PRAKTISK CYBERSÄKERHET

FÖR MOBIL- OCH DATORANVÄNDARE, SYSTEMADMINISTRATÖRER, CIO´S, DATACHEFER, LINJECHEFER SAMT LEDNING OCH STYRELSE

STOCKHOLM, FEBRUARI 2023

Praktisk cybersäkerhet för:

- Mobil- och datoranvändare
- Systemadministratörer, CIO´s och datachefer
- Linjechefer
- Ledning och styrelse

Stockholm, februari 2023

Redaktör: Nils Bildt

Medförfattare: Anders Candell, Hugo Barklund, Marcus Murray, Mats Mägiste, Nils Bildt, Patrik Fällström, Pontus Johnson, Staffan Truvé, Ulrik Franke

Källor & Bearbetningar: Cisco, Concia, Foreign Affairs, F-secure, IVA, KTH, Lockheed Martin – Mitre Attack Framework, Microsoft support, Moderaterna, MSB, NCSC, Netnod, Recorded Future, Telia, TrueSec, UK Cyber Reserve Force, mfl.

Detta dokument är tänkt att vara en instruktion och/eller påminnelse för olika personalkategorier och för att göra informationen så användbar som möjligt så används tre skedestyper:

	Före en cyberattack	**Pågående cyberattack**	**Efter en cyberattack**
Medarbetare	Kap 2.1	Kap 2.2	Kap 2.3
IT/System-ansvariga	Kap 3.1	Kap 3.2	Kap 3.3
Linjechefer	Kap 4.1	Kap 4.2	Kap 4.3
Företagsledningar	Kap 5.1	Kap 5.2	Kap 5.3

Tanken är att en person som har någon av rollerna ovan och befinner sig i ett av de nämnda skedena, snabbt och enkelt skall kunna ”slå upp” sin flik och läsa på om åtgärder.

Innehåll

1 Förord

Den 25 februari 2022, dagen efter Rysslands invasion av Ukraina, samlades ett antal Officerare i näringslivet med ansvar och erfarenhet i cyberfrågor. Samhället och det militära försvaret fungerar inte utan ett kraftfullt cyberförsvar som säkrar grundläggande samhällsfunktioner och det militära försvarets förmåga.

Närvarande var Genmj Stefan Kristiansson, tidigare C MUST, dvs den Militära Underrättelse- och säkerhetstjänsten, Håkan Buske, tidigare VD SAAB och chef för Ingenjörsvetenskaps-akademins (IVA´s) arbetsgrupp för Cybersäkerhet för ökad konkurrenskraft, samt Lars-Johan Jarnheimer, ordförande i TeliaSonera med flera. De tre pekade på behovet av praktiska råd; vad kan och bör alla veta och göra; före, under och efter ett cyberangrepp, på alla nivåer i ett företag, organisation eller förvaltning.

Företagsledare och alla i beslutande ställning behöver förstå cyber på riktigt som en del av den kontinuitetsplanering de ansvarar för. Idag är vissa vilsna och tror att det "hanteras" av IT-avdelningen". Ansvariga chefer måste äga frågan och tydligt behålla ansvaret men delegera arbetsuppgifter. Alla behöver veta vad de kan och bör göra.

Ingenjörsvetenskapsakademin, lanserade nyligen "Cybersäkerhet för ökad konkurrenskraft" med politiska råd. Kungliga Krigsvetenskapsakademins skrift " Cyberförsvaret - en introduktion" betonar vikten att omsätta allmänna resonemang till praktiskt användbara råd och åtgärder. Parallellt lanserade den liberala takesmedjan Fores, med stöd av bland andra Genmj Stefan Christiansson, "Sveket mot Cybersäkerheten" som också pekade på behovet av praktiska råd.

MSB, Myndigheten för Samhällsberedskap har givit ut allmänna råd, men behovet, bredden och omfattningen är större än så. Utvecklingen i Ukraina visar tyvärr på behovet av starkt militärt och ett robust samhällsförsvar, dvs behovet av kunskap om cyber i ett totalförsvars-perspektiv där alla vet vad de kan och bör göra för att bistå och säkra samhällsfunktionerna.

Resultatet av mötet den 25 februari är denna skrift med praktiska råd till chefer och hand-läggare om hur hantera cybersäkerhetsfrågor vid myndigheter, företag och andra organisationer. Den kan ses som en fortsättning på både Ingenjörsvetenskapsakademins och Kungl Krigs vetenskapsakademiens inventering av de förutsättningar som behöver uppfyllas för att skydda samhället mot olika typer av cyberhot.

Nils Bildt
Stockholm, februari 2023

1.1 Inledning

Utan bra IT- och Cyberförsvar samt kontinuitetsplanering, så är det risk att din dator stannar, och dessutom din mobil, din elleverantör, din teleoperatör, bussar & transporter, din bank, dina kunder, din kommun, våra myndigheter, vårt försvar, ja – allt!

Kriminalitet på nätet ökar dramatiskt, liksom påverkansoperationer från andra stater för att påverka dig omärkbart och alla andra i vårt samhälle i stor skala med dunkla syften. Inför ett krig kommer storskaliga cyberattacker att ingå i en angripares plan att försvaga eller förlama samhället!

Företagsledningar av idag måste hantera cyberhot som alla andra hot i sitt rullande säkerhetsskyddsarbete.

Att jobba proaktivt och hantera IT-risker och cyberhot löpande måste bli det nya normala.

1.2 Det pågående cyberkriget, vi är redan under attack!

Målen för attackerna behöver ej – inledningsvis - vara direkt militära.
Målen kan vara:

Förstå scenarier och mål kan bestå i stöd och kampanjer för att väcka debatt, förstå opinioner och för att få andra att delge information för att i sin tur kunna identifiera och kartlägga uppfattningar om nyckelpersoner och beslutsfattare. Det kan gälla attacker för att förstå hur försvaret är uppbyggt, vilka svarstider och resurser som finns, var gränserna finns och hur man kan röra sig mellan olika domäner och ansvarsområden.

Förbereda scenarier och mål kan bestå i att skapa vilande ”dissidentplattformar” för kommande egna framtida förvillande/förvärvande och försvagande attacker. Förvillande scenarier och mål kan paradoxalt nog även bestå av infiltration och stöd till diffusa motsatta uppfattningar till de man själv företräder för att kunna ”härska och söndra”. Stöd ges av angripare till den svagare av polariserade diskussioner i det angripna landet, även om man inte delar uppfattningen. På det sättet ”förbereder” och stöttar de som inte har samma åsikt som de själva företräder. Detta ökar polariseringen och försvagar ledningen samt fördröjer och försenar beslutsprocesser.

Andra scenarion kan vara stöld av information för att använda i andra syften såsom stöld av Jägarregistret i syfte att få kännedom om vilka som potentiellt kan ha vapen och då kunna vidta andra åtgärder mot dessa.

Försvaga/förvärva scenarier och mål kan bestå av attacker så att samhällsviktiga digitala tjänster blir långsammare och ligger nere med överbelastningsattacker, dvs. DDOS, attacker för att minska tillgänglighet mot betalningssystemen som Bankgiro och Swish, eller attacker och insatser för att sänka prestanda som att slå ut en operatör som Telia kundsystem så att förtroendet för Telia och därmed aktiekursen sjunker. Det kan följas av

kampanjer med krav på proffsiga ägare, dvs ej staten, och åtgärder för att sänka kursen, så att privata P/E aktörer kan köpa in sig, ev. genom bulvaner, som senare säljer innehaven med vinst till annat lådföretag (kontrollerat av egna intressen).

Försvaga/förvärva scenarier kan även syfta till ekonomisk utpressning med ”ransomware” mot företag, förvaltning/riksbank och regering för att visa att man redan finns på Det kan följas av hot att stänga av kritiska delar samhället och ytterst göra det för att skapa kaos.

Därefter kan en angripare i förvirringen militärt komma in, besätta landet och ”sätta på strömmen” och ”förvärva” Sverige.

Andra scenarion som kan ske är att få tillgång till privilegier eller på annat sätt bedra personal så att man får tillgång till organisationers kassaflöden och på så sätt kunna överföra och stjäla pengar som kan användas till andra ändamål.

2 Medarbetare

2.1 Före en cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Cyber-hygien;
  - Starka lösenord som byts varje kvartal
  - Var vaksam på spam/phishing som vill lura dig att klicka på länkar med skadlig kod
  - Genomför de systemuppdateringar som åläggs från IT-admin
  - Läs och sätt dig in i ditt företags IT-säkerhetspolicies vad avser tex VPN vid uppkoppling på andras nätverk än dem som anses säkra

- Deltag i / efterfråga utbildning och träning.

- Var på din vakt vid spontana kontakter via telefon, Sms, chatt eller mejl där någon ber dig utföra någonting. Åter-ring/mejla till annan ”förmodad” kontakt för att testa giltigheten. Använd aldrig kortläsare eller BankID på någon annans uppmaning.

