Cybersäkerhet i Sverige 2022

Del 2: Rekommenderade säkerhetsåtgärder

NATIONELLT CYBERSÄKERHETSCENTER

Rapporten är en sammanställning av rekommenderade cybersäkerhetsåtgärder.
Den är framtagen av Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen samt Säkerhetspolisen inom ramen för en fördjupad samverkan.

FMV FRA FÖRSVARSMAKTEN

MSB Myndigheten för samhällsskydd och beredskap

Polisen PTS Säkerhetspolisen

Innehåll

Sammanfattning

De rekommendationer som sammanställs här avser att motverka de sårbarheter som lyfts upp i rapporten *Cybersäkerhet i Sverige 2022 – hot, metoder, brister och beroenden.*

1 Installera säkerhetsuppdateringar så fort det går

Prioritera att uppdatera informationssystem som exponeras mot internet, de som är verksamhetskritiska och de där sårbarheter riskerar att utnyttjas. Ha som målsättning att installera säkerhetsuppdateringar snarast efter att de publicerats.

2 Förvalta behörigheter och använd starka autentiseringsfunktioner

Ha kontroll på alla konton i IT-miljön, inaktivera de som inte används. Var strikt med de behörigheter 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.

3 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.

4 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.

5 Gör säkerhetskopior och testa om informationen går att läsa tillbaka

Skapa säkerhetskopior på information utifrån verksamhetens behov. Hantera säkerhetskopiorna säkert och testa periodiskt att det går att återställa informationen utifrån tagna säkerhetskopior.

6 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.

7 Säkerställ att endast godkänd mjukvara får köras (vitlistning)

Endast tillåten mjukvara får köras i IT-miljön. Förhindra att otillåten programvara körs.

8 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

9 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

10 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.

11 När du upptäckt en säkerhetshändelse

Oavsett hur väl man skyddar sina system med de åtgärder som beskrivs i de tidigare kapitlen i den här rapporten behöver man ändå vara beredd att hantera det oväntade.

Denna sammanställning av rekommenderade säkerhetsåtgärder ersätter inte ett systematiskt säkerhetsarbete utan utgör ett stöd i arbetet med att prioritera vad som behöver göras. I det systematiska säkerhetsarbetet ingår även, men är inte begränsat till, administrativa åtgärder och rutiner.

Förord

Den här rapporten och dess systerrapport, *Cybersäkerhet i Sverige 2022 – hot, metoder, brister och beroenden*, erbjuder en god grund för att ge den egna organisationen förutsättningar att tänka mer cybersäkert. För den som redan tillämpar ett systematiskt cybersäkerhetsarbete, kan de fungera som checklista. Genom 30 sidor i vardera rapport ges en god förståelse för ämnet cybersäkerhet.

Alla verksamheter – offentliga, privata eller ideella – bör nalkas frågan om sin informationssäkerhet med systematik. Det kan antingen leda till slutsatsen att åtgärder är enkla att genomföra och upprätthålla, eller att det behövs ambitiösa och kostbara metoder för att skydda sina nätverk. Bara ett systematiskt tillvägagångssätt, där alla funktioner i organisationen har sin roll, kan avgöra hur väl man lyckas med att skapa ett tillräckligt skydd. Exempelvis utifrån sina systems önskade tillgänglighet och känsligheten hos sin data.

Nationellt cybersäkerhetscenter är en plattform för samverkan inom cybersäkerhet. Det handlar bland annat om saker som lägesbilder och incidenthantering. Vi utvecklar i skrivande stund metoder för att denna samverkan ska breddas från att bara vara mellan de inblandade myndigheterna till att också omfatta andra myndigheter, branschorganisationer och näringslivet. Vartefter vi utvecklas, breddas vår verksamhet. Cybersäkerheten i Sverige behöver, på alla nivåer, gå vidare och matcha de hot vi ser omkring oss.

Thérèse Naess
Chef för Nationellt cybersäkerhetscenter

Inledning

I den här rapportens systerrapport, *Cybersäkerhet i Sverige 2022 – hot, metoder, brister och beroenden* beskriver Nationellt cybersäkerhetscenter varför cybersäkerhet är ett så väsentligt område för vårt samhälle. I den här rapporten, *Cybersäkerhet i Sverige 2022 – rekommenderade säkerhetsåtgärder*, följer vi upp med rekommendationer kring hur man skyddar sig.

Nationellt cybersäkerhetscenter är en plattform för samverkan för sju myndigheter. Vi har olika roller och mandat inom svensk cybersäkerhet. Genom tillkomsten av Nationellt cybersäkerhetscenter har regeringen skapat en plattform för samverkan, som går utöver den samverkan som är naturlig alla myndigheter emellan.

Metoder och verktyg för cyberangrepp utvecklas ständigt och spelplanen förändras. En angripare använder sig ofta av enklast möjliga metod för att uppnå önskat resultat. I många fall behövs inte avancerade metoder, eftersom målen så ofta har cybervärldens motsvarigheter till ”låsta entrédörrar men olåsta källarfönster”.

Listan nedan med sårbarheter som en angripare kan använda utgår från rapporten *Cybersäkerhet i Sverige 2022 - hot, metoder, brister och beroenden*.

Vanligt förekommande sårbarheter

- Brister i autentiseringsfunktionerna
- Brister i konto och behörighetshantering
- Svagheter i IT-miljöns arkitektur, såsom segmentering, filtrering och virtualisering
- Brister i underhålls och uppdateringsrutiner
- Otillräckligt underhåll av äldre informationssystem
- Bristande härdning av utrustning så att onödiga tjänster och protokoll är aktiva
- Inga spärrar för vilken mjukvara som kan köras (vitlistning), övertro på svartlistning
- Utrustning som inte är sanktionerad ansluts till nätverket
- Bristfällig loggning och kunskap om upptäcka och hantera incidenter
- Brister i att kunna återställa information från säkerhetskopior

Målgrupp

Rekommendationerna i denna sammanställning riktar sig till statliga myndigheter, kommuner och regioner, men kan även användas av andra organisationer. Innehållet vänder sig till den som är ansvarig för IT-miljön, exempelvis CIO eller IT-chef.

Syfte

De rekommendationer som ges i denna sammanställning är åtgärdsområden för att motverka de sårbarheter som lyfts upp i rapporten *Cybersäkerhet i Sverige 2022 - hot, metoder, brister och beroenden*.

För varje åtgärdsområde finns en beskrivning av sårbarheten som behöver hanteras. Utöver det finns också ett rekommenderat arbetssätt som är tänkt att visa hur en verksamhet praktiskt kan gå tillväga. Det är tänkt att användas som inspiration och ska inte ses som en uttömmande lista.

Det finns fler, både mer och mindre avancerade, åtgärder som kan införas utöver de beskrivna. Varje åtgärdsområde har en lista med referenser där mer information kan hämtas.

Denna sammanställning av rekommenderade säkerhetsåtgärder ersätter inte ett systematiskt säkerhetsarbete utan kan utgöra ett stöd i arbetet med att prioritera vad som behöver göras. Ytterligare säkerhetsåtgärder måste införas utifrån gjorda riskbedömningar och rättsliga regler.

De rekommendationer som presenteras här medför behov av resurser hos den del av organisationen som arbetar med IT-säkerhet. Den behöver tid för att planera, testa och införa de rekommenderade åtgärderna på ett systematiskt och effektivt sätt. I många fall behövs ett mer ändamålsenligt arbetssätt inom organisationen och i några fall behov av ny utrustning eller nya tjänster.

1

Installera säkerhets-uppdateringar så fort det går

För att minska den vanligt förekommande riskenatt en angripare utnyttjar kända sårbarheter i hård- och mjukvara är det viktigt att installera säkerhetsuppdateringar från hård- och mjukvaruleverantörer så snart det är möjligt.

Risken i praktiken

Nya sårbarheteter och attackmöjligheter upptäcks regelbundet och kan utnyttjas av angripare som vill komma åt information eller på annat sätt inverka negativt på informationssystemet och därmed verksamheten. Många angripare söker aktivt efter informationssystem som innehåller kända sårbarheter.

Angripare övervakar också de säkerhetsuppdateringar som leverantörer publicerar. Genom att analysera och förstå vilken del i koden som säkerhetsuppdateringen avser åtgärda kan en angripare få fram underlag till att skapa skadlig kod. Denna kan sedan användas för att utnyttja sårbarheten innan organisationer har installerat säkerhetsuppdateringen. Det är således en kapplöpning mellan organisationen och angriparen om vem som hinner agera först.

