CYBERHOT MOT SVERIGE

- En sammanfattning för ledare och beslutsfattare

Centrum för cybersäkerhet
September 2022

RI.SE

Sammanfattning

Parallellt med den tilltagande digitaliseringen av samhället ökar antalet cyberangrepp, globalt och i Sverige. Kombinationen av relativt låg risk och potentiellt hög utdelning, i form av såväl effekt som ekonomisk vinning, gör det till ett effektivt verktyg för hotaktörer att gynna sina intressen.

Cyberangrepp med ekonomiska motiv kan orsaka stor skada men det största hotet bedöms för närvarande komma från stater, särskilt i det rådande försämrade säkerhetsläget. Effekterna av statligt understödda angrepp kan få allvarliga konsekvenser på samhället, där utvecklingen av cybersäkerhet för närvarande inte håller jämna steg med digitaliseringstakten. Utöver faktiska störningar i exempelvis samhällsbärande infrastruktur kan cyberangrepp även orsaka negativa effekter på medborgarnas tilltro till samhällets institutioner. Robusta system och resiliens mot antagonistiska cyber- och påverkansoperationer är därför av största vikt.

Denna rapport syftar till att skapa en kunskapsöversikt för ledare och beslutsfattare om cyberhot mot Sverige och ger ett antal förslag på säkerhetsåtgärder. Proaktiva åtgärder kan minska risken för att utsättas för angrepp och möjliggöra tidig upptäckt, och en god förmåga att verkställa reaktiva åtgärder kan dämpa dess effekter.

Om centrum för cybersäkerhet

Centrum för cybersäkerhet på RISE stärker den tillämpade forskningen och kompetensutvecklingen inom cybersäkerhet i Sverige. RISE är ett oberoende, statligt ägt forskningsinstitut. Centret skapar en neutral nationell plattform som stöttar näringsliv och offentlig sektor genom expertstöd, forskningspartnerskap, innovationsledning samt test-och demonstrationsmöjligheter. Ett samarbete med RISE innebär tillgång till ett stort nätverk av tvärvetenskapliga team som innehar både en bred domänkompetens såväl som en djup cybersäkerhetsexpertis. Vi kan erbjuda stöd inom olika tillämpningsnivåer av cybersäkerhet – från forskning och utveckling, certifiering, utbildning/träning till systemtest i kontrollerade virtuella miljöer. Läs mer på vår hemsida.

1. Inledning

Medierapportering, såväl globalt som i Sverige, har under senare år i tilltagande grad fokuserat på cyberhot och cybersäkerhet. Detta till följd av att antalet cyberangrepp ökat betydligt och att kostnaderna de medför för de som utsätts är substantiella, både i form av eventuella lösensummor och förlorad/förstörd data samt tid då system ligger nere. Cyberangrepp utförs av bland annat hackare och kriminella organisationer och individer, men även stater.

Motiven, liksom modus, varierar. Det vanligaste motivet är pengar och cyberangrepp som utförs med ekonomiska motiv sker inte sällan genom ransomware [1]. I dessa fall tillskansar sig angriparen filer eller hela system, ofta genom att infektera offrens system med skadlig kod, kryptera datan, och hota med att publicera eller förstöra den om inte en lösensumma betalas [2]. Betalning av en lösensumma innebär dock inga garantier att data återfås och kan förvärra situationen för den som utsätts då det åskådliggjort villighet att betala för att återfå data.

Samtidigt som angrepp från cyberkriminella har blivit vanligare bedöms de allvarligaste cyberhoten mot Sverige nu komma från andra stater. Detta då det framför allt är stater som har resurser att utveckla avancerade virus som kan ta sig in i IT-system som styr elnät, vattenverk och industrier. Stater kan således använda cyberangrepp dels för att gagna sina ekonomiska intressen, dels för att orsaka allvarliga samhällsstörningar [3]. Signalspaningsmyndigheten Försvarets radioanstalt (FRA) skriver i sin senaste årsrapport (2021) att en viktig del av den breddade hotbilden som riktas mot Sverige utspelar sig i just cyberdomänen [4]. Myndigheten uppgav i januari 2017 att de upptäckte ungefär 10 000 aktiviteter per månad mot mål i Sverige från statliga utländska angripare - siffran uppgavs vara betydligt högre två år senare [5]. Syftet med aktiviteterna beskrivs kunna vara att identifiera sårbarheter i kritisk infrastruktur, samla information om försvarsförmåga och försvarsplanering men även att tillskansa sig patent, forskningsresultat och industrihemligheter [6].