- Var extra försiktig med att utföra betalningsuppdrag via mejl. Säkerställ alltid att du pratar med rätt person och att kontouppgifter verkligen stämmer innan betalning utförs.

- Allt du gör på nätet kan observeras och registreras och användas för att bygga upp ”profiler” om dig, med en sådan information om dig - som inte ens din fru, man, partner eller dina vänner vet om dig.

- Datorer och mobiler kan avlyssna dig och filma dig. Stäng av datorn och mobilen när den inte används.

- Kontrollera avvikande information och uppgifter från okända avsändare eller från nya hemsidor. Kolla med flera och tidigare använda och säkra källor.

- Observera nätadresserna, dvs. URL, när du går in på okända hemsidor, så att de stämmer. Observera att 0 kan vara utbytt mot ett O och leda dig till en bedragare. Gå ner flera långt ned på webbsidor och kolla att dessa är aktuella och uppdaterade.

- Svara inte på okända adresser. Gör inga okända nedladdningar. Låt ingen okänd sätta in en USB i din dator. Låt ditt virusskydd kontrollera USB först.

- Var försiktig när det gäller att klicka på länkar eller bifogade filer i mejl eftersom ransomware annat som phishing till största del sprids på det sättet.

- Koppla inte in okända enheter i din dator eftersom det kan få till följd att oönskad mjukvara sprids från dessa enheter till din dator.

- Se till att du använder en modern och uppdaterad webbläsare.
- Besök inte oseriösa webbplatser (piratsidor, porrsidor, tvivelaktiga kontaktsiter osv.) eftersom dessa kan vara infekterade och försöka utnyttja sårbarheter i din webbläsare eller andra program.
- Ladda inte ned filer från opålitliga sidor.
- Använd inte ett administratörskonto till vardags om du inte verkligen behöver det. Det ökar risken för att ransomware och annan oönskad mjukvara kan köras på din dator och spridas vidare till nätverksanslutna enheter.

2.2 Pågående cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Var lyhörd och genomför det du vet att du skall göra

Efterfråga instruktioner om där inte finns några, var aktiv och gör din del av jobbet

- Ifall du misstänker att du har öppnat en bifogad fil eller liknande som innehåller ransomware eller annan skadlig mjukvara bör du stänga av datorn så snart som möjligt och kontakta IT-support.

2.3 Efter en cyberattack

En incident ska ha ett väldefinierat slut. En definition är att det team som hanterat incidenten anser att de har dels lyckats återställa acceptabel funktionalitet, dels skapat sig en god överblick över incidenten. Detta avslut kan hanteras som ett möte där ett antal punkter slås fast, och alla på mötet godkänner protokollet. Detta möte kallas ofta ***post mortem.***

Deltagarna i en Post Mortem kan variera och vara olika i olika organisationer.

3 IT/System-ansvariga

3.1 Före en cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Planera och förbered med 3 års horisont
- Ha handlingsplaner för de fall som prioriterats av FTG-ledning
- Ha instruktioner och förberedda tillvägagångssätt till alla nivåer och enheter som utgör en risk

Öva strukturerat – Train-as-you-fight

3.1.1 Håll ordning & reda

- **Installera säkerhetsuppdateringar så fort det går**
  Prioritera att uppdatera informationssystem som exponeras mot internet, de som är verksamhetskritiska och de där sårbarheterna riskerar att utnyttjas. Ha som målsättning att installera säkerhetsuppdateringar snarast efter att de publicerats.

- **Förvalta behörigheter och använd starka autentiseringsfunktioner**
  Ha kontroll på alla konton i it-miljön, inaktivera de som inte används. Var strikt med de behörigheterna som är tilldelade. Använd flerfaktorsautentisering på alla publikt exponerade tjänster, för åtkomst till information med högt värde och för konton med systemadministrativa behörigheter. Där flerfaktorsautentisering inte stöds använda unika och långa lösenord.

- **Begränsa och skydda användningen av systemadministrativa behörigheter**
  Använd separata konton för systemadministrativa behörigheter. Avgränsa även de systemadministrativa behörigheterna till uppgifter, roller och delar i it-miljön. Tilldela inte vanliga användare systemadministrativa behörigheter.

- **Inaktivera oanvända tjänster och protokoll (härda systemen)**
  Säkerställ att funktioner som inte behövs för önskvärd funktionalitet i informationssystemen stängs av, blockeras eller avinstalleras. Konfigurera informationssystemen att ha en hög säkerhet.

- **Gör säkerhetskopior och testa om informationen går att läsa tillbaka**
  Skapa säkerhetskopior på information med regelbundenhet utifrån verksamhetens behov. Hantera säkerhetskopiorna säkert och testa periodiskt att det går att återställa informationen utifrån tagna säkerhetskopior.

- **Tillåt endast godkänd utrustning i nätverket**
  Endast tillåten utrustning får kopplas till nätverket. Otillåten utrustning behöver upptäckas och dess åtkomst till tjänster och information i it-miljön förhindras.

- **Säkerställ att endast godkänd mjukvara får köras (vitlistning)**
  Endast tillåten mjukvara får köras i it-miljön. Förhindra att otillåten programvara körs.

- **Segmentera nätverken och filtrera trafiken mellan segmenten**
  Upprätta olika nätverkssegment och skapa kontrollerade trafikflöden mellan segmenten med hjälp av filtreringsfunktioner som skyddar mot att oönskad trafik kan flöda fritt i nätverket.

- **Uppgradera mjuk- och hårdvara**
  Byt ut och ersätt föråldrad hård- och mjukvara för att motverka sårbarheter som över tiden exponerats och för att få avsedd funktion och tillräcklig säkerhet.

- **Säkerställ en förmåga att upptäcka säkerhetshändelser**
  Skaffa förmågan att upptäcka säkerhetshändelser i IT-miljön så tidigt som möjligt. Övervaka händelser i it-miljön med manuella, tekniska och automatiska åtgärder. Skapa säkerhetsloggar som kan användas för övervakningen och som skyddas mot obehörig åtkomst eller förändring.

- **Se regelbundet över företagets och egna fullmakter och beloppsbegränsninga**
  Ha flera personer involverade i att godkänna betalningar. Tänk på att rensa bort behörigheter för tidigare anställda.

3.1.2 Systemadministrativa rättigheter

- **Ta bort onödiga administratörsrättigheter på klientdatorer**
  Detta är den enskilt viktigaste metoden för att förbättra klientsäkerheten. Utmaningen är att hitta balansen mellan säkerhet och användarens produktivitet. Denna balans beror naturligtvis på de specifika kraven i din organisation. Ju färre administratörsrättigheter som delats ut desto färre möjligheter finns för skada rent generellt. Det finns även metoder för att öka flexibiliteten för användaren, men minska riskexponeringen i vardagen. Ett exempel på detta kan vara tillfälligt utdelad administratörsrättighet som automatiskt tas bort t.ex. efter ett dygn.

  Det viktiga är att hitta metoder som gör att administratörsrättigheter stannar hos personer som skall ha dem och att de tas bort så fort individens roll förändras eller de inte längre behövs.

  En organisations vanligaste dilemma är att behörigheter stannar med individen och förnyas ”för säkerhets skull” även när de inte längre behövs.

- **Minimera antalet globala administratörer, men till minst 2**
  Endast globala administratörer kan återställa lösenordet för en annan global administratör, därför så rekommenderar vi att du har minst 2 globala administratörer i organisationen i händelse av kontoutelåsning. Har du riktigt känslig information bör de globala lösenorden var för sig vara skapade av två personer som bara tillfört halva lösenordet utan att känna till den andres del. Personerna har sedan låst in sina lösenordshalvor i förseglade kuvert i ett kassaskåp. På detta sätt finns ingen chans att lösenordet har läckts. Ingen enskild individ känner till lösenordet, men en manuell oberoende metod finns för att få fram lösenordet.

  Metoden är ett effektivt sätt att skydda globala administratorslösenord. För att fungera i praktiken kräver det att det går att utfärda underadministratörer eller alias.

  Superadministratörens lösenord används bara vid extrema situationer och måste då omedelbart ersättas. Denna metod kallas även för ”break the glass” precis som för brandlarmsknapparna i en byggnad.

- **Tilldela begränsade roller**
  Genom att tilldela begränsade roller får underadministratörerna bara den behörighet som behövs för att få jobbet gjort. Om du till exempel vill att någon ska återställa lösenord för anställda bör du inte tilldela den obegränsade rollen som global administratör, i stället kan du tilldela en begränsad roll som lösenordsadministratör eller supportadministratör. På så sätt skyddar du dina data bättre.

  Om ditt system har en revisorsfunktion (loggning), se då till att inte ens den globala administratören har access till denna, utan dela upp ansvaret strikt. På detta sätt kan inte någon som använt en administratörsbehörighet dölja några spår efter sig.