För att ha en så säker IT-miljö som möjligt är det bästa att alltid ha den senaste säkerhetsuppdateringen installerad på varje enskilt informationssystem och förstå risken med att dröja med att installera säkerhetsuppdateringarna.

Rekommenderat arbetssätt

Inventera alla informationssystems behov av säkerhetsuppdateringar, vilket inkluderar alla mjukvaror t.ex. inbyggda programvaror (eng. firmware), drivrutiner, operativsystem och applikationer. Prioritera att uppdatera de informationssystem som bedöms utsatta för störst risk, t.ex. de med störst exponering (åtkomliga från internet), de med sårbarheter som fått höga poäng enligt Common Vulnerability Scoring System (CVSS), de som är verksamhetskritiska och de där det på annat håll uppmärksammats att sårbarheten redan utnyttjas. Om uppdatering inte går att utföra, skydda då informationssystemet tillfälligt genom alternativa sätt som minskar sårbarheten (om sådana finns).

Inför ett arbetssätt som säkerställer att nya säkerhetsuppdateringar för olika informationssystem blir identifierade. Bedöm behovet av testning innan informationssystemen blir uppdaterade. Installationen av prioriterade säkerhetsuppdateringar bör ske snarast efter att de blivit släppta. Automatisera utrullning och installation av säkerhetsuppdateringar för att skydda informationssystemen snabbare.

Installera enbart uppdateringar som kan säkerställas vara tillhandahållna av leverantören. Kontroll av detta kan t.ex. vara att uppdateringarna är digitalt signerade av leverantören och att uppdateringarna hämtas över en

Tänk på

- Det är viktigt att löpande hålla sig underrättad om nya hot och kända sårbarheter som är relevanta för den egna IT-miljön.
- I många fall kan ändringar som ökar säkeheten i informationssystem ingå i andra typer av uppdateringar som leverantören inte kallar för säkerhetsuppdateringar. Se till att även installera dessa uppdateringar.
- Förseningar i arbetet med att installera uppdateringar gör att uppgiften blir mer omfattande. Det i sin tur innebär ökade risker och kostnader samt riskerar att påverka förtroendet för organisationen.
- Det är bättre att börja smått och göra framsteg än att känna sig överväldigad av uppgiften och inte göra någonting.

skyddad förbindelse mot leverantörens server för uppdateringar. Uppdateringar som tillhandahålls på annat sätt kan innehålla skadlig kod.

Mer information om säkerhetsuppdateringar finns i

- (US) Center for Internet Security (CIS) CIS Controls . Avsnitt: Continuous Vulnerability Management; CIS Control 7.
- UK NCSC 10 steps to cyber security. Avsnitt: Secure Configuration och Vulnerability management.
- AU ACSC Essential Eight.
  Avsnitt: Patch operating systems och Assessing Security Vulnerabilities and Applying Patches.

Exempel från verkligheten

2017 utsattes ett stort antal organisationer för ekonomisk utpressning som i öppna källor kallas för WannaCry och NotPetya. Utpressningskampanjerna möjliggjordes av en sårbarhet i Windows SMBv1-protokoll som utnyttjades för att installera skadlig kod i form av så kallad ransomware. Microsoft hade publicerat en säkerhetsuppdatering ett par månader innan den skadliga koden spreds, men många organisationer hade inte installerat den. Bland de utsatta fanns även organisationer i Sverige. Konsekvenser av denna typ av cyberangrepp kan bli stora och kostsamma för organisationerna som drabbas.

2

Förvalta behörigheter och använd starka autentiserings-funktioner

För att förhindra att en angripare kan använda sig av existerande konton som finns i IT-miljön behöver organisationen har kontroll på konton och tilldelade behörigheter. En viktig del är att ha starka autentiseringsfunktioner samt att vara medveten om att lösenord ofta är en sårbarhet som en angripare gärna utnyttjar.

Risken i praktiken

En angripare som använder sig av ett existerande konto gör det svårt för de som övervakar IT-miljön att upptäcka felaktig användning. Det förekommer att konton som utgivits till tidigare leverantörer och anställda både är aktiva och är tilldelade behörigheter även långt efter att leverantörsrelationen eller anställningen avslutats. Även konton som använts av tjänster och system kan vara aktiva långt efter att tjänsten eller systemet tagits ur drift. Konton som använts när säkerhetstester gjorts i produktionsmiljön kan också glömts kvar i IT-miljön. Detta ger möjlighet för en angripare att nyttja dessa konton för åtkomst till organisationens information.

Att använda samma kontouppgifter i test- och utvecklingsmiljöer som i produktionsmiljön öppnar för angripare att komma över kontouppgifterna i de ofta mindre skyddade test- och utvecklingsmiljöerna och sedan nyttja dessa för att bereda åtkomst till produktionsmiljön.

Kvalitén på lösenord är ofta väldigt låg vilket innebär att en stor del av lösenorden går att gissa sig till utifrån modifierade ordlistor eller genom att prova ett litet antal mycket vanligt förekommande lösenord
mot ett stort antal kontonamn (lösenordssprejning).
I informationssystem där standardlösenordet inte är ändrat räcker det för en angripare att prova det lösenord som står i systemdokumentationen som ofta är publicerad på internet.

En angripare kan på relativt enkelt sätt få tillgång till ett lösenord genom att lura användaren att skriva in uppgiften på en förfalskad webbsida (nätfiske, eng. phishing). Genom att få vetskap om lösenordet i ett informationssystem kan angriparen använda det även i andra informationssystem där användaren använder samma lösenord.

Rekommenderat arbetssätt

Tilldela endast specifika och unika konton för användare och tjänster. Etablera ett arbetssätt (företrädesvis automatiserat) att förvalta konton som innebär att hela livscykeln hos ett konto aktivt följs så att när en användare slutar eller en tjänst har tagits ur drift inaktiveras kontot. Konton som förväntas vara kortlivade, t.ex. sådana som ges ut till konsulter, förses med en tidpunkt för när de inaktiveras. Åtgärder införs för att följa upp att detta är gjort och att behörigheter är återtagna. Konton som inte använts under en viss tid inaktiveras automatiskt.

Radera inte konton, utan inaktivera dem och ta bort tilldelade behörigheter. Ett konto som raderas blir svårt att följa i äldre säkerhetsloggar, samt att det finns en risk att samma kontonamn återanvänds vid ett senare tillfälle.

Tänk på

- Säkerställ att alla konton är personliga, och att även systemkonton har en ansvarig person.
- Ett lösenord som en angripare på något sätt kommit över ska inte kunna återanvändas av angriparen i andra tjänster. Sålunda ska varken samma konto eller lösenord användas i utvecklings- och testmiljön som i produktionsmiljön.
- Ändra alla standardlösenord i informationssystem före produktionssättning. Detta inkluderar alla typer av komponenter, t.ex. applikationer, operativsystem, routrar, brandväggar och accesspunkter.

Prioritera att använda flerfaktorsautentisering för

- samtliga informationssystem som medarbetare kan få åtkomst till via internet t.ex. intranät, epost, VPN, RDP och SSH,
- all åtkomst till informationstillgångar med högt skyddsvärde,
- konton med systemadministrativa behörigheter.

Säkerställ att flerfaktorsautentiseringen är korrekt implementerad. Om ett informationssystem accepterar åtkomst med enbart lösenord parallellt med flerfaktorsautentiseringen så finns det från en angripares perspektiv ingen flerfaktorsautentisering utan säkerheten är i slutändan baserad på lösenord. Tillse därför att konton där flerfaktorsautentisering inte stöds tvingas använda unika och långa lösenord. Tillhandahåll systemstöd för lösenordshantering för att motverka att lösenord skrivs ned i klartext eller att de återanvänds mellan olika tjänster.

Logga användningen av konton och övervaka t.ex. om den förväntade användningen ändras i form av inloggningstid, antal inloggningar inom en tidsperiod, längd på aktivitet och från vilka informationssystem inloggning sker. Säkerhetsloggarna behöver skyddas mot obehörig åtkomst och förändring, t.ex. mot att ändras av en angripare eller illojal medarbetare i syfte att undanröja spår. Skyddet bör vara av sådan art att organisationen med säkerhet kan lita på innehållet i loggarna och att uppgifter om enskild persons aktivitet särskilt skyddas.

Var uppmärksam på de konton som inte hanteras av en central behörighetsfunktion, i synnerhet sådana konton som till sin natur har systemadministrativa behörigheter. Det kan handla om inbyggda konton som används för systemadministration av en molntjänst, en databasinstans, eller nätverksutrustning.

