki, Japan. Regionen är hem för en av mikrochipp-tillverkaren Renesas anläggningar. Jordbävningen ledde till elavbrott som i sin tur avbröt chipproduktionen. Anläggningen kan dessutom ha drabbats av skador. Samma anläggning drabbades också i den stora jordbävningen 2011 då Fukushima-kärnkraftverket drabbades av en härdsmälta. Den gången förstördes anläggningens huvudbyggnad och det tog tre månader att få i gång produktionen igen.

I och med de pågående klimatförändringarna förväntas extrema väderhändelser bli mer frekvent förekommande. Värmeböljor, som väntas bli vanligare på vissa håll, medför behov av mer kylning, vilket påfrestar elförsörjningen och även leder till en kraftigt ökad efterfrågan på fjärrkyla som inte alltid kan mötas på kort varsel. Köld och snöoväder, som också förväntas bli vanligare på vissa håll, medför plötsliga behov av mer energi som elnäten inte alltid kan leverera, med följden att den el som finns måste prioriteras till samhällsviktig verksamhet (och, ibland, för att värma människors hem) med följden att den industriella produktionen avbryts. När väl produktionen har avbrutits tar det lång tid att starta processen som innehåller hundratals steg som precist måste följas i en strikt ordning.

Snöoväder i Texas stoppade Samsungs, NXP:s och Infineons produktion av mikrochipp

Typ av incident i digital leveranskedja: Avsaknad av leverans av något (en framgångsfaktor eller ett skydd) som ska levereras.

I februari 2021 uppstod i Nordamerika ett väderfenomen där ovanligt mycket kyla, snö och is nådde ovanligt långt söderut. Väderfenomenet täckte stora delar av kontinenten och resulterade i att bland annat Texas under minst en vecka hade ett snötäcke, med temperaturer långt under det normala. Ovädret ställde till stora skador i en delstat där sådana fenomen är mycket ovanliga, och där beredskapen för att hantera sådana händelser inte var fullt utbyggd.

En konsekvens av ovädret blev att elnätet fort överbelastades, med följden att många industriella verksamheter fick stängas ned eller avbrytas, däribland chipproduktionen hos tillverkarna NXP, Samsung (där avbrottet varade i mer än en månad) och Infineon (där produktionskapaciteten beräknades vara återställd i juni 2021). NXP meddelade i mars 2021 att produktionsstoppet hade pågått i cirka en månad. Orsaken till det var flera: att elbristen varade ett tag efter att ovädret hade bedarrat, att man behövde analysera om ovädret hade medfört några skador på anläggningen, att uppstarten av produktionen måste ske på ett kontrollerat sätt samt att situationen behövde hanteras med beaktande av pandemin och gällande restriktioner. Företaget beräknade de ekonomiska konsekvenserna av ovädret och produktionsstoppet till 100 miljoner dollar.

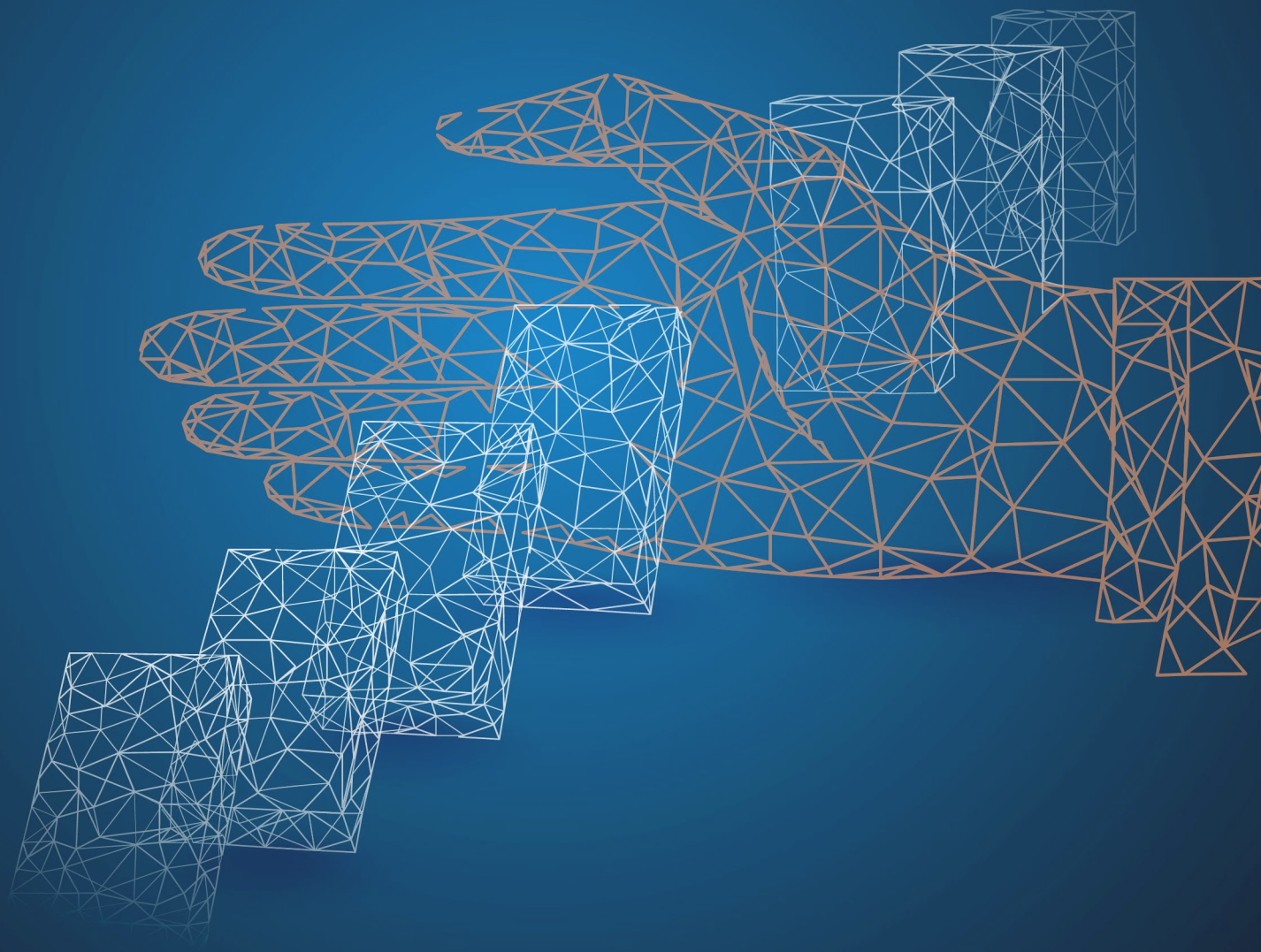
Samtidigt kräver produktionen av hårdvarukomponenter stora mängder vatten som hämtas från omgivningen. Behovet av vatten gör att produktionen är känslig för minskningar i nederbörden till vattendragen som vattnet hämtas från, men det innebär också att produktionens behov kan komma att konkurrera med andras behov av vatten.

