2021

Cybersäkerhet i Sverige

– i skuggan av en pandemi

FRA

FÖRSVARSMAKTEN

MSB Myndigheten för samhällsskydd och beredskap

Polisen

PTS

Säkerhetspolisen

Grafisk form: Sinfo Yra
Illustrationer: Matilda Petersson
Foto: iStockphoto

Innehåll

Inledning

Denna rapport syftar till att presentera lärdomar dragna utifrån hur covid-19pandemin (hädanefter pandemin) har påverkat Sveriges cybersäkerhet och att lämna rekommendationer för hur det går att förbereda sig inom cybersäkerhetsområdet inför en ny stor kris. Rapporten har avgränsats till händelser under 2020 och utgår från ett nationellt perspektiv.

Målgruppen för rapporten är beslutsfattare inom offentlig och privat verksamhet som arbetar inom cybersäkerhetsområdet, med kontinuitets- och beredskapsplanering samt ledningsgrupper.

Rapporten är framtagen av Försvarets radioanstalt (FRA), Försvarsmakten, Myndigheten för samhällsskydd och beredskap (MSB), Polismyndigheten, Post- och telestyrelsen (PTS) samt Säkerhetspolisen, inom ramen för det nyinrättade nationella cybersäkerhetscentret.

Inledningsvis beskrivs hotaktörers agerande under pandemin. Därefter redogörs för de observationer som gjorts avseende svenska verksamheters agerande. Ur dessa dras sedan lärdomar som resulterar i ett antal rekommenderade åtgärder.

Rapporten har medvetet undvikit att i detalj peka ut specifikt berörda verksamheter. Anledningen är bland annat att inte i onödan peka på sårbarheter hos dessa.

BEGREPP

- Med **hotaktör** avses statliga eller till en stat knuten aktör likväl som rent kriminella aktörer som på ett eller annat sätt bedriver en verksamhet mot svenska intressen som kan beskrivas som säkerhetshotande.
- Begreppet **verksamhet** är i rapporten en medvetet bred definition. Begreppet omfattar institutioner såsom myndigheter, statliga, kommunala och privata bolag, organisationer och andra typer av sammanslutningar.

Hotaktörers agerande

Då en pandemi har global påverkan är det naturligt att även hotaktörer påverkas av pandemins konsekvenser. Detta kan innebära ändrad inriktning från uppdragsgivare eller att det uppstår nya sårbarheter att utnyttja med anledning av krisen.

Flera hotaktörer utnyttjade människors oro och intresse för pandemin och smittskyddsåtgärder. Pandemin belyser hur hotaktörer utnyttjar aktuella omvärldshändelser för att förleda eller locka till sig måltavlors uppmärksamhet. Att utnyttja händelser med högt nyhetsvärde för att förleda någon eller locka till sig uppmärksamhet är dock inte unikt för pandemin. Företeelsen är en beprövad metod som används av såväl kriminella som statliga aktörer generellt. Under pandemin yttrade sig detta genom bland annat nätfiske, där pandemin användes som lockbete för att lura mottagaren att göra något skadligt. Ett annat exempel är bedrägliga mobilapplikationer och hemsidor som utgav sig för att bistå med information om pandemin.

I de blå rutorna i följande två kapitel beskrivs några exempel på ageranden under pandemin.

Kriminella aktörer var snabba på att kapitalisera på människors intresse för pandemin. Aktörer publicerade tidigt skadliga webbplatser med smittspridningskartor och även applikationer till mobiltelefoner som innehöll skadlig kod. Smittspridningskartorna förmedlades även som vanliga program, som tilltänkta offer lurades att installera.

Statsunderstödda cyberoperationer bedrivs generellt utifrån underrättelsebehov kopplade till nationella prioriteringar.
De kan syfta till att ge det egna landet utrikes- och säkerhetspolitiska fördelar eller till att skapa konkurrensfördelar för inhemska företag. Sådana cyberoperationer bedrivs av grupper inom staters säkerhets- och underrättelsetjänster, alternativt av grupper som utför cyberoperationer på uppdrag av dessa tjänster. Sådana grupper benämns ofta Advanced Persistent Threat (APT).

Som en följd av pandemins globala påverkan fick vissa stater ett utökat underrättelsebehov avseende vaccinforskning och olika länders strategier för att hantera och motverka smittspridning.
Statliga aktörer var snabba med att anpassa sin verksamhet utefter de ändrade nationella behoven och agerade tidigt i krisens skede. Det utökade underrättelsebehovet yttrade sig i att flera statliga aktörer uppvisade ett utökat intresse för företag, myndigheter och forskningsinstitut inom hälso- och sjukvårdssektorn globalt. I samband med detta utsattes även verksamheter i Sverige.

