It när de externa anslutningarna går ner

Konsekvenser och reservalternativ i offentliga verksamheter

Henrik Karlzén

FOI-R--5260--SE

Februari 2022

FOI

Henrik Karlzén

It när de externa anslutningarna går ner

Konsekvenser och reservalternativ i offentliga verksamheter

Titel	It när de externa anslutningarna går ner – Konsekvenser och reservalternativ i offentliga verksamheter
Title	IT when the external connections go down – Consequences and backup options in public organisations
Rapportnr	FOI-R--5260--SE
Månad	Februari
Utgivningsår	2022
Antal sidor	27
ISSN	1650-1942
Uppdragsgivare	Justitiedepartementet
Forskningsområde	Krisberedskap och civilt försvar
FoT-område	Inget FoT-område
Projektnr	A1211807
Godkänd av	Malek Finn Khan
Ansvarig avdelning	Försvarsanalys

Sammanfattning

Offentliga organisationers datornätverk står inför många hot. Hoten inkluderar allt från att den fysiska kommunikationslänken skadas till att slutanvändares datorer tas över av angripare. Om hoten realiseras kan det leda till att nätverksanslutningarna går ner. Rapporten beskriver vad sådan otillgänglighet skulle få för konsekvenser. De exakta konsekvenserna beror på den specifika organisationen, men i allmänhet är it-beroendet stort och säkerheten låg vilket gör konsekvenserna stora. De möjliga konsekvenserna exemplifieras med skildringar av inträffade incidenter.

Rapporten beskriver hur konsekvenserna kan minskas genom användning av reservalternativ till det ordinarie nätverket. Reservalternativen kan skötas internt i en organisation eller i samordning med andra organisationer. Vilka reservalternativ som passar bäst för en organisation beror på den specifika verksamheten. Oavsett valet av reservalternativ är det svårt att nå funktionell likhet med ordinarie nätverk utan att också drabbas av likartade hot. Därtill ökar betydelsen för rätt reservalternativ med teknikberoendet i samhället. Å andra sidan möjliggör den tekniska utvecklingen också nya lösningar och därmed ökad motståndskraft.

Nyckelord: datornätverk, anslutning, tillgänglighet, otillgänglighet, reservalternativ, redundans, konsekvenser, resiliens

Summary

Public organisations' computer networks face many threats. The threats include everything from damage to the physical communications link, to the compromise of end users' computers. If the threats are realised, they can lead to the network connections going down. This report describes the consequences of such unavailability. The exact consequences depend on the specific organisation, but in general, the IT dependence is large, and the security level low, making the consequences high. The possible consequences are exemplified by depictions of real incidents.

The report describes how the consequences can be reduced, by using backup options to the regular network. The backup options include both internal efforts, and coordination with other organisations. Which backup options are best suited for an organisation depends on the specific business of the organisation. Regardless of the choice of backup options, it is difficult to achieve functional equivalence with ordinary networks without also suffering similar threats. In addition, the importance of the right backup option increases with the technological dependence in society. On the other hand, the technological development also enables new solutions, thus increasing the resilience.

Keywords: computer networks, connection, availability, unavailability, backup options, redundancy, consequences, resilience

Innehållsförteckning

1 Inledning

Offentliga organisationers datornätverk står inför många hot. Hoten inkluderar allt från att den fysiska kommunikationslänken skadas till att slutanvändares datorer tas över av angripare. Om hoten realiseras kan det bland annat leda till att nätverksanslutningarna går ner. Den här rapporten undersöker vad sådan otillgänglighet skulle kunna få för konsekvenser och hur konsekvenserna kan minskas.[1]

Rapporten har tagits fram inom ramen för anslagsposten *Säkerhets- och försvarspolitisk forskning och analys (SOFFA)*, på uppdrag av Justitiedepartementet.

1.1 Syfte och forskningsfrågor

Rapporten syftar till att ge krisberedskapsstöd till verksamhetsrepresentanter och it-ansvariga vid offentliga organisationer. Mer specifikt är syftet att ge en introduktion till vilka konsekvenser som kan uppstå när en organisations externa it-anslutning går ner samt hur konsekvenserna kan minskas. För att sätta konsekvenserna i ett sammanhang ger rapporten också en bakgrund som talar om hur datornätverk typiskt fungerar och vilka hot nätverken står inför. Hoten som beskrivs är sådana vars realisering skulle ge upphov till de konsekvenser som är rapportens primära fokus. Hur sannolikt det är att hoten realiseras ligger däremot utanför ramen för denna rapport.

Rapporten undersöker följande forskningsfrågor:

1. *Vad blir konsekvenserna när den externa it-anslutningen går ner?*
2. *Hur kan konsekvenserna minskas?*

De konsekvenser som avses är i första hand de som påverkar själva it-systemen och nätverken. I andra hand inkluderas även indirekta konsekvenser som rör it-nära verksamhetsdelar. Det ligger dock utanför ramen för denna rapport att undersöka alla möjliga konsekvenser för alla typer av verksamheter eller alla möjliga sätt att undvika konsekvenserna. Rapportens svar på forskningsfrågorna ska därför inte ses som fullständiga utan som allmänt introducerande och exemplifierande. Specifika bedömningar av konsekvenser och möjligheterna att minska konsekvenserna måste göras av varje verksamhet för sig. Sådana specifika bedömningar kan stödjas av den här rapporten. Ytterligare stöd ges

[1] Ofta fokuserar informationssäkerhet och it-säkerhet istället på hot mot informations *konfidentialitet*, eller i vissa fall informations och datornätverks *riktighet*. Tillsammans med *tillgänglighet* brukar de tre säkerhetsegenskaperna sammanfattas som CIA-triaden efter engelskans confidentiality, integrity och availability.

dessutom av en annan FOI-rapport med samma tema som kommer att publiceras kort efter denna rapport.[2]

1.2 Metod

För att besvara forskningsfrågorna gjordes två olika explorativa litteratursökningar. Den ena sökningen gjordes i databasen Google Scholar för att hitta akademiska forskningsartiklar som rör bristande it-anslutningar. Den andra sökningen gjordes med vanliga Google-sök för att identifiera dokument från myndigheter med särskilt ansvar för att upprätthålla samhällets it-anslutningar. Relevanta myndigheter valdes ut utifrån författarens erfarenhet inom it-säkerhetsområdet. De två typerna av litteratur sammanställdes och redovisas i rapporten på ett sätt som avses vara pedagogiskt.