Uteblivet monsunregn i Taiwan ledde till vattenbrist och torka – och produktionsproblem för Taiwan Semiconductor Manufacturing Company (TSMC)

Sedan 2020 har Taiwan inte haft något monsunregn – trots att landet historiskt varit en världens regnigaste platser. Torkan har tvingat regeringen att vidta strikta ransoneringsåtgärder, med följden att många verksamheter – såsom jordbruket, har fått dra ner på eller avbryta sin verksamhet.

Landet är tack vare TSMC centrum för cirka 90 procent av världens samlade produktion av vissa former av avancerade mikrochipp. Företagets behov av vatten för sin produktion är omfattande. Under 2019 konsumerade företaget 156 000 ton vatten per dygn på sina anläggningar i Taiwan. Även om stora mängder vatten kan återanvändas innebär det att signifikanta andelar av öns vattenresurser måste avdelas till TSMC om produktionen ska kunna fortgå där.

Taiwan har klassats som ett högriskområde när det gäller oönskade effekter av klimatförändringarna, och det kan därför komma att bli allt vanligare att förväntad nederbörd uteblir.



Konsekvenser för samhällssäkerheten

Konsekvenser för samhälls-säkerheten

Incidenter i organisationers informationssystem kan leda till allvarliga konsekvenser och omfattande hantering för såväl enskilda organisationer som inom och mellan stater. I det här kapitlet analyserar vi konsekvenser på de tre nivåerna som är specifika för just incidenter i digitala leveranskedjor.

Konsekvenser för NIS-leverantörer och andra organisationer

När sådant som inte ska levereras ändå levereras

De flesta organisationer använder sig idag av digitala leveranskedjor. Gemensamt för alla sådana 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. Det är vanligt att organisationer börjar använda det som de har fått levererat så fort och så brett som möjligt efter att det har inkommit. Ofta finns det en förberedd kanal in i organisationen som ska minimera tiden mellan mottagande och tillämpning. Detta gäller i synnerhet mjukvaruuppdateringar. Mottagande organisationer upprättar en sådan kanal dels när de har förtroende för den avsändande respektive (eller de) transporterande organisationen, dels när fördröjning i tillämpningen eller snäv tillämpning kan innebära att man går miste om sådana fördelar som det som har införskaffats är tänkt att generera. Om det som har levererats exempelvis innehåller kod som orsakar skada eller förhindrar nytta så kan effekterna av den koden materialiseras på flera håll samtidigt i organisationen.

När det gäller viss mjukvara som levereras genom digitala leveranskedjor, såsom säkerhetsuppdateringar av redan installerad mjukvara, är rådet som organisationer i allmänhet får att de ska genomföra installation så fort och så brett som möjligt. Skälet till det är för att organisationen som tagit fram uppdateringen har upptäckt, eller har blivit uppmärksammad på, en sårbarhet som behöver täppas till eller ett hot som behöver blockeras. Trots att det generellt är lämpligt att snabbt installera säkerhetsuppdateringar innebär det samtidigt att om skadlig kod finns i uppdateringen kan uppdateringen underminera säkerheten i vissa fall samtidigt som den höjer säkerheten i andra. Det stora

behovet av att snabbt behöva åtgärda en känd sårbarhet eller ett känt hot kombinerat med den förtroendefulla relationen mellan tillhandahållaren och mottagaren av uppdateringen gör tillhandahållare av betrodda mjukvaruuppdateringar till ett attraktivt mål för angripare. Detta gäller i synnerhet om tillhandahållaren levererar uppdateringar till flera av angriparens tilltänkta mål.

Det finns också en omvänd problematik för säkerhetsuppdateringar. Om en sådan uppdatering görs allmänt tillgänglig kan den laddas ned av vem som helst, inklusive hotaktörer. Sådana aktörer kan i vissa fall, om de har god kunskap om baklängeskonstruktion (”reverse engineering” på engelska), analysera koden i säkerhetsuppdateringen för att därigenom sluta sig till vad det är för sårbarhet som uppdateringen ska ersätta med ett skydd.[42] Därefter kan en angreppsmetod som utnyttjar sårbarheten, eventuellt i form av en programvara, skapas. Följden blir att organisationer som vill undvika att utsättas för angrepp får ett starkt tryck på sig att installera säkerhetsuppdateringen direkt, eftersom risken för att de ska utsättas för ett angrepp som utnyttjar sårbarheten som säkerhetsuppdateringen ska ersätta med ett skydd ökar i samband med att säkerhetsuppdateringen släpps.