Mer information om konton och autentisering finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Account Management; CIS Control 5.
- UK NCSC 10 steps to cyber security. Avsnitt: Managing user privileges och Introduction to identity and access management.
- AU ACSC Essential Eight. Avsnitt: Multi factor authentication.

Exempel från verkligheten

En användare hade under sin tid som anställd haft möjlighet att skapa ett antal konton utöver sitt vanliga konto. Dessa konton gavs behörighet för inloggning via VPN och åtkomst till ett centralt verksamhetssystem. När användaren slutade i organisationen använde personen sitt gamla konto samt de nya kontona för att under lång tid efteråt ta del av information i verksamhetssystemet. Tre brister gav möjlighet till detta: att användarens konto inte inaktiverades när anställningen avslutades, att personens skapande av nya konton till sig själv inte upptäcktes och att inloggning via VPN kunde ske med enbart användarnamn och lösenord.

Säkerställ att åtkomsten till sessionerna på arbetsstationer och i applikationer blir låsta efter en viss tids inaktivitet.

3

Begränsa och skydda användningen av system-administrativa behörigheter

För att minska risken att en angripare kan nyttja användar- och systemkonton med höga behörigheter, ska tilldelningen och användningen av dessa behörigheter avsevärt begränsas.

Risken i praktiken

Ju fler användare och konton med systemadministrativa behörigheter, desto större risk att autentiseringsuppgifter (t.ex. lösenord) för denna typ av konton kan komma obehöriga till del. En angripare kan också dölja sig i mängden på ett lättare sätt.

En användare kan oavsiktligt köra skadlig kod. Har användaren systemadministrativa behörigheter kan den skadliga koden köras med dessa höga behörigheter vilket kan resultera i ett mycket kraftfullt genomslag, jämfört med om koden körs på ett konto med lägre behörighet.

Många informationssystem kräver systemkonton med justerade behörigheter, men exakt vilka behörigheter är ofta illa dokumenterade av leverantören. Detta leder till att konton tilldelas alltför höga behörigheter för att underlätta att informationssystemet ska fungera direkt efter installationen. Angripare utnyttjar detta för att utöka sin åtkomst.

Att ha konton med högre behörigheter än vad verksamheten kräver kan också resultera i att oavsiktliga händelser får allvarligare konsekvenser, såsom att information raderas eller att systeminställningar råkar ändras av misstag.

Rekommenderat arbetssätt

Inventera användningen och tilldelningen av konton med systemadministrativa behörigheter och sådana konton som hanterar informationstillgångar med högt skyddsvärde. En generell regel är att ju högre behörighet ett konto har desto mindre ska det användas och ett konto ska inte ha högre behörigheter än det behöver.

Förutom att begränsa användningen behöver arbete med systemadministrativa behörigheter särskilt skyddas.

- Använd olika konton för olika funktioner, t.ex. för system-administration av användare, servrar respektive klienter. Alla dessa konton ska ha unika autentiseringsuppgifter.
- De systemadministrativa behörigheterna bör så långt som möjligt vara separerade i sina funktioner, t.ex. att samma konto ska inte ha behörighet att lägga till konton och samtidigt ändra loggar.
- Använd olika konton med systemadministrativa behörigheter i olika delar av IT-miljön. Detta motverkar att en eventuell kompromettering av ett administratörs-konto inte ger samma höga behörigheter till hela, eller stora delar av, IT-miljön.
- Använd särskilda arbetsstationer för systemadministrativa uppgifter. Isolera arbetsstationerna från övriga nätverk, t.ex. internet, och se till att de endast innehåller nödvändig mjukvara för den systemadministrativa uppgiften.

Tänk på

- I systemdokumentation från leverantörerna kan det stå att tillhörande systemkonton ska ha höga behörigheter. Försök att ta reda på från leverantören exakt vilka behörigheter som behövs.
- Återkalla högre behörigheter när de inte längre behövs.
- Dokumentera tilldelningen av behörigheter: vem som godkänt förändringen, vem som utfört förändringen och när behörigheterna ska återkallas.

Mer information om behörighetshantering finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Account Management; CIS Control 5.
- UK NCSC 10 steps to cyber security. Avsnitt: Managing user privileges .
- AU ACSC Essential Eight. Avsnitt: Restricting Administrative Privileges.

4

Härda systemen

För att minska exponeringen ska informationssystem ha så få aktiva tjänster, protokoll och nätverkskopplingar som möjligt. De tjänster, protokoll och nätverkskopplingar som inte behövs för informationssystemets funktion ska stängas av, tas bort eller blockeras.

Risken i praktiken

Ett informationssystem exponerar vanligtvis ett flertal tjänster mot de nätverk det är anslutet till. Varje tjänst består av mjukvara med tillhörande protokoll för att ge funktionalitet. All mjukvara innehåller sårbarheter som kan innebära en möjlig väg in för en angripare. Ju fler tjänster och protokoll som är tillgängliga desto fler möjliga sårbarheter.

I synnerhet bör sådana informationssystem som är avsedda för att exponeras externt, t.ex. webb- eller DNS-servrar härdas. Efter en standardinstallation har de ofta fler tjänster och protokoll aktiverade som standard än vad som behövs för informationssystemets funktion.

I många tjänster och protokoll finns programkomponenter med avsikt att vara bakåtkompatibla med äldre informationssystem. Det betyder att efter uppgraderingar installerats behöver de extra tjänsterna och protokollen avaktiveras. Att installera uppgraderingar är trots arbetsinsatsen som krävs viktig då äldre versioner ofta är mer sårbara än nyare versioner.

Rekommenderat arbetssätt

Härdning innebär att de operativsystem, inbyggda programvaror, nätverkskomponenter, databaser och andra applikationer som ingår i ett informationssystem konfigureras på ett så säkert sätt som möjligt. Funktioner och tjänster som inte behövs i IT-miljön stängs av, blockeras eller tas bort från informationssystemet. Det gäller även protokoll som finns aktiverade för en eventuell bakåtkompatibilitet, men som inte behövs för att få önskad funktion.

Aktivera lokal brandvägg på både klientdatorer och servrar och tillåt bara nödvändig nätverkstrafik.

Ta råd från leverantörerna i hur produkterna kan härdas och kan konfigureras till att ha en hög säkerhet. Stora leverantörer har i många fall sådana råd publicerade, även om kvaliteten på rekommendationerna kan vara svår att bedöma och varierar utifrån tillverkarens ambitionsnivå.

Mer information om att härda system finns i

- (US) Center for Internet Security (CIS) CIS Controls.
  Avsnitt: Application Software Security; CIS Controls 16.
- UK NCSC 10 steps to cyber security.
  Avsnitt: Secure Configuration.
- AU ACSC Essential Eight.
  Avsnitt: User application hardening.

Tänk på

- För att identifiera sårbarheter och angrepps-vägar som kan användas för att utnyttja informationssystem är det viktigt att planera och genomför regelbundna säkerhetstester och säkerhetsgranskningar, som initieras både utanför och innanför perimeterskyddet.
- Alla informationssystem i IT-miljön behöver härdas: mobiltelefoner, nätverksenheter, servrar, arbetsstationer, skrivare, molntjänster, IP-telefoner m.fl.

5

Gör säkerhetskopior och verifiera att informationen går att läsa tillbaka

För att kunna återställa förlorad eller felaktigt ändrad information eller systemkonfigurationer behöver organisationen göra säkerhetskopior och ha en förmåga att läsa tillbaka informationen från dessa. Förmågan gäller både enskilda filer såsom att kunna återställa hela informationssystem.

Risken i praktiken

Vid angrepp, eller vid oavsiktliga händelser, kan konfigurationer, mjukvara eller information ändras, raderas eller förstöras. Ett exempel är angrepp där kryptovirus används och som resulterar i att hela eller delar av informationssystem krypteras så att de blir otillgängliga. Ett annat exempel kan vara att ett centralt lagringssystem får sitt filsystem korrupt på grund av felaktig hårdvara.

Även själva hanteringen av säkerhetskopior kan medföra risker. Säkerhetskopian är en avbild vid en viss tidpunkt av den information som lagras i ett eller flera informationssystem. Om den hanteras eller lagras på ett bristfälligt sätt, kan informationen komma obehöriga till del, ändras eller förstöras. Säkerhetskopior som är filbaserade och som går att nå via vanliga filsystemanrop är sårbara vid incidenter där kryptovirus förstör data på alla skrivbara filytor.