- **Konfigurera multifaktorautentisering (MFA)**
  Det är en bra idé att kräva MFA för alla användare, men administratörer i synnerhet bör använda MFA för att logga in. MFA gör att användarna måste använda ytterligare en identifieringsmetod för att verifiera sin identitet. Denna metod kan vara av engångskaraktär, åldras snabbt och ständigt förnyas genom tex. en app. eller lösenordsdosa.

  Observera att i alla system finns fortfarande en sista utväg, dvs. ett fast lösenord eftersom även ett multifaktorsystem kan sättas ur spel. Kontrollera därför alltid i dessa fall att superlösenordet inte används och att det är uppdelat och inlåst enligt beskrivningen på globala administratörer. Begränsa denna typ av inloggning till väldigt specifika platser/nät. Ett sådant konto skall typiskt inte kunna användas från en hemarbetsplats. Där används alltid MFA.

- **Kom ihåg att MFA inte automatiskt skyddar mot tex. utpressningssituationer där individen står under hot!**
  Har ni riktigt känslig hantering i några system, bör tex. den andra faktorn låsas in på kontoret efter arbetstid, eller så bör så kallad tvåhandsfattning tillämpas där ytterligare en oberoende person är inblandad för godkännandet av transaktionen.

3.1.3 Säkerhetskopiering om du gör det själv!

- Det är viktigt att ta säkerhetskopior regelbundet, ju mer aktuella kopior du har desto mindre förlorar du. Se även till att säkerhetskopiorna förvaras separat och inte är i ständig åtkomst med systemen som kopieras, för annars kan den skadliga koden kryptera säkerhetskopiorna också. Verifiera även att säkerhetskopieringen fungerar som den ska genom att testa att göra en återställning.

3.1.4 Försvar mot ransomware-attacker

Ransomware-attacker kan vara extremt skadliga när de väl händer. Men att förhindra dem är vanligtvis enkelt om du planerar i förväg.

- **Håll alltid ditt antivirus och alla andra kritiska program och system, uppdaterade**
  Vissa antivirusprogram har automatiska uppdateringar, medan andra inte har det. Oavsett kommer du att vilja vara noga med att se till att du har installerat alla de senaste versionerna, virusdefinitionerna och korrigeringarna som din leverantör skickar ut för att hålla sig förberedd. Du bör också uppdatera ditt operativsystem och andra viktiga programvaror regelbundet. Vanligtvis innehåller nya versioner eller uppdateringar kritiska säkerhetskorrigeringar som du inte vill ignorera.

- **Gör backup av din viktigaste data på ett separat nätverk eller enhet (kalla backups)**
  Om ransomware faktiskt kommer igenom dina försvar och infekterar din dator kan du minska dess inverkan ordentligt genom att säkerhetskopiera din data. Säkerhetskopior i molnet är fantastiska och kan vara praktiska, men i bästa fall gör du “kalla backups” av dina viktigaste filer. Detta innebär att du lagrar dem på en USB eller hårddisk som du håller helt åtskilda och inte inkopplade till din dator och nätverk.

- **Förebygg ransomware från början**
  Att ransomware hittar en bakdörr till din dator är en sak. Att öppna upp ytterdörren och välkomna den in är en annan!

  Praktisera alltid säkert beteende online för att undvika virus och annan skadlig programvara. Detta betyder: Undvik misstänkta och opålitliga webbplatser. Ladda bara ner programvara, appar och media från officiella marknadsplatser. Ladda aldrig ner e-postbilagor om du inte vet vad de är och vem de kommer från.

- **Koppla bort nätverket för att skydda andra datorer**
  Det sista du behöver är att ransomware sprids till en annan dator i ditt nätverk eller får tag på filer du har lagrat på en separat nätverksansluten enhet. Inaktivera din nätverksanslutning så snart du ser ransomware-varningen.

- **CMDB**
  Säkerställ att det i varje givet tillfälle finns en lista, eller hellre automatiskt uppdaterad databas över informationstekniktillgångar (CMDB). Den databasen är ett uppdaterat register över både fysiska och logiska tillgångar, var de finns både fysiskt och logiskt, vilka versioner av mjukvara och hårdvara som används, vem som ansvarar för dessa samt annan information som organisationen kan ha nytta av.

En uppdaterad CMDB är ovärderlig vid alla slags mer eller mindre allvarliga incidenter.

3.2 Pågående cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Fight-as-you-train
  - Använd de övade metoderna
  - Gör nytt om/när det förberedda inte ger avsedd verkan
- Rapportera uppåt, åt sidorna och nedåt med timmar till dygns rapport/aktivitets-cykler med:
  - Aktuellt läge / Analys och rekommenderade/beslutade aktiviteter
  - Uppfattning om framtiden (timmar / dagar) / Analys och rekommenderade/beslutade aktiviteter
- Om utrymme finns, tillse att de enheter som inte är drabbade kan fortsätta att arbeta i så stor utsträckning som möjligt

Viktiga åtgärder omedelbart efter upptäckt av ransomware

1. Koppla bort drabbat systemet från nätverket.

2. Sätt ihop ett dedikerat team för att hantera incidenten. Detta team ska vara definierat i förväg. Det bör bestå av personer från: organisationens ledning, juridik, kommunikation och tekniker (med åtkomsträttigheter).

3. Initiera incidenten enligt i förväg bestämd rutin. Ingår externa parter (till exempel externt incidenthanteringsteam), kalla in dessa.

4. Rapportera IT-incident till CERT-SE enligt beskrivna rutiner och mallar. IT-incidenter kan påverka myndigheter och företag allvarligt. Information om vad IT-incidenter är, vilka incidenter som ska rapporteras in och hur hittar ni information om på CERT-SE hemsida.

   Ring CERT-SE på 010-240 40 40 eller skicka e-post till cert@cert.se.

   Vid användning av PGP finns CERT-SE:s publika PGP-nyckel.

5. Anmäl incidenten till andra myndigheter efter de lagar och föreskrifter som täcker det drabbade, tex Säkerhetsskyddslagen och -förordningen, NIS, lagen om elektronisk kommunikation eller GDPR (integritetsincident).

3.2.1 Om systemet och den interna kunskapen tillåter, viktiga åtgärder:

1. Samla in data: Spara loggfiler och annat genom att använda forensiska verktyg, och samla därmed in så mycket data och annan information som möjligt, vilket kan vara användbart vid ytterligare utredning. Se till att tidsangivelser är korrekta, eller att du vet vilket fel det kan vara på tidsstämplar så dessa kan korrigeras i efterhand. Forensiska verktyg kan ibland anslutas direkt till tidsövervakningssystem, så att man kan förstå attackens händelseförlopp.

   Att säkra den data du har fått från ditt system är bland de viktigaste stegen i din hantering av incidenten.

2. Jämför data du har samlat in med annan information som finns tillgänglig online. Kontrollera checksummor (HASH-värden), IP-adresser, domännamn du har hittat. Alla spår kan hjälpa dig att reagera snabbare och mer korrekt på en incident. Du bör försöka ta reda på vilken typ av attack det var. Försök också att samla in så mycket information som möjligt om angriparna, till exempel vilka typer av attacker de brukar använda.

3. Samla alla tillgängliga loggar från de system du använder, händelser i datorer, brandväggar, nätverksdata, antivirusdata etc. Det är mycket viktigt att du beaktar händelsen både ur nätverks- och datorperspektiv.

4. Kalla omedelbart in incidenthanteringsteam (ev från den leverantör som du har avtal med) och förse dem med all information du har samlat in.

5. Vid informationsinsamlingen är det viktigt att vara medveten om att kommunikation kan avlyssnas (e-post), använd därför endast de verktyg som krypterar kommunikation och tryggar en säker användning. Lita på proffsen som kommer att ta dig igenom hela processen av viktiga åtgärder säkert och utan panik, eftersom endast med rätt kommunikation och samarbete kommer det att finnas en möjlighet att lösa attacken utan att betala den begärda lösensumman.

3.3 Efter en cyberattack

- Kontrollera säkerhetskopior: Se till att data på säkerhetskopiorna inte påverkats av attacken. Enbart med inte påverkad information kommer det att vara möjligt att återställa förlorad data.

- Gå igenom: **3.1 Före en cyberattack** och vidta påkallade åtgärder

4 Linjechefer

4.1 Före en cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Efterfråga företagsledningens prioriteringar vad avser informationssäkerhetsskydd
- Efterfråga ”IT-ledningens” prioriteringar och instruktioner vad avser IT/Cyber-säkerhet
- Planera och genomför övningar

- Efterfråga en Risk- och Sårbarhetsanalys

- Öva, dra slutsatser och återkoppla till ansvarig enhet

4.2 Pågående cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Var lyhörd och genomför det du vet att du skall göra, genomför de förberedda åtgärderna
- Efterfråga instruktioner om där inte finns några, var aktiv och gör din del av jobbet
- Rapportera i enlighet med överenskomna format och tidsramar

Du måste vara proaktiv. Läs Försvar mot ransomware en gång till och följ råden. Om du blir smittad finns det en risk att du inte får tillbaka dina uppgifter utan att betala lösen-summan. De flesta experter rekommenderar dock inte att du betalar lösen. Här är varför:

För det första uppmuntrar din betalning av lösensumman de kriminella att fortsätta sina bedrägerier.