En motsvarande utmaning gäller säkerhetsprogramvaror. För att organisationer som tillhandahåller sådana tjänster ska kunna ta fram exempelvis skydd mot nya former av skadlig kod så måste de ges tillgång att bevaka och samla information i många av de känsligaste delarna av ett informationssystem. Informationen de samlar in måste sedan skickas tillbaka till organisationen som använder den för att kunna analysera och, om det visar att skadlig kod upptäcks, ta fram ett sätt att blockera, deaktivera eller ta bort den skadliga koden. Sådana organisationer kan därmed få tillgång till känsliga och skyddsvärda system och information. Men om organisationen som tillhandahåller tjänsten i sig på eget bevåg, genom eget misstag eller genom ett angrepp läcker informationen de kommer över, eller tvingas att göra det av någon annan (såsom sin hemstat), kan en tjänst som syftar till att höja säkerheten användas för att underminera den.

Vilka konsekvenserna, i termer av konfidentialitet, riktighet och tillgänglighet, som oönskat innehåll i hård- eller mjukvara medför beror på karaktären hos det oönskade innehållet. Innehåll kan leda till direkta konsekvenser i form av:

3. **Konfidentialitet** – Obehöriga får kontroll över ett informationssystem eller att information kopieras och skickas vidare till obehöriga.
4. **Riktighet** – Informationssystem omkonfigureras så att de beter sig på andra sätt än de förväntade, informationsmängder ändras så att de förmedlar annan information eller inte går att lita på.
5. **Tillgänglighet** – Behöriga förlorar kontroll över ett informationssystem[43] eller information blir otillgänglig för behöriga.

42. En sårbarhet definieras som en avsaknad av något som förhindrar, eller bidrar till att förhindra, en incident. Ett skydd definieras som en förekomst av något som förhindrar, eller bidrar till att förhindra, en incident. Skydd ersätter därför sårbarheter. Se Bilaga Om analys av incidenter i digitala leveranskedjor för mer information om rapportens terminologi och analysmetodik.

43. Såsom under incidenten hos Västra Götalandsregionen som beskrivs tidigare i rapporten.

Innehållet kan också leda till indirekta konsekvenser när det blockerar, deaktiverar eller tar bort skydd som tidigare har förhindrat oönskade händelser varpå angrepp eller misstag kan resultera i att sådana händelser sker.[44]

Det är viktigt att notera att det sätt på vilket organisationer behandlar leveranser de har mottagit inom ramen för sina digitala leveranskedjor kan underminera en del av de skydd som de har implementerat. Organisationer kan exempelvis ha segmenterat sina interna nätverk och valt att aldrig placera all sin känsliga information i ett och samma segment av nätverket. Men, om instanser av en mjukvaruuppdatering som innehåller skadlig kod installeras samtidigt i flera eller alla av de segmenten kan respektive instans var för sig kopiera och skicka vidare känslig information som finns i respektive segment.

Många av de senaste årens mest uppmärksammade angrepp har skett genom att utnyttja de förtroendefulla relationer som digitala leveranskedjor bygger på. Eftersom behovet av effektivitet ofta innebär att organisationer behöver blotta sig mot sina leverantörer utgör det en lockande väg in i känsliga system – i synnerhet för angripare som har ett intresse av att penetrera många organisationers skydd och brottas med att organisationers generella it-säkerhet successivt utvecklas. Följderna kan i värsta fall bli mycket kostsamma. Exempelvis drog Maersk på sig kostnader på 100-tals miljoner kronor av förstörd utrustning och stora störningar i verksamheten i spåren av NotPetya. Likaså är andra utpressningsvirus något som kostar mycket för organisationer, vare sig det handlar om betalning av höga lösensummor, tillfälliga produktionsstopp eller skador på varumärket.

Kaseya-incidenten inträffade hos en leverantör till Coops leverantör av betalsystem. Visma Esscoms betaltjänst baserades på ett system som tillhandahölls av Kaseya. Det visar hur svårt det kan vara att skaffa sig en välgrundad uppfattning om hur exponerad man är. När en första organisations tjänst utgör en komponent i en annan organisations tjänst och tusentals organisationer är beroende av den andra organisationens tjänst kommer en infektion av skadlig kod i den första organisationens tjänst (som organisationerna i ledet efter den andra organisationen kanske inte ens vet om existerar) omedelbart och obehindrat att slå mot alla eller nästan alla av de organisationer som är beroende av den andra organisationen.

När sådant som ska levereras inte levereras

Digitala leveranskedjor kan delas in i fyra typer: digitala leveranskedjor för hårdvara, mjukvara, tjänster samt för information.

Den första typen av leveranskedja omfattas av alla de utmaningar som moderna logistikkedjor har. Organisationer lagerhåller i allmänhet inte hårdvara till sina informationssystem, utan förlitar sig på just in time-leveranser. I många fall är det dessutom inte meningsfullt att lagerhålla hårdvarukomponenter eftersom de riskerar att vara föråldrade och inte tillräckligt kapabla i relation till de behov som en organisation har när det blir dags att installera den lagerhållna komponenten. När det gäller den andra typen av leveranskedja har organisationer som har ett välfungerande driftsäkerhetsarbete ofta en slags lagerhållning i den bemärkelsen att man har säkerhetskopior och andra lösningar som möjliggör återställning av programvara till tidigare, och stabila, versioner. Sådana återställningsmöjligheter löser dock inte sådana problem som uppstår med anledning

44. Såsom i SolarWinds-angreppet som beskrivs tidigare i rapporten.

av incidenter i digitala leveranskedjor av den här typen eftersom det inte är nya exemplar av exakt samma mjukvara som ska levereras, utan snarare nya versioner av mjukvaran, eller helt ny mjukvara, som tillför funktionalitet eller säkerhetsfunktioner som tidigare versioner inte har haft.