FRA menar vidare att den snabba digitala utvecklingen generellt varit gynnsam för Sverige men att den även öppnat nya sårbarheter [7]. Argumentet lyder något förenklat: ju högre nivå av digitalisering desto fler angreppsytor, som behöver skyddas.

Denna rapport syftar till att skapa ett kunskapsunderlag för ledare och beslutsfattare om cyberhot mot Sverige och ger ett antal förslag på prioritering av säkerhetsåtgärder.

Rapporten kan ses i ljuset av att flertalet experter anser att man inte lägger tillräckligt mycket resurser på cybersäkerhet, och att

1. (2020) ENISA Threat Landscape - The year in review https://www.enisa.europa.eu/publications/year-in-review (s. 11)
2. Eklund, H. (2020-06-29). Cyberangrepp för 20 miljarder i Sverige. Svenska Dagbladet https://www.svd.se/a/70bjXw/svenska-notan-for-cyberangrepp-20-miljarder
3. Alpman, M. (2018-04-12). Sverige under cyberattack Forskning och Framsteg. https://fof.se/artikel/2018/4/under-attack/
4. (2021). FRA Årsrapport. s. 5 https://www.fra.se/download/18.3262020817e4dcd6ffc257/1652872280257/FRA-arsrapport-TGA-2021.pdf
5. (2022-02-02). FRA: Cyberattacker mot mjukvaruleverantörer allt vanligare SVT Nyheter https://www.svt.se/nyheter/inrikes/fra-cyberattacker-mot-mjukvaruforetag-allt-vanligare-efter-coops-nodstangningar I sammanhanget innebär en aktivitet förberedelse, försök eller genomförd cyberattack (ibid.)
6. Alpman, M. (2018-04-12). Sverige under cyberattack. Forskning och Framsteg. https://fof.se/artikel/2018/4/under-attack/
7. (2021) FRA Årsrapport. s. 5 https://www.fra.se/download/18.3262020817e4dcd6ffc257/1652872280257/FRA-arsrapport-TGA-2021.pdf

cyberförsvarsförmågan inte håller samma takt som digitaliseringen.

2. Exempel på tillvägagångssätt

Så här långt har Sverige inte utsatts för långvariga cyberangrepp som orsakat omfattande skador eller lett till starka missnöjesyttringar och flertalet experter bedömer för närvarande att den mest sannolika utmaningen inte är samhällelig kollaps utan snarare en situation där man exempelvis under en period inte kan ta ut pengar eller där man drabbas av tillfälliga strömavbrott. Med det sagt kan det försämrade säkerhetsläget bidra till att omständigheterna förändras och i ett allvarligt scenario skulle cyberangrepp mot kritisk infrastruktur i Sverige kunna leda till att hela samhället stannar under en lång tid.

Cyberangrepp kan se ut på många olika sätt – detta avsnitt innehåller några exempel på tillvägagångssätt och illustreras med exempel på aktörer i olika sektorer i Sverige som utsatts.

Syftet är att ge en förståelse för hur man bör prioritera utvecklingen av sin cybersäkerhet, och ett antal förslag för detta redogörs för i avsnitt 3.

2.1 Distributed-denial-of-service (DDos)

DDoS-angrepp [8] tillskrivs ibland inte särskilt stor betydelse, främst på grund av att de tenderar att inte vara tekniskt avancerade. Däremot kan de orsaka stora störningar om de riktas mot kritisk infrastruktur som energi-, kommunikation-, transport- eller banksektorn för att nämna några exempel. DDoS-angrepp mot denna typ av sektorer kan även utgöra ett led i en främmande stats kartläggning av kritisk infrastruktur, dess cybersäkerhetsförmåga och samhällets resiliens mot störningar.

Ett cyberangrepp i Sverige som inte blev särskilt omskrivet i media men som likväl är relevant inträffade under hösten 2017. Incidenten rörde ett DDoS-angrepp mot Trafikverkets internetleverantörer TDC och DGS, vilket påverkade tågtrafiken runtom i Sverige och orsakade förseningar [9]. Angreppet beskrevs som

8. Ett DDoS-angrepp, även kallat överbelastningsangrepp, har i regel som mål att överbelasta en webbplats eller en server, och på så sätt göra den tillfälligt otillgänglig för legitima användare. Källa: Jelver, N. (2022-03-11). Vad innebär en DDoS-attack - och hur kan man skydda sig? Svensk Handel. https://www.svenskhandel.se/nyhetscenter/nyheter/2022/vad-innebar-en-ddos-attack---och-hur-kan-man-skydda-sig/