För det andra finns det ingen garanti att du får tillbaka filerna om betalningen görs. (Om din data är utomordentligt viktig eller känslig, då är det helt upp till dig. Det finns gott om dokumenterade fall där offren betalar lösensumman och får tillbaka sina uppgifter i ett stycke.)

4.3 Efter en cyberattack

- Efterfråga erfarenhetsåtervinning från IT-enheten
- Genomför Post Mortem (som i 2.3)

  En incident ska ha ett väldefinierat slut. En definition är att det team som hanterat incidenten anser att de har dels lyckats återställa acceptabel funktionalitet, dels skapat sig en god överblick över incidenten. Detta avslut kan hanteras som ett möte där ett antal punkter slås fast, och alla på mötet godkänner protokollet. Detta möte kallas ofta ***post mortem*** och en mall för detta möte är:

- **Summary** Vad var det som hände?
- **Impact** Vad påverkades?
- **Root cause** Vad orsakade händelsen?
- **Trigger** Vad genererade upptäckten?
- **Detection** Hur upptäcktes incidenten?
- **Action items** Vilka åtgärder rekommenderas för minskad sannolikhet för incident, alternativt minskas konsekvensen, eller båda?
- **Lessons learned**
- **What went well** Vad gick bra?
- **What went wrong** Vad gick fel?
- **Where we got lucky** Var hade vi tur?
- **Timeline** Fullständig händelselogg.
- **Supporting information** Vilken (extern) kommunikation skedde, vad, till vem, och när.

Det viktiga är att incidenten avslutas och lämnas över från incidentansvarig till den som är ansvarig för den funktion som drabbats. Denna har som ansvar att dels återställa från acceptabel nivå till normalläge, dels välja vilka av de föreslagna åtgärderna som ska implementeras och när.

5 Företagsledningar

5.1 Före en cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Planera med 3 – 5 års sikt framåt, synkroniserat med IT/System-ansvariga
- Inventera och värdera informationstillgångar för att:
  - Planera och genomföra rätt åtgärder: Ska riskerna minskas (genom säkerhetsåtgärder), medvetet accepteras, undvikas (genom att anpassa verksamheten) eller delas med andra (genom exempelvis SLA eller försäkring)?
  - Värdera och förbereda beloppsgränser för användande vid ”Ransomware-attacker” där en lösensumma är oundviklig
- Besluta om återkommande praktiska övningar och mer teoretiska scenarioövningar

Utan IT ingen verksamhet. Det är avgörande att IT-kompetens finns representerat i ledningsgruppen.

När alla aktiviteter och hot blir digitala bör IT-säkerhet stå högt upp på prioriteringslistan i varje företagsstrategi.

Säkerställ att era IT-chefer och säkerhetschefer är kompetenta och har de resurser de efterfrågar för att kunna nå sina operativa och säkerhetsmål.

Besluta om styrande dokument / policies, förankra dem med ett tydligt ansvar och delegerade mätbara mål och med kvalitetskrav.

Följ upp polices och kontrollera genom tester och övningar. Följ upp omvärlden och den tekniska utvecklingen. Lär av andras misstag. Utveckla/ompröva den egna cybersäkerheten. Revidera halvårsvis!

Öva, öva, (minst årligen m.h.t. teknisk utveckling) pröva (ta bra externa hjälp!) och var beredd!

Ta hjälp av proffs som till exempel; Recorded Futures, TrueSec, F-secure bland andra.

Kontinuitetsplanering

I grunden är det att ha kontroll över det man håller på med. Att saker fungerar. Att rätt information är tillgänglig för rätt person eller funktion vid rätt tidpunkt, och inget annat.

Vidare;

- **Att ha en förmåga som innebär att saker fungerar även under stress**
  Saker ska fungera som förväntat. Information ska vara åtkomlig som förväntat. Och inte på något annat sätt. Även om saker går sönder, även under en attack, även om en annars betrodd person medvetet eller inte medvetet förstör.

- **Att ha gjort en risk- och sårbarhetsanalys (RSA) så man känner sina risker**
  I grunden består en risk- och sårbarhetsanalys av en uppräkning av hot eller situationer som man är orolig för. För varje sådan situation beskrivs sannolikheten för att det kan inträffa, och dessutom vilken konsekvens händelsen får om den inträffar. Enkelt beskrivet kan man säga att risk är (sannolikhet x konsekvens).

- **Att ha åtgärder på plats som sänker sannolikhet och minskar konsekvens för varje situation i sin RSA**
  I den RSA som skapats ser man vilka händelser som skulle innebära störst risk. Metodiskt kan man gå igenom dessa och undersöka vilka åtgärder som kan minska risk eller minska konsekvens Slutligen att välja vilka åtgärder man väljer att implementera. Målet är att minimera mängden överraskning vid en incident. Ju mer man planerat, övat och implementerat åtgärder, desto bättre.

- **Att den risk (sannolikhet x konsekvens) som är beräknad återfinns i övergripande affärsplan eller motsvarande**
  Även om det skulle gå att bygga bort alla risker går det inte i praktiken. En webbaserad tjänst måste vara ansluten till internet, för annars kan kunder inte använda tjänsten. Att koppla bort tjänsten från internet för att minska risk för intrång är därför ingen åtgärd man kan använda. Om man gör en tjänst extremt stabil kan den bli så dyr att implementera att man aldrig får intäkter som överstiger kostnaderna. Vilka åtgärder man till slut beslutar att implementera måste därför finnas i affärsplanen eller annat underlag för beslut som ledningen för organisationen måste ta. Det är viktigt att fattade beslut gällande risker är kända. Val av hur problem ska lösas kan delegeras, men aldrig ansvar.

- **Att ha processer, kunskap och kompetens att ta hand om en incident när den inträffar**
  När, inte om, en incident inträffar gäller det att man kan hantera den. Naturligtvis kommer det alltid finnas okända saker som inträffar, och om inget annat är det en överraskning att inciden-ten inträffar precis när den sker. Att reaktionstiden måste vara kort vid detta tillfälle gäller oavsett vilken typ av incidenter det gäller, och oftast är största felet att vänta för länge med att bestämma att det är en incident. Att man inte trycker på den röda knappen snabbt nog. Kompetens kan man antingen ha internt eller så kan man ta hjälp utifrån.

- **Att ha så mycket planerat i sin RSA att överraskningar (okända saker) minimeras, det ska vara kända saker som händer, inte okända**
  Ju bättre RSA är, desto lättare att hantera händelsen. Det ska vara ett medvetet val att inte ha bättre skydd än vad man har för just det incidenten beror på. Därmed är man medveten om att felet kan inträffa. När något inträffar vid sådana tillfällen kan därför redan planerade och inövade processer och handgrepp användas. Dessutom, ju mer som kan övas i förväg, desto färre saker måste uppfinnas under incidenten, vilket underlättar. Man bör också öva att ha en incident, det vill säga själva incidentprocessen ska övas. Man ska veta vem som ska leda incidenten, hur den dokumenteras, hur den avslutas och liknande praktiska saker. Glöm inte bort uthållighet. Incidenter kan pågå under lång tid. Det är viktigare än vad man tror att se till att personal kan sova, äta, och bytas ut.

5.2 Pågående cyberattack

Vad du i din roll i din organisation kan förväntas kunna i detta skede

- Upprätta kris-stab
    - Sätt staben i arbete (OODA)
        1. Analysera attackens art och verkan
        2. Stadfäst läge
            1. Vad är skadat
            2. Vad är hotat
            3. Vad fungerar
        3. Våra möjligheter → Analys → Rekommendation
        4. Beslut → Genomför
        5. Go to 1.
- Genomför traditionell kris-kommunikation
- Se till att nyckelpersoner får sina Maslowska behov tillgodosedda så de håller under hela insatsen

- **Du måste vara proaktiv.**
  Om du blir smittad finns det en risk att du inte får tillbaka dina uppgifter utan att betala lösensumman. De flesta experter rekommenderar dock inte att du betalar lösen.

  Här är varför:
  För det första uppmuntrar din betalning av lösensumman de kriminella att fortsätta sina bedrägerier.

  För det andra finns det ingen garanti att du får tillbaka filerna om betalningen görs. (Om din data är utomordentligt viktig eller känslig, då är det helt upp till dig. Det finns gott om dokumenterade fall där offren betalar lösensumman och får tillbaka sina uppgifter i ett stycke.)