Effekten av avbrott i digitala leveranskedjor för hård- eller mjukvara kan vara att organisationen som skulle ha mottagit hårdvarukomponenterna eller mjukvaran måste dra ned på eller stänga av sin produktion, sina processer eller sitt tillhandahållande av tjänster, att nya funktioner som ska upprättas inte kan upprättas, eller att inträffade incidenter vars hantering förutsätter installation av nya komponenter fortgår i stället för att kunna åtgärdas. Problemen kan bli särskilt stora om den leverans som avbryts är något som organisationen har ett monoberoende till. Organisationer som använder sig av löpande försörjning (i form av en tjänst eller informationsflöden) i realtid över digitala leveranskedjor är särskilt sårbara för detta – och samtidigt är störningar i samhällsviktiga tjänster som orsakas av incidenter i digitala leveranskedjor som löpande och i realtid levererar en tjänst eller data bland de absolut vanligaste incidenterna i incidentrapporteringen MSB mottar.

Hård- och mjukvara kan också levereras i en ofullständig form. Det kan ske genom att en hård- eller mjukvara levereras, men utan att innehålla alla de komponenter eller funktioner som de ska ha, eller utan den konfiguration som de ska ha. Följden av att implementera sådan hård- eller mjukvara kan vara att en organisation felaktigt tror att den har skydd som förhindrar att misstag och angrepp leder till sådana konsekvenser i termer av konfidentialitet, riktighet och tillgänglighet som beskrivs i det föregående avsnittet.

Effekterna av att tjänster eller information inte levereras är på många sätt liknande de som uppstår vid avbrott i leveransen av mjuk- eller hårdvara. När ett avbrott uppstår i leveransen av en tjänst försvinner den funktionalitet eller det skydd som tjänsten ska tillhandahålla. När ett informationsflöde avbryts kommer system och funktioner som behöver information som levereras via det flödet antingen inte fungera alls, eller (exempelvis) inte fungera i enlighet med de senaste instruktionerna. Om en antivirusprogramvara exempelvis inte försörjs med signaturer över hot att leta efter, kommer programvaran att fortsätta leta efter hot vars signaturer den redan har mottagit, men inte efter nya hot vars signaturer skulle ha levererats om flödet fungerade som det skulle.[45]

Viskleksproblematik och ovisshet

Eftersom en digital leveranskedja kan bestå av många organisationer i led kan det också uppstå *viskleksproblematik*. 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 skickades i väg inte är densamma som den information som når organisationer några steg längre ned i kedjan.

Sådan problematik syns återkommande i NIS-rapporteringen. Ett typexempel är att en leverantör av en samhällsviktig tjänst hyr en sensortjänst från en annan

45. Eller åtminstone hot som fungerar på sätt som inte liknar hur andra hot fungerar och som programvaran redan känner till.

organisation. Organisationen som tillhandahåller sensortjänsten (sensor-leverantören) hyr i sin tur en tjänst från en tredje organisation (dataöverförings-leverantören) för att överföra data från sina utplacerade sensorer till leverantören av den samhällsviktiga tjänsten. Dataöverföringsleverantören har i sin tur ett avtal med en fjärde organisation (infrastrukturleverantören) om att använda densammas infrastruktur. Om infrastrukturleverantören drabbas av en incident kanske den organisationen rapporterar om den incidenten till dataöverföringsleverantören. Dataöverföringsleverantören tolkar informationen som den får, varpå den skriver en egen incidentrapport som den vidarebefordrar till sensorleverantören. Incidentrapporten består av en tolkning av infrastrukturleverantörens information, samt en del tillägg om vad incidenten innebär för dataöverföringsleverantören. Viss information i infrastrukturleverantörens rapport till dataöverförings-leverantören har dessutom inte kommit med i rapporten som dataöverförings-leverantören har upprättat. När sensorleverantören mottar sin rapport från dataöverföringsleverantören inträffar samma sak igen, varpå leverantören av den samhällsviktiga tjänsten till slut får en rapport från sensorleverantören. När det sker kan informationen som leverantören av den samhällsviktiga tjänsten mottar vara radikalt annorlunda, och i värsta fall motsägande, än sådant som har förmedlats tidigare i kedjan.

Effekten av viskleksproblematiken kan leda 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. Det kan också, av samma skäl, hända att organisationer fattar dåliga beslut.

Utöver att viskleksproblematiken kan medföra att information som vidareförmedlas i flera led successivt förvanskas så är det inte heller säkert att den första aktören i kedjan nödvändigtvis delar med sig av sådan information som efterföljande aktörer behöver, i synnerhet när det gäller aktörer några led ner i kedjan. Om informationsdelningen inte är reglerad i lag eller någon annan formell systemövergripande formell bestämmelse, är den i allmänhet endast reglerad genom kontrakt mellan en aktör och dess omedelbara grannar uppströms och nedströms. I vissa fall har en aktör upprättat avtal med grannar i kedjan som innebär att de i sin tur måste ställa vissa krav på informationsdelning på sina respektive leverantörer. Men det är svårt att kravställa om att en annan aktör ska kravställa på ett sätt som gör att ytterligare krav ställs längre och längre bort i kedjan. Om aktören har behov av information från en aktör bortom dess omedelbara grannar och dess grannar inte har avtalat om att dela sådan information som aktören behöver är utsikterna att få sådan information helt beroende av välvilja mellan de inblandade.

När de digitala leveranskedjorna blir allt längre och får allt fler förgreningar blir det svårare och svårare (och till slut i praktiken omöjligt) för organisationer långt ”nedströms” att på eget initiativ få inblick i och förstå på vilka sätt de är sårbara, hur de är hotade och vilka och hur starka beroenden de har. Det är dels för att sådana undersökningar blir mer och mer resurskrävande ju mer komplexa och långa leveranskedjorna blir, dels för att aktörer som omfattas av sådana undersökningar inte nödvändigtvis är beredda att dela med sig av information.

Konsekvenser för stater

Incidenter i digitala leveranskedjor har en stor potential för negativ samhällspåverkan. Effekternas samlade verkan på samhällen beror på vad incidenten består av – installation av skadlig kod som orsakar informationsläckage får vissa konsekvenser medan avstannad produktion på grund av brist på komponenter får andra konsekvenser. Effekternas samlade verkan beror också på kontextuella faktorer, varav dessa är särskilt viktiga:

1. Hur många organisationer som använder samma digitala leveranskedja.
2. Hur många av de organisationerna som har stor betydelse för den nationella ekonomin eller enskilda regioners ekonomier.
3. Hur många av de organisationerna som tillhandahåller samhällsviktiga tjänster.
4. Hur många organisationer eller människor som i sin tur påverkas av att sådana samhällsviktiga tjänster påverkas.
5. Om organisationer och människor som påverkas av att tjänster de normalt använder har alternativ.