9. Arstad Djurberg, J. (2017-10-11). Bekräftat: ddos-attack bakom tågförseningar. Computer Sweden. https://computersweden.idg.se/2.2683/1.690504/ddos-bakom-tag-forseningar

ett standardmässigt DDoS-angrepp och de reservsystem som skulle träda in när det ordinarie inte fungerade gjorde det. Tänkbara motiv med angreppet kommunicerades inte offentligt men går inte att utesluta att det kan ha utgjort ett slags trycktest för att observera dels hur väl reservsystemen och återställningen fungerade, dels för att observera allmänhetens reaktioner på störningarna och tiden det tog för att återställa systemen. Var medborgarnas motståndskraft mot den tillfälliga störningen av kollektivtrafiken robust och gav det någon indikation på eventuella framtida reaktioner om störningarna hade varit mer omfattande och pågått under längre tid?

”Utöver den faktiska skada som DDoS-angrepp kan tillfoga system bör även de kognitiva effekter de kan ha hos en målgrupp som haft tilltro till system/organisationer beaktas.”

DDoS- eller överbelastningsangrepp mot webbsidor som tillhandahåller viktig samhällsinformation, såsom myndighetssidor eller medier, skulle enligt Myndigheten för samhällsskydd och beredskap (MSB) kunna orsaka stora störningar och tillfoga svenska samhället skada [10]. Utöver den faktiska skada som DDoS-angrepp kan tillfoga system bör även de kognitiva effekter de kan ha hos en målgrupp som haft tilltro till system/organisationer beaktas. Ett DDoS-angrepp - oavsett dignitet - kan leda till att den drabbade organisationens integritet eller möjlighet att fortsätta leverera en behövd tjänst ifrågasätts. Detta även om angreppet inte fått särskilt allvarliga långsiktiga effekter på systemet - perceptionen av hotet och dess verkan hos en befolkning, inte bara den reella effekten, är en viktig dimension av cyberangrepp.

2.2 Ransomwareangrepp

Ransomewareangrepp har ökat mycket under senare år och en viktig anledning är att de tenderar att vara lönsamma samt är förenade med relativt låg risk för de som utför dem [11]. De riktas mot aktörer i det offentliga såväl som i näringslivet och har ofta ekonomiska motiv, men kan utöver det även utgöra en metod för att trycktesta ett samhälles resiliens och robusthet när det utsätts för störningar. Organisationer av alla storlekar och inom alla sektorer är potentiella måltavlor för ransomewareangrepp.

Kalix kommun utsattes för ett ransomwareangrepp i december 2021. Till följd av angreppet slogs IT-system ut, vilket påverkade hela verksamheten. Det tog över en månad innan alla system åter var i drift och de sammanlagda kostnaderna för kommunen uppgick till cirka 2,5 miljoner kronor [12]. Under sommaren 2021 utsattes en amerikansk mjukvaruleverantör, Kaseya, för ett

10. (2022-05-09). Cyberhoten från Ryssland: Så kan de iscensättas. Göteborgs-Posten. https://www.gp.se/nyheter/sverige/cyberhoten-fr%C3%A5n-ryssland-s%C3%A5-kan-de-iscens%C3%A4ttas-1.72250986

11. Enligt Jan Olsson, kriminalkommissarie på Nationellt IT-Brottscentrum, betalar omkring 80 procent av drabbade företag hela eller delar av lösensumman. Dessutom tror man att få, kanske under fem procent, av drabbade personer och företag polisanmäler att de utsatts för cyberangrepp. Anledningar till detta kan exempelvis vara skam, rädsla för negativ publicitet och/eller skada på ett företags varumärke. Källa: Oscarson, T. (2021-10-19). Pressas på pengar av hackare – stort problem att få vågar anmäla. Ny Teknik. https://www.nyteknik.se/sakerhet/pressas-pa-pengar-av-hackare-stort-problem-att-fa-vagar-anmala-7022797

12. Westergren, E. Cyberattacken mot Kalix kommun. Microsoft Pulse. https://pulse.microsoft.com/sv-se/work-productivity-sv-se/na/fa1-cyberattacken-mot-kalix-kommun/

ransomwareangrepp. Angreppet drabbade bland annat flera svenska företags kassasystem, däribland Coops, genom att låsa dem och omöjliggöra transaktioner. Enligt IT-säkerhetsexperten David Jacoby var angreppet unikt i sitt slag då butiker tvingades att fysiskt stänga, vilket ledde till att konsekvenserna av angreppet blev direkt kännbara för konsumenterna [13].