Enligt en offentlig rapport från brittiska, kanadensiska och amerikanska cybersäkerhetsmyndigheter har en gruppering kallad APT29 under 2020 angripit olika organisationer som är involverade i utvecklingen av vaccin mot covid-19 i Kanada, USA och Storbritannien.

Läs mer på
https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development

Statliga aktörer fortsatte även med verksamhet kopplad till ordinarie underrättelsebehov under pandemin.
Hotet från statliga aktörer kvarstod i oförminskad styrka och pandemin belyser hur cyberangrepp utgör ett viktigt verktyg även under kriser.

Cyberkriminalitet är ofta en gränsöverskridande brottslighet som riktas mot såväl enskilda individer som privata och offentliga verksamheter.
Aktörer som bedriver cyberkriminalitet kan vara allt från enskilda individer till professionella grupper. Gemensamt är att kriminella aktörer i huvudsak drivs av ekonomiska incitament.

I Europa har en uppgång i cyberrelaterade brott rapporterats under pandemin.
Den internationellt rapporterade uppgången i cyberrelaterade brott speglas inte i antalet inrapporterade brottsanmälningar i Sverige. Det går inte heller att belägga en uppgång i antalet inträffade incidenter, utifrån den rapportering som inkommer till MSB. Utifrån rapporteringen har varken antalet incidenter i stort eller antalet incidenter som orsakas av antagonistiska handlingar ökat under perioden. Det finns dock ett stort mörkertal över cyberrelaterade brott i Sverige, och det har troligen ökat under pandemin.

Kriminella aktörer utnyttjade förändringar i verksamheters tekniska infrastruktur för distansarbete.
Den ökade användningen av fjärrinloggningstjänster har bland annat utnyttjats genom så kallade *password spraying*-attacker för att få åtkomst till verksamheters interna nätverk.

Smittskyddsåtgärder har inte nödvändigtvis begränsat kriminella aktörer i sina möjligheter att verka.
Kriminella aktörer har få geografiska begränsningar för sin verksamhet. Angrepp och annan olaglig verksamhet kan utföras hemifrån. Smittskyddsåtgärder, exempelvis i form av karantänsrelaterade nedstängningar, har därför inte nödvändigtvis begränsat kriminella aktörer i sina möjligheter att verka.

Verksamheters agerande

Under 2020 ställdes verksamheter i Sverige inför stora utmaningar med anledning av pandemin. De rekommenderade smittskyddsåtgärderna, såsom att jobba hemifrån och hålla fysisk distans, innebar i många fall ett stort förändringsarbete och nya arbetssätt för att kunna verka trots rådande förhållanden. I detta snabba förändringsarbete har verksamheter behövt väga olika risker mot varandra, exempelvis smittspridningsrisken kontra risker inom cybersäkerhet. Det här kapitlet tar upp olika observationer gällande verksamheters agerande och andra förändringar som rör cybersäkerheten i Sverige.

Det uppstod snabbt ett behov av att hitta nya arbetsformer som kunde fungera i samband med fysisk distansering.

För många innebar pandemiutbrottet att arbetsplatsen förflyttades till hemmet och att nya digitala kommunikationslösningar och tjänster infördes. Säkerhetshöjande åtgärder har i vissa lägen fått stå tillbaka då verksamheter begränsade användningen av sin personal för att prioritera beredskap inför potentiella it-incidenter.

En grundläggande förutsättning för att klara den stora omställningen till distansarbete och ökad digital kommunikation var infrastrukturen för elektronisk kommunikation.
Driften av näten har varit stabil och det uppstod inte heller några kapacitetsproblem i Sverige. Operatörerna var snabba med att ställa om, bland annat genom att aktivera kontinuitetsplaner, införa åtgärder för att minska smittspridning samt skapa

förutsättningar för uthållighet. Flera operatörer hade en uttalad prioritering av att vidmakthålla drift framför utbyggnad eller förändringsarbeten.

Operatörer noterade förändringar i användarbeteenden under den första perioden av pandemin. Den fasta datatrafiken ökade under dagtid hos vissa operatörer med cirka 30 till 50 procent och på kvällstid med cirka 15 till 20 procent. Vad gäller mobil datatrafik ökade uppladdningen med cirka 50 procent i en operatörs nät, sannolikt på grund av videokonferenser. De ökade trafikvolymerna medförde inga kapacitetsproblem hos operatörerna.