1.3 Läsanvisning

Rapporten är indelad på följande sätt. I kapitel 2 målas en bakgrundsbild upp av hur datornätverk fungerar samt hur tillgängligheten kan påverkas. Därefter beskriver kapitel 3 konsekvenser av bristande it-anslutningar utifrån ett allmänt perspektiv och utifrån två allvarliga historiska exempel. Därtill beskriver kapitel 4 vilka reservalternativ det finns till den vanliga anslutningen, dvs. vad som kan användas för att minska konsekvenserna. Rapporten avslutas med en diskussion i kapitel 5.

[2] Den andra rapporten har arbetsnamnet *”Bortkopplad från omvärlden. Stöd för bedömning av verksamheters beroende av extern anslutning”*. Rapporten är författad av Johan Bengtsson, Camilla Eriksson och Matilda Olsson.

2 Bakgrund

I detta kapitel beskrivs grunderna för vanliga datornätverk som baseras på den typ av teknik som används i internet. Därtill beskrivs hur datornätverk säkras samt vilka hot som finns mot dem.

2.1 Vanliga datornätverk

Datornätverk består av datorer som länkats samman med så kallade kommunikationsmedier. Kommunikationsmedierna kan vara i form av en fysisk tråd som till exempel optisk fiber, telefonkabel eller elnätskabel. Kommunikations-medierna kan också vara trådlösa i form av radiovågor (såsom wifi eller 4G) eller mikrovågor (såsom satellitkommunikation). Därtill finns datornätverk i olika storlekar[3] och kan vara interna för en organisation (intranät) eller i kombination med andra organisationers nätverk (för att till exempel bilda internet).

Datorerna i ett nätverk kan skicka paket till varandra. På paketens väg finns bland annat routrar som typiskt styr trafiken till den smartaste vägen så att det inte blir köbildning med paket på en viss huvudled och inga paket alls på bakgatorna. Det kan nämnas att det typiskt inte finns några garantier för vilken geografisk väg paketet tar. Det innebär att internettrafik mellan två svenska datorer kan gå via en utländsk del av internet.[4]

Förutom routrar och andra enheter för vidarebefordran behöver paketleveranser i datornätverk också ett system för adressering så att routrarna vet vilken mottagare som ska ha vilket paket. Adressystemet är komplext och finns på olika nivåer, ungefär som vanlig post fungerar med länder, städer, postnummer, gator, gatunummer, trappor och personnamn. Förenklat fungerar datornätverkens adressystem som följer:

- **Användning av IP-adresser**
  En dator som är del av ett nätverk tilldelas en, för nätverket, unik IP-adress.
- **Användning av portnummer**
  Utöver IP-adress har varje dator också ett stort antal portnummer. Portnumren är som en sorts dörrar på datorn och används för att paket ska kunna styras till en viss applikation (ett program) på datorn.

[3] Exempelvis finns mindre Local Area Network (LAN) och större Wide Area Network (WAN).
[4] Relaterat till detta är att det visats att trafik som går mellan två datorer i Schengen-området i ungefär en tredjedel av fallen går via servrar utanför Schengen (Dönni m.fl., 2015).

- **Översättning till människovänligt format**
  För människor ter sig IP-adresser typiskt slumpmässiga och svårmemorerade. För att underlätta för människor kan därför IP-adresserna översättas till adresser med domännamn. Det gör att FOI:s webbplats kan nås genom att i en webbläsare skriva in adressen www.foi.se varpå en särskild server hjälper datorn att översätta till IP-adressen 150.227.2.8.

Förutom adressering har datornätverk också andra standardiserade sätt att utforma paket på. Det gäller exempelvis var på paketen adressen ska stå samt hur stora paketen får vara. Ett sådant standardiserat sätt som används för överföring av en viss typ av information i nätverk kallas nätverksprotokoll (eller enbart protokoll).

2.2 Datornätverks säkerhetsfunktioner

Precis som för vanlig post finns illasinnade aktörer som till exempel vill stjäla vissa paket eller skicka paket fyllda med otrevligheter. I datornätverken finns det flera standardmässiga säkerhetsfunktioner som försvar mot sådana antagonister:

- **Kryptering av paketen för att inte utomstående ska kunna förstå paketens innehåll**
  Numera är kryptering vanlig på internet. Exempelvis använder många webbplatser HTTPS vilket är en krypterad[5] variant av det normala webböverföringsprotokollet HTTP. Liknande kryptering används också ofta som en komponent i virtuella privata nätverk (VPN) vilka bland annat används för att möjliggöra distansarbete.
- **Certifikat för att kontrollera att adressystemen inte manipulerats**
  De grundläggande adressystemen kan i grova drag jämföras med att be en främling på gatan om en vägbeskrivning. För att slippa bli förd bakom ljuset och bli rånad på en bakgata vore det bra om man kan kontrollera att främlingen är pålitlig. För datornätverk kan sådana kontroller göras genom att den främmande entiteten uppvisar ett slags id-handling i form av ett certifikat (poststämpel), vilket datorn kan kontrollera har utfärdats av en tillförlitlig källa i en hierarki av certifikat. Med hjälp av HTTPS kan en dator (eller applikation) också kontrollera att den inleder en privat konversation med rätt dator (eller applikation) snarare än med en imiterande bedragare. Exempelvis kan webbsidan https://foi.se visa upp ett certifikat som intygar att den verkligen är https://foi.se varpå certifikatets äkthet kan kontrolleras av besökarens webbläsare genom ett fabriksinställt rot-certifikat.

[5] Krypteringen i HTTPS bygger på protokollet TLS vilket i sin tur använder krypteringsalgoritmer som exempelvis RSA och AES.