Att incidenterna som drabbade Kalix kommun och Kaseya rörde sig om ransomwareangrepp antyder ekonomiska motiv vilket i sin tur skulle kunna indikera att angriparna var någon form av cyberkriminella individer eller organisationer [14] , men detta utesluter inte någon form av stöd från en stat - stöd som även kan ta formen av underlåtenhet mot att ingripa mot cyberhotaktörer. Ur ett perspektiv kan det vara mindre relevant vem som låg bakom angreppen: viktigt i sammanhangen var att incidenterna blottlade Kalix kommuns och Kaseyas bristfälliga cybersäkerhetslösningar - omfattningen av angreppen skulle kunna antyda att angriparna tagit sig in i systemen långt tidigare och väntat på rätt förutsättningar för att verkställa dem, och att det inte upptäckts. Vidare demonstrerade incidenterna skadeverkningarna som omfattande ransomewareangrepp kan tillfoga en kommuns verksamhet och dess medborgares tillvaro samt hur sårbar detalj- och livsmedelshandeln i Sverige är för cyberrelaterade störningar. Incidenterna utgjorde även en möjlighet för andra cyberhotaktörer runtom i världen att observera händelsernas förlopp under och efter angreppen, hur de hanterades och allmänhetens reaktioner på dem.

2.3 Dataintrång och doxing

Dataintrång kan bland annat innebära att mer eller mindre känslig data förstörs, eller stjäls, ibland för att publiceras eller säljas. Denna typ av angrepp kan ha ekonomiska såväl som ideologiska motiv och kan utgöra ett verktyg för att demonstrera förmåga såväl som tröskel för att använda den.
Säkerhetspolisen skriver i sin årsbok (2021) att Riksidrottsförbundet mellan december 2017 och maj 2018 utsattes för upprepade dataintrång, som de tillskrev den ryska militära underrättelsetjänsten GRU [15]. Intrången beskrivs ha varit en del i en rysk kampanj riktad mot nationella och internationella antidopingorganisationer och motivet misstänktes vara hämnd till följd av att ryska idrottare stängts av från deltagande i idrottstävlingar på grund av anklagelser om doping. Skadan av intrånget innefattande bland annat att sekretessbelagd medicinsk information rörande svenska idrottare publicerades på internet.

Doxing är ytterligare en form av cyberangrepp som uppmärksammats under senare år. Det innebär att söka, inhämta och publicera information av en privat karaktär på internet utan tillstånd, och kan användas för att misskreditera en samhällsaktör

13. (2021-07-05). Expert om attacken som sänkt Coop: Utpressning mot detaljhandeln har exploderat. SVT Nyheter. https://www.svt.se/nyheter/inrikes/it-attacker-och-utpressningar-mot-detaljhandeln-allt-vanligare

14.. I fallet som rör Kaseya krävde aktörerna bakom angreppet 70 miljoner dollar för att öppna systemen igen och misstankarna riktades mot ryska hackernätverket Revil. Källa: (2021-07-05). Joe Biden beordrar utredning av cyberattacken. SVT Nyheter. https://www.svt.se/nyheter/joe-biden-beordrar-utredning-av-cyberattacken
Persson, F. (2021-11-08). Flera gripna efter cyberattacker – tvingade Coop att hålla stängt. Göteborgs-Posten. https://www.gp.se/nyheter/v%C3%A4rlden/flera-gripna-efter-cyberattacker-tvingade-coop-att-h%C3%A5lla-st%C3%A4ngt-1.58798790

15.. (2021). s. 14 Säpo årsbok.https://www.sakerhetspolisen.se/download/18.650ed51617f9c29b552287/1649683389251/Sakerhetspolisen_arsbok%202021.pdf

eller flytta fokus från en fråga till en annan i en inhemsk debatt. En kombination av en cyberoperation som lägger grunden för en kommande påverkansoperation. Den ryska hackergruppen APT 28, även benämnd Fancy Bear, med kopplingar till ryska militära underrättelsetjänsten GRU använde sig av denna metod både inför det amerikanska valet 2016 [16] och franska valet 2017 [17]. Man fick då genom spear-phishingangrepp [18] tillgång till privat data från, i första fallet Hillary Clintons kampanjansvarige John Podesta och i det andra fallet Emmanuel Macrons kampanjstab. Datan spreds sedan på olika sociala medieplattformar och forum på nätet i ett försök att smutskasta presidentkandidaterna vid kritiska tidpunkter under valkampanjerna [19]. Enligt Mikael Tofvesson, Operativ Chef på Myndigheten för Psykologiskt försvar, går det inte att utesluta att Sverige kan komma att bli en måltavla för denna typ av angrepp i och med att valet 2022 sker i ett försämrat säkerhetsläge [20].