När sådant som inte ska levereras ändå levereras

Digitala leveranskedjor opererar ofta enligt en ”en-till-många-princip” där många instanser av en och samma produkt, såsom en mjukvaruuppdatering, skickas till eller hämtas av många organisationer på en och samma gång. Effekterna av att exempelvis skadlig kod förmedlas via digitala leveranskedjor och sedan installeras hos de mottagande organisationerna[46] kan därmed drabba många organisationer på en och samma gång. Utöver de faktorer som listas i det föregående avsnittet är alltså mängden organisationer som på kort tid brett[47] installerar mjukvara eller komponenter som har en skadlig verkan särskilt avgörande.

Många organisationer kommer i ett sådant läge potentiellt ha behov av stöd för att hantera incidenten och återställa sina system. Därför finns det också en risk att samhällets stödfunktioner, såsom CERT- och CSIRT-team, räddningstjänst, personal inom samhällsviktig verksamhet och tekniska funktioner som upprätthåller samhällsviktiga tjänster (såsom VA-tekniker, elektriker, etc.), kommer att vara hårt belastade.

När sådant som ska levereras inte levereras

Det finns två varianter av den här typen av incident i en digital leveranskedja, dels när hårdvara, mjukvara eller information inte levereras alls, dels när hårdvara, mjukvara eller information levereras i ett *ofullständigt format*.

Den första varianten kan, om den blir långvarig, innebära att nationellt eller regionalt ekonomiskt viktiga aktörer måste dra ner på eller avbryta produktion eller processer, potentiellt med neddragningar av arbetsstyrkan om en lösning på problemet inte materialiserar sig. Om en stor och centralt placerad aktör får

46. Såsom nedstängning av eller förlorad kontroll över informationssystem och tjänsterna de upprätthåller, läckage av information etc.

47. D.v.s. i många system eller nätverkssegment.

avbrott i exempelvis försörjningen av halvledare, varpå produktionen först dras ned och sen avstannar kommer den aktören inte ha behov av komponenter från andra leverantörer förrän produktionen kommer igång igen. Ett avbrott i en leveranskedja kan därför medföra att en mottagande aktör måste avbryta leveranser från andra kedjor. Ofta har stora, centrala aktörer ett regionalt kluster av underleverantörer som försörjer aktören med komponenter och tjänster. Aktörens behov av att dra ned på leveranserna kan därför generera en negativ kaskadeffekt som slår brett i en region. Följden kan bli minskade skatteintäkter och ökade sociala utgifter för att hantera en växande arbetslöshet.

Den andra varianten kan innebära att en hård- eller mjukvara saknar funktionalitet som den ska ha, eller att den saknar skydd som den ska ha. När sådan hård- eller mjukvara installeras och används kan problem uppstå när förväntade funktioner eller effekter visar sig saknas eller inte uppstå. Ett annat problem kan vara att många organisationer installerar något som saknar skydd, varpå de blir sårbara för angrepp eller misstag som de inte förväntar sig ska kunna vara skadliga för dem. Vid exempelvis mjukvaruuppdateringar installerar många organisationer samma uppdateringar ungefär samtidigt, varpå många blir sårbara på samma sätt. Det är viktigt att notera att konsekvenserna av att sårbarheter eller hot uppstår i system i samband med exempelvis uppdateringar inte nödvändigtvis måste efterföljas av misstag eller angrepp som leder till omfattande oönskade effekter. I vissa fall kan det saknade skyddet adderas, eller det identifierade hotet tas bort eller blockeras, innan något annat händer. Men om ett misstag eller ett angrepp sker och skyddet som saknades inte har lagts till eller hotet som introducerades inte har tagits bort eller blockerats kan följderna bli desamma som de som beskrivs i tidigare avsnitt, det kan alltså uppstå allvarliga konsekvenser, höga kostnader och stora påfrestningar på olika stödfunktioner i samband med incidenthanteringen.

Monoberoenden

En organisation har ett monoberoende av (exempelvis) en tjänst när den är beroende av den tjänsten och det inte finns några alternativa tjänster att använda ifall den tjänst man redan använder upphör.

I vissa fall kan staters egna policyer och lagar leda till att incidenter bli värre än vad de hade behövt vara, det gällde exempelvis vid NotPetya-incidenten. Genom att tvinga organisationer att använda en viss typ av programvara (i NotPetya-fallet för skatteredovisning och liknande) istället för att tillåta organisationer att välja bland ett utbud av olika programvaror som uppfyller samma funktion ökar man sannolikheten för att många ska drabbas av skada på en och samma gång när det uppstår en incident i den programvarans digitala leveranskedja. Den omständigheten innebär också att antagonisters incitament att använda den digitala leveranskedjan för att genomföra angrepp stärks.

När något som inte ska levereras ändå levereras inom ramen för ett monoberoende som många är bundna till, såsom i NotPetya-fallet, innebär det att omfattande skador kan uppkomma inom många organisationer på en och samma gång. Om monoberoendet, återigen som i NotPetya-fallet, är koncentrerat till organisationer i eller med koppling till en viss stat, kan den staten drabbas av många, samtidiga och allvarliga konsekvenser.

När sådant som ska levereras inte levereras alls inom ramen för ett monoberoende finns det ingen möjlighet att undvika avbrott i produktion eller processer, återställa en incident eller utveckla en funktion genom att använda sig av en alternativ lösning. Medan monoberoenden som inte är påtvingade genom lagstiftning eller liknande innebär att organisationer är fria att undersöka om det finns sätt att hantera avbrott i leveranserna genom mer omfattande omställningar, kan påtvingade monoberoenden innebära att organisationer inte har något annat val än att invänta att avbrottet i leveransen ska vara över. Om avbrottet blir långvarigt kan de behöva dra ner på sin egen verksamhet, vilket kan medföra arbetslöshet och andra utmaningar.

