Källa: Nationellt centrum för Cybersäkerhet, ncsc.se

Broschyr: Cybersäkerhet i Sverige 2024 (sid-hänvisning per kapitel)

Innehåll

1. Rekommendationer för bättre säkerhet

Ingen organisation är immun mot cyberhot, men rätt förberedelser kan minska skadorna och förbättra motståndskraften. Kapitlet erbjuder rekommendationer för att åtgärda vanliga sårbarheter som bristande loggning, svaga autentiseringsrutiner och osäkra systemkonfigurationer. Det understryker vikten av att öva på incidenthantering, upprätta tydliga kommunikationsvägar och förbereda resurser för att möta kritiska situationer. Genom systematiskt arbete och regelbundna övningar kan organisationer inte bara hantera säkerhetshändelser effektivt utan även stärka sin beredskap inför framtida hot.

Broschyren innehåller rekommendationer för att hantera sårbarheter, inklusive beskrivningar av problem och praktiska arbetssätt för att åtgärda dem.

Rekommendationerna är tänkta som inspiration och ska inte ses som en uttömmande lista. Det finns fler åtgärder, både enklare och mer avancerade, som kan införas.

Vanligt förekommande sårbarheter

1. Bristande loggning och upptäckt av säkerhetshändelser.
2. Bristande underhålls- och uppdateringsrutiner.
3. Brister i autentiseringsfunktioner.
4. Otillräcklig hantering av konton och behörigheter.
5. Osäkra konfigurationer där onödiga tjänster och protokoll är aktiva.
6. Oförmåga att återställa information från säkerhetskopior.
7. Svagheter i it-arkitektur, såsom bristande segmentering och filtrering.
8. Avsaknad av mjukvarukontroller (t.ex. vitlistning) och övertro på svartlistning.
9. Sårbarheter i äldre informationssystem.
10. Kontrollerad internetåtkomst.

Sammanfattning av rekommenderat arbetssätt

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.

1. **Säkerställ förmågan att upptäcka säkerhetshändelser**
   För att effektivt kunna upptäcka säkerhetshändelser i it-miljön är det viktigt att skapa en förmåga att identifiera dessa så tidigt som möjligt. Det kan göras genom en kombination av manuella, tekniska och automatiserade metoder.

2. **Installera säkerhetsuppdateringar skyndsamt** Se till att prioritera uppdateringar för informationssystem som är exponerade mot internet, är verksamhetskritiska, eller har sårbarheter som riskerar att utnyttjas. Målet bör vara att installera säkerhetsuppdateringar så snart de publiceras.

3. **Förvalta behörigheter och använd stark autentisering** Kontrollera alla konton i it-miljön och inaktivera de som inte längre används. Tilldela bara nödvändiga behörigheter.

4. **Begränsa och skydda användningen av höga behörigheter** Skyddet av administrativa behörigheter är viktigt för att minska säkerhetsrisker i it-miljön. Genom att införa tydliga rutiner för tilldelning och användning av dessa behörigheter kan organisationer skydda sina system och data.

5. **Inaktivera oanvända tjänster och protokoll** För att skydda informationssystem från hot är det viktigt att stänga av funktioner som inte behövs för systemets drift. Genom att använda rätt säkerhetsåtgärder minskar risken för att systemet utsätts för attacker.

6. **Säkerhetskopiera och testa återställning av information** Att skapa och testa säkerhetskopior är viktigt för att skydda information och system mot informationsförlust. Genom regelbundna säkerhetskopior kan organisationer snabbt återställa data och minimera störningar vid incidenter.

7. **Segmentera och kontrollera åtkomst i nätverket** För att skydda organisationens it-miljö är det avgörande att segmentera nätverket för att begränsa och övervaka trafik-flödena mellan olika delar av systemet. Det är också viktigt att säkerställa att endast godkänd utrustning tillåts ansluta.

8. **Säkerställ att endast godkänd mjukvara får köras – vitlistning** Endast tillåten mjukvara ska köras i it-miljön. Genom att använda vitlistning kan organisationen skydda sina system och information genom att förhindra att otillåten mjukvara används.

9. **Uppgradera mjuk- och hårdvara** Byt ut och ersätt gammal mjuk-och hårdvara för att minska sårbarheter och säkerställa att systemen fungerar som de ska och har tillräcklig säkerhet. För att minska sårbarheter i organisationens it-system bör man använda mjuk- och hårdvara som fortfarande får uppdateringar och support från leverantören.