Statligt understödda cyberangrepp kan utgöra ett instrument för att uppnå utrikespolitiska mål och vara ett effektivt verktyg för stater att orsaka störningar och vilseleda, i konflikter och under fredstid. På kort sikt kan en angripande stats målsättning vara att orsaka varierande grader av störningar och orsaka viss ekonomisk förlust. Parallellt med detta kan den angripande staten även tillskansa sig affärshemligheter och information om exempelvis spetsforskning för att gagna sina egna intressen, konkurrenskraft och ekonomiska utveckling. På längre sikt kan målsättningen vara att destabilisera och splittra samhället, för att göra det till en svagare konkurrent som är mer formbar, så att ens egna intressen kan gynnas. Detta kan bland annat uppnås genom att misskreditera statsledningen och dess institutioner och få dem att framstå som inkompetenta, så att tilliten i samhället skadas. Användare kan börja tvivla på tjänsters robusthet vilket kan påverka trovärdigheten både för leverantörer och eventuellt på sikt den sociala tilliten och synen på samhällets resiliens.

”Att kostnaderna för att genomföra cyberangrepp är relativt låga jämfört med konventionell krigföring gör även att mindre stater med rätt kompetens har möjlighet att åstadkomma stor skada.”

Cyberforskaren Jan Kallberg menar att det allvarligaste hotet är när ” […] cyberförmågor används för att skapa splittring i samhället och minska förtroendet för myndigheter och de styrande. Det gör att

16. US Senate Select Committee on Intelligence (2017-06-21) Hearing on Russian Interference in the 2016 U.S. Elections. https://www.intelligence.senate.gov/hearings/open-hearing-russian-interference-2016-us-elections#

17. Jeangène Vilmer, J-B et al. (2018) Information Manipulation: A Challenge for our Democracies. 18. Att använda e-post för att genomföra angrepp kallas nätfiske (phishing). I de fall angreppet är riktat mot en eller ett fåtal individer kallas det riktat nätfiske (spear phishing). Källa: Metoder som används vid cyberangrepp https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/cyberhot/metoder-som-anvands-vid-cyberangrepp/

19. Palmertz, B. (2021). Influence operations and the modern information environment. In M. Weissmann, N. Nilsson, B. Palmertz & P. Thunholm (Authors), Hybrid Warfare: Security and Asymmetric Conflict in International Relations (pp. 113–131). London: I.B. Tauris.

20. 2022-08-01 Myndigheten för psykologiskt försvar: Finns risk för valpåverkan. Intervju med Mikael Tofvesson, Operativ Chef, Myndigheten för Psykologiskt försvar i SR P4. https://sverigesradio.se/artikel/myndigheten-for-psykologiskt-forsvar-finns-risk-for-valpaverkan

motståndskraften minskar mot samhällsstörningar, som då kan leda till kaos och underkastelse inför en främmande makt" [21].

Ytterligare en långsiktig målsättning kan vara att destabilisera ett lands ekonomi så att andra länder inte ser det som en trovärdig handelspartner, genom exempelvis storskalig spridning av skadlig kod i system som förstör eller låser system och samhällsviktig verksamhet ur drift, exempelvis telekommunikation och energi- eller banktjänster [22]. Att kostnaderna för att genomföra cyberangrepp är relativt låga jämfört med konventionell krigföring gör även att mindre stater med rätt kompetens har möjlighet att åstadkomma stor skada.

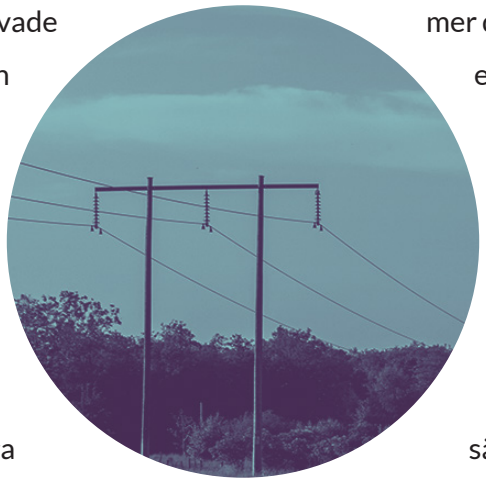
3. Säkerhetsåtgärder

Samhället och näringslivet bör vara så robust och resilient mot cyber- och påverkansangrepp som möjligt. Proaktiva åtgärder kan minska risken för att utsättas för cyberangrepp och en infrastruktur för att verkställa genomtänkta, övade och skalbara reaktiva åtgärder kan dämpa effekterna av angrepp när de sker.