Liknande adressatkontroll[6] finns också för att säkerställa att översättningen mellan domännamn och IP-adress inte manipulerats, dvs. att foi.se verkligen leder till 150.227.2.8.

- **Brandväggar för att stoppa potentiellt farliga kontakter**
  Ungefär som vakter i en reception kan datorers brandväggar stoppa oönskade kontakter. Brandväggar kan till exempel hålla ordning på vilka applikationer och datorer som får skicka vilken typ av trafik till vilken applikation på datorn och tvärtom.
- **Tidssynkronisering för att begränsa illasinnade aktörer i tid**
  Att upprätthålla en gemensam tid är viktigt för att till exempel kontrollera att certifikat fortfarande gäller och huruvida en inloggning skedde på kontorstid eller mitt i natten. Den gemensamma tiden upprätthålls typiskt genom att regelbundet inhämta[7] uppgift om tiden från en publik tidsserver.

De ovan beskrivna säkerhetsfunktionerna är rimliga i datornätverk. Utöver dessa tillägg finns ytterligare säkerhetsfunktioner som typiskt används för it-system men som inte nödvändigtvis är en funktion på nätverksnivå. Det rör sig till exempel om uppdatering av säkerhetskritisk mjukvara, härdning som avlägsnar onödiga komponenter,[8] simulering av angrepp (penetrationstestning) för att upptäcka säkerhetshål samt övervakning för att upptäcka intrång. Det rör sig också om granskning av leverantörers säkerhetsarbete, riskbedömning samt beredskapsplanering (engelska: *contingency planning*). Men trots alla säkerhetsfunktioner finns det fortfarande många hot kvar att hantera. Med tanke på att denna rapport fokuserar på it när de externa anslutningarna går ner är hoten som påverkar nätverkets tillgänglighet mest relevanta. Denna typ av hot beskrivs i nästa avsnitt.

2.3 Hot mot datornätverks tillgänglighet

Det finns flera vanliga hot mot ett datornätverks tillgänglighet. Hoten kan vara avsiktliga och antagonistiska, eller mänskliga men oavsiktliga, alternativt utgöras av naturkatastrofer. Dessa tre typer av hot beskrivs nedan.

Tillgänglighetsangrepp (engelska: *Denial of Service*, *DoS*) har varit vanliga hot i årtionden. Det finns flera typer av tillgänglighetsangrepp som kan utföras av en antagonist:

[6] Denna adressatkontroll sker med hjälp av DNSSEC som är en säkrare variant av protokollet DNS.
[7] Inhämtandet sker normalt med protokollet NTP.
[8] Ett exempel på en onödig komponent är ett standardprogram som följer med Windows men som en viss användare inte har nytta av.

- **Överbelastning**
  En antagonist gör stora mängder anrop mot en dator eller server (exempelvis webbplats) som kraschar till följd av överbelastning. Angrepp med överbelastning kan liknas vid en störsändning där trådlös kommunikation störs ut av kraftfulla sändningar.
- **Avledning av trafik**
  En antagonist imiterar ett offer och manipulerar därmed adressystemet för att på så sätt avleda (stjäla) trafik som avsetts för offret.
- **Censur**
  En antagonist (till exempel en myndighet i en totalitär stat) använder censurfunktioner såsom nationell blockering av vissa webbplatser.[9]
- **Kinetiska angrepp**
  En antagonist använder fysiska angrepp mot nationell infrastruktur vilket gör att centrala delar av viktiga datornätverk blir otillgängliga.
- **Handelshinder och handelsblockader**
  En antagonist (till exempel en myndighet i en totalitär stat) utövar påtryckningar som leder till att leveranserna av viktiga komponenter stoppas.[10] Utan sådana komponenter blir det svårt att ersätta delar av nätverken som går sönder eller som behöver uppdateras.
- **Kryptovirus och utpressningsprogram**
  En antagonist infekterar en dator med skadlig kod i form av så kallat kryptovirus som gör datorns filer obrukbara genom kryptering. I vissa fall kräver antagonisten betalning (lösensumma) för att (utlovas det) dekryptera filerna. I de fallen utgör den skadliga koden ett så kallat utpressningsprogam (engelska: *ransomware*).
- **Stöld av beräkningskraft**
  En antagonist tar över en dator och använder den för sina ändamål, exempelvis för att utvinna kryptovaluta eller för att med andra övertagna datorer skicka stora mängder trafik i överbelastningsangrepp. Den legitima datoranvändningen försvåras på grund av att datorn är upptagen med antagonistens kommandon.

[9] Exempelvis blockerar kinesiska myndigheter i stor utsträckning utländska webbsidor och tjänster som den kinesiska staten anser olämpliga. Blockeringsfunktionen benämns ofta Great Firewall of China (Wright, 2014).

[10] Det är mycket ekonomiskt utmanande att undvika beroendet av utländska komponenter (Polatin-Reuben och Wright, 2014). En relevant jämförelse är Rysslands begränsade framgång i att bygga en egen infrastruktur med syfte att dess del av internet ska fungera utan den globala internetinfrastrukturen (Vendil Pallin och Hjelm, 2021).

Det finns också hot som inte drivs av antagonister utan beror på mänskliga misstag, undermålig planering eller olyckor:

- **Misstag i samband med att inställningar ändras**
  Ett exempel är hur Youtube (YT) blev nästan helt onåbart i två timmar under 2008. Cisco Press (2008) beskriver att YT:s servrar fungerade men att en pakistansk internetleverantör censurerade YT inte bara nationellt utan, oavsiktligt, också internationellt. Internetleverantören ändrade i sitt adressregister så att dess kunder inte skulle hitta till YT:s servrar utan istället hänvisas till en del av YT:s registrerade IP-adresser där ingen server fanns. Eftersom den nya adressen var mer specifik valde internets routrar den nya istället för den gamla adressen som, så att säga, bara ledde till Youtubes gata där en karta sedan leder till rätt gatunummer. Världens övriga internetleverantörer valde alltså att lita på en felaktig vägvisare hos en enskild internetleverantör. Ett mer färskt exempel från 2021 är hur Facebooks tjänster slutade fungera till följd av ett misstag vid inställningen av det interna router- och adressystemet (Martinho och Strickx, 2021).
- **Underlåtenhet att ta höjd för alla situationer en mjukvara kommer användas i**
  Några exempel är att bara uttrycka årtal med två siffror vilket var ett problem inför millennieskiftet; att inte dimensionera för de kraftiga trafikflöden som uppkommer sista dagen deklarationer kan lämnas in; eller att inte räkna med att användare är mobila och därför kan hamna i en sorts radioskugga.
- **Olyckor som påverkar infrastrukturen**
  Ett exempel är att en internetkabel råkar grävas av, vilket i ett fall ledde till att hela Armeniens internetåtkomst kraftigt begränsades i flera timmar (Parfitt, 2011). Liknande effekter uppstår vid strömavbrott.