De verksamheter som var förberedda med redan genomförda informationsklassningar av befintliga informationstillgångar hade lättare att snabbt implementera nya tjänster med adekvat säkerhet för ändamålet.
De kunde identifiera krav på kryptering, krav på användarnas behörigheter, behov av autentisering och vilka system, utrustning eller applikationer som får användas för att hantera informationen.

Under januari till september 2020 ökade antalet utgående leveranser från FRA av signalskydd (kryptosystem godkända för skydd av säkerhetsskyddsklassificerade uppgifter) till den civila sektorn med 38 procent jämfört med motsvarande period 2019. I mars 2020 var ökningen 112 procent. Ökningen beror till viss del på pandemin och behovet av distansarbete.

Nya och breddade kommunikationsbehov uppstod när arbetstagare arbetade på olika platser.
För att snabbt lösa verksamheters nya och breddade kommunikationsbehov har många verksamhetsutövare nedprioriterat eller i olika utsträckning övervägt cybersäkerhetsrisker eller riskhantering vid inköp och implementering av nya lösningar. I vissa fall innebar det att teknik införskaffades eller implementerades på ett ogenomtänkt eller otillräckligt sätt.
Exempelvis införskaffade många verksamheter en av ett fåtal populära tjänster. Detta fick till följd att andra verksamheter som hade behov av samma typ av tjänster fick ett extra incitament att också välja en av dessa. Det finns exempel på hur vissa av dessa tjänsteleverantörer snabbt hävdade att deras produkter hade ändamålsenliga säkerhetsfunktioner, trots att detta inte var korrekt.

Den 2 april 2020 gick CERT-SE ut med rekommendationer angående användning av en videokonferenstjänst. Rapportering från olika källor visade att intrång i flera fall hade skett på videokonferenser och att tjänsten var sårbar för specifika angreppsmetoder. Man noterade också att företaget bakom tjänsten hävdat att den omfattas av end-to-end-kryptering, men senare visade det sig att företaget hade menat något annat än det som normalt avses med begreppet.

Förflyttningen av arbetsplatsen till hemmet har inneburit en ökad exponering för cyberangrepp vilket skapat nya angreppsvägar.
På ordinarie arbetsplats kan verksamheter oftare ha en bättre kontroll över miljön som arbetstagaren befinner sig i, både vad gäller it-lösningar och den fysiska miljön. Möjligheterna till insyn i och uppföljning av säkerhetsloggning av trafik och nätverksuppkoppling kan försämras när arbetsplatsen förflyttas till hemmet. En annan risk är att arbetstagare använder privat utrustning som inte uppfyller säkerhetskrav för arbetet eller att man använder tjänsteutrustning för privat bruk på ett sätt som exponerar den för angrepp. I de fall tjänsteutrustning blivit infekterad i hemmamiljön ökar risken för att interna nätverk på arbetsplatsen blir

drabbade när utrustningen tas tillbaka till arbetsplatsen och kopplas in på nätverket. Många verksamheter har också behövt tillgängliggöra interna system genom ett ökat användande av fjärrinloggningstjänster, oaktat om detta är säkert eller inte.

Angrepp upptäcks inte alltid när de genomförs och det kan finnas en betydande fördröjning innan de upptäcks. Konsekvenserna av ett intrång, med exempelvis informationsförluster som följd, kan därmed bli att de upptäcks och blir kännbara lång tid efter att angreppet inträffat.

Under pandemin har antalet tillgängliga RDP-tjänster (Remote Desktop Protocol) i Sverige ökat med cirka 30 procent, från ungefär 20 000 i december 2019 till 26 000 i september 2020. Tjänsterna har i många fall kopplats upp direkt mot internet för att möta användarnas förändrade behov, ibland utan nödvändiga säkerhetsåtgärder såsom flerfaktorsautentisering. Detta medför en sårbarhet som hotaktörer har kunnat utnyttja genom exempelvis password spraying-attacker.

Förfrågningar om huruvida skyddsvärd verksamhet kunde bedrivas från hemmamiljö aktualiserades i ökad omfattning.
I många fall har arbetstagare i sin hemmamiljö inte fullgod möjlighet att skydda sekretessbelagd information. Många har exempelvis delat hemmakontor med familjemedlemmar under pandemin. I många hushåll finns dessutom smart hemteknik som kan fånga upp vad som sägs. Då kollegor inte träffas på den gemensamma arbetsplatsen ökar även risken för att känslig information kommuniceras i digitala tjänster som inte är tänkta att kunna hantera detta. Det finns exempel på hur gratistjänster för gemensamt arbete användes i väntan på upphandlad kapacitet i säkrade tjänster. En sådan hantering innebär en ökad risk för att obehöriga kan få tillgång till sekretessbelagd eller i övrigt känslig information.