Beroende på hur säkerhetskopian är gjord, eller lagrad, kan återläsningstiden påverkas eller i vissa fall till och med medföra att återläsning är omöjlig. En uppgradering av funktionen för säkerhetskopiering kan påverka förmågan för återläsning, exempelvis äldre säkerhetskopior.

När exempelvis en angripare förstört informationen med ett kryptovirus så räcker det inte med att läsa tillbaka informationen från en säkerhetskopia. Det fotfäste en angripare har i IT-miljön påverkas ofta inte av att enskild information återläses, utan angriparen kan vid senare tillfälle återigen utföra skadlig aktivitet.

Om organisationen upptäcker en angripare i sin IT-miljö kan det vara mycket svårt att helt återställa informationssystemen till en tidpunkt där det med säkerhet går att säga att angriparen inte påverkat IT-miljön. Säkerställ att det finns säkerhetskopior som går att lita och som kan läsas tillbaka.

Rekommenderat arbetssätt

Upprätta en dialog med informationsägaren eller motsvarande för att avgöra hur ofta säkerhetskopior behöver tas och hur länge informationen måste sparas samt vilket skydd säkerhetskopiorna behöver och vilka hanteringsregler som ska gälla.

Om inget annat beslutats, planera för att skapa säkerhetskopior på daglig basis för ny och förändrad information, inklusive systemdokumentation, säkerhetsloggar, konfigurationsinställningar i applikationer och operativsystem. Se även över behovet att skapa säker-

Tänk på

- Även om systemet som hanterar säkerhetskopior visar att säkerhetskopian är intakt och funktionell, så kan detta vara missledande. Testa alltid återläsning av information.
- Säkerhetskopiera även konfigurationer och konto- och behörighetskataloger så att även dessa kan återskapas.
- Öva återläsning till ett helt nyinstallerat informationssystem och inte bara till befintligt. I händelse av angrepp kan hela eller delar av IT-miljön behöva ominstalleras.

hetskopior på själva installationen av applikationer.

Spara säkerhetskopior där de inte är åtkomliga över nätverk för att skydda dem mot obehörig förändring, t.ex. vid angrepp av kryptovirus. Säkerhetskopior behöver också skyddas mot brand- och vattenskada. Hur många versioner av säkerhetskopior som ska sparas, och hur länge, avgörs genom en riskbedömning.

Testa minst årligen (eller vid större förändringar av IT-miljön) att det går att återställa informationen utifrån tagna säkerhetskopior. Testa både partiell återläsning (t.ex. enskilda filer) och full återställning.

Mer information om säkerhetskopior och återställning finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Data Recovery; CIS Control 11.
- UK NCSC 10 steps to cyber security. Avsnitt: Incident management.
- AU ACSC Essential Eight. Avsnitt: Daily backups.

Exempel från verkligheten

En anställd på en myndighet hade skickat in en begäran om att tre lagringsytor skulle tas bort, då arbetet med informationen var avslutat och IT-systemet inte längre behövdes, vilket en tekniker utförde. Den anställde var dock inte medveten om att både backup- och arkivdata ingick i samma lagringsyta, vilket teknikern inte heller upplyste om.

Två månader efter verkställandet återkom den anställde och ville läsa arkivdata från dessa lagringsytor, vilket inte var möjligt då all information som var sparad i dessa ytor var raderad.

6

Tillåt endast godkänd utrustning i nätverket

För att motverka att obehöriga enheter som ansluts till nätverket får åtkomst till organisationens informationssystem och tjänster behöver organisationen aktivt inventera och upptäcka nya enheter. Organisationen behöver också agera så att endast godkända enheter ges åtkomst till tjänster och informationssystem.

Risken i praktiken

Bristande fysisk och logisk säkerhet kan medföra att en angripare får åtkomst till tillgångar i IT-miljön. En bristfälligt konfigurerad wifi-accesspunkt i en publikt tillgänglig zon, eller ett oskyddat nätverksuttag i ett konferensrum, ger exempelvis en angripare möjlighet att koppla in obehörig utrustning och få tillgång till det övriga nätverket och IT-miljön. Även andra trådlösa lösningar kan vara sårbara, såsom bluetooth.

Organisationens nätverk sträcker sig många gånger utanför kontorslokalen genom att informationssystem är utkontrakterade, att det trådlösa nätverket (t.ex. wifi och bluetooth) går att nå utanför fastigheten och att det finns möjlighet att koppla upp sig mot nätverket över VPN. Anslutning av organisationens IT-miljö mot internet eller andra nätverk utanför den egna kontrollen exponerar systemen och ökar angreppsytan.

I valet mellan säkerhet och verksamhetens behov kommer organisationen ofta behöva acceptera att enheter med lägre skyddsnivå än önskvärt är uppkopplade i IT-miljön. De risker som detta innebär bör vara analyserade och motiverade så att inga risker tas i onödan. Det är viktigt att organisationen är medveten om vilka val den står inför, undviker de onödiga riskerna, och balansera verksamhetens behov mot kvarvarande risker.

Rekommenderat arbetssätt

Tillåt endast anslutning av sådan utrustning som är godkänd av organisationen. Informera medarbetarna om detta.

Använd aktiva och passiva åtgärder för att ta reda på vilken utrustning som är inkopplad på nätverket. Aktiva åtgärder kan vara att skydda nätverket mot anslutande utrustning med hjälp av t.ex. 802.1x-standarden. Passiva åtgärder kan vara att t.ex. använda sig av en teknik som kallas DHCP-snooping.

Skapa en förteckning över varje nätverksansluten utrustning som har en IP-adress på nätverket. Säkerställ att förteckningen innehåller nätverksadresser, ev. maskinnamn, syfte, ansvarig ägare och vilken del av organisationen utrustningen tillhör. Förteckningen bör inkludera stationära och bärbara datorer, servrar, närverksutrustning (till exempel accesspunkter, routrar, switchar och brandväggar), skrivare, lagringsnätverk, IP-telefoner och IoT-enheter.

Minimera antalet möjliga angreppspunkter genom att inaktivera nätverksportar och fysiskt koppla ifrån oanvända nätverkskablar. Se också till att fysiskt skydda nätverksutrust-

ningen, t.ex. genom låsta skåp med tillhörande access-loggning.

Skydda trådlösa nätverk med säkerhetsåtgärder för att autentisera och auktorisera både användare och klienter. Privat utrustning, om sådana får användas, bör användas endast i för ändamålet avskilda delar i organisationens infrastruktur.

Mer information om inventering av utrustning finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Inventory and Control of Enterprise Assets; CIS Control 1.

7

Säkerställ att endast godkänd mjukvara får köras

För att motverka att obehörig och otillåten mjukvara körs i organisationens informationssystem behöver det finnas säkerhetsfunktioner aktiverade. Detta skydd bör bestå av vitlistning som hindrar att otillåtna mjukvaror körs. Även användningen av ett modernt operativsystem som har förmåga att ställa krav på signerad mjukvara och skript ökar skyddet.

Risken i praktiken

Skadlig kod kan orsaka stora problem för en organisation såsom dataläckage, dataförlust eller stopp i verksamhetskritiska system. Sättet som skadlig kod kan föras in i IT-miljön kan ske på många olika sätt:

- **E-post:** En av de vanligaste kanalerna för att sprida skadlig kod är genom ”bifogad fil” eller genom att få användaren att klicka på länkar som leder till webbsidor där skadlig kod finns.
- **Webbläsare:** Användare går till, eller luras att gå till, webbsidor som innehåller skadlig kod.
- **Webbtjänster:** Sociala medier och gratistjänster kan nyttjas för att få användaren att ladda ned skadlig kod.
- **Enheter som kan anslutas, exempelvis personliga enheter:** Det finns möjligheter att importera skadlig kod från enheter som kopplas in som USB-enheter; även smarta telefoner som kopplas in i datorer i syfte att ladda kan överföra skadlig kod till datorn och vidare in i IT-miljön.

