Enheten för strategi och samordning (CS-ST)
Denim Nygren
Isaac Mintz

Regeringskansliet
Finansdepartementet
103 33 Stockholm

Svar på frågor om dagens och framtidens utmaningar på konnektivitetsområdet

Robusthet och säkerhet

Med dagens samhällsutveckling har den digitala infrastrukturen blivit en samhällskritisk infrastruktur. För att samhället ska fungera utan allvarliga störningar ökar behovet av att stärka robusthet och säkerhet för infrastrukturen. Det försämrade säkerhetspolitiska läget har ytterligare ökat vikten av en säker och robust infrastruktur. Beskriv önskad målbild för att uppnå en robustare och säkrare digital infrastruktur. Vilka risker ser ni i dagsläget? Vad skulle krävas för att nå målbilden? (Fi2023/01693).

Robusthet, resiliens och redundans

MSB instämmer att det finns ett ökat behov av att stärka robusthet och säkerhet för den digitala infrastrukturen. Samhällskritisk infrastruktur måste vara rustad att stå emot faktorer som kan leda till allvarliga störningar. Det uppnås bland annat genom systematiskt informations- och cybersäkerhetsarbete. Utöver förmågan att motstå hot (d.v.s. robusthet), är förmågan till (snabb) återhämtning efter en incident avgörande (resiliens). Ytterligare är redundans, d.v.s. tillgång till flera av varandra oberoende (kritiska) tjänster av samma typ (såsom tjänster för internetåtkomst) centralt. Organisationer som har redundanta kritiska tjänster har alternativ att ta till när deras vanliga, primära, lösning fallerar och blir därför inte nödvändigtvis beroende av att alltid kunna motstå hot (robusthet) eller snabb återställning (resiliens). För att öka den tekniska redundansen är det också viktigt att säkerställa möjligheten till olika uppkopplingsalternativ, till exempel genom satellituppkoppling. Kombinationen av robusthet, resiliens och redundans säkerställer tillhandahållandet av samhällsviktiga tjänster och är grundläggande för ett tryggt samhälle.

Samtidigt är det viktigt att komma ihåg att ökade krav på robusthet och resiliens för aktörer som levererar digital infrastruktur kan bli dyrt, med följden att färre aktörer har resurser för att verka på marknaden. Krav på robusthet, resiliens och redundans hos enskilda aktörer kan därför resultera i lägre redundans på samhällsnivå. Det är därför viktigt att ha en bra balans – det är aldrig önskvärt att samhället hamnar i ett läge där ett bortfall av en enskild organisations tjänst innebär att det inte finns *någon* tjänst av den typen att använda sig av överhuvudtaget.

För att bygga ett robust, resilient och redundant samhälle gäller det att bryta monoberoenden, se till allriskperspektivet, och integrera ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete på samtliga nivåer inom samhällsviktig verksamhet.

Samhällsviktiga aktörers behov av robusta, resilienta och redundanta digitala tjänster

Digitaliseringen av samhället ställer allt högre krav på att samhällsviktiga aktörer utvecklar sina tjänster och har tillgång till pålitlig och säker konnektivitet, både i områden där människor vistas och vid olyckshändelser. MSB och regeringen har under många år arbetat med att adressera behoven av säkra och robusta bredbandstjänster för samhällsviktiga aktörer. Genom initiativ som Rakel Generation 2 och SGSI utvecklar MSB och Trafikverket nya moderna tjänster för dessa aktörer. Myndigheternas utveckling av tjänster och tillhörande infrastruktur, där staten har omfattande inflytande, öppnar även dörren för kommersiella och offentliga aktörer att etablera tillhandahålla egna pålitliga tjänster.

Risker

De incidentrapporter som inkommer till MSB visar att de flesta it-incidenter påverkar informations och informationssystems tillgänglighet. Vilka konsekvenser detta medför varierar beroende på vilken typ av system eller information som berörs, vilken typ av störning som påverkar systemet, samt dess varaktighet. Samhällskonsekvenserna vid dessa typer av incidenter har i de allra flesta fall varit begränsad. Då det ofta finns flera aktörer som erbjuder samma tjänst, kan det digitala samhället anses vara delvis redundant. Trots detta finns det situationer där en it-incident, även om Sverige har en generellt redundant infrastruktur, kan få omfattande konsekvenser på samhällsnivå. Exempel på detta kan vara när en samhällsviktig tjänst är beroende av en enskild aktörs verksamhet, eller när fler leverantörer av en samhällsviktig tjänst är sårbara för samma typ av hot.

Mellan början av 2020 och juni 2021 har två tredjedelar av alla inrapporterade it-incidenter haft sitt ursprung i en leveranskedja. En orsak till detta kan vara att organisationer i större utsträckning fokuserar på sin mest centrala verksamhet och utkontrakterar de funktioner som inte hör till kärnverksamheten, till andra organisationer. Många organisationer väljer även att avgränsa sin egen specifika nisch i värdekedjan, vilket ytterligare gör deras produkter mer särpräglade. Detta medför ett utökat beroende till underleverantörer, som i sin tur har ett utökat beroende till ytterligare underleverantörer. Organisationer som är beroende av särpräglade produkter eller tjänster som erbjuds av endast en, eller ett fåtal, organisationer har ett så kallat monoberoende.