- **Målet med aktiviteter under en incident är att först komma tillbaka till bra funktion och sedan komma tillbaka till normalläge.**
  Samtidigt ska man naturligtvis skriva dagbok och samla information så man kan förstå vad det var som hände. Svara på grundfrågor som vad det är som är trasigt, och hur man kan lösa problemet? Ibland sjösätter man en temporär lösning, för att sedan i ett senare läge återställa det riktiga systemet. Det viktiga för gruppen som arbetar med incidenten är att den fokuserar genom att vara överens om vilket mål man har. Denna fokusering är mycket viktig. Annars kan man bli fast i incidenten under alldeles för lång tid genom att olika åtgärder motarbetar varandra.

5.3 Efter en cyberattack

När incidenten stängts, vilket kan vara långt innan man är tillbaka vid normalläge, måste man noga gå igenom den. Vad tror man hände? Var det fel i den risk- och sårbarhetsanalys som använts? Fanns det fel som kunde ha åtgärdats? Finns det förbättringar som kan göras? Även incidentprocessen i sig ska ses över. Har den fungerat? Kunde man kommit tillbaka till funktion snabbare? Fungerade kommunikationen? Har rätt parter (interna såväl som externa) fått den information de förväntade sig? Alla dessa frågor måste man besvara för att slutligen få en åtgärdslista som kan vara riktigt lång. Denna lista ska ses över och rullas in i den normala listan över förändringar och prioriteras precis som vilka önskemål som helst.

Den bästa situationen är att inte vara överraskad när en incident inträffar. Vid sådana situationer säger man att denna risk var inom accepterad riskaptit.

- Genomför Post Mortem (som i 2.3)

  En incident ska ha ett väldefinierat slut. En definition är att det team som hanterat incidenten anser att de har dels lyckats återställa acceptabel funktionalitet, dels skapat sig en god överblick över incidenten. Detta avslut kan hanteras som ett möte där ett antal punkter slås fast, och alla på mötet godkänner protokollet. Detta möte kallas ofta ***post mortem*** och en mall för detta möte är:

- **Summary** Vad var det som hände?
- **Impact** Vad påverkades?
- **Root cause** Vad orsakade händelsen?
- **Trigger** Vad genererade upptäckten?
- **Detection** Hur upptäcktes incidenten?
- **Action items** Vilka åtgärder rekommenderas för minskad sannolikhet för incident, alternativt minskas konsekvensen, eller båda?
- **Lessons learned**
    - **What went well** Vad gick bra?
    - **What went wrong** Vad gick fel?
    - **Where we got lucky** Var hade vi tur?
- **Timeline** Fullständig händelselogg.
- **Supporting information** Vilken (extern) kommunikation skedde, vad, till vem, och när.

Det viktiga är att incidenten avslutas och lämnas över från incidentansvarig till den som är ansvarig för den funktion som drabbats. Denna har som ansvar att dels återställa från acceptabel nivå till normalläge, dels välja vilka av de föreslagna åtgärderna som ska implementeras och när.

6 Cybersäkerhet för småföretag

6.1 Hur ska du som företagare tänka säkert

- En genomtänkt lösenordshantering är viktigt.
- Se över vilka tjänster, appar och inloggningar som används i företaget. Behöver alla i företaget ha åtkomst till all information?
- Se till att medarbetare använder starka lösenord till egna personliga inloggningar (konton).
- Ha skärmlås på alla företagets datorer, mobiltelefoner och surfplattor.
- Hur ska du som företagare tänka säkert kring back-up rutiner enligt MSB?
- Stillestånd för en verksamhet kan vara förödande. Se därför till att ha en fungerande säkerhetskopia så du inte förlorar dyrbar information och kan fortsätta din verksamhet utan längre avbrott.
- Ha tydliga rutiner för hur du ska säkerhetskopiera företagets information.
- Förvara säkerhetskopior säkert, helst i brandsäkert skåp.
- Ta hjälp av din it-support om du är osäker.

6.2 Försvar mot ransomware-attacker

Installera ett Topprankat Antivirus med Ransomware-Skydd
Att köra viruskontroller är en bra idé, men att ha en helt stabil första försvarslinje på din dator är ännu bättre. De bästa antivirusprogrammen idag kommer att ha någon sorts ransomware-skydd, inklusive proaktivt försvar mot nolldagsangrepp och ibland en speciellt krypterad mapp där du kan hålla din viktigaste data säker från hackare.

6.3 Säkerhetskopiering

- Ha en säkerhetskopia i form av exempelvis USB-minne, extern hårddisk, databas eller molntjänst.
- Säkerhetskopiera ofta och med jämna mellanrum. Har du endast en säkerhetskopia från några dagar tillbaka, riskerar du att även denna blivit smittad av eventuellt virus.

- Testa din säkerhetskopia i förväg, så du vet hur du ska göra om du behöver återställa information.
- Koppla ur din säkerhetskopia från din dator mellan kopieringarna. Annars kan även den utsättas för virus eller annan skadlig kod.

6.4 Checklista för småföretag

6. **Identifiera företagets mest värdefulla tillgångar**
   En cyber-riskbedömning kan kännas för mycket för de minsta företagen men att känna till de mest värdefulla tillgångarna för ditt företag hjälper dig att skydda dem. Lista din viktiga information i en prioriterad ordning, till exempel kunddata, betalningsinformation, webbplats, recept, idéer, ekonomi eller sociala medier-konton.

7. **Du behöver ett anti-virus för småföretag — och mer**
   Det finns inget enskilt verktyg som kan stoppa de många former av cyberhot idag. Ett anti-virus är avgörande för att hålla borta skadlig programvara men du bör dessutom ha flera skyddslager för att göra ditt försvar starkare. Se därför till att ha en lösning som skyddar alla dina enheter, din integritet och online-identitet — på en gång.

8. **Förenkla det du kan**
   När du är småföretagare med en miljon saker att göra, vill du undvika komplexitet på alla områden. Det bästa skyddet är det som är så lätt att använda och som du faktiskt kommer att använda och installera på alla enheter. Välj en säkerhetslösning som har allt-i-ett som är enkel att installera och arbetar i bakgrunden utan att det påverkar din dators eller telefons prestanda.

9. **Skydda dina mobila enheter**
   Småföretag hanterar många saker på språng. Att arbeta från ett hotell, café, bibliotek eller ett annat land gör arbetet flexibelt för dig och dina anställda, men kan du vara säker på att det är säkert? Om du har företagsinformation tillgänglig på mobila enheter måste även de skyddas. En VPN kommer att kryptera din anslutning från hackare och andra snokare på offentliga Wi-Fi-nätverk.

10. **Använd starka lösenord**
    Vi har alla tiotals eller hundratals lösenord. Och vi vet alla att de bör vara svåra att gissa och hållas privata. Men att memorera så många starka lösenord med slumpmässiga karaktärer eller ha ett system som cyber-brottslingar inte kan knäcka är i stort sett omöjligt. Det enda sättet att effektivt skydda dina lösenord — och följaktligen dina online-konton och identitet — är med en lösenordshanterare.

11. **Skydda dina online-konton och identitet**
    Populära tjänster online som Facebook, Linked-In, Google och Dropbox har varit inblandade i flera data-intrång under åren. Att förlora personlig information som lagras på dessa konton eller att bli utelåst från ditt konto kan få ovälkomna konsekvenser för frilansare och småföretagare. God lösenordspraxis, multifaktor-autentisering och att undvika att dela konton hjälper till att hålla dina online-konton säkra. Använd ett kostnadsfria verktyg för att kontrollera om din e-postadress har varit inblandad i data-intrång.

12. **Se till att stoppa ransomware**
    Ransomware är ett av de mest dominerande hoten mot småföretag. Det kan

låsa dig ute från dina data eller enheter och sedan kräva en stor betalning för att släppa din information. Du bör aldrig betala lösensumman, eftersom det inte finns någon garanti för att du skulle få tillbaka dina filer. Ransomware kan vara dyrt, så att ha ett effektivt skydd mot det är vettigt.

13. **Uppdatera program-varor och ha alltid en backup**
    Säkerhetskopiera dina data regelbundet. En backup säkerställer att du alltid har dina viktiga data och filer tillgängliga ifall du skulle råka ut för ransomware. Du bör också se till att hålla dina enheter och programvaror uppdaterade. Sårbarheter i programvaror är säkerhetshål som gör det enkelt för cyber-brottslingar att infektera dina system.

14. **Skydda dina pengar**
    Banker är ett vanligt mål för bedrägerier. Cyber-brottslingar nätfiskar dina bankuppgifter genom att skapa falska webb-platser som ser identiska ut med din internetbanks inloggningssida. När du betalar fakturor eller gör online-köp för ditt företag, se till att dina pengar är skyddade. Ett enkelt sätt att vara säker är ett bankskydds-program som låter dig veta när du går in på en säker bank-sajt och säkrar din anslutning till webb-platsen.