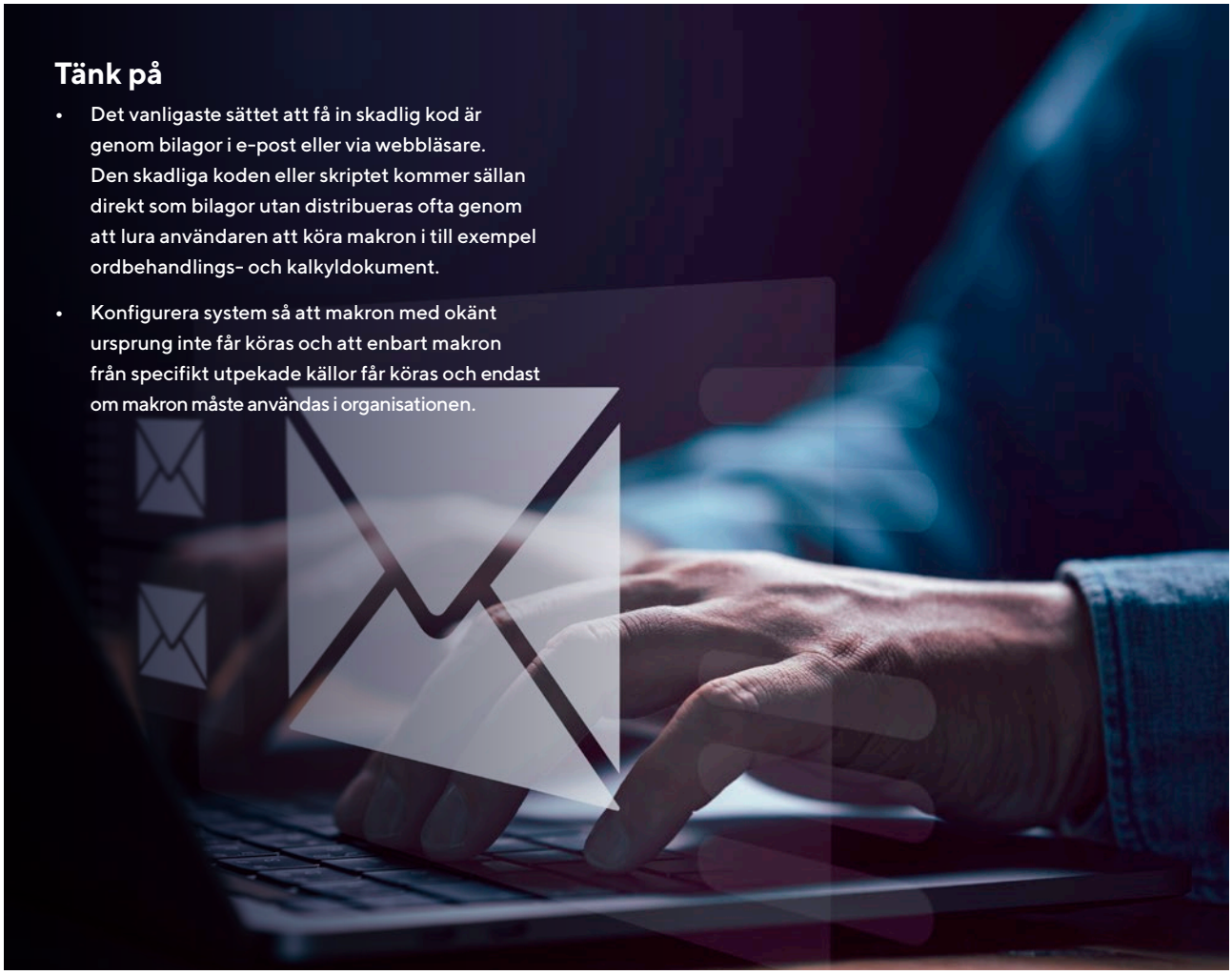
Den skadliga koden kan ge olika resultat: t.ex. ge angripare tillgång till delar av IT-miljön, ge obehöriga åtkomst till information, förstöra eller obehörigt ändra information eller utnyttja organisationens resurser till obehörigt ändamål såsom beräkning av kryptovalutor eller att skicka ut skräppost.

Rekommenderat arbetssätt

Inför funktioner som endast tillåter att godkänd mjukvara, kod och skript får köras, så kallad vitlistning. Skyddet införs på servrar och klienter. Detta gör det svårare för en angripare att använda egna verktyg, men det finns fortfarande möjligheter att använda de program som är vitlistade på sätt som tillåter angriparen att få till liknande funktionalitet. För att motverka detta införs funktioner som loggar och övervakar användningen av vitlistad mjukvara.

Tillåt inte användare att själva installera mjukvara på sina klienter och mobiltelefoner.

Ett bra sätt att börja är att inleda användningen av vitlistningsfunktionen i ett inlärningsläge för att se vilka mjukvaror som kommer att bli hindrade att köra. På så



Tänk på

- Det vanligaste sättet att få in skadlig kod är genom bilagor i e-post eller via webbläsare. Den skadliga koden eller skriptet kommer sällan direkt som bilagor utan distribueras ofta genom att lura användaren att köra makron i till exempel ordbehandlings- och kalkyldokument.
- Konfigurera system så att makron med okänt ursprung inte får köras och att enbart makron från specifikt utpekade källor får köras och endast om makron måste användas i organisationen.

sätt kan vitlistningsfunktionen ”trimmas in” utan att användarna i onödan blir hindrade att köra tillåten mjukvara. När vitlistningsfunktionen är intrimmad så aktiveras det tvingande läget vilket ger effekt av säkerhetsåtgärden.

Att använda svartlistning, d.v.s. att blockera känd skadlig kod, ger otillräckligt skydd. Denna åtgärd ger ett sämre skydd mot ny skadlig kod. Svartlistning är en vanlig funktion hos antivirusprodukter.

Mer information om vitlistning finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Inventory and Control of Software Assets; CIS Control 2.
- UK NCSC 10 steps to cyber security. Avsnitt: Malware prevention.
- AU ACSC Essential Eight. Avsnitt: Configure Microsoft Office macro settings.

Exempel från verkligheten

I början på 2019 mottog två statliga organisationer, en i Europa och en i Nordamerika, e-postmeddelanden om en kommande försvars- och säkerhetskonferens. Avsändaren såg ut att vara konferensarrangören och e -postmeddelandena innehöll en bilaga som påstods vara ett konferensschema. Det följde också med instruktioner om hur mottagaren skulle göra för att aktivera ett makro för att kunna läsa innehållet i bilagan.

En, för användaren osynlig, funktion i makrot skrev ner och körde skadlig kod på mottagarens dator. Den skadliga koden innehöll funktioner för att injicera sig i offrets webbläsare för att kunna kommunicera med angriparens kommandoserver på internet. Angriparen hade därefter tillgång till organisationens IT-miljö.

8

Segmentera nätverken och filtrera trafik mellan segmenten

För att hindra eller försvåra för en angripare att få tillgång till IT-miljön måste nätverket skyddas mot både interna och externa hot. Skyddet ska också reducera skadan om angriparen ändå har kommit över behörigheter och därmed också resurser i nätverket.

Risken i praktiken

En angripare kartlägger vilka möjligheter det finns att ta sig vidare in i IT-miljön med utgångspunkt utifrån den plats i nätverket där angriparen kunnat ta sig in. Målet är ofta att nå andra informationssystem där angriparen kan skaffa sig högre behörigheter och bättre åtkomst till känsligare information eller informationssystem.

I ett nätverk sker majoriteten av kommunikationen mellan klient och server. Vanligtvis delas servrar och klienter upp genom att sätta dem i olika nätverkssegment och filtrera trafiken med hjälp av centraliserade nätverksbrandväggar. Men ofta sätts alla klienter i ett och samma nätverkssegment och nätverkstrafik tillåts mellan alla klienter. Detta underlättar det för en angripare att både sprida skadlig kod och förflytta sig i IT-miljön.

Ett nätverk är en kritisk del i IT-miljön. Ju fler tjänster som nyttjar samma nätverk desto lättare för en angripare att förflytta sig i IT-miljön. Det blir också svårare att begränsa och avgränsa andra problem. Stödresurser i nätverket (såsom katalogtjänster, DHCP, DNS och systemadministration av nätverksenheter) är kritiska för IT-miljön och behöver särskilt skyddas. Slutar någon del av nätverket eller dess stödresurser att fungera är risken stor för allvarliga störningar i IT-miljön.

Organisationer är ofta bra på att filtrera ingående trafik genom den yttre nätverksgränsen, men ofta sämre att filtrera utgående trafik. Om en angripare har fått åtkomst till någon del av IT-miljön brukar de förändra interna informationssystem så de t.ex. kan användas för att skicka spam eller skapa nätverkstrafik ut från nätverket till en kontrollserver (eng. command-and-control-server, C2-server). Finns ingen filtrering eller övervakning av utgående trafik kommer denna kommunikation inte upptäckas och angriparen kan undgå upptäckt medan information lämnar organisationen.