För att samhället ska vara robust är det centralt att grundläggande samhällstjänster- och funktioner fungerar och finns tillgängliga för medborgarna, och att medborgarna upplever att så är fallet. Till de samhällskritiska funktionerna räknas bland annat försörjning av energi, vatten och livsmedel, liksom hälso- och sjukvården och system för IT och kommunikation [23]. Även om ansvaret för dessa verksamheter inte huvudsakligen åligger aktörer i näringslivet, kan de utgöra en viktig del av leveranskedjan genom tillhandahållande av varor och tjänster som är nödvändiga för att dessa verksamheter ska fungera. På så vis är det viktigt på många plan för aktörer i näringslivet att skydda sin verksamhet, dels på företagsnivån - att företaget ska utvecklas och vara konkurrenskraftigt - dels på samhällsnivå, då man har en del i ansvaret för att det ska fungera. Detta belyser också vikten av samverkan mellan näringslivet och det offentliga.

3.1 Vikten av kontinuerlig genomlysning av verksamheten

När de samhällskritiska funktionerna blir alltmer digitaliserade utgör cyberdomänen en allt större potentiell angreppsyta. Verksamheter inom bland annat telekom, energiförsörjning, livsmedelsförsörjning, transport, rättsväsende samt bank och finans har skyldighet att utreda om de bedriver säkerhetskänslig verksamhet eller hanterar säkerhetsskydds-



21. Alpman, M. (2018-04-12). Sverige under cyberattack. Forskning och Framsteg. https://fof.se/artikel/2018/4/under-attack/
22. (2022-05-04). Förhöjd risk för cyberangrepp under Nato-debatten. SVT Nyheter. https://www.svt.se/nyheter/inrikes/forhojd-risk-for-cyberangrepp-under-nato-debatten
23. (2021) MUST årsöversikt. S. 44. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/musts-arsoversikt-2021-.pdf

Foto: Axel Josefsson

klassificerade uppgifter och därmed behöver skydda sin verksamhet mot antagonistiska hot enligt säkerhetsskyddslagen [24] . Även om ens verksamhet bedöms inte omfattas av säkerhetsskyddslagen, kan delar av lagen utgöra ett bra verktyg för att inventera skyddet av sin verksamhet. Här åsyftas framför allt säkerhetsskyddsanalysen, som ska ge svar på vad som ska skyddas, mot vad det ska skyddas och hur det ska skyddas [25]. I säkerhetsskyddsanalysen identifieras och bedöms skyddsvärden utifrån hur allvarlig konsekvensen av en viss skada blir, snarare än hur hög sannolikheten är för att ett säkerhetshot realiseras [26]. Detta är relevant att begrunda, för att inte förminska omfattande hot och framför allt förberedelser för att hantera dem, på grund av att de bedöms vara alltför osannolika.

”När de samhällskritiska funktionerna blir alltmer digitaliserade utgör cyberdomänen en allt större potentiell angreppsyta.”

Cybersäkerhetsarbetet inom en organisation behöver utvecklas och anpassas kontinuerligt. Dessutom behöver detta ta hänsyn till både tekniska och mänskliga aspekter eftersom försök till manipulation av ackrediterade användare, så kallad social engineering, är en vanlig metod vid genomförande av cyberangrepp. En kunskapsgenomlysning är en bra början - vad kan slutanvändarna egentligen om risker och säkerhet så att man kan fokusera och utvärdera gjorda insatser. Man bör även analysera olika medarbetares roller och den informationstillgång det medför i IT-miljön. Regelverk, rutiner och kompetensstöd behöver upprätthållas, men med en realistisk förväntan på användarna. Om säkerhetsrelaterade processer upplevs som komplexa, onödiga eller ologiska leder det inte till förståelse och efterlevnad, och kan ge en falsk bild från ledningsperspektiv av organisationens egentliga säkerhetsnivå. Utöver utbildning och övning för verksamhetens användare är det också viktigt att underlätta för en responsiv incidentrapportering. Därutöver att medarbetarna inte känner att detta förknippas med ett stigma vilket kan minska viljan att rapportera när det behövs som mest, i ett så tidigt stadium som möjligt. Ett verktyg som kan agera temperaturmätare är till exempel penetrationstester som utifrån försöker hitta vilka tekniker organisationen är sårbar för, vilket ger en grund för hur implementering av olika motåtgärder kan prioriteras.