Konsekvenser på internationell nivå

Digitala leveranskedjor är ofta globala och involverar leveranser över många landsgränser. Organisationers beroenden av leveranser från organisationer i andra stater gör dem sårbara, i synnerhet när beroendet är ett monoberoende.

Särskilt betydelsefulla beroenden kan få geopolitiska återverkningar. Om en stat ser att organisationer inom dess gränser som upprätthåller samhällsviktig verksamhet eller har stor betydelse för den nationella ekonomin själva är beroende av digitala leveranskedjor från en eller flera organisationer i en annan stat kan det påverka den statens relation till den andra staten. Om staten får indikationer på att leveranserna är osäkra, eller att det som levereras genom de digitala leveranskedjorna på grund av misstag eller angrepp kan komma att medföra hot eller sårbarheter, eller skada, kan det påverka hur staten ser på sin relation till den andra staten. Om den andra staten dessutom inte önskar samarbeta kring att stärka säkerheten, eller om den första staten misstänker att den andra staten kan komma att använda beroendeförhållandet för att vinna otillbörliga fördelar, kan det också påverka hur staten ser på sin relation till den andra staten.

Ett exempel på sådana geopolitiska återverkningar är när USA utestängde säkerhetsföretaget Kasperskys produkter från amerikanska myndigheter och försvarsindustriella organisationer efter att företaget hade pekats ut som en möjliggörare av spionage för ryska myndigheters räkning. Ett annat exempel finns inom 5G-området där företag som kinesiska Huawei och ZTE har utestängts från uppbyggnaden av 5G-nät i vissa länder. Anledningen har varit farhågor om att bolagen bistår Kina i landets underrättelseverksamhet[48] eller att de skulle kunna hota med att stoppa den nödvändiga försörjningen av nya komponenter för underhåll eller utveckling av sådana nät[49] om staten där nätet finns, eller organisationer som är verksamma där, agerar på sätt som Kina har invändningar emot.

Många länder betraktar nyckelkomponenterna i digitala leveranskedjor, som halvledare och mikrochipp, som strategiska resurser. När misstro kring säkerheten i leveransen av sådana resurser ifrån andra stater uppstår kan stater och sammanslutningar av stater vidta åtgärder för att bryta beroendet av leveranser från stater vars intentioner man misstror. När brist på halvledare och mikrochipp

48. Exempelvis i form av att komponenter som bolagen tillhandahåller skulle kunna innehålla kod eller delkomponenter som läser av och skickar vidare kommunikationer som passerar genom 5G-näten (ett exempel på när något som inte ska levereras ändå levereras) eller att sådana komponenter avsiktligen saknar skydd mot vissa typer av angrepp, varpå de angreppstyperna sedan kan användas för att få åtkomst till näten när de väl är upprättade (ett exempel på när något som ska levereras inte levereras).

49. Ett exempel på när något som ska levereras inte levereras.

uppstod 2020 och 2021 ledde det till breda diskussioner i bland annat EU och USA om behovet av att trygga en inhemsk produktion. USA:s president ville se statliga investeringar om 50 miljarder dollar och uttalade att ”Kina och resten av världen väntar inte”[50], medan EU:s industrikommissionär kallade unionens hållning för ”alldeles för naiv och öppen” och menade att den egna chipproduktionen behövde fördubblas. En viktig ambition med EU:s policy på området är att få till stånd mer innovation och forskning för att långsiktigt stärka EU:s egen förmåga att tillhandahålla de tjänster och produkter som efterfrågas och behövs. Forskningsmedel ska användas för att utveckla teknik och tjänster som behövs för en säker digitalisering men också för att försvara sig mot de risker och hot man ser. I mars 2021 presenterade EU-kommissionen även ett antal digitaliseringsmål till 2030, ett av dessa var att tillverkningen av halvledare inom Europa ska stå för en femtedel av den globala produktionen.

För att kunna ligga i framkant och bryta beroendet av leveranser från stater som man misstror krävs mycket stora investeringar. Samtidigt har marknadsutvecklingen när det gäller produktion av exempelvis halvledare snarare inneburit att allt färre tillverkare klarar sig i konkurrensen. Strategiska val inom sådana industrier får återverkningar under många år, och om man satsar på fel saker kanske man inte kan återta en ledande position när andra aktörer som har gjort andra val vinner fördelar. Stora investeringar i uppbyggnaden av industrier som syftar till att minska beroendet av globala digitala leveranskedjor är därmed mycket riskabla, och leder inte nödvändigtvis till industrier som klarar sig på egen hand i konkurrensen.

Därutöver kan man särskilt rikta fokus mot de politiska konsekvenserna när en stat, eller en aktör i en stat, misstänks eller bekräftas ha genomfört ett angrepp mot en digital leveranskedja som drabbar en annan stat.[51] Om den stat som misstänks ha genomfört, eller misstänks husera de som har genomfört, angreppet dessutom varken erkänner angreppet eller bidrar till att lösa incidenten eller dess orsaker kan det få stora konsekvenser för relationerna mellan staterna. Ytterst skulle den drabbade staten eller staterna kunna se händelsen som en krigshandling.

50. Vita huset, 12 april 2021, *Remarks by President Biden at a Virtual CEO Summit on Semiconductor and Supply Chain Resilience*, länk: https://www.whitehouse.gov/briefing-room/speeches-remarks/2021/04/12/remarks-by-president-biden-at-a-virtual-ceo-summit-on-semiconductor-and-supply-chain-resilience/ (hämtad 2021-07-16) och Vita huset, 31 mars 2021, *fact sheet: The American Jobs Plan*, länk: https://www.whitehouse.gov/briefing-room/statements-releases/2021/03/31/fact-sheet-the-american-jobs-plan/ (hämtad 2021-07-16).