Rekommenderat arbetssätt

Skydda IT-miljön genom att upprätta olika nätverkssegment med fysisk och logisk separation och skapa kontrollerade trafikflöden mellan segmenten med hjälp av brandväggsfunktioner som skyddar mot att oönskad trafik kan flöda fritt i nätverket. Med fysisk separation avses att ett nätverk inte har några fysiska sammankopplingar med ett annat nätverk. Logisk separation är motsvarande uppdelning genom t.ex. VLAN på datalänk- eller nätverkslagret. Nätverket bör segmenteras utifrån informationssystemens funktion och värdet på informationen som hanteras i ingående informationssystem.

Identifiera och separera informationssystem som inte behöver kommunicera med varandra, t.ex. att klient-till-kli-

Tänk på

- Analysera och dokumentera vilken trafik som ska nå internet direkt, vilken som ska gå genom en aktiv filtreringsfunktion (t.ex. proxy) och vilken trafik som inte alls ska nå internet.
- Se till att filtreringen (såsom brandväggsregler) har en beskrivning av varför trafiken behövs, vilka informationssystem som använder sig av regeln, en notering om vem (verksamhetsansvarig) som beslutat om regeln och när den skapades. Revidera filtreringen regelbundet.
- Se över hur trafik från betrodda samarbetspartners filtreras och övervakas. En angripare kan använda andra organisationer som ingång till det egentliga målet för angreppet.

entkommunikation förhindras så långt det är möjligt. Uppnå detta genom funktioner i nätverksenheterna (brandväggar, switchar, routrar) och lokala brandväggsregler på klienterna.

Viss trafik kan behöva flöda mellan de olika nätverkssegmenten, men denna trafik bör vara filtrerad, det vill säga kraftfullt begränsad till trafik som behövs för att få den funktionalitet som organisationen behöver. Ingen annan trafik bör vara tillåten. Begränsningen kan bestå i att filtrera på IP-adresser, TCP/UDP-portar, typ av trafik och riktning. Övervaka den filtrerade trafiken.

Systemadministration bör, om det är möjligt, ske från dedikerade systemadministrationsklienter placerade på ett särskilt väl skyddat nätverkssegment. Tillåt endast dessa systemadministrationsklienter att nå systemadministrativa gränssnitt.

Skilj de IT-miljöer som är avsedda för utveckling eller test från den IT-miljö som är avsedd för organisationens information som används för produktion.

Mer information om segmentering finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Network Infrastructure Management; CIS Control 12 och Data Protection; CIS Control 3
- UK NCSC 10 steps to cyber security
  Avsnitt: Network security

Exempel från verkligheten

En organisation hade satt upp inpasserings- och larmsystem samt fastighetsdriftsystem i samma nätverksinfrastruktur som de kontorsadministrativa informationssystemen. Vid ett tillfälle slutade nätverket fungera vilket bl.a. medförde att medarbetarna inte kunde ta sig in i fastigheten med inpasseringskort. Det fungerade bara att komma in med tillgång av fysisk nyckel. Många medarbetare blev utelåsta.

Att nätverket slutat att fungera berodde på uppdateringar av de kontorsadministrativa systemen. Hade organisationen haft systemet i olika nätverkssegment hade detta kunnat undvikas. Miljön hade dessutom blivit mycket säkrare mot angrepp oavsett mot vilket segment en sådan riktat sig.

9

Uppgradera mjuk- och hårdvara

Organisationen bör sträva efter att använda av leverantören supporterad mjuk- och hårdvara. Användning av föråldrad mjuk- och hårdvara kommer att öka antalet sårbarheter i organisationens infrastruktur och informationssystem.

Risken i praktiken

Alla mjuk- och hårdvaror blir med tiden sämre på att ge avsedd funktion och tillräcklig säkerhet. Det kan bero på att upptäckta sårbarheter över huvud taget inte kan hanteras, eller att leverantören slutar att skicka ut uppdateringar eller ge support på produkten. Försämringen av produkten gäller för alla typer av informationssystem, t.ex. klienter, servrar, nätverksutrustning, mobiltelefoner eller IoT-utrustning.

Om digitaliseringen bygger på föråldrade produkter uppstår risker. Alla organisationer behöver efter en viss period byta ut hela, eller delar av, informationssystem och kontinuerligt uppgradera mjuk- och hårdvara i produkter där en angripare kan utnyttja kända sårbarheter. I takt med att nya informationssystem integreras med äldre IT-lösningar som inte har funktioner för en säker integration uppstår stora utmaningar för informationssäkerheten.

Vissa informationssystem kan vara svåra att uppgradera, t.ex. utifrån de störningar själva uppgraderingsarbetet kan innebära eller att det finns beroenden som är svåra att hantera. En angripare tar dock inte hänsyn till detta, utan ser möjligheter i de sårbarheter som kan finnas i föråldrade informationssystem.

Rekommenderat arbetssätt

Vid anskaffning av komponenter till informationssystem (mjuk- och hårdvara, externa tjänster och övrig infrastruktur) behöver organisationen ta fram en omsättningsplan där det framgår när komponenter ska bytas ut. Planen underlättar för planering av vilka resurser (exempelvis pengar och arbetstid) som behövs och ger stöd i att identifiera beroenden mellan olika informationssystem. En anskaffning av ett informationssystem är inte en engångskostnad, utan ska ses som en kontinuerlig kostnad så länge funktionen behövs.

Ofta innehåller modernare versioner av mjuk- och hårdvara fler och bättre säkerhetsfunktioner. Dessa kan vara avstängda av leverantören vid leverans för att minska risken för kompatibilitetsproblem. Se till att aktivera och använda de säkerhetsfunktioner som ingår i leveransen och som passar in i organisationens säkerhetsarkitektur. Efter uppgradering behöver informationssystemen åter härdas.

Mer information om uppgradering av mjuk- och hårdvara finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Continuous Vulnerability Management; CIS Control 7.
- UK NCSC 10 steps to cyber security. Avsnitt: Secure Configuration.
- AU ACSC Essential Eight. Avsnitt: Patch operating systems.

Tänk på

- Många produkter av enklare slag, t.ex. vissa IoT-enheter kan varken uppgraderas eller uppdateras. Detta måste beaktas vid anskaffning, placering, driftsättning och livscykelplanering.
- Isolera föråldrad utrustning och komponenter, som inte går att ersätta, i särskilda nätverkssegment som är skilda från övriga delar av IT-miljön och som omgärdas av kompenserande säkerhetsåtgärder för att minska risken för angrepp.
- När nyare produkter med inbyggda säkerhetsåtgärder används bör behovet bedömas om att behålla tredjepartsprodukter som tidigare behövts för att få önskad funktion. Överväg att ta bort de tredjepartsprodukter som blivit onödiga för att minska komplexiteten i IT-miljön.

10

Säkerställ en förmåga att upptäcka säkerhets-händelser

För att kunna upptäcka IT-relaterade säkerhetshändelser behöver organisationen upprätta en funktion med uppgift att övervaka IT-miljön ur ett säkerhetsperspektiv. För att vara effektiv behöver funktionen ha förmåga att samla och analysera säkerhetsloggar för att så tidigt som möjligt upptäcka pågående angrepp samt felaktig och obehörig användning.

Risken i praktiken

På samma sätt som organisationen t.ex. har larm i sina lokaler och bevakning för att upptäcka inbrott eller brand, behöver organisationen ha åtgärder för att upptäcka intrång och oavsiktliga händelser i sin IT-miljö. Brister i detta kan medföra att angripare kan dölja sin närvaro, att skadlig kod oupptäckt kan spridas och att andra oönskade aktiviteter kan pågå i verksamhetens IT-miljö. I många organisationer upptäcks inte cyberangrepp förrän de påtagligt påverkar verksamheten. I värsta fall upptäcks aldrig ett angrepp.

Loggning, logganalys och övervakning används för att upptäcka, begränsa och hantera säkerhetspåverkande händelser och angrepp. Säkerhetsloggning underlättar att:

- upptäcka och utreda felaktig eller obehörig användning,
- reagera på och genomföra relaterade åtgärder för att begränsa oönskade händelser, eller
- ha någon spårbarhet i hur systemen använts vilket i sin tur försvårar möjligheten att påvisa felaktig användning.