Säkerhetspolisen har noterat en uppgång i antalet förfrågningar om rådgivning om hur krav på säkerhet ska tillämpas. Av innehållet i dessa förfrågningar går det att dra slutsatsen att ökningen kan relateras till de förändrade förutsättningar som pandemin skapade.

Planerade utvecklingsprojekt och säkerhetshöjande åtgärder senarelades eller ställdes in i större omfattning än normalt.
Det finns exempel på att löpande underhållsarbete till stöd för informations- och cybersäkerhet begränsats under pandemin: Därtill undvek flera tjänsteleverantörer av it-infrastruktur och -säkerhet att göra uppdateringar om det inte var absolut nödvändigt. Så var även fallet med många offentliga verksamheter.. Detta eftersom de ville begränsa användningen av sin personal till nödsituationer. Vidare vågade vissa verksamheter inte göra ändringar i sina system på grund av risken för oförutsedda problem till följd av åtgärden.

Att senarelägga eller ställa in underhållsåtgärder och utvecklingsinsatser i det kontinuerliga cybersäkerhetsarbetet innebär att det skapas en förvalt-

ningsskuld i en verksamhet. Konsekvensen blir att verksamheten ökar cybersäkerhetsriskerna.

Samhällsviktiga verksamheter valde i samband med pandemin att skjuta upp arbete med säkerhetsåtgärder. Dels krävdes it-kunnig personal för nya uppgifter som hade att göra med omställningen som pandemin krävde, dels innebar smittskyddsrekommendationerna att det blev svårt att bedriva arbete som krävde att personal samlades i fysiska utrymmen, såsom datahallar.

Skyddsvärden förändrades under krisen.
Med anledning av pandemin fick många verksamheter i Sverige på kort tid nya eller utökade uppdrag. Detta innebar att behovet av skydd dels ökade i deras ordinarie arbete, men även att det uppstod ett behov av högt skydd i nya tillgångar och processer. Ett tydligt exempel på detta är inom sjukvården där störningar skulle leda till större risk för förlust av liv. Den risken skulle exempelvis också bli större om allvarliga fel uppstod i den statistikföring som ligger till grund för beslut om folkhälsobestämmelser i Sverige. Behovet av att snabbt samla in data ledde också till att det uppstod känsliga informationstillgångar som en hotaktör skulle kunna använda för att skada eller hota enskilda individer, samhällsviktiga verksamheter eller Sverige i stort.

Under en kris är det även viktigt att allmänheten nås av korrekt information om vad som händer och hur den pågående situationen ska hanteras för att undvika förvirring och eskalering av krisen. Legitima informationskanaler såsom nyhetssidor och myndighetssidor blir då extra skyddsvärda eftersom behovet av pålitlig information är extra stort och många aktivt söker efter information.

Det är därför viktigt att höja nivån på cybersäkerhetsarbetet för flera verksamheter att kunna stå emot cyberangrepp från hotaktörer som tar tillfället i akt att agera i egna syften.

Den 9 december 2020 publicerade European Medicine Agency (EMA) information om att de utsatts för ett dataintrång. Hotaktören lyckades få åtkomst till intern och konfidentiell e-postkorrespondens avseende processerna för att utvärdera covid-19-vaccin. Delar av denna korrespondens manipulerades av aktörerna på ett sätt som enligt EMA var tänkt att underminera den allmänna tilliten till vaccin när resultatet av utvärderingen slutligen publicerades på internet.

Verksamheter behövde genomföra vissa förändringar snabbt. Detta omöjliggjorde användning av verksamhetens ordinarie rutiner.
Till följd av att många verksamheter på kort tid fick nya eller utökade uppdrag uppstod behov av samordning och ledning, företrädelsevis inom det svenska sjukvårdssystemet. För att tillgodose behoven togs det på relativt kort tid fram informationssystem som kunde understödja en lägesbild över kapacitet, påverkan och resursbehov. Eftersom informationssystemen behövdes omgående byggdes de i många fall på redan befintliga lösningar vilka tagits fram i annat syfte. Då sådana informationssystem är skyddsvärda ur flera perspektiv medförde det utmaningar för säkerhetsorganisationen som kravställare, kontrollfunktion och möjliggörare. Sådana snabba förändringar kunde därför i vissa fall inte genomföras enligt ordinarie rutiner där informationsklassning, riskanalys och säkerhetsskyddsanalys är grundläggande inslag.