Antalet monoberoenden verkar öka över tid, vilket medför två växande risker. Den första är att avbrott i leveranserna av en viss digital produkt leder till avstannad verksamhet hos allt fler. Med det följer en ytterligare risk där behovet av att fort installera, aktivera eller använda den digitala produkt som levereras, undviker att testa och granska leveransen för att slippa förlora tid. Risken 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.[1]

Samhället är idag beroende av en kontinuerlig leverans av varor och tjänster. De digitala leveranskedjorna är således en ytterligare faktor att beakta vid skydd av samhällskritiska verksamheter och informationssystem. Incidentrapporteringen som kommer in till MSB visar att incidenter i digitala leveranskedjor är mycket vanliga. Av dessa incidenter är den

[1] Hoten mot de digitala leveranskedjorna - 50 rekommendationer för att stärka samhällssäkerheten

stora majoriteten orsakade av misstag och systemfel (icke-antagonistiska hot). Dessa incidenter kan leda till konsekvenser som är minst lika allvarliga som de som följer av angrepp. Denna utmaning behöver hanteras utifrån allriskperspektivet på organisationsnivå, den nationella nivån och den internationella nivån.

Lösning

Samhället måste bryta monoberoenden där det är möjligt och hitta sätt att hantera nya problem och utmaningar utan att upprätta nya, eller befästa befintliga, monoberoenden. Ytterligare är det väsentligt att bygga in mer säkerhet i de digitala leveranskedjorna så att den destruktiva potentialen de medför minskar. Det är även gynnsamt att stärka informationsdelningen mellan de ingående organisationerna i en digital leveranskedja så att incidenter kan hanteras mer samordnat och effektivt.

För att skapa robusta och säkra organisationer krävs det att hela organisationen bedriver ett systematiskt och riskbaserat informations- och cybersäkerhetsarbete. Det skapar möjlighet att fatta välgrundade beslut om tekniska, organisatoriska och personella säkerhetsåtgärder. Organisationen behöver således klargöra ansvarsförhållanden, identifiera tillgångar, värdera information och informationssystem, samt bedöma riskerna vad gäller tillgänglighet, riktighet och konfidentialitet. Det kommer möjliggöra att mer effektivt och etablerat kunna bedöma och prioritera vilka säkerhetsåtgärder som bör införas för att säkerställa ett ändamålsenligt skydd.

Organisationernas redundans kan ökas ytterligare genom att säkerställa fler uppkopplingsalternativ, till exempel att nyttja satelliter för konnektivitet i enlighet med de satsningar som följer av EU-initiativ som exempelvis Govsatcom. Govsatcom är ett EU-initiativ som ska förse samhällsviktig verksamhet med robust och säker satellituppkoppling och kan vara en viktig pusselbit för att bygga redundanta konnektivitetslösningar som inte är beroende av privata aktörer utanför EU.

Idag omfattas långt ifrån alla samhällsviktiga aktörer av uttryckliga krav på att bedriva ett systematiskt informations- och cybersäkerhetsarbete för all sin information i den samhällsviktiga verksamheten. Därutöver behöver fler samhällsviktiga verksamheter omfattas av krav på att rapportera it-incidenter, för att därigenom bidra till en samlad bild över läget och utifrån den bilden generera riktade åtgärder mot de vanligaste förekommande problemen. Staten behöver kunna lägga resurser på att centralt hantera problem som påverkar många, så att inte alla problem måste hanteras av varje enskild organisation.

Dagens regelverk ger begränsat med styrning avseende hur samhällsviktig verksamhet säkerställer robusthet, resiliens och redundans för att upprätthålla nödvändiga samhällsfunktioner.[2] Privata och offentliga aktörer har ett behov av att veta vilka krav som ska uppfyllas för att driva samhällsviktig verksamhet. Införandet av NIS2-direktivet, samt ytterligare EU-lagstiftning på informations- och cybersäkerhetsområdet, kommer att möta en del av de utmaningar som samhället står inför. Samtidigt finns det en risk för att den stora mängd reglering som nu är på väg att införas leder till just den typ av effekt som

[2] När kriget kom nära : årsrapport it-incidentrapportering 2022

beskrivs ovan, d.v.s. att organisationer på olika marknader blir säkrare, men att antalet organisationer som kan verka på marknaden minskar. För att upprätthålla, och samtidigt öka, redundansen i samhället är en välavvägd balans väsentlig. Att skapa sig en bild av samhällets sårbarheter, på en teknisk, organisatorisk, personell och samhällelig nivå är en viktig pusselbit för att rätt krav ställs på rätt plats.

Ett exempel på bristande reglering som påverkar samhället är krav på täckning i exempelvis glesbygdsområden. Ökade krav kan förbättra täckningen och därmed tillgängligheten och konnektiviteten i dessa områden.

En annan åtgärd är MSB och Trafikverkets nu pågående planerings- och förberedandeuppdrag för etablering av Rakel G2, för ett statligt kontrollerat radionät för verksamheter inom allmän ordning, säkerhet, hälsa och försvar. Uppdraget innehåller omfattande investeringar i fysisk infrastruktur. Myndigheterna har i svar till regeringen föreslagit att den nya infrastruktur som etableras kan merutnyttjas av andra aktörer, såsom mobiloperatörer. Operatörerna kan inplacera sin utrustning i master, nyttja elförsörjningen och transmissionsinfrastrukturen (kanalisation) som etableras av myndigheterna. Sådana inplaceringar kan då bidra till en ökad bredbandstäckning i bland annat glesbygd.