Exempel från verkligheten

En anställd på ett tillverkningsföretag fick en dag en bilaga från en tillförlitlig avsändare. Det mottagaren inte visste var att denna bilaga innehöll skadlig kod som inte upptäcktes av antivirusprogramvaran. Den skadliga koden gav angriparen tillgång till organisationens IT-miljö och väl inne i den så kunde angriparen efter ett antal steg få åtkomst till ett konto med systemadministrativa behörigheter. Genom att ändra i Active Directory-inställningarna kunde sedan angriparen få klienter och servrar att ladda ned skadlig kod. Inget av detta märktes av organisationens övervakning. Den nu spridda skadliga koden var ett ransomware och hade som uppgift att kryptera samtliga infekterade system vid ett visst givet tillfälle. Detta sista steg i angreppet genomfördes vid tvåtiden på natten, cirka tre månader efter att angriparen fått initial åtkomst. Organisationen betalade inte någon lösensumma till utpressarna. Istället började organisationen bygga upp sin IT-miljö från grunden vilket tog nästan tre månader och till en hög kostnad.

Det kan dessutom krävas att det i efterhand, ibland efter lång tid, behövs tillgång till innehållet i säkerhetsloggarna för att kunna rekonstruera ett händelseförlopp. Detta om organisationen upptäcker att någon säkerhetshändelse skett först långt efter att den verkligen hände.

Rekommenderat arbetssätt

Organisationen bör skaffa sig förmågan att upptäcka säkerhetshändelser i IT-miljön så tidigt som möjligt. Detta sker ofta i form av en funktion som utför säkerhetsmonitorering, även kallad SOC (eng. Security Operations Center). Detta kräver att det finns personal som har till uppgift att övervaka händelser i IT-miljön. Övervakningen kan ske genom egen personal eller genom att avtala tjänsten med en leverantör.

En SOC använder sig av manuella och tekniska hjälpmedel för att analysera logghändelser. Det tar förhållandevis lång tid att bygga upp automatiska funktioner som på ett tillförlitligt sätt kan larma på logghändelser från informationssystem.

Planera hur säkerhetsloggning ska genomföras. Utgå från att en säkerhetslogg bör innehålla information om var, när och hur en händelse har inträffat och vem som var orsak till att aktiviteten utfördes. Händelser som exempelvis kan loggas är:

- lyckade och misslyckade inloggningar,
- privilegierade aktiviteter,
- förändringar eller försök till förändringar av säkerhetskonfigurationer och behörigheter,
- förändringar i nätverket och inkoppling av utrustning,
- händelser som påverkat loggfunktionen, och
- åtkomst till sekretessbelagd information eller åtkomst och förändring av information som av annat skäl är särskilt viktig för organisationen.

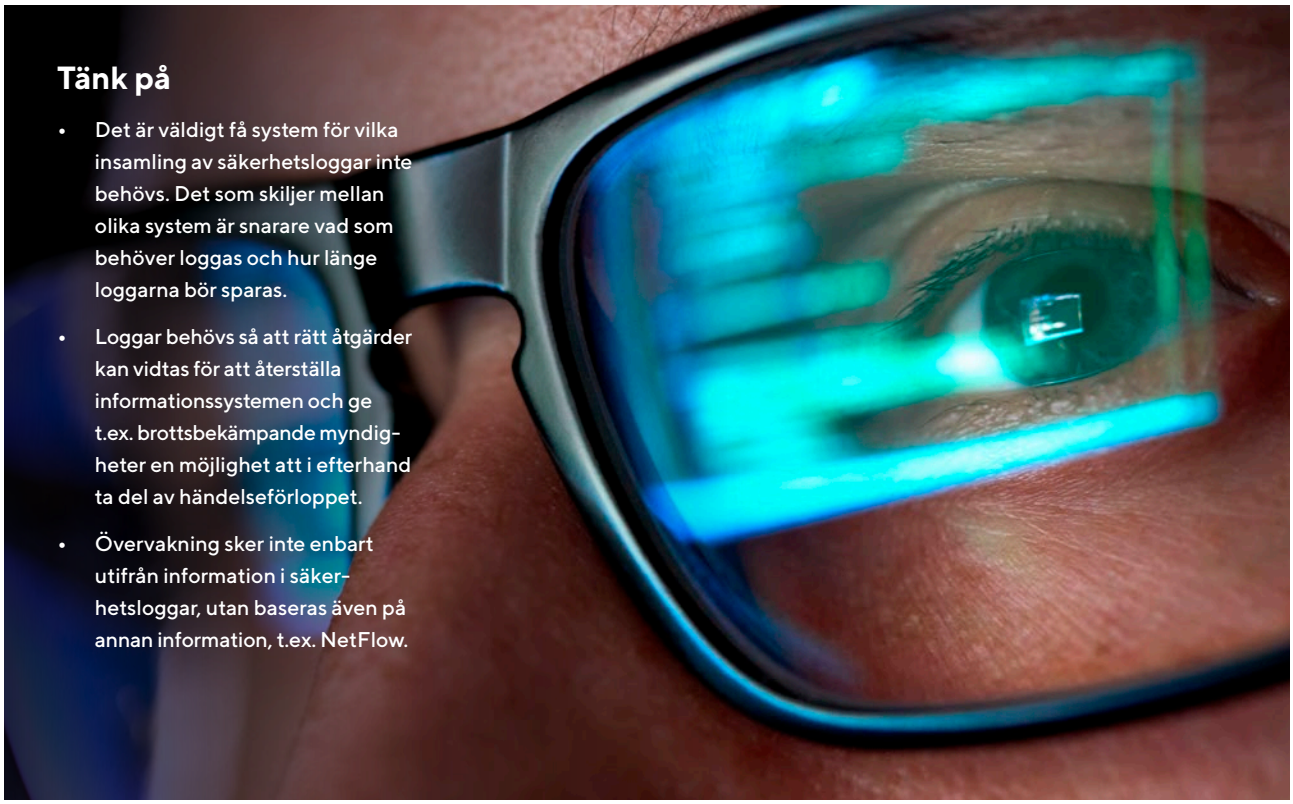
Insamlade loggar bör skickas till en central tjänst för lagring och logganalys. Se till att alla system som regelbundet sparar loggar har tillräckligt med lagringsutrymme så att loggfiler inte fylls upp mellan rotationsintervallen. Spara loggarna i enlighet med rättsliga regler och verksamhetens behov. Det är viktigt att behörighetsstyrningen förhindrar att obehöriga tar del av, eller kan ändra, innehållet i loggar.

Synkronisera alla system där loggning sker mot samma tidskälla och samma tidszon för att underlätta analys och korrelation av loggposter.

Om säkerhetsövervakningen indikerar en händelse med brottsligt uppsåt, uppmanas organisationen att göra en polisanmälan.

Mer information om säkerhetsloggning och detektion finns i

- (US) Center for Internet Security (CIS) CIS Controls. Avsnitt: Audit Log Management; CIS Control 8.
- UK NCSC 10 steps to cyber security. Avsnitt: Monitoring.



Tänk på

- Det är väldigt få system för vilka insamling av säkerhetsloggar inte behövs. Det som skiljer mellan olika system är snarare vad som behöver loggas och hur länge loggarna bör sparas.
- Loggar behövs så att rätt åtgärder kan vidtas för att återställa informationssystemen och ge t.ex. brottsbekämpande myndigheter en möjlighet att i efterhand ta del av händelseförloppet.
- Övervakning sker inte enbart utifrån information i säkerhetsloggar, utan baseras även på annan information, t.ex. NetFlow.

11

När du upptäckt en säkerhets-händelse

När en säkerhetshändelse upptäckts är det viktigt att man redan innan har en förankrad incidenthanteringsprocess. Om medarbetare som arbetar med hantering av system till vardags i ens organisation är insatta i vad som ska göras så har man ett avsevärt bättre utgångsläge när problemet uppstår. Oavsett hur väl man skyddar sina system med de åtgärder som beskrivs i de tidigare kapitlen i den här rapporten behöver man ändå vara beredd att hantera det oväntade. Om man kartlägger alla tänkbara risker och scenarios kan man räkna med att något annat än just dessa kommer att inträffa men att förberedelserna inför dessa hjälper organisationen att hantera de oväntade händelserna.