Förutom avsiktligt och oavsiktligt mänskligt agerande kan anslutningen också påverkas av naturkatastrofer som exempelvis jordbävningar, extremt väder och solstormar. Som naturkatastrofer räknas också pandemier såsom Covid-19, vilken också ökat beroendet av externa anslutningar med ändrade arbetssätt i form av mer hemarbete och distansundervisning. Redan 2010 förutspådde Sterbenz m.fl. att en pandemi skulle kunna ge effekter på internet, exempelvis på grund av att personal inte kunde åka ut och ta hand om infrastrukturen.

3 Konsekvenser av bristande it-anslutning

Olika typer av hot mot datornätverk och it-system kan ge olika konsekvenser om de realiseras. Det kan handla om att nätverket inte fungerar som tänkt, att informationen i systemet ändras eller förstörs, eller att informationen i systemet läcker ut till obehöriga. I detta avsnitt är fokus på konsekvenserna av bristande tillgänglighet i it-anslutningar.

3.1 Allmänt om konsekvenserna

Vilka specifika konsekvenser som bristande it-anslutningar leder till beror dels på vilket system det är som drabbas, dels på verksamheten som använder sig av systemet. Det är inte möjligt att i detta avsnitt gå igenom alla typer av system och potentiella konsekvenser för dem. Ett sätt att beskriva vilka konsekvenserna blir är dock att för varje relevant fall ställa sig följande frågor:[11]

- Har bara en viss typ av trafik stoppats eller har hela nätverksanslutningen tappats?
- Har övriga delar av nätverket skadats?
- Har nätverket tagits över av en angripare?
- Har bara mjukvara och logisk infrastruktur påverkats eller även den fysiska infrastrukturen?
- Har bara en avgränsad del av organisationen drabbats eller även andra delar av organisationen eller samhället?
- Har it-anslutningen brustit under lång tid eller förväntas den göra det?
- Har orsaken till den bristande it-anslutningen betydelse för upplevelsen av konsekvenserna?

På en övergripande nivå blir konsekvenserna av att en organisation är utan extern it-anslutning att externa kontakter försvåras med medborgare, samarbetspartner och geografiskt spridd personal (till exempel distansarbetare). Förutom en organisations eget beroende av externa anslutningar har i regel också andra organisationer ett beroende av samma anslutningar. Om alla sådana beroenden i samhället ritades upp skulle det innebära ”ett oöverskådligt nät med kopplingar till alla verksamheter” (MSB, 2009, s. 44). Att en extern anslutning tappas i en organisation kan alltså leda till kaskadeffekter på övriga samhället. Det är också möjligt att samma grundorsak påverkar flera organisationer direkt. Så är

[11] Frågorna har bland annat inspirerats av de typer av fel som nämns i Avizienis m.fl. (2004) samt för frågan om orsak kapitel 4 i Frost m.fl. (2004). Därtill bör det noteras att det inte finns någon enighet i forskningslitteraturen för hur olika konsekvenser borde beskrivas och särskilt då på mätbar kvantitativ form (Aceto m.fl., 2018).

exempelvis fallet vid naturkatastrofer eller när flera organisationer använder samma mjukvara.

3.2 Ett allvarligt exempel

Ett exempel på allvarliga konsekvenser vid bristande it-anslutning är problemen som följde av utpressningsprogrammet NotPetya för ungefär fem år sedan. NotPetya riktades mot en ukrainsk revisionsmjukvara som bland annat användes av det stora transportbolaget Maersk. Konsekvensen för Maersk, som bara var en bland flera drabbade organisationer, blev att filer på deras datorer krypterades. Kryptering ledde i sin tur till störningar i datornätverken vilket bland annat gjorde att bokningsdata för containrar inte kunde hanteras. Störningarna ledde till en kostnad på flera miljarder kronor (Svensson m.fl., 2019).

Hur normal funktion återupprättades för Maersk beskrivs av Greenberg (2018). Först rensades infekterade datorer innan den senaste veckans säkerhetskopia (backup) lästes in. Ett problem var dock att säkerhetskopior saknades för de viktiga inloggningsservrarna (så kallade domänkontrollanter). Normalt kördes 150 sådana servrar, men alla utom en hade infekterats. Att en hade klarat sig från angrepp berodde på slumpen – servern som kördes i ett kontor i Ghana hade drabbats av ett strömavbrott kort innan NotPetya slog till. Servern som klarade sig behövde användas för att återföra information till övriga systemet. Den lokala bandbredden i kontoret var dock för låg för distansöverföring varför servern istället flögs till it-avdelningen i Storbritannien där den kunde användas för att återställa de övriga. Innan normal it-drift kunde återupprättas kommunicerade Maersks anställda med kunder via bland annat privata mejlkonton och mobilappen WhatsApp.

3.3 Strömavbrott som jämförelse

Strömavbrottet i västra Stockholm 2001 utgör ett intressant exempel på konsekvenser för störningar i datornätverk men också på bredare konsekvenser för hela samhället. Den här beskrivningen utgör en sammanfattning av en tidigare undersökning av FOI (se Jönson och Fischer, 2005; för andra strömavbrott se Waleij m.fl., 2019). Strömavbrottet drabbade framförallt stadsdelarna Akalla, Husby, Kista, Rinkeby och Tensta. Strömavbrottet pågick i 34 timmar och drabbade 16 000 hushåll samt 30 000 anställda. Eftersom Kista har en stor koncentration av företag inom it-branschen drabbades många it-företag av strömavbrottet. De direkta och indirekta konsekvenserna var framförallt enligt Tabell 1.