51. Exempelvis som i fallet med angreppet mot SolarWinds leveranskedja.

Om analys av incidenter i digitala leveranskedjor

Bilaga 1: Om analys av incidenter i digitala leveranskedjor

För att läsaren dels ska kunna följa hur vi övergripande har analyserat hot, sårbarheter, risker och incidenter med koppling till digitala leveranskedjor i arbetet med denna rapport, och för att läsaren själva ska kunna göra egna analyser, presenterar vi här det ramverk som vi har använt.

Analysen tar sin utgångspunkt i en stringent tillämpning av följande begrepp:

Ramverkets begrepp	
Incident: En inträffad oönskad händelse	**Risk:** En möjlig oönskad händelse
Framgång: En inträffad önskad händelse	**Chans:** En möjlig önskad händelse
Hot: Något som orsakar, eller bidrar till att orsaka, en incident	**Sårbarhet:** Avsaknad av något som förhindrar, eller bidrar till att förhindra, en incident
Hinder: Något som förhindrar, eller bidrar till att förhindra, en framgång	**Brist:** Avsaknad av något som orsakar, eller bidrar till att orsaka, en framgång
Framgångsfaktor: Något som orsakar, eller bidrar till att orsaka, en framgång	**Möjlighet:** Avsaknad av något som förhindrar, eller bidrar till att förhindra, en framgång
Skydd: Något som förhindrar, eller bidrar till att förhindra, en incident	**Frihet:** Avsaknad av något som orsakar, eller bidrar till att orsaka, en incident

Begreppen kan kombineras för att fördjupa en analys. Exempelvis kan det som gör att en inträffad händelse räknas som en incident vara att ett hot eller ett hinder uppstår, att en framgångsfaktor eller ett skydd upphör (det vill säga att en brist eller en sårbarhet ”uppstår”).[52] På motsvarande sätt kan det som gör att en inträffad händelse räknas som en framgång vara att ett hot eller ett hinder upphör (det vill säga att en möjlighet eller en frihet ”uppstår”), eller att en framgångsfaktor eller ett skydd uppstår.

52. I den mån en avsaknad av något kan sägas kunna uppstå.

Med incident i digital leveranskedja menar vi:

1. En händelse där något som:
    a. ska levereras i den digitala leveranskedjan (en framgångsfaktor eller ett skydd) inte levereras, eller
    b. inte ska levereras i den digitala leveranskedjan (ett hot eller ett hinder) ändå levereras, och
2. Där händelsen resulterar i antingen en oplanerad negativ påverkan[53] eller en oönskad avsaknad av positiv påverkan[54] på informationssystems, eller informationen i informationssystems, konfidentialitet, riktighet eller tillgänglighet.

En incident i en digital leveranskedja av den första typen kan bestå i att en framgångsfaktor eller ett skydd (såsom en ny programvarufunktion eller antivirussignatur i en uppdatering) inte levereras eller levereras utan att fungera som de ska. En incident av den andra typen kan i stället bestå i att ett hot eller ett hinder (såsom ett virus som döljer sig i en programvaruuppdatering eller en begränsande konfiguration i en komponent) levereras trots att de inte ska levereras.

Med hot i mjuk- och hårdvara avses här kod, konfigurationer, komponenter eller annat som finns i mjuk- eller hårdvara och som orsakar, eller bidrar till att orsaka, incidenter. Med sårbarheter i mjuk- och hårdvara menas kod, konfigurationer, komponenter eller annat som saknas i mjuk- eller hårdvara och som hade kunnat förhindra, eller hade kunnat bidra till att förhindra, incidenter.

MSB delar in orsaker till incidenter i tre huvudsakliga kategorier: mänskligt agerande, tekniska fel eller systemfel och naturhändelser. Mänskligt agerande kan genomföras i antagonistiskt syfte, det vill säga ett angrepp. Mänskligt agerande kan även ske i olika icke-antagonistiska syften. Det kan röra sig om misstag[55], men det kan också röra sig om medvetna handlingar som utförs med andra motiv än att orsaka en incident. Handlingar som inte är misstag, men som inte heller begås med antagonistiska uppsåt, kan exempelvis handla om att agera medvetet utifrån ett egenintresse, trots att det medför oönskade konsekvenser (för andra).

Utifrån definitionerna och de olika sätt som mänskligt handlade kan resultera i incidenter i digitala leveranskedjor, kan det nedanstående ramverket användas för att analysera leveranskedjerisker.

53. Såsom när skadlig kod installeras i ett informationssystem p.g.a. av en mjukvaruuppdatering som skickats ut inom ramen för en digital leveranskedja.

54. Såsom när en ny komponent som behövs för att reparera ett trasigt informationssystem inte levereras trots att det är beställt.

55. Misstag kan begås hos en leverantör under programmeringen av en mjukvara, i konfigurationen eller uppdateringen av en tjänst eller informationssystem eller när en fysisk it-komponent ska installeras. Denna typ av misstag får antas vara den vanligaste orsaken till att *hot och sårbarheter* finns i dagens mjuk- och hårdvara.

Angrepp och ingrepp i digitala leveranskedjor

Anta att det finns en sändarorganisation **S** som levererar en digital produkt **P** (**P** kan vara olika slags hårdvarukomponenter, mjukvaruuppdateringar, kodbibliotek, data, etc.) till en mottagarorganisation **M**. Anta också att det finns en aktör **A** (**A** kan vara sändarorganisationen **S**, någon anställd på **S**, någon annan organisation, etc.).