15. **Använd goda säkerhetsvanor**
    Cyber-attacker börjar ofta med att intet ont anande individer laddar ner en skadlig bilaga eller fyller i sina uppgifter på en phishing-webb-plats. Därför är det viktigt att utbilda anställda om cybersäkerhet även för de minsta företagen. Medvetenhet, hälsosam dos av skepsis, bra lösenordspraxis och att vara smart när det gäller att dela data, särskilt kundinformation, kommer att hjälpa till att skydda dina affärsdata och ditt rykte.

16. **Ta bort Ransomware**
    Att rota igenom din dator och kryptera dina filer tar tid, så du vill ta bort ransomware så snart som möjligt för att minimera skadan. Om du har ett kraftfullt antivirusprogram på din dator borde det vara enkelt. Om inte så kan du alltid prova ett av de bästa gratis alternativen för en snabb fix. Att ta bort den skadliga filen släpper dock inte dina filer fria.

17. **Leta efter en Dekrypteringsnyckel Online**
    Lyckligtvis finns det en enorm gemenskap av vänliga hackare och cybersäkerhetsexperter som arbetar hårt för att knäcka de senaste ransomware-stammarna. Använd ett verktyg som Crypto Sheriff för att avgöra vilken stam som har infekterat din dator, och leta igenom resurser som ‘No More Ransom’ för att se om en dekrypteringsnyckel har skapats. Om du har attackerats av en vanlig sorts ransomware finns det en bra chans att någon har knäckt den och kanske kan hjälpa dig återställa dina filer.

18. **Ring Ett Proffs (Och ev. Polisen)**
    Om du fortfarande inte kan återställa dina filer eller din systemåtkomst, och du desperat behöver dem tillbaka, då kanske du vill ringa ett proffs. Prova din lokala datorreparatör eller Geek Squad – de har ofta antivirus- eller ransomware-tjänster och de kan kanske hjälpa till. Du bör också rapportera ransomware-attacken till din lokala polisstation, de kanske till och med spårar cyberattacker via ett klagomålscenter.

7 Om hot, risk och riskhantering

Med **hot** avses en möjlig oönskad händelse med negativ konsekvens för verksamheten. En sådan verksamhet kan avse säkerhetskänslig verksamhet eller en verksamhet som inte är säkerhetskänslig.

(Reglemente Säkerhetstjänst - R SÄK 2021 , 1.6.1. Hotbedömning)

Med **risk** avses ofta:

- effect of uncertainty on objectives
- möjlighet att något oönskat skall inträffa
- möjligheten för skadliga konsekvenser som uppkommer av framtida händelser som till tidpunkt, utsträckning eller utformning är okända.
- Risken kan beskrivas på olika sätt, till exempel sannolikheten för att en *händelse uppkommer, omfattningen av händelsen och typen av händelse.*

(ISO 31 000 Risk Management)

Med **riskhantering** avses det pågående arbetet med att kartlägga olika hot och bedöma sannolikheten för att de olika hoten samt det aktiva arbetet att minska hotens inverkan eller dess sannolikheter att inträffa.

Arbetsgången är att analysera vilka potentiella risker som skulle kunna drabba verksamheten negativt, utvärdera hur sannolikt det är att risken inträffar, samt klassa hur allvarlig risken är för verksamheten för att sedan planerat hantera de risker som bedömts allvarligast:

- Riskidentifiering
- Riskvärdering
- Riskhantering.

Riskhantering kan genomföras enligt följande metod:

1) **Identifiera vad, vilket mål, som riskeras?** (Praktisk innebörd/Kvalitet, Tid eller Resurser)

    1) Vem / vilken intressent (roll & individ) är den tydligaste och mest direkta ägaren

    2) Hur allvarligt är det om målet inte nås, IOM den inträffade/ej-inträffade händelsen? (se ”**Inverkan**”)

2) **Vilken händelse**, eller brist på händelse, är det som om den infaller, hindrar målet från att uppnås?

    1) Vem / vilken intressent (roll & individ) har det tydligaste ansvaret för den aktuella händelsen?

    2) Hur sannolikt är det att händelsen händer/inte-inträffar? (se ”**Sannolikhet**”)

3) **Uppdatera ”Riskanalys”**
…i XLS-bladet preliminärt för att fånga risken

					1 - Försumbar 2 - Ringa 3 - Betydlig 4 - Stor 5 - Mycket stor			1 - Mycket låg (< 2%) 2 - Låg (2 - 5%) 3 - Medel (5 - 25%) 4 Hög (25 - 50%) 5 -Mycket hög (> 50%)		
#	Datum	# Risk No	Mål som riskeras	Ägare	Påverkan	Risk-händelse	Ägare	Sannolikhet	Riskvärde	Referenser
8	2022-09-01	R8		?	5		?	5	25	
6	2022-09-01	R6		?	4		?	5	20	
2	2022-09-01	R2		?	4		?	4	16	
1	2022-09-01	R1		?	3		?	4	12	
4	2022-09-01	R4		?	3		?	4	12	
7	2022-09-01	R7		?	3		?	4	12	
5	2022-09-01	R5		?	2		?	3	6	
3	2022-09-01	R3		?	1		?	4	4	
9	2022-09-01	R9		?						
10										

4) **Uppdra ägare till ”Riskerat Mål” och ägare till ”Risk-händelse”**
… att bedöma Påverkan och Sannolikhet och uppdatera ”Riskanalys”

5) **Bedöm vilka risker som måste hanteras och kalla relevanta intressenter**

    1) Uppdra Intressenter att förbereda vad som måste göras för att hantera risken och sänka sannolikheten och/eller minska inverkan

    2) Genomför mötet och stadfäst vem som, gör vad i **Riskhaneringen**

6) **Återupprepa minst en gång per kvartal och följ upp Intressenter löpande**

7) Rapportera och eskalera i de sammanhang som krävs

En generell beskrivning av **Inverkan** kan se ut som nedan

Kvalitativ bedömning		**Kvantitativ värdering**
Haveri och ingen framdrift. Hantering av följdeffekter och tillvaratagande av artefakter inför haverirapport och ev nästa steg.	Mycket stor	5
Stora utmaningar med fara för haveri. Omedelbara åtgärder, eskalering och ett stärkt ledarskap är nödvändiga	Stor	4
Verksamheten har utmaningar och analys, åtgärdsplan samt genomförande och löpande återkoppling är påkallat	Betydlig	3
Verksamheten fortlöper i stort sett utan anm. på tid, budget och med rätt kvalitet. Normala störningar hanteras framgångsrikt	Ringa	2
Verksamheten fortlöper utan anmärkning, på tid, på budget med rätt kvalitet.	Försumbar	1

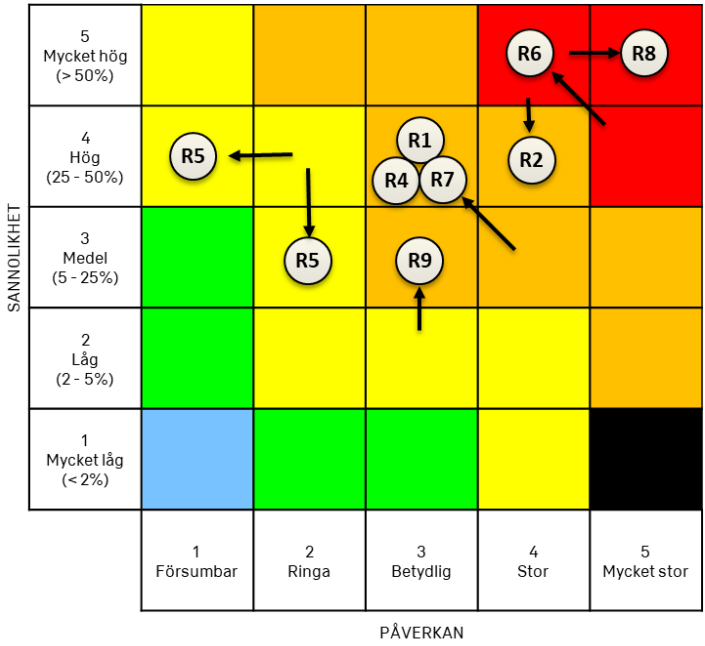
En generell beskrivning av **Sannolikhet** kan se ut som nedan

Kvalitativ bedömning		**Kvantitativ värdering**
> 50%)	Mycket hög	5
25 - 50%)	Hög	4
5 - 25%)	Möjlig	3
2 - 5%	Låg	2
< 2%	Försumbar	1

Uppdatera **Riskanalysen**

					1 - Försumbar 2 - Ringa 3 - Betydlig 4 - Stor 5 - Mycket stor			1 - Mycket låg (< 2%) 2 - Låg (2 - 5%) 3 - Medel (5 - 25%) 4 Hög (25 - 50%) 5 -Mycket hög (> 50%)		
#	Datum	# Risk No	Mål som riskeras	Ägare	Påverkan	Risk-händelse	Ägare	Sannolikhet	Riskvärde	Referenser
8	2022-09-07	R8		?	5		?	5	25	
6	2022-09-07	R6		?	4		?	5	20	
2	2022-09-07	R2		?	4		?	4	16	
1	2022-09-07	R1		?	3		?	4	12	
4	2022-09-07	R4		?	3		?	4	12	
7	2022-09-07	R7		?	3		?	4	12	
9	2022-09-07	R9		?	3			3	9	
5	2022-09-07	R5		?	2		?	3	6	
3	2022-09-07	R3		?	1		?	4	4	
10										

Ett vanligt sätt att visualisera en riskanalys är i en **riskmatris** där riskernas aktuella läge plottas och deras relativa rörelse kan visas med en pil, för att visa från vilket läge som risken rört sig sedan den senaste **riskanalysen**



Det viktigaste är att **riskanalysen** övergår i **riskhantering**, dvs att löpande jobba med att hantera riskerna, med tydliga uppdrag, ansvar och tidsramar.