Tabell 1: Konsekvenser av strömavbrottet i västra Stockholm 2001. Sammanfattning av FOI-rapporten Jönson och Fischer (2005).

Direkt konsekvens	**Indirekt konsekvens**
Problem med fjärrvärme.	Kyla inomhus på grund av vinter utomhus.
Lågt vattentryck och begränsat med varmvatten.	Svårigheter att duscha och tvätta.
Indikation på fel med avloppssystemet och farhåga om att soprum kunde bli överfulla.	Oro.
Matvaror i kyl och frys förstördes.	Ekonomisk förlust och oro rörande vilken ersättning som skulle ges av bland annat försäkringsbolag.
Svårighet att laga mat på normalt sätt.	Grillning inomhus orsakade brand som gav skador på flera personer.
Brist på varor som det var stor efterfrågan på, exempelvis värmeljus och batterier.	Svårt få tag i nödvändiga varor.
Ej fungerande kassaapparater.	Försvårat inköp i butiker.
Vissa svårigheter att arbeta eftersom arbetsplatserna var stängda och eftersom det fanns behov av att stanna hemma och ta hand om anhöriga.	Ekonomisk skada.
Ej fungerande hiss.	Försvårade möjligheten att ta sig upp och ner i trapphus.
Avsaknad av elektrisk belysning.	Användning av levande ljus vilket i sin tur ökade brandrisken och då särskilt på toaletter där inga fönster fanns för naturligt ljus. Avsaknaden av belysning gjorde det också svårare att ta sig fram utomhus och i trapphus.
Bristande belysning och ej fungerande elektroniska lås.	Ökade datorstölder. Oro för brott. Krav på kraftigt ökad polisnärvaro (för att hålla brottsligheten på normala nivåer).
Bristande belysning vid vissa tunnelbanestationer.	Osäkerhet för trafikanterna varför vissa tunnelbanestationer fick stängas.
Uteblivna trafiksignaler.	Biltrafiken etc. försvårades samtidigt som många valde att tillfälligt flytta till bekanta i andra delar av staden.

Direkt konsekvens	Indirekt konsekvens
De främsta kommunikationskanalerna (tv, telefoni, internet och även i huvudsak radio) var elberoende.	Svårighet att kommunicera. Vidare fanns ingen central webbplats där information kunde läggas ut när de lokala förvaltningarnas webbplatser gick ner. Därtill saknade förvaltningarna el till sina datorer och mobilnätet var mycket instabilt. Därutöver var ett stort tidningstryckeri i närheten strömlöst vilket försvårade den analoga kommunikationen. Dessutom försenades aktiveringen av beredskapsplanen på grund av sen kontakt mellan SOS Alarm och Socialjouren.

Trots konsekvenserna som redovisas ovan kan det noteras att strömavbrottet inte gav några större problem för skolor, äldreboenden eller sjukhus. Det bör dock noteras att it-beroenden ökat kraftigt sedan händelsen och det finns anledning att tro att konsekvenserna skulle bli värre om något liknande skedde idag.

4 Reservalternativ för att minska konsekvenserna av bristande it-anslutningar

När it-anslutningen tappas är första åtgärden sannolikt att försöka återställa anslutningen. Återställning utgörs typiskt av olika former av reparation och av att data läses tillbaka från säkerhetskopior. Om återställning inte fungerar eller tar för lång tid är nästa möjlighet att använda ett reservalternativ i form av en annan anslutning eller annan kommunikationsform än den som gått ner. I detta kapitel beskrivs olika sådana reservalternativ som kan användas för att uppnå resiliens[12] och därmed minska konsekvenserna av bristande it-anslutning. Utöver reservalternativ som rör kommunikationen finns det även reservalternativ som rör upprätthållandet av verksamheten på andra sätt än med alternativa kommunikationsvägar. Exempelvis kan en forskares kommunikationsmöjligheter med en artikeldatabas delvis ersättas av ett lokalt bibliotek medan en fjärrstyrd eller fjärrövervakad industriprocess även kan styras eller övervakas mer lokalt genom att den ansvariga tar sig till industrilokalen.

4.1 Allmänt om reservalternativen

De reservalternativ som presenteras i de följande avsnitten är tänkta att vara tillämpliga för många olika verksamheter och kunna införas på kort tid när den ordinarie anslutningen går ner. Det ställer generellt krav på att användningen av reservalternativ förbereds innan störningar inträffar. Det är också viktigt att notera att reservalternativ är mindre önskvärda än det ordinarie nätverket. I vissa fall kan resultatet av att använda reservalternativ visserligen bli i stort sett identiskt[13] men i de flesta fall måste någon form av verksamhetspåverkan accepteras. Reservalternativen är alltså till för att minska konsekvenserna av bristande it-anslutningar snarare än att garantera att det inte blir några konsekvenser alls.

Vilket reservalternativ som ska väljas beror på den specifika organisationen och den specifika situationen. I generella termer rör det sig om en prioritering av det alternativ som är mest kostnadseffektivt, exempelvis vad gäller vilka tjänster som ska upprätthållas. Valet av reservalternativ påverkas också av hur lika

[12] Sterbenz m.fl. (2010) beskriver flera vanliga begrepp med den ungefärliga innebörden att minimera konsekvenser när något negativt inträffat. Det rör sig förutom *resiliens* (eng. resilience) om begreppen *feltolerans* (eng. fault tolerance), *robusthet* (eng. robustness), *överlevnadsförmåga* (eng. survivability), *pålitlighet* (eng. dependability) och *reliabilitet* (eng. reliability). Därtill nämner Avizienis m.fl. (2004) det snarlika *självläkande* (eng. self-healing).