Många verksamheter hade redan befintliga brister i sitt ordinarie säkerhetsarbete vilket medförde ytterligare utmaningar vid hanteringen av den snabba omställningen.
En konsekvens av detta blev att bedömningen av hur verksamheter hade förändrats inte utreddes systematiskt. Därmed saknade vissa verksamheter relevanta underlag för beslut om extra säkerhetsåtgärder.

Flera samhällsviktiga verksamheter rapporterade att deras tjänsteleverantörer inte kunde tillhandahålla avtalad tjänst under en period.
Tillgängligheten och effektiviteten hos samhällsviktiga tjänster och verksamheter är ofta beroende av stöd eller underliggande tjänster som tillhandahålls av externa leverantörer. Ofta är dessa i sin tur beroende av tjänsteleverantörer i flera led.

Incidenter som rapporteras av myndigheter och leverantörer av samhällsviktiga respektive digitala tjänster har under året legat på normala, eller strax under normala, nivåer.
Avbrott hos tjänsteleverantörer till samhällsviktiga tjänster och verksamheter har i några fall pågått längre än vad de hade gjort under normala förhållanden, bland annat på grund av rekommendationer kring hur smittspridningen ska begränsas. Detta har medfört att vissa samhällsviktiga verksamheter har fått hitta alternativa, mindre effektiva eller mer resurskrävande, sätt att bedriva verksamhet. Pandemin har också inneburit ökade beroenden till digitala tjänster. När de har fallerat så har människor som är beroende av den samhällsviktiga verksamheten drabbats hårdare än vad de skulle ha gjort av sådana incidenter under normala omständigheter.

Under pandemin har vårdenheter över landet tvingats utöka sina möjligheter att använda digital teknik som en del av den vård som bedrivs. Beroendet av sådan teknik har även ökat när smittskyddsåtgärder inneburit att anhörigas fysiska besök har fått ersättas av kontakt över digitala kommunikationstjänster. I ett fall drabbades en leverantör av digitala tjänster till flera vårdenheter av ett omfattande elavbrott som innebar att vårdenheterna inte kunde använda dessa. Detta ledde bland annat till att vårdtagarnas möjlighet att ha kontakt med sina närstående försvann.

Tjänsteleverantörer har haft svårare än vanligt att snabbt få fram information.
I flera fall har det när fel uppstått varit svårt för verksamheter att få information från sin leverantör om vad som hänt. Denne har i stället i sin tur hänvisat till sin egen leverantör av nätverkstjänster och hävdat att felet ligger där, och att det inte går att säga eller göra mer förrän de får information därifrån. Tjänsteleverantörernas möjligheter att snabbt få fram information om incidenter förvärrades på grund av vidtagna smittskyddsåtgärder. Samtidigt som den pressade situationen i vissa fall inneburit att behovet ökat av att snabbt få just sådan information, parallellt med att möjligheterna att verifiera denna information minskat. Den begränsade möjligheten att verifiera information kan bli ett stort problem när tjänsteleveransen är beroende av bakomliggande tjänster i flera led och där informationen som tas emot ska tolkas, kompletteras och sedan skickas vidare i flera led innan den når den samhällsviktiga tjänsten.

Lärdomar från pandemin

Följande lärdomar baseras på de observationer som har gjorts under 2020. Flera av dem bekräftar sådant som har observerats även innan pandemin, och som kommer att vara relevant även vid framtida kriser.

Förberedd står bättre rustad inför kriser.

En kris skapar oväntade utmaningar. För att hantera dessa på bästa sätt behöver verksamheter ha en hög nivå på sitt cybersäkerhetsarbete redan innan krisen slår till. Den som är förberedd har bättre förutsättningar att fatta snabba och korrekta beslut med bibehållen säkerhet.

Oförberedd kan tvingas ta fler eller större risker.

De verksamheter som inte är förberedda och inte har ett systematiskt och grundläggande säkerhetsarbete riskerar att i större utsträckning fatta beslut som ökar sårbarheterna för cyberangrepp. Det är vanligt att lösningar som tas fram akut blir permanenta och risken att utsättas för angrepp fortsätter tills dess att säkerhetsåtgärder är vidtagna. Under sådana omständigheter kanske det inte heller finns tid eller möjlighet att beakta konsekvenser för cybersäkerheten som uppstår till följd av verksamhetens krishantering.

Kriser tar fokus från mycket annat.