Risken i praktiken

Om du är förberedd och övad i rutinerna för hanteringen av en säkerhetshändelse ökar sannolikheten för att organisationen framgångsrikt ska kunna hantera den. Att inte vara förberedd riskerar att leda till exempelvis:

- Felaktiga prioriteringar utifrån att man inte vet vilka system och vilken verksamhet som är viktigast
- Otydlig kommunikation då flera individer, med olika god lägesuppfattning, kommunicerar genom olika kanaler
- Incidenthantering startas för sent eftersom säkerhetshändelser inte upptäcks och tas om hand
- Utsliten personal då man inte tagit höjd för att medarbetare behöver sova, äta och skiftplaneras
- Otydlig ledning av incidenthantering och verksamhet som berörs av den

Sammantaget finns mycket att vinna på att förbereda organisationen men det finns också en stor negativ påverkan i att inte förbereda sig. De negativa konsekvenserna att inte förbereda sig riskerar att vara omfattande och långtgående.

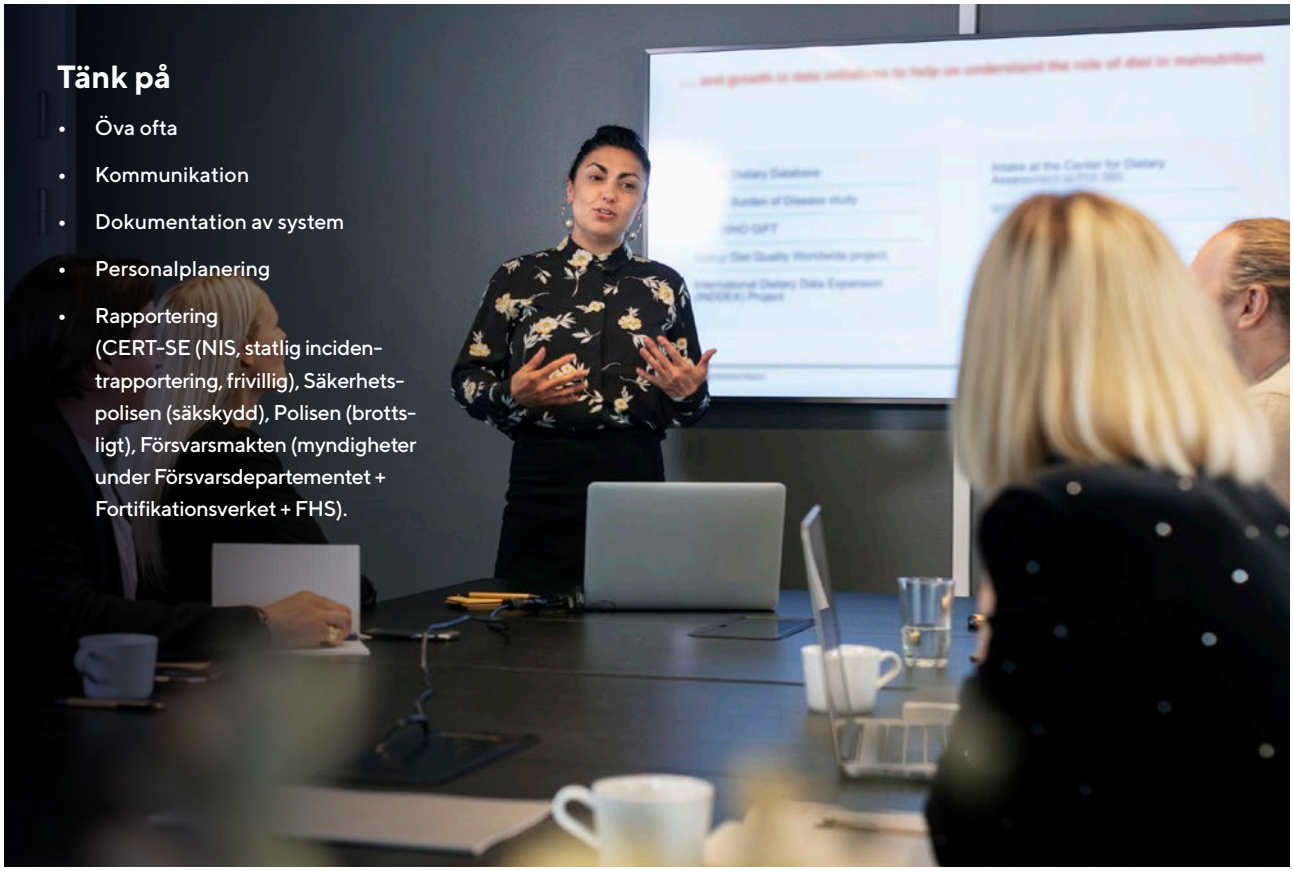
Rekommenderat arbetssätt

Så snart en säkerhetshändelse misstänks bör incidenthantering med incidentledare inledas så snart som möjligt för att samla resurser baserat på incidentledarens behov och snabbt genomföra åtgärder. Här ingår att alla användare av organisationens system ska veta hur och varför misstänkta händelser rapporteras.

För att skapa arbetsro för tekniska resurser i organisationen bör kommunikationskompetens tas med i incidenthanteringsgruppen, den resursen kan ansvara för exempelvis talepunkter, tidslinje och kontakt med media.

Då man inte vet hur hanteringen av en säkerhetshändelse kan komma att utvecklas bör organisationen ha en planering för att hålla personal i tjänst dygnet runt med allt vad det innebär i form av mat, sömn och skiftplanering för att erhålla nödvändig dygnsvila och uthållighet över tid.

Öva hellre ofta och smått än stort och omfattande. Man kan öva på olika nivåer i sin organisation och tillsammans



med andra. Exempelvis kan man öva i sin ledningsgrupp, med en kollega eller i en grupp vid fikabordet som en mikroövning.

Förbered hur man ska hantera en situation när de egna resurserna inte räcker till, vilka kontaktytor har man till de som förväntas stödja vid incidenthantering. Tillse att dokumentation för de egna systemen är uppdaterad så att ett nytillskott av resurser inte blir en börda för incidenthanteringsgruppen iochmed att dessa behöver utbildas.

När väl dammet lägger sig efter en hanterad säkerhetshändelse finns en bra möjlighet att lära av hur hanteringen skett. Att lära av vad som eventuellt fungerat mindre bra ger en chans att hantera nästa situation på ett bättre sätt.

Mer information om ramverk för incidenthantering

- ISO27000 – Standard för informationssäkerhet, cybersäkerhet och dataskydd.
- ITIL – Information Technology Infrastructure Library är en samling principer för hantering av IT-tjänster.
- LIS – Ledningssystem för informationssäkerhet är ett stöd för hur informationssäkerhetsarbetet styrs i verksamheter.

Exempel från verkligheten

En användare tog emot ett mail med en länk som användaren klickade på och uppgav användarnamn och lösenord. Användaren upplevde att detta var konstigt med vidtog inte någon åtgärd. Tio dagar senare hade skadlig kod hunnit sprida sig på nätverket och krypterat organisationens lagrade filer. Resultatet av detta blev en stor hantering med begränsning av organisationens kärnverksamhet över flera veckors tid. Om användaren istället hade rapporterat händelsen och incidenthantering påbörjats hade händelsens påverkan sannolikt kunnat begränsas.

Referenser

Det material som det hänvisas till i denna sammanställning återfinnspå följande platser.

- **(US) Center for Internet Security (CIS) CIS Controls**
  https://www.cisecurity.org/controls
- **UK NCSC 10 steps to cyber security**
  https://www.ncsc.gov.uk/collection/10-steps
- **AU ACSC Essential Eight**
  https://www.cyber.gov.au/publications/essential-eight-explained

De myndigheter som deltagit i arbetet har på sina webbplatser ett omfattande informationsmaterial.

- **Försvarets materielverk**
  https://www.fmv.se
- **Försvarets radioanstalt**
  https://www.fra.se
- **Försvarsmakten**
  https://www.forsvarsmakten.se
- **Myndigheten för samhällsskydd och beredskap**
  https://www.msb.se
- **Polismyndigheten**
  https://www.polisen.se
- **Post- och telestyrelsen**
  https://www.pts.se
- **Säkerhetspolisen**
  https://www.sakerhetspolisen.se

NATIONELLT CYBERSÄKERHETSCENTER

Rapporten är en sammanställning av rekommenderade cybersäkerhetsåtgärder. Den är framtagen av Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Myndigheten för samhällsskydd och beredskap, Polismyndigheten, Post- och telestyrelsen samt Säkerhetspolisen inom ramen för en fördjupad samverkan.

Läs mer om Nationellt cybersäkerhetscenter: ncsc.se

FMV FRA FÖRSVARSMAKTEN MSB Myndigheten för samhällsskydd och beredskap Polisen PTS Säkerhetspolisen