						Ej påbörjad	
						WIP	
						Stängd	
#	Datum	# Risk No	Vad skall göras?	Av vem?	Tills när?	Status	Referenser
1	2022-09-07	R1	?	?	?	Ej påbörjad	
2	2022-09-07	R2	?	?	?	Ej påbörjad	
3	2022-09-07	R3	?	?	?	Ej påbörjad	
4	2022-09-07	R4	?	?	?	Ej påbörjad	
5	2022-09-07	R5	?	?	?	Ej påbörjad	
6	2022-09-07	R6	?	?	?	Ej påbörjad	
7	2022-09-07	R7	?	?	?	Ej påbörjad	
8	2022-09-07	R8	?	?	?	Ej påbörjad	
9	2022-09-07	R9	?	?	?	Ej påbörjad	
10							
11							
12							

Återbesök riskanalysen löpande och uppdatera den samt följ upp med ägare till risker och händelser att de hanterar sina ansvar.

8 Appendix – checklistor och mer läsning

8.1 Säkra dina lösenord

- Använd unika lösenord för olika tjänster, framför allt dina viktigaste tjänster.
- Använd långa lösenord, gärna en lösenordsfras som är lätt att minnas.
- Aktivera flerfaktorinloggning där det går.
- Använd lösenordshanterare.
- Lämna aldrig ut dina lösenord.

8.2 CIO och systemadministratörer

Datorer och mobila enheter

- Är lösenord till alla användarkonton unika och starka?
- Har ni aktiverat kryptering på lagringsutrymmet till datorer och mobila enheter?
- Säkerhetskopierar ni all viktig information regelbundet?
- Är program för skydd mot skadlig kod, exempelvis antivirusprogram, installerad på alla enheter som är anslutna till, eller kan anslutas till, internet?
- Uppdaterar ni programmen för skydd mot skadlig kod automatiskt alternativt genom en särskild rutin?
- Är det reglerat om och hur privata datorer och mobiler får användas i organisationens verksamhet.

Mjukvaror och applikationer

- Är det reglerat vilka appar som får laddas ner till jobbmobilen?
- Installeras endast mjukvaror och applikationer som är nödvändiga för verksamheten?
- Avinstallerar ni mjukvaror och applikationer som inte används?
- Tar ni bort programvaror och applikationer som inte längre säkerhetsuppdateras?

Nätverk

- Har ni brandväggar installerade mellan internet och ert interna nätverk?
- Har ni ändrat standardlösenorden till unika och starka lösenord, innan ni installerar nätverkskomponenter som exempelvis trådlösa routrar?
- Är alla trådlösa nätverk hos er krypterade och skyddade med unika och starka lösenord eller certifikat?
- Om det finns ett särskilt gästnätverk, är det avskilt från organisationens interna nätverk?

Behörigheter

- Har enskilda medarbetare endast åtkomst till de system och delade lagringsytor som befattningen kräver?
- Byter ni lösenord regelbundet och efter verksamhetens behov?
- Tilldelas systemadministratörsbehörighet endast till godkända personer som utför systemadministrativa tjänster?

8.3 Mätetal för utvärdering av en CIO-organisation

- Resultat av simulerade nätfiskeattacker.
- Tiden det tar att återhämta sig (om den tiden möter, överskrider eller faller under målet i förhållande till den risk som organisation fastställt att man är beredd att ta).
- Tid för upptäckt. Hur lång tid det tog från det att en framgångsrik attack inträffade tills den upptäcktes – eftersom det också indikerar hur väl ett säkerhetsprogram fungerar och gör att man kan gå bakåt och se förbättringar. Sådana mätvärden uppmuntrar också kontinuerlig förbättring: som att få ner snittiden för upptäckt till minuter rentav att sikta mot att minska det till sekunder.
- Penetrationstester indikerar hur väl en organisation kan stå emot sådana händelser och också spåra förbättringar över tid.
- Sårbarhetshantering för att mäta säkerhetsavdelningens förmåga att hantera sårbarheter som ger den största effekten på organisationens säkerhet för att se till att just det som utgör den största risken tas om hand så snabbt som möjligt.
- Säkerhetsrevisioner; ett styrkort som utvecklats utifrån ramverk från National institute of standards and technology, Nist, Information technology infrastructure library, Itil, och Center for internet security, Cis.

8.4 Checklista för cyberförsäkring

På senare år har cyberförsäkringar blivit ett omtalat och alltmer använt verktyg att använda som komplement till andra sätt att hantera cyberrisk. Det är viktigt att understryka att cyberförsäkringar inte *ersätter* andra åtgärder, utan *kompletterar* dem, på samma sätt som en hemförsäkring inte ersätter behovet av en brandvarnare och en brandvarnare inte ersätter behovet av en hemförsäkring.

För att en ledningsgrupp ska kunna dra full nytta av cyberförsäkringsverktyget är det helt avgörande att förstå relationen mellan försäkringen och den egna verksamheten, det vill säga vilket skydd man kan förvänta sig att försäkringen ger

vid olika tillfällen. Följande checklista är framtagen för att ge stöd i att förstå vilken ersättning en cyberförsäkring kan ge för *intäktsbortfall vid driftavbrott*:

- **Försäkringar har självrisk.** För driftavbrott består självrisken dels av ett belopp, dels av en *väntetid* innan försäkringen träder i kraft. Om väntetiden exempelvis är 8 timmar så utgår ingen ersättning för intäktsbortfall om avbrottet är kortare än 8 timmar.

- **Angrepp och olyckor.** De flesta försäkringar täcker angrepp, men icke-antagonistiska incidenter såsom olyckor, slarv, mänskliga misstag etc. täcks inte alltid. Eftersom olyckor kan ha lika stora effekter som angrepp är det värt att överväga vilket skydd som egentligen passar den egna verksamheten bäst.

- **Force majeur.** Avbrott i el- och telenäten räknas som force majeur och täcks i princip aldrig. Om detta är det hot man vill skydda sig mot så är försäkring inte det rätta verktyget.

- **Interna och externa tjänster.** Försäkringar täcker typiskt avbrott i den försäkrades IT-miljö, inte avbrott i externa tjänster. I en modern molnmiljö är detta problematiskt. Vid teckning av en försäkring blir det alltså viktigt att säkerställa att rätt tjänster faktiskt täcks. Vissa försäkringsbolag kan utvidga försäkringen till att täcka externa tjänster (ibland enligt en lista som definieras i förväg) mot en premiehöjning.

- **Beräkningsprinciper för ersättning.** Olika försäkringsbolag kan beräkna det intäktsbortfall som ska ersättas enligt olika principer. Här finns inget rätt eller fel, men den som tecknar en försäkring bör jämföra principerna för olika försäkringsgivare så att försäkringen passar den egna verksamheten. En snabbväxande startup är exempelvis kanske inte så betjänt av att ersättningen beräknas utifrån förra årets intäkter, om dessa bara är en bråkdel av årets.

8.5 Lockheed Martins Cyber Kill Chain

1. **Rekognosering.** Angriparen tar reda på hur den aktuella it-miljön skulle kunna angripas. Vilka tekniska svagheter finns? Vilka personer har tillgång till it-systemet? Vilka av användarna är mest påverkbara?

2. **När angriparen landat i en metod** är det dags att välja “vapen". Det handlar ofta om phishing, mejl som skickas till användare som sitter innanför it-systemets skydd och innehåller skadlig kod.

3. **Mejlet med den skadliga koden** skickas till ett urval av personer. Koden kallas ofta trojansk häst då den är dold i vad som verkar vara ett legitimt dokument eller annan mejlbilaga.

4. **Enligt studier öppnar** ungefär tre av tio användare mejl med skadlig kod, och klickar på den länk eller öppnar den bilaga som aktiverar koden.

5. **När detta sker installeras** ett litet program som ger angriparen kontroll över datorn.

6. **Angriparen befinner sig nu** alltså inne i det skyddade nätverket och kan med hjälp av det lilla programmet söka sig vidare i företagets nätverk, på jakt efter en dator som gör det möjligt att slutföra planen.