Under en kris är det naturligt att fokus i första hand ligger på att motverka krisen och dess negativa effekter, inte på åtgärder för att stärka cybersäkerheten. Detta leder till en ökad förvaltningsskuld.

Vad som ska skyddas vidgas och förändras under kriser.

Samhället blir mer sårbart under en kris och många samhällsviktiga verksamheter blir mer skyddsvärda som resultat av utökat ansvar. Samtidigt kan fler verksamheter, ny information och ny data bli skyddsvärda. Påverkan på dessa, i och med krisen skyddsvärda, verksamheter kan förvärra krisen ytterligare.

Cyberangrepp är ett viktigt verktyg för hotaktörer även under kriser.

Under en kris kvarstår hotet från statliga och kriminella aktörer. Hotet från dessa kan även öka mot vissa målgrupper och sektorer. Ett förändrat agerande kan uppstå snabbt och i ett tidigt skede av en kris. Statliga aktörer får en ändrad inriktning och kriminella tar tillfället i akt och utnyttjar ökad sårbarhet hos individer och verksamheter.

Rekommenderade åtgärder

Pandemin har inneburit nya eller förändrade hot och sårbarheter, samtidigt som redan existerade finns kvar. I en framtida kris är det möjligt att dessa hot och sårbarheter kan komma att få allvarligare konsekvenser för samhället än vad de fick under denna kris. Utifrån de lärdomar som dragits har rekommenderade åtgärder tagits fram, så att Sverige inför nästa stora kris ska stå bättre rustat på cybersäkerhetsområdet.

Skapa förutsättningar för att kunna agera i kris genom ett grundläggande cybersäkerhetsarbete.

Det är viktigt att ha ett löpande, systematiskt och riskbaserat informations- och cybersäkerhetsarbete som möjliggör snabba omställningar. Av samma skäl behöver riskbedömningar, säkerhetsskyddsanalyser för verksamheter och särskilda säkerhetsskyddsbedömningar för informationssystem vara utförda. Det är viktigt att säkerställa skyddet av det mest skyddsvärda då brister kan leda till omfattande långvariga skador som är svåra eller omöjliga att återställa. Även för verksamheter som inte omfattas av säkerhetsskyddslagen är motsvarande arbete viktigt för att inte bli av med affärshemligheter eller riskera sin tillgänglighet.

Verksamheter bör ha identifierat situationer som de av olika skäl inte får hamna i. Genom att på förhand identifiera gränser och nivåer för sin risktolerans skapas en tydlighet. När förändringar sker snabbt kan detta användas för beslut om vilka insatser som behöver ske och när, för att undvika oacceptabla konsekvenser.

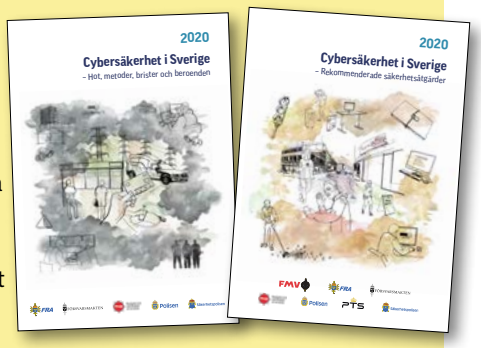
Planera för att ha kontinuitet vid en kris.

Verksamheters kontinuitets- och krisplaner ska alltid adressera cybersäkerhet. I det kontinuerliga cybersäkerhetsarbetet ingår att ha genomarbetade och övade kontinuitetsplaner som tillåter en snabb omställning från etablerade till alternativa arbetssätt. Dessa planer bör på ett konkret sätt beskriva hur arbetet kan fortsätta under kriser, både rutinmässigt och tekniskt. Pandemin har bland annat visat på behovet av att planera för säker kommunikation även under distribuerade arbetsformer.

Organisationer bör som regel inkludera förberedelser för säkert distansarbete i sina kontinuitetsplaner. Genom att ta fram en plan för hur arbetet kan fortgå även om personal behöver befinna sig på annan plats, blir övergången smidigare och säkrare. Ett bra stöd är att ha uppdaterade riskanalyser som ger insikter om riskbilden vid alternativa arbetssätt innan omställningen påbörjas.

TÄNK PÅ

Genom att höja den generella säkerhetsnivån ökar motståndskraften mot många cyberhot. I de båda rapporterna *Cybersäkerhet i Sverige – Hot, metoder, brister och beroenden* samt *Cybersäkerhet i Sverige – rekommenderade säkerhetsåtgärder* har flera myndigheter i samverkan lämnat en grundläggande bakgrundsbeskrivning samt gemensamma råd om vilka åtgärder som rekommenderas att införa. Dessa råd ersätter inte ett systematiskt säkerhetsarbete utan är ett stöd för prioriteringsarbetet.