10. **Kontrollera internetåtkomst** För att skydda interna system och data från obehörig kommunikation med omvärlden är säker internetåtkomst avgörande. Genom att införa rätt åtgärder förhindrar man att ett angripet system kan missbrukas för fjärrstyrning eller datastöld.

Rätt säkerhetsåtgärder bara halva jobbet

Trots god cybersäkerhet kan verksamheter drabbas av attacker. Internetkopplade system riskerar överbelastning, intrång och manipulation. Dålig säkerhet gör verksamheten till ett lätt byte, medan ett systematiskt arbete ger bättre motståndskraft – men ingen är immun.

Därför måste varje verksamhet vara redo att hantera incidenter. Man ska vara beredd och veta hur man agerar. Kraven på nätverkets tillgänglighet och känsligheten hos sin data är exempel på saker som avgör hur en incidenthantering bäst genomförs. Men rutiner behöver alla ha, den dag man märker att nätverket drabbats av en säkerhetshändelse.

Att öva olika tänkta scenarier är en utmärkt metod för att förbereda en organisation.

Genomför regelbundna övningar i olika nivåer av organisationen, både internt och i samarbete med andra aktörer. Exempelvis kan man öva i sin ledningsgrupp, med en kollega eller i en grupp vid fikabordet som en mikroövning.

Samtidigt vet man aldrig om den händelse som inträffar passar in i mallen för något av de övade scenarierna. Genom att ha övat på sina rutiner, har man förmågan att agera, även om det som inträffar är något annat än de risker man betraktat som mest överhängande.

Exempel på vad som kan hända vid en incident om man inte är förberedd:

- Felprioriteringar på grund av bristande kunskap om kritiska system.
- Otydlig kommunikation mellan olika aktörer och kanaler.
- Försenad incidenthantering på grund av oupptäckta säkerhetshändelser.
- Överbelastad personal utan plan för skiftarbete.
- Bristande ledning av incidenthanteringen.

Det finns alltså mycket att vinna på att förbereda sig på att ens nätverk råkar ut för en säkerhetshändelse.

Rekommenderat arbetssätt vid incident

Så snart en säkerhetshändelse misstänks startar en incidenthantering. En incidentledare samlar resurser efter behov och genomför snabba åtgärder.

För att skapa arbetsro för de tekniska resurserna, bör kommunikationskompetens tas med i incidenthanteringsgruppen. Intern kommunikation är lika viktig som kontakter med exempelvis kunder och massmedier.

Om incidenten berör nätverk som har höga krav på tillgänglighet, bör organisationen planera för att ha personal i tjänst dygnet runt med allt vad det innebär i form av mat och skiftplanering för att erhålla uthållighet.

Förbered hur man ska hantera en situation när de egna resurserna inte räcker till. Vilka kan stödja? Ser till att all dokumentation för systemen är uppdaterad så att ett nytillskott av resurser inte behöver utbildas, de som bäst kan systemen kommer att behöva ägna sig åt incidenthantering.

När väl dammet lagt sig efter en hanterad säkerhetshändelse ska man ta möjligheten att dra lärdom av hur hanteringen skett. Då går det smidigare nästa gång.

2.1 Säkerställ förmågan att upptäcka säkerhetshändelser, s.18

För att effektivt kunna upptäcka säkerhetshändelser i it-miljön är det viktigt att skapa en förmåga att identifiera dessa så tidigt som möjligt. Det kan göras genom en kombination av manuella, tekniska och automatiserade metoder. Säkerhetsloggar som används i övervakningen bör skapas och skyddas mot obehörig åtkomst eller ändring.

Risker vid bristande övervakning På samma sätt som organisationer använder larm och bevakning för att upptäcka inbrott eller brand i sina lokaler, måste liknande åtgärder implementeras för att identifiera intrång eller oavsiktliga händelser i it-miljön. Bristande övervakning kan leda till att angripare obemärkt kan hålla sig kvar, att skadlig kod sprids oupptäckt, eller att andra oönskade aktiviteter kan fortgå. Många cyberangrepp upptäcks inte förrän verksamheten märkbart påverkas – och i värsta fall upptäcks de inte alls.

Loggning och analys av säkerhetsloggar är viktiga verktyg för att:

- upptäcka och utreda felaktig eller obehörig användning,
- reagera på och genomföra åtgärder för att begränsa oönskade händelser,
- säkerställa spårbarhet för att försvåra möjligheten att dölja felaktig användning.