7. **När måldatorn är nådd** kan angriparen utföra sitt slutliga dåd. Det kan handla om manipulering eller stöld av information eller sabotage av utrustning som kontrolleras av datorsystem.

8.6 ”Cyberkriminaliteten ökar kraftigt mot företag…”

Kriminella aktörer på nätet söker kontinuerligt efter svaga punkter och utvecklar nya sätt att penetrera eller kringgå traditionella IT-försvar. De stjäl autentiseringsuppgifter från betrodda tredje parter och använd dem för att gräva in i företagssystem.

De skördar personlig information från sociala medieplattformar för att producera övertyga nätfiske-kampanjer och skapa typo-squatting webbplatser för att utge sig för att vara varumärken och bedra kunder.

De plotta cyberattacker och utnyttja fysiska händelser mot fjärranslutna anläggningar runt om i världen. De utformar attacker som, utan förvarning, kan inte upptäckas av konventionell IT-säkerhetslösningar.

Programmen sprids till stor del med skräppost. Hackern designar ett program som tar gisslan och filen som innehåller programmet skickas som en biogad fil i ett email. Programmet söker igenom offrets dator och letar efter filer som har en viss ändelse exempelvis .xls, .pdf och .doc filer och krypterar dessa. Offret kan bara låsa upp dem genom en unik kod.

Enligt FBI omsatte ransomware-attacker 209 miljoner dollar under första kvartalet 2016*, dvs. motsvarande en årsinkomst på ungefär en miljard dollar under förra året.

Dagens Nyheter gjorde under 2016 en undersökning där det framgick att 80 svenska myndigheter och 130 kommuner (44 procent av Sveriges kommuner) fått sina filer krypterade till följd av ransomware. 4 procent av svenskarna har drabbats av ransomware och fått sin enhet krypterad enlgit en rapport från Sensor 2021.

Enligt Wikipedia; Ransomware är väldigt lukrativ business för cyberkriminella och nischen har ökat i omfattning. 2015 betalades det ut 40 miljoner USD. Cloudwards har gjort en uppskattning att ska-dorna från ransomwre kommer kosta 265 miljarder USD år 2031. Alla organisationer är utsatta och man räknar med att 37% av alla företag drabbades 2021.

Betalningarna till hackerföretagen sker oftast i Bitcoin. Cryptolocker malware krypterar offrets filer och ger en nyckel till filerna om den som drabbas inte betalar 300 dollar via Bitcoin.

Dagens typiska utpressningsbelopp är cirka 4 % av brottsofferorganisationens årliga omsättning eller en femtedel av företagens årliga vinster. När förhandlingarna blir "normaliserade" finns det mindre utrymme för skrämseltaktik.

RaaS-modellen (ransomware-as-a-service) som antagits av många ransomware-gäng gör också det cyberkriminella ekosystemet mycket motståndskraftigt mot försök att ta ner deras verksamhet.

8.7 Sju aktuella hotbilder

1. **Threat Actors Are Faster**
   Challenge Highly Scripted and Automated Attacks Major ransomware gangs are becoming faster. By using heavily scripted attacks and something that could be likened to assembly line operations, these cybercriminals can increase the number of victims by spending less time on each attack. Solution Constant monitoring of your environment is key to proper cybersecurity. No matter how well hardened your network is, protection will never be 100% effective. With proper monitoring, you can still evict threat actors before they can cause too much harm.

2. **It's Too Easy to Get Full Control of a Network**
   Challenge; As soon as cybercriminals gain a foothold in a network, their next objective is to take control of. An account that has administrative privileges, typically a domain administrator account. After that, it is often" game over" as the threat actor will have the ability to take over the entire network and deactivate defenses. The fact that administrators use high-privilege accounts such as domain admins to access arbitrary systems highly increases the spreading of these credentials, and therefore, the likelihood of an intruder obtaining them.

   Solution When a high-privilege account is logged on to a system in a lower security tier, any attacker with control of this system could obtain the high-privilege credentials and therefore escalate their privileges. Identity tiering should be used to tackle this issue. Tiering defines a domain model to avoid the exposure of credentials to systems in a lower-security zone. For example, domain admins should only be able to access domain controllers and other systems in the same tier.

3. **Increased Use of Vulnerability Exploits**
   Challenge: Cybercriminals are constantly evolving their business model. They are also becoming more and more efficient at exploiting vulnerabilities to gain a foothold in environments. Zero-day exploits represent the pinnacle of vulnerability exploits Solution more than 40% of all attacks originated from publicly accessible and vulnerable systems. Once a vulnerability in a popular software has been disclosed, it may be only a matter of hours until worldwide scanning is initiated to search for vulnerable systems.

4. **Passwords Are Not Enough**
   The Challenge Single Factor Authentication is not enough Solutions should be implemented to ensure that all internet-facing authentication services require MFA, with a high priority on systems that authenticate using internal credentials.

5. **Dependencies**
   Can Be Exploited Supply chain attacks are an advanced form of cyber-attack, where the threat actor targets an outside service and uses the permissions the service provider must gain access to the network. Such an attack usually represents a high-risk, high-reward strategy.

Solution: Mitigating supply chain attacks is a complex subject, and the actions to take are very much dependent on the specific environment and the risk appetite of the organization. There are two main types of dependencies that are often leveraged in supply chain attacks: - Trusted relationships: external service providers, such as IT services contractors, managed and service providers, etc. These third-party external providers have access to manage systems and applications. - Software dependencies: external vendors of software that can usually affect the distribution of the software and/or its updates, and third-party software dependencies, such as open-source libraries included in applications.

6. **Denial of Service Attacks Are Increasing**
   Challenge: During 2021, we saw attackers targeting different types of victims with one common goal, extorting their victims for a large ransom. Typical ransom amounts today are 1-5 Bitcoin. Solution Implement Proper DDoS Protection Being available on the internet will always make you a potential victim for these kinds of attacks Samt 5 Ways to Prepare Your Website for High Traffic.

7. **Large Flat Networks Are Easy to Exploit**
   Challenge; The larger an organization is and the more sites it has connected to its network, the greater the risk of a cyber attack. Solution When operating a distributed network that spans several sites or branch offices, each site should be capable of disconnection at the network level from the rest of the environment.

8.8 Råd för bedömningen av risker från Norska cyber security center

A) Identifiera alla enheter och programvara

1. Kartlägg alla enheter och programvara i dina datorsystem och ha en uppdaterad nätverkskarta som visar länkar mellan segment, system och andra företag.

B) Skydda information och system

2. Se till att ha god kontroll över internetexponerade tjänster och sårbarhetsytor och framtvinga säkerhetsuppdateringar så snart de finns.

   Tänk på Allvis NOR och/eller andra åtgärder för sårbarhetskartläggning.

3. En uppdaterad säkerhetskopia av datorsystem (dvs. både programvara och data) måste regel-bundet lagras på ett isolerat system för att skydda mot avsiktlig och oavsiktlig radering, manipulering och läsning. Kontrollera också att det är möjligt att läsa av säkerhetskopian och göra en omstart av systemet baserat på säkerhetskopian.

4. Det är absolut nödvändigt att ha kontroll över alla identiteter och åtkomster. Granska regelbundet användar- och systemkonton och kontrollera om alla är relevanta. Se till att alla användaridentiteter har

starka, unika lösenord. Använd två- eller multifaktorautentisering om möjligt. C) Upptäck säkerhets-indrudering aktivitet och säkerhetsöverträdelser.

5. Säkerhetsövervakning måste upprättas och det måste finnas kapacitet att analysera data från sådan övervakning. Central och skyddad loggning av relevanta digitala system är viktig.

6. Upprätta grundläggande identifierings-kapacitet och förmåga att svara på misstänkt aktivitet.

C) Hantera oönskade incidenter

7. Ta fram en beredskapsplan i händelse av en incident och se till att upprätta en händelse-hanteringsplan.

Observera att dessa sju åtgärder endast är ett startstöd. Det är viktigt att bolagets ledning etablerar ett systematiskt arbete med säkerhetshantering och riskhantering.

Exempel på åtgärder är ytterligare övervakning, trafikisolering, vitlistning och kontinuerlig bedömning av behovet av tillgång till/från relevanta organisationer och länder. Dessutom påminner ncsc oss om vikten av att ta itu med sårbarheter som nyligen har varit mycket relevanta

Företag uppmuntras att kontakta ncsc eller deras respektive svarsmiljö om aktivitet observeras som misstänks ha samband med situationen i Ukraina.

PRAKTISK CYBERSÄKERHET

FÖR MOBIL- OCH DATORANVÄNDARE, SYSTEMADMINISTRATÖRER,
CIO´S, DATACHEFER, LINJECHEFER SAMT LEDNING OCH STYRELSE

STOCKHOLM, FEBRUARI 2023