3.2 Vaksamhet vid outsourcing

Det är inte ovanligt att företag lägger ut drift eller underhåll av en viss del av verksamheten till en utomstående leverantör, ibland i ett annat

24. Säkerhetsskydd och säkerhetsskyddslagen. PwC. https://www.pwc.se/sv/cyber-security/sakerhetsskyddslagen.html
25. (Juni 2019) Vägledning i säkerhetsskydd. Säkerhetsskyddsanalys. Säkerhetspolisen. s. 5. https://www.sakerhetspolisen.se/download/18.310a187117da376c6601d3f/1636446528512/Vagledning-Sakerhetsskyddsanalys.pdf
26. (Juni 2019) Vägledning i säkerhetsskydd. Säkerhetsskyddsanalys. Säkerhetspolisen. s. 5. https://www.sakerhetspolisen.se/download/18.310a187117da376c6601d3f/1636446528512/Vagledning-Sakerhetsskyddsanalys.pdf

land. Anledningar till detta kan exempelvis vara effektivitets- eller besparingsskäl och outsourcing kan således vara gynnsamt för verksamheten. Däremot innebär outsourcing en del risker och ökad sårbarhet, även rörande risken för cyberangrepp. Detta är främst till följd av att outsourcing innebär minskad kontroll i leveranskedjor, gällande såväl kompetens som rutiner för informationssäkerhet. Ett exempel från närtid rör Transportstyrelsen, vars IT-upphandling blev uppmärksammad under 2017. I korthet ska svensk sekretesskyddad information från Transportstyrelen ha gjorts tillgänglig för icke-säkerhetsprövad personal i utlandet genom att Transportstyrelsen outsourcat IT-drift till ett företag som i sin tur använde underleverantörer [27]. Leverantörer som är en del av företag baserade i ett annat land kan vara föremål för påtryckningar från det landets regering att få tillgång till och exfiltrera information för att stötta det landets säkerhets- och underrättelsetjänster. Underleverantörers data kan även routas genom andra länder, vars säkerhets- och underrättelsetjänster i sin tur kan kräva tillgång till den. Genom att tidigt granska leverantören, ledningen, eventuella investerare och de som ska utföra arbetet går det att upptäcka tänkbara brister innan eventuell skada är skedd [28]. Ingen kedja är starkare än sin svagaste länk.

3.3 Vikten av kommunikation

Att kunna vara både långsiktig och responsiv vad gäller kommunikation är idag särskilt viktigt, detta i synnerhet i en situation med allvarliga och mer långdragna störningar. Osäkerhet och ett intryck av kontrollförlust kan utnyttjas av aktörer som har som målsättning att skapa oro och instabilitet i samhället, genom att det kan skapa mer gynnsamma förutsättningar för påverkansoperationer. Att vara transparent och kontinuerligt uppdatera allmänheten om relevanta delar av förloppet när en verksamhet utsätts för ett cyberangrepp kan bidra till att öka medvetenhet kring cyberhot, att äga narrativet och dämpa risken för spridning av felaktig information och i värsta fall våldsamma missnöjesyttringar.

Att Kalix kommun valde att fortlöpande uttala sig i media om vad som hänt bidrog förmodligen till att skydda och möjligen stärka kommunens trovärdighet gentemot kommunmedborgarna. Incidenten kan även ha bidragit till att såväl minska stigmat förknippat med att utsättas för ett cyberangrepp, som att förmå andra kommuner att se över sina cybersäkerhetslösningar. Samma kan nämnas om Coop, som den svenska medierapporteringen till stor del fokuserade på i fallet rörande Kaseya. Att man var transparent kan ha bidragit till att dämpa eventuella missnöjesyttringar mot stängda livsmedelsaffärer såväl som bristande

27. (2018-05-14). Transportstyrelsens it-affär: Detta har hänt. SVT Nyheter. https://www.svt.se/nyheter/inrikes/transportstyrelsens-sakerhetsskandal-detta-har-hant
28. (2021) MUST årsöversikt. s.56. https://www.forsvarsmakten.se/siteassets/4-om-myndigheten/dokumentfiler/rapporter/musts-arsoversikt-2021-.pdf

cybersäkerhetslösningar. Dessutom kan detta ha fungerat som en demonstration av motståndskraften mot de relativt kortvariga lokala samhällsstörningarna, som i dessa fall var robusta.