En del av kontinuitetsplaneringen bör även vara att planera för hur cybersäkerhetsarbetet ska genomföras vid bortfall av personal.

Verksamheter med höga krav på kontinuitet behöver redan i sina avtal med underleverantörer ta hänsyn till krissituationer. Man behöver även kommunicera generellt hur man ser på leverantörens roll i sin krisplanering och involvera leverantörerna i övningar. I de fall underleverantören i sin tur är beroende av andra leverantörer bör kravställning utföras på ett sådant sätt att snabb information om inträffade incidenter säkerställs.

Organisationer bör ha en prioriteringslista för underhåll och utveckling av system som oundvikligen behövs eller som innehåller kritisk eller känslig information, samt välja ut vilka projekt som kan pausas. En kris kan dock behöva en särskild rutin för åtgärdsprioritering som beskriver under vilka omständigheter som vissa säkerhetsåtgärder ska prioriteras och hur det ska ske, och vilka som alltid ska utföras.

Ta fram rutiner för hantering av snabba förändringar.

Organisationer bör ha färdiga rutiner som med kort varsel kan vara stöd vid uppkomna situationer där beslut snabbt behöver fattas. Dokumentera en process som möjliggör snabba säkerhetsbedömningar när plötsliga behov av nya tekniska lösningar uppstår.

Säkerställ att verksamheten har tillgång till säkerhetskompetens för framtida och plötsliga omställningsperioder, exempelvis genom avtal med säkerhetskonsulter som kan bistå med expertis och erfarenhet.

Utse en befattning med ansvar för att godkänna nya tekniska eller administrativa lösningar i kriser. Inriktningen för sådana lösningar som behöver tas fram hastigt, bör vara att de ska vara temporära och hanteras enligt ordinarie rutin så snart tillfälle ges. Under långvariga kriser bör organisationer ge sig själva tid för detta. Det är lämpligt att öka säkerhetsövervakningen när hastiga lösningar tagits fram. Det ökar möjligheten till att upptäcka incidenter.

Uppdatera bedömningar av vad som ska skyddas.

Vid en kris behöver förändrade förutsättningar analyseras. Vid nya uppdrag behöver befintliga säkerhetsskydds- och riskanalyser uppdateras. Ett högre skyddsvärde innebär sannolikt att verksamhetens behov av cybersäkerhet ökar.

I säkerhetsskyddsanalysen bör det framgå vilka värden som är prioriterade för en verksamhet och hur dessa kan skyddas i olika krisnivåer. Prioritera hanteringen av risker som kan ge långa och svårhanterliga konsekvenser.

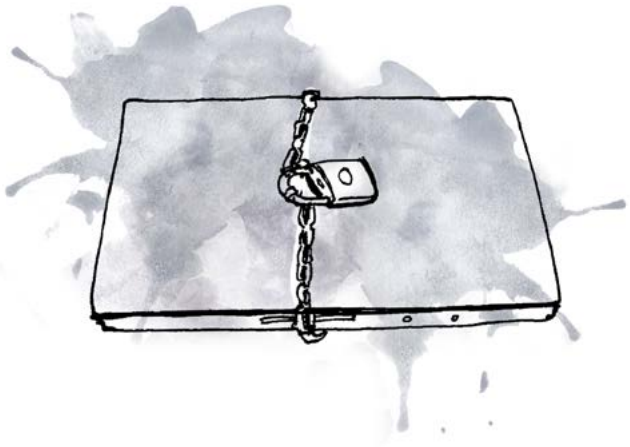
Organisationer bör i sina kontinuitetsplaner ta fram rutiner för hur existerande och tillkommande funktioners skyddsvärden ska bestämmas vid omställning till distansarbete.

Hantera och minimera förvaltningsskulden.

En kris och dess efterverkningar kan pågå under lång tid. Därför är det viktigt att säkerställa att eventuell förvaltningsskuld hanteras så snart som möjligt. Genomför säkerhetsuppdateringar eller andra säkerhetshöjande cybersäkerhetsåtgärder i möjligaste mån. Ju längre tid det tar att åtgärda en sårbarhet, desto högre blir risken att den utnyttjas av en hotaktör.