[13] Ofta används begreppen *redundans* och *lastbalansering* om situationer där reservalternativet har stor likhet med det ordinarie, medan begreppet *diversifiering* används när skillnaden i utformning är större.

alternativen är det ordinarie nätverket och därmed hur väl reservalternativen klarar den avvikande situationen utan att också drabbas av problem. För säkerhetskopior (backuper) är det med liknande resonemang ofta lämpligt att ha flera kopior där en kopia är nära till hands och lagrad på ett sätt som är likt det ordinarie systemet, medan en annan kopia lagras på ett annat sätt och på en annan plats.

4.2 Distansarbete med molntjänster

Molntjänster är en typ av it-outsourcing som normalt är internetbaserad och där kunden snabbt och enkelt kan få tillgång till mer datorkraft (Karlzén, 2012). När de interna servrarna inte fungerar kan en organisation förlita sig på molntjänster istället. Interna organisationsdokument kan visserligen inte nås (om de inte redan laddats upp i molnet) men molntjänsterna möjliggör att medarbetare arbetar på distans och oberoende av anslutningarna i organisationens egna lokaler. De flesta molntjänster erbjuds av företag men det finns även exempel på alternativ som erbjuds av statliga aktörer såsom Försäkringskassans samordnade it-drift för myndigheter (Försäkringskassan, 2021). Ett problem med användningen av molntjänster är att rättsläget är oklart för hur offentliga organisationer får dela information med molnleverantörer. Den statliga it-driftsutredningen (SOU 2021:1) har därför föreslagit en ändring i Offentlighets- och sekretesslagen (2009:400).

4.3 Ett separat myndighetsnätverk

I statlig regi driver MSB *Swedish Government Secure Intranet (SGSI)*. SGSI är ett nätverk där i huvudsak offentliga organisationer kan dela information i databaser, skicka skyddad e-post och ha skyddade videokonferenser (MSB, 2021a). Det går också att skapa egna interna nätverk samt ansluta till EU:s säkerhetsskyddade kommunikationsnätverk *Testa* (MSB, 2020b). SGSI är utformat för att klara höga krav på tillgänglighet och driftsäkerhet samt vara skilt från internet (MSB, 2021a). För att två ansluta organisationer (kunder) ska kunna kommunicera måste de begära en öppning mellan varandra (MSB, 2020a). Trafiken mellan kunderna sker i VPN baserade på Försvarsmaktens krypteringslösning (MSB, 2020a). Varje kund har ett ansvar gällande it-säkerhet för sina interna nätverk (MSB, 2020a) och för att få ansluta sig ställs krav på kundernas arbete med it-säkerhet motsvarande ISO-standarden 27001 (MSB, 2021a).

4.4 Improviserade ad-hoc-nätverk

När anslutningsmöjligheterna är sporadiska kan så kallade ad-hoc-nätverk användas. Som beskrivs av Liu och Chlamtac (2004) saknar sådana nätverk routrar och annan infrastruktur på vägen mellan dem som vill kommunicera. Istället sker kommunikationen direkt från dator till dator (eller via en likadan tredje dator) och det oftast trådlöst. Nätverken kan därför byggas snabbt och används bland annat för direktkommunikation mellan mobiltelefoner, fordon eller sensorer.

4.5 Radio för samhällsviktig verksamhet

MSB driver det digitala radiokommunikationssystemet *Radiokommunikation för effektiv ledning (Rakel)*. Enligt MSB (2021b) används Rakel av samhällsviktiga aktörer i vardag, kris och höjd beredskap. Det främsta användningsområdet för Rakel är talkommunikation, men det finns även funktioner för text, att visa användares geografiska positioner mm. Därtill har Rakel god redundans och en infrastruktur planerad för att klara svåra väderförhållanden och långa elavbrott. Av MSB (2019) framgår att Rakel har en prioritetsfunktion för larmsamtal via en särskild knapp. Dessutom kan terminalerna användas som walkie-talkies det vill säga ad-hoc i direktkommunikation mellan terminaler utan stöd av övriga nätverket (MSB, 2021b).

När det gäller radiokommunikation är det också värt att nämna Sveriges Radio (SR) som har uppgiften att sända ut viktiga meddelanden från myndigheter till allmänheten vid kris, allvarlig störning och krig (Krisinformation.se, 2021). Enligt samma källa har SR:s radiokommunikation lång uthållighet vid exempelvis strömavbrott och andra störningar.

4.6 Kommunikation och styrning utan it och radio

Förutom kommunikation via it och radio finns även andra kommunikationssätt som exempelvis vanlig post, anslagstavlor och fysiska informationspunkter (lite som fysiska varianter av molntjänster). Därtill är kurirer särskilt nämnvärda eftersom de kan användas inte bara vid elektroniska störningar utan är också lämpade för kommunikation med höga krav på att den kommunicerade informationens konfidentialitet upprätthålls. Förutom för kommunikation används it även för att styra olika typer av industriella processer. Vad gäller anslutningsproblematiken är skillnaden liten mellan att kommunicera människor emellan och att kommunicera styrning från en människa (eller enhet) till ett styrsystem. Vad som redan framgått kan därför appliceras även på industriella styr- och kontrollsystem. Exempelvis kan kommunikation via kurir likställas med industriell styrning som sker efter att en medarbetare tagit sig från sin typiska

fjärrstyrningsplats till en plats som är samlokaliserad med det industriella systemet.

5 Diskussion

I detta kapitel diskuteras de två forskningsfrågorna i tur och ordning. Därefter beskrivs behov av ytterligare konkretisering av organisationers analysarbete.

5.1 Vad blir konsekvenserna när den externa it-anslutningen går ner?

Offentliga organisationer har ett stort beroende av externa anslutningar. Samtidigt finns en stor hotbild mot anslutningarna. Förhållandet mellan behov och hot inses dock ofta för sent. Incidentutredningar visar återkommande att organisationer slarvat med basal it-säkerhetshygien i form av säkerhetskopior, segmentering, säkerhetskritiska uppdateringar, riskanalyser och liknande. Dessa organisationer har förmodligen hellre sparat pengar än investerat i säkerhet (som ju i bästa fall aldrig visar sig behövas). Sådan kulturell förnekelse av säkerhetsproblemen är vanlig, liksom förhållningssättet att försöka klistra på säkerheten i efterhand. Med tanke på att hotbilden är stor kommer det låga säkerhetsfokuset leda till att många it-anslutningar går ner och dåliga möjligheter att hantera konsekvenserna av detta. Därtill ökar beroendet av anslutningarna vilket gör att konsekvenserna blir allt större över tid.