3.4 Vikten av samverkan och kompetensutveckling

En annan viktig säkerhetsåtgärd inom kommunikationsområdet är säkra och insynsskyddade forum och nätverk där medlemmar kan dela information och erfarenheter. I denna typ av forum kan exempelvis aktuella cyberangrepp lyftas och diskuteras och medlemmarna kan hjälpas åt att utröna om man utsatts för ett isolerat, standardmässigt DDoS-angrepp eller om det går att observera mönster eller indikationer på att angrepp är samordnade, om andra medlemmar utsatts osv.

Kunskapen om cybersäkerhet behöver förbättras i alla delar av samhället, både genom ökad medvetenhet bland allmänheten, men också genom att höja den specialiserade kompetensen. Genom att öka medvetenheten om cybersäkerhet bland medborgare stärks den kollektiva resiliensen mot de vanliga typer av angreppsmetoder, till exempel phishing, som potentiellt kan tillfoga organisationer och i förlängningen samhället stor skada. Dessutom kan en ökad medvetenhet om cyberhot förbereda medborgare på eventuella störningar, samt öka förståelsen för de konsekvenser som ett cyberangrepp kan innebära. Med andra ord, om det finns en viss nivå av motståndskraft hos befolkningen behöver inte försenade tåg, stängda livsmedelsbutiker eller driftstörningar i bankväsendet uppfattas som samhällets undergång.

”Kunskapen om cybersäkerhet behöver förbättras i alla delar av samhället, både genom ökad medvetenhet bland allmänheten, men också genom att höja den specialiserade kompetensen”

FRA betonar i sin senaste årsrapport att cybersäkerhet kräver engagemang på högsta nivå och måste vara en fråga för styrelser och ledningsgrupper och inte ett ansvar som stannar hos IT-chefen [29].

En viktig säkerhetsåtgärd är således att höja

29. (2021) FRA årsrapport. s. 5, https://www.fra.se/download/18.3262020817e4dcd6ffc257/1652872280257/FRA-arsrapport-TGA-2021.pdf

kunskapen om cybersäkerhet hos ledningsgrupper och styrelser genom målgruppsanpassade utbildningar med stöd i den senaste forskningen och tekniken. Ledningar behöver även acceptera att cybersäkerhet kostar pengar, men det bör ställas i relation till priset för alltför låg prioritering på cybersäkerhet och bristande cybersäkerhetsmedvetande hos anställda. En värdefull investering i cybersäkerhet är tester där sytem och organisationer utsätts för cyberangrepp under säkra och kontrollerade former i övningsmiljöer inriktade på detta område.

Behovet av kompetens inom cybersäkerhet är stort och en säkerhetsåtgärd som behöver prioriteras är att öka antalet cybersäkerhetsexperter. Enligt vissa uppskattningar saknas närmare 200 000 cybersäkerhetsexperter i Europa för att kunna bemöta cyberangrepp och hitta lösningar [30]. Ett initiativ för att möta detta behov är Cybercampus, som är ett samarbete mellan Kungliga tekniska högskolan, forskningsinstitutet RISE, Försvarsmakten och MSB för att stärka och samla utbildning, forskning och kompetens i en gemensam satsning. Om det blir verklighet ska andra myndigheter, företag och universitet också kunna delta i arbetet för att stärka cybersäkerheten. Ytterligare ett initiativ är nyinrättade Nationellt cybersäkerhetscenter. Syftet med cybersäkerhetscentret är att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot som utgör en av källorna till de IT-incidenter som drabbar Sverige. Inom ramen för denna nya plattform ska de deltagande myndigheterna bland annat koordinera arbetet för att förebygga, upptäcka och hantera cyberangrepp och andra IT-incidenter samt förmedla råd och stöd avseende hot, sårbarheter och risker. Samverkan med privat sektor utgör en viktig del av centrets uppdrag [31].

30. (2022-04-29). Sårbarhet och säkerhet i fokus. Kungliga tekniska högskolan. https://www.kth.se/om/nyheter/centrala-nyheter/sarbarhet-och-sakerhet-i-fokus-1.1166119
31. https://www.ncsc.se/

Kontakt:
Kim Elman
Centrum för cybersäkerhet
kim.elman@ri.se
070 518 17 47

www.ri.se/sv/centrum-for-cybersakerhet

RI.
SE