Verksamheter behöver så fort som möjligt undersöka vilka infrastrukturella och tekniska förändringar som genomförts under krisen som kan ha bäring på cybersäkerheten. Ett sätt är att analysera den förändrade riskexponeringen till följd av tekniska och administrativa förändringar, och ta fram eller modifiera en handlingsplan utifrån detta.

Det är lämpligt att kontinuerligt genomföra säkerhetsgranskningar av driftsatta informationssystem. Nya tekniska lösningar bör säkerhetsgranskas i de fall detta inte har gjorts och säkerhetshöjande åtgärder implementeras. När resurser finns tillgängliga bör man åtgärda eventuella säkerhetsbrister som kan ha uppstått som en följd av åtgärder man har vidtagit för att hantera krisen.



Informera om hoten och riskerna.

En proaktiv åtgärd är att skapa förståelse inom verksamheten för att cyberhotet kvarstår även under kriser och att hotaktörer tar tillfället i akt att agera. Att hålla en hög nivå på cybersäkerheten är viktigt även under kriser och genom att främja medvetenheten om hot och risker hos personalen stärks säkerhetskulturen.

Om verksamheter har färdiga material om olika former av cyberhot och hur de kan bemötas kan dessa snabbt anpassas efter krisens karaktär. Information om cybersäkerhet och hur arbetet bedrivs för att skydda verksamheten och stoppa cyberangrepp är också en säkerhetshöjande åtgärd som kan höja säkerhetsmedvetandet.

Flera myndigheter och privata företag analyserar och kommunicerar kontinuerligt hotbilder som kan användas i den egna analysen av vilka hot man bör förhålla sig till i sitt cybersäkerhetsarbete.

Utbilda och öva personalen.

Stötta medarbetarna genom att ta fram riktlinjer, rutiner och utbildningar. Informera proaktivt om hur krisen påverkar cybersäkerheten. Då minskar risken för misstag och säkerhetskulturen stärks. När organisationen införskaffar nya tjänster och lösningar är det viktigt att samtidigt informera om hur de kan och bör användas, för att undvika onödiga risker.

Genomför övningar med cybersäkerhetsfokus och en nära koppling till det dagliga arbetet för att skapa en rutin och vana att hantera incidenter och större påfrestningar. Variera gärna scenarier ur perspektiven konfidentialitet, riktighet eller tillgänglighet för övningarna, så att en bred medvetenhet skapas. Övningar kan även bidra till att stärka och utveckla både det ordinarie cybersäkerhetsarbetet och kontinuitetsplaneringen. Genom att exempelvis genomföra enkla övningar med utgångspunkt i hur pandemin påverkade verksamhetens arbete med cybersäkerhet kan nya insikter nås.

Anmäl och rapportera incidenter för att stärka den nationella motståndskraften mot cyberangrepp.

Genom att anmäla brott och rapportera incidenter får centrala myndigheter vetskap om händelser och kan agera utifrån sitt uppdrag, exempelvis bekämpa och förebygga brottslig verksamhet. Myndigheterna får då också ett bättre underlag om vad som händer. Information som lämnas i samband med incidentrapporteringar behövs för att upprätthålla och utveckla lägesbilden, för att kunna varna och informera andra och för att kunna engagera resurser i syfte att lösa uppkomna problem.

Slutord

Den övergripande bedömningen är att Sverige i stort har mött utmaningarna kring cybersäkerheten under pandemin väl. Det finns dock en risk för att incidenter som inträffar under och med anledning av pandemin kommer att upptäckas långt senare, vilket kan påverka cybersäkerheten framöver. Mot bakgrund av den pågående smittspridningen i samhället är det sannolikt att smittskyddsåtgärder och hotaktörers utnyttjande av pandemin fortsatt kommer att vara en utmaning för cybersäkerheten i Sverige, som kommer att kräva fortsatta cybersäkerhetsåtgärder.

Under och efter krisen behöver erfarenheter kontinuerligt samlas in och analyseras för att kunna stärka motståndskraften mot cyberhot. Pandemin är inte den sista kris som kommer att drabba Sverige.

Rapporten syftar till att presentera lärdomar dragna utifrån hur covid-19pandemin har påverkat Sveriges cybersäkerhet samt att lämna rekommendationer för hur det går att förbereda sig inom cyber-säkerhetsområdet inför en ny stor kris.

Den är framtagen av Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen samt Säkerhetspolisen, inom ramen för det ny-inrättade nationella cybersäkerhetscentret.

FRA

FÖRSVARSMAKTEN

MSB Myndigheten för samhällsskydd och beredskap

Polisen

PTS

Säkerhetspolisen