Rekommenderat arbetssätt, s.19

- **Organisationen bör etablera** en funktion för säkerhetsövervakning, ofta kallad SOC, Security Operations Center. En SOC kan drivas med egen personal eller som en tjänst från en extern leverantör, beroende på verksamhetens behov och resurser.
- **En effektiv övervakning** använder både manuella och automatiserade metoder för att analysera loggar. Automatiserade funktioner, som larmar vid avvikelser, tar tid att utveckla och kräver noggrann testning. För att upptäcka avvikelser är det också viktigt att ha en god förståelse för både system och hur de används i verksamheten.

- **Planera för loggning** av säkerhetshändelser. En säkerhetslogg bör innehålla information om var, när och hur en händelse inträffade samt vem som utförde den. Exempel på händelser som kan loggas är: lyckade och misslyckade inloggningar,
    - privilegierade aktiviteter,
    - förändringar i säkerhetsinställningar och behörigheter,
    - nätverksförändringar och inkoppling av ny utrustning,
    - händelser som påverkar loggfunktionen, och
    - åtkomst till eller ändringar av känslig eller viktig information.

- **De insamlade loggarna** bör skickas till en central tjänst för lagring och analys. Denna tjänst bör vara fristående och fungera även om övriga it-system blir otillgängliga. Genom att ha ett separat system för logghantering kan loggar fortsätta samlas in och analyseras, även vid intrång eller andra störningar, vilket förhindrar att angripare kan manipulera eller radera loggarna.
- **Se till att system** har tillräckligt med lagringsutrymme för loggar och att loggfiler roteras regelbundet så att de inte fylls upp. Loggarna ska sparas enligt gällande lagar och verksamhetens behov. Behörighetskontroller måste säkerställa att obehöriga inte kan se eller ändra loggarna. Synkronisera alla system som loggar mot samma tidskälla och tidszon för att underlätta analys och korrelation mellan loggar.
- **Om övervakningen upptäcker** händelser som tyder på brottslig verksamhet bör organisationen överväga att göra en polisanmälan.

Tänk på

- **De flesta system behöver** samla in säkerhetsloggar, men vad som loggas och hur länge loggarna sparas kan variera mellan system.
- **Loggar är avgörande** för att säkert återställa system och för att brottsbekämpande myndigheter ska kunna analysera händelseförloppet i efterhand.
- **Övervakning handlar inte** bara om loggar, utan kan också inkludera analyser av nätverkstrafik och annan data.
- **Utveckla övervakningen kontinuerligt** genom att identifiera brister i spårbarhet eller förmåga att upptäcka avvikelser.
- **Implementering av säkerhetsövervakning** tar tid och kräver ett nära samarbete med verksamheten, även om tjänsten tillhandahålls av en extern leverantör.

2.2 Installera säkerhetsuppdateringar skyndsamt, s.20

Se till att prioritera uppdateringar för informationssystem som är exponerade mot internet, är verksamhetskritiska, eller har sårbarheter som riskerar att utnyttjas. Målet bör vara att installera säkerhetsuppdateringar så snart de publiceras. Att snabbt installera säkerhetsuppdateringar från leverantörer minskar risken för att angripare utnyttjar kända sårbarheter i hård- och mjukvara.

Risker med att dröja

Nya sårbarheter och angreppsmetoder upptäcks ständigt och kan utnyttjas av angripare som vill komma åt information eller på annat sätt påverka informationssystem och verksamheten negativt. Angripare letar aktivt efter system med kända sårbarheter och övervakar leverantörers säkerhetsuppdateringar. Genom att analysera uppdateringarna kan de snabbt skapa skadlig kod för att angripa sårbarheter innan de har åtgärdats.

Det är därför en kapplöpning mellan organisationer och angripare om vem som agerar först. Fönstret mellan att en uppdatering släpps och att sårbarheten utnyttjas har krympt och kan handla om timmar. För att upprätthålla säkerheten i din it-miljö bör du alltid ha de senaste säkerhetsuppdateringarna installerade och förstå risken med att dröja med installationen av uppdateringarna.