Generellt är det alltså enkelt att säga att konsekvenserna av otillgänglig anslutning kan bli stora. Men vilka specifika konsekvenser som uppstår beror på det system som drabbas i det specifika fallet och därmed även vilken verksamhet och organisation som systemet finns i. För att avgöra potentiella konsekvenser måste därför varje viktig specifik situation analyseras enligt gängse metoder för konsekvensanalys (engelska: *business impact analysis*), beroendeanalys och riskanalys. En viktig parameter i sådana analyser är hur kritiska verksamhetsdelarna som skulle drabbas är. En annan viktig parameter är själva hotets natur och därmed hur svårt det är att återställa tillgängligheten, dvs. om problemet blir långvarigt och kanske rentav följs av fler orsaker som en jordbävnings efterskalv eller en angripares nästa steg i ett större angrepp. Därtill är en viktig parameter vilka möjliga reservalternativ som finns (vilket diskuteras i nästa avsnitt). Analyserna kräver flera typer av kompetenser där verksamhetsrepresentanter (både ledning och andra) samsas med säkerhetsexperter på både icke-antagonistiska hot och på antagonistiska hot. Därtill behöver vissa hot hanteras i samverkan med andra organisationer. Exempelvis kan en ensam organisation knappast själv stoppa ihärdiga internetbaserade stöldligor, handelsblockader, eller angrepp som initierats av andra länders myndigheter. En närliggande aspekt är de kaskadeffekter som en organisations problem kan få på övriga samhället. För kaskadeffekterna behöver det redas ut vem som ska ta ansvar för dem samt hur konsekvenser i många led ska förutses.

5.2 Hur kan konsekvenserna av bristande it-anslutningar minskas?

När en it-anslutning brister gäller det att organisationen är förberedd och har reservalternativ att gå över till. Samtidigt är det väldigt svårt att uppnå en funktionell likhet hos reservalternativen utan att också ha ett likartat sårbarhetsberoende. Exempelvis finns en motsättning mellan att ha säkerhetskopiorna redo att använda och att förvara dem avskilt från standardsystemet så att inte även säkerhetskopiorna råkar ut för samma brand eller dylikt. Därtill finns det i it-domänen några få väldigt inflytelserika it-bolag samt i övrigt ett komplext inbördes beroende mellan olika it-produkter. Med andra ord är det svårt att faktiskt sprida risken. Den fysiska redundansen är också svår att lyckas med fullt ut, varför det alltid kommer finnas svaga länkar. Ett exempel nämns av Franzén m.fl. (2004, sid. 21): ”Ofta dras av praktiska skäl och kostnadsskäl många olika kablar i samma kabeltrummor och förläggs tillsammans med annan viktig infrastruktur”.

En aspekt på både teknisk och strategisk nivå är huruvida en offentlig organisation bör uppnå ökad resiliens på egen hand eller genom att använda samordnad it-drift i myndighetsnätverk eller molntjänster. Ingen organisation klarar sig visserligen helt på egen hand men å andra sidan innebär samordning minskad självständighet och risker kopplade till konfidentialitet. Vilken organisatorisk form som är den rätta påverkas också av förekomsten av pandemier. Om smittsamma sjukdomar ska bekämpas är distansarbete mer lämpligt vilket ökar de externa beroendena, medan en större teknisk hotbild istället gör det mer lämpligt med fysiskt samlokaliserad personal. En annan påverkande faktor är det ökade teknikberoendet i samhället. Det beroendet utmålas ofta som en risk där ett ständigt ökat beroende kräver nya lösningar. Men det vore mer logiskt om teknikberoendet tvärtom följde av de nya tekniska lösningarna och att möjligheterna till resiliens därmed förbättras på köpet. För att gå denna mer optimistiska väg krävs dock att lösningarnas införande görs på goda grunder. Oavsett vägval råder det ingen tvekan om att de offentliga organisationernas beroende av en stabil extern elektronisk anslutning kommer att kvarstå för överskådlig framtid.

5.3 Analys av konkreta konsekvenser

Rapporten har besvarat forskningsfrågorna på ett allmänt sätt utan koppling till något särskilt scenario eller till en viss typ av verksamhet eller datornätverk. För att en organisation ska kunna bedöma konsekvenserna av bristande it-anslutningar i en mer konkret situation behövs ett analysarbete som även det är mer konkret. Ett sådant analysarbete måste visserligen varje organisation göra på egen hand, men det finns anledning att ge mer stöd för hur organisationen kan utföra analysen. Under 2022 kommer därför FOI att ge ut en rapport som syftar till att vägleda en sådan analys.

6 Referenser

Aceto G., Botta A., Marchetta P., Persico V., Pescapé A. 2018. A comprehensive survey on internet outages. Journal of Network and Computer Applications. https://doi.org/10.1016/j.jnca.2018.03.026

Avizienis A., Laprie J.-C., Randell B., Landwehr C. 2004. Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing. https://doi.org/10.1109/TDSC.2004.2

Cisco Press. 2008. Attacking and Defending the Internet with Border Gateway Protocol (BGP). https://www.ciscopress.com/articles/article.asp?p=1237179

Dönni D., Sperb Machado G., Tsiaras C., Stiller B. 2015. Schengen Routing: A Compliance Analysis. IFIP International Conference on Autonomous Infrastructure, Management and Security. https://doi.org/10.1007/978-3-319-20034-7_11

Franzén G., Barck-Holst S., Fischer G. 2004. Telekommunikationernas sårbarhet och risker för samhället. FOI-R--1227--SE. Totalförsvarets Forskningsinstitut (FOI). https://www.foi.se/rest-api/report/FOI-R--1227--SE