A begår ett lyckat angrepp på en digital leveranskedja om…	**A begår ett misslyckat ingrepp på en digital leveranskedja (ett misstag) om…**
(1) **A** gör något med **P** eller med infrastrukturen som används för att föra över **P** från **S** till **M**,	(1) **A** gör något med **P** eller med infrastrukturen som används för att föra över **P** från **S** till **M**,
(2) **A** inte har rätt att göra det **A** gör med **P**,	(2) **A** har eller inte har rätt att göra det **A** gör med **P**,
(3) **A** gör det **A** gör med **P** i ett antagonistiskt syfte,	(3) **A** gör det **A** gör med **P** i ett icke-antagonistiskt syfte,
(4) Det uppstår en incident i **P**:s digitala leveranskedja i form av att något som inte ska levereras ändå levereras (ett hot eller ett hinder), *eller* något som ska levereras inte levereras (en framgångsfaktor eller ett skydd), och så attkonfidentialiteten, riktigheten eller tillgängligheten i **M**:s informationssystem, eller i information i **M**:s informationssystem, påverkas negativt, *eller* en positiv påverkan på konfidentialiteten, riktigheten eller tillgängligheten i **M**:s informationssystem, eller information i **M**:s informationssystem, som annars skulle ha inträffat uteblir[56], *eller* informationssystem eller information i informationssystem som annars skulle ha upprättats inte upprättas.	(4) Det uppstår en incident i **P**:s digitala leveranskedja i form av att något som inte ska levereras ändå levereras (ett hot eller ett hinder), *eller* något som ska levereras inte levereras (en framgångsfaktor eller ett skydd), och så att konfidentialiteten, riktigheten eller tillgängligheten i **M**:s informationssystem, *eller* i information i **M**:s informationssystem, påverkas negativt, eller en positiv påverkan på konfidentialiteten, riktigheten eller tillgängligheten i **M**:s informationssystem, eller information i **M**:s informationssystem, som annars skulle ha inträffat uteblir, *eller* informationssystem eller information i informationssystem som annars skulle ha upprättats inte upprättas.
(5) **A** uppnår sådana, och endast sådana, effekter som var syftet med det som **A** gjorde med **P** eller med infrastrukturen som används för att föra över **P** från **S** till **M**. (Det är detta villkor som gör angreppet ”lyckat”)	(5) **A** inte uppnår sådana effekter, eller uppnår andra effekter, än de som var syftet med det som **A** gjorde med **P** eller med infrastrukturen som används för att föra över **P från S** till **M.** (Det är detta villkor som ingreppet ”misslyckat”)

Utöver de två möjligheter som behandlas i tabellen kan naturligtvis även misslyckade angrepp och lyckade ingrepp ske, och båda kan resultera i incidenter.

Se kapitlet hot mot digitala leveranskedjor nedan för några exempel på hur några samtida och uppmärksammade incidenter kan förstås med stöd av modellen.

56. Det här villkoret handlar om att ingrepp eller ett angrepp istället resulterar i en incident där någon eller några av tillstånden som beskrivs i de kommande tabellerna Påverkan på informationssystem och Påverkan på information i informationssystem inte kan åtgärdas, eller där ny funktionalitet i termer av konfidentialitet, riktighet eller tillgänglighet inte kan upprättas.

Om ett ingrepp eller ett angrepp resulterar i en incident av typen (4.1) kan det som gör händelsen till en incident bestå i påverkan på informationssystems, eller information i informationssystems, befintliga konfidentialitet, riktighet eller tillgänglighet. Exempel på sådan påverkan (det vill säga omständigheter som uppstår på grund av incidenten) finns i de två följande tabellerna:

Påverkan på informationssystem		
Konfidentialitet	Riktighet	Tillgänglighet
Behöriga användare har fått för höga behörigheter till informationssystem	Konfigurationer har lagts till i informationssystem	Behöriga användare har fått för låga behörigheter till informationssystem
Tillgång för obehöriga kan upprättas till informationssystem	Konfigurationer har ändrats i informationssystem	Tillgång för behöriga användare kan inte upprättas till informationssystem
Obehöriga har tillgång till informationssystem	Konfigurationer har tagits bort i informationssystem	Avbrott har uppstått i behöriga användares befintliga tillgång till informationssystem
Information kan tas emot från obehöriga användare i informationssystem	Konfigurationer i informationssystem har gjorts otillförlitliga	Information kan inte tas emot från behöriga användare i informationssystem
Information från obehöriga användare kan behandlas i informationssystem	Informationssystemet utför inte uppgifter det ska utföra	Information från behöriga användare kan inte behandlas i informationssystem
Information från obehöriga användare kan skickas i informationssystem	Informationssystemet utför uppgifter det inte ska utföra	Information från behöriga användare kan inte skickas i informationssystem
Uppgifter utförs på obehörigas begäran i informationssystem	Informationssystemet utför inte uppgifter det är konfigurerat att utföra	Uppgifter utförs inte på behöriga användares begäran i informationssystem
Informationssystemet kan konfigureras av obehöriga användare	Informationssystemet utför uppgifter det inte är konfigurerat att utföra	Informationssystemet kan inte konfigureras av behöriga användare

Påverkan på information i informationssystemen		
Konfidentialitet	Riktighet	Tillgänglighet
Behöriga användare har fått för höga behörigheter till informationstillgångar	Information har lagts till i informationstillgångar	Behöriga användare har fått för låga behörigheter till informationstillgångar
Tillgång för obehöriga kan upprättas till informationstillgångar	Information har ändrats i informationstillgångar	Tillgång för behöriga användare kan inte upprättas till informationstillgångar
Obehöriga har tillgång till informationstillgångar	Information har tagits bort i informationstillgångar	Avbrott har uppstått i behöriga användares befintliga tillgång till informationstillgångar
Konfidentialiteten har påverkats negativt på annat sätt	Information har gjorts otillförlitlig i informationstillgångar	Tillgängligheten har påverkats negativt på annat sätt
	Riktigheten har påverkats negativt på annat sätt	

Ett samarbete mellan:

Myndigheten för samhällsskydd och beredskap

Medfinansierat av Europeiska unionens fond för ett sammanlänkat Europa

651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Publ.nr MSB1855 – november 2021 ISBN 978-91-7927-194-7