Rekommenderat arbetssätt, s.21

- **Gör en inventering av** alla informationssystem och deras behov av säkerhetsupp-dateringar. Detta omfattar all mjukvara som inbyggd programvara (eng Firmware), drivrutiner, operativsystem och applikationer. Prioritera system som är mest utsatta, exempelvis de som är tillgängliga från internet, de med sårbarheter med höga poäng enligt Common Vulnerability Scoring System (CVSS) eller där sårbarheter är under aktivt utnyttjande. Om uppdatering inte kan genomföras omedelbart, vidta tillfälliga skyddsåtgärder för att minska risken.
- **Inför rutiner som** kombinerar manuella metoder, som omvärldsbevakning, med tekniska verktyg, exempelvis sårbarhetsskanning, för att snabbt identifiera och installera säkerhetsuppdateringar. Utvärdera om uppdateringens påverkan på systemets funktionalitet behöver testas innan installationen genomförs. Prioritera installation av kritiska säkerhetsuppdateringar och säkerställ att dessa implementeras omedelbart när de blir tillgängliga. Automatisera installationsprocessen där det är möjligt för att effektivisera och påskynda arbetet, samtidigt som risken för att missa sårbara komponenter och programvaror minskas.
- **Installera endast uppdateringar** som verifierats från leverantören. Kontrollera att uppdateringarna är digitalt signerade och hämtas via en skyddad förbindelse. Uppdateringar från osäkra källor kan innehålla skadlig kod.
- **Var medveten om** att angripare letar efter nolldagssårbarheter (eng Zero Day), det vill säga sårbarheter som inte har åtgärdats av leverantören. Det kan också vara viktigt att söka efter tecken på intrång efter att uppdateringar har installerats, särskilt om systemen varit sårbara.

Tänk på

- **Håll dig uppdaterad** om relevanta sårbarheter för din it-miljö.
- **Även uppdateringar som** inte är säkerhetsrelaterade kan innehålla viktiga förbättringar. Installera även dessa.
- **Kontrollera noggrant vilka** funktioner som påverkas av uppdateringar för att undvika driftstörningar.
- **Att fördröja installationer** gör att uppgiften blir mer omfattande eftersom uppdateringarna ackumuleras över tid.

2.3 Förvalta behörigheter. Använd stark autentisering, s.22

Kontrollera alla konton i it-miljön och inaktivera de som inte längre används. Tilldela bara nödvändiga behörigheter. Använd flerfaktorsautentisering för publika tjänster, känslig information och konton med administrativ åtkomst. Om flerfaktorsautentisering inte är tillgänglig, använd långa och unika lösenord.

För att förhindra att angripare utnyttjar existerande konton måste organisationen ha full kontroll över konton och deras behörigheter. Det är viktigt att använda stark autentisering, eftersom lösenord ofta är en svag punkt. Flerfaktorsautentisering, särskilt med lösningar som smartkort, höjer säkerheten jämfört med enbart lösenord och skyddar effektivt mot nätfiske och många andra typer av intrångsförsök.

Risker med dålig kontroll över konton

Om en angripare får tillgång till ett existerande konto blir det svårt att upptäcka obehörig aktivitet. Det är vanligt att konton som tilldelats tidigare leverantörer eller anställda förblir aktiva och har tilldelade behörigheter långt efter att leverantörsrelationen eller anställningen avslutats. Konton kopplade till tjänster och system kan också vara aktiva efter att systemen tagits ur drift. Sådana konton kan utnyttjas av angripare för att få åtkomst till organisationens information.

Användning av samma kontouppgifter i både test- och produktionsmiljöer skapar risker. Om angripare får tag på dessa uppgifter i en mindre skyddad testmiljö kan de använda dem för att få åtkomst till produktionsmiljön.

Svaga lösenord är ett annat problem, eftersom många lösenord kan gissas fram med hjälp av ordlistor eller vanliga kombinationer. Om standardlösenord inte ändras kan angripare enkelt hitta dem i offentlig dokumentation.

Nätfiske där användare luras att ange sina uppgifter på falska webbsidor, är ett vanligt sätt för angripare att få tillgång till lösenord. Om samma lösenord används i flera system ökar risken ytterligare.

Rekommenderat arbetssätt, s.23

- **Ge varje användare** och tjänst unika konton. Använd ett automatiserat system för att hantera konton under hela deras livslängd. När en användare slutar eller ett system tas ur drift, ska kontot omedelbart inaktiveras. Konton för tillfälliga användare, som konsulter, ska automatiskt inaktiveras efter en viss tid. Kontrollera regelbundet att inaktivering har skett och att behörigheter har återkallats. Konton som inte använts på länge ska automatiskt inaktiveras