Frost C., Barck-Holst S., Ånäs P., Lövkvist Andersen A.-L. 2004. Acceptabla elavbrott? Fyra strategier för säker elförsörjning. FOI-R--1163--SE. Totalförsvarets Forskningsinstitut (FOI). https://www.foi.se/rest-api/report/FOI-R--1163--SE

Försäkringskassan. 2021. Svar på regeringsuppdrag. Rapport – Delredovisning avseende Uppdrag att erbjuda samordnad och säker statlig it-drift dnr Fi2017/03257/DF. FK 2020-001438. https://www.forsakringskassan.se/wps/wcm/connect/500d9bcf-a7c3-49d2-bebb-356234f286d4/delredovisning-avseende-uppdrag-att-erbjuda-samordnad-och-saker-statlig-it-drift-svar-pa-regeringsuppdrag-dnr-2020-001438.pdf

Greenberg A. 2018. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Jönson K., Fischer G. 2005. Elavbrottet i Kista-området mars 2001 – Konsekvenser för hushåll och befolkning. FOI-R--1548--SE. Totalförsvarets forskningsinstitut (FOI). https://www.foi.se/rest-api/report/FOI-R--1548--SE

Karlzén H. 2012. Molnet – möjligheter och begränsningar. FOI-R--3381--SE. Totalförsvarets forskningsinstitut (FOI). https://www.foi.se/rest-api/report/FOI-R--3381--SE

Krisinformation.se. 2021. (26 aug). Sveriges Radios roll vid kris. https://www.krisinformation.se/detta-gor-samhallet/sveriges-radio

Liu J.J.N., Chlamtac I. 2004. Mobile Ad-hoc networking with a view of 4G Wireless: Imperatives and Challenges. IEEE. ISBN 0-471-37313-3. https://doi.org/10.1002/0471656895.ch1

Martinho C., Strickx T. 2021. (4 okt). Understanding How Facebook Disappeared from the Internet. Cloudflare. https://blog.cloudflare.com/october-2021-facebook-outage

MSB. 2009. Faller en – faller då alla? En slutredovisning från KBM:s arbete med samhällskritiska beroenden. https://www.msb.se/siteassets/dokument/amnesomraden/krisberedskap-och-civilt-forsvar/stod-i-att-analysera-beroenden/faller-en---faller-da-alla.pdf

MSB. 2019. Grundabonnemang. https://www.msb.se/sv/verktyg--tjanster/rakel/abonnemang-och-tillaggstjanster/grundabonnemang

MSB. 2020a. Så fungerar SGSI. https://www.msb.se/sv/verktyg--tjanster/sgsi/sa-fungerar-sgsi

MSB. 2020b. Tjänster i SGSI. https://www.msb.se/sv/verktyg--tjanster/sgsi/tjanster-i-sgsi

MSB. 2021a. (26 okt). SGSI - Swedish Government Secure Intranet. https://www.msb.se/sv/verktyg--tjanster/sgsi

MSB. 2021b. (13 dec). Om Rakel. https://www.msb.se/sv/verktyg--tjanster/rakel/om-rakel/

Parfitt T. 2011. Georgian woman cuts off web access to whole of Armenia. Guardian. https://www.theguardian.com/world/2011/apr/06/georgian-woman-cuts-web-access

Polatin-Reuben D., Wright J. 2014. An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet. 4th Usenix workshop on free and open communications on the internet. https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf

SOU 2021:1. Säker och kostnadseffektiv it-drift – rättsliga förutsättningar för utkontraktering. Delbetänkande av It-driftsutredningen. Statens offentliga utredningar. Nås via https://www.regeringen.se/rattsliga-dokument/statens-offentliga-utredningar/2021/01/sou-20211/

Sterbenz J.P.G., Hutchison D., Çetinkaya E.K., Jabbar A., Rohrer J.P., Schöller M., Smith P. 2010. Resilience and survivability in communication networks: Strategies, principles, and survey of disciplines. Computer Networks. https://doi.org/10.1016/j.comnet.2010.03.005

Svensson E., Magnusson J., Zouave E. 2019. Kryptomaskar och deras konsekvenser. FOI-R--4774--SE. Totalförsvarets forskningsinstitut (FOI). https://www.foi.se/rest-api/report/FOI-R--4774--SE

Vendil Pallin C., Hjelm M. 2021. Moscow's Digital Offensive – Building Sovereignty in Cyberspace. Totalförsvarets forskningsinstitut. FOI Memo 7521. https://www.foi.se/rest-api/report/FOI%20Memo%207521

Waleij A., Simonsson L., Liljedahl B. 2019. Konsekvenser av energibortfall på samhällets funktionalitet och civilbefolkningens hälsa. FOI-R--4755--SE. Totalförsvarets forskningsinstitut (FOI). https://www.foi.se/rest-api/report/FOI-R--4755--SE

Wright J. 2014. Regional variation in Chinese internet filtering. Information, Communication & Society, 17:1. https://doi.org/10.1080/1369118X.2013.853818

Offentliga organisationers datornätverk står inför många hot. Hoten inkluderar allt från att den fysiska kommunikationslänken skadas till att slutanvändares datorer tas över av angripare. Om hoten realiseras kan det leda till att nätverksanslutningarna går ner. Rapporten beskriver vad sådan otillgänglighet skulle få för konsekvenser. De exakta konsekvenserna beror på den specifika organisationen, men i allmänhet är it-beroendet stort och säkerheten låg vilket gör konsekvenserna stora. De möjliga konsekvenserna exemplifieras med skildringar av inträffade incidenter.

Rapporten beskriver hur konsekvenserna kan minskas genom användning av reservalternativ till det ordinarie nätverket. Reservalternativen kan skötas internt i en organisation eller i samordning med andra organisationer. Vilka reservalternativ som passar bäst för en organisation beror på den specifika verksamheten. Oavsett valet av reservalternativ är det svårt att nå funktionell likhet med ordinarie nätverk utan att också drabbas av likartade hot. Därtill ökar betydelsen för rätt reservalternativ med teknikberoendet i samhället. Å andra sidan möjliggör den tekniska utvecklingen också nya lösningar och därmed ökad motståndskraft.

FOI

ISSN 1650-1942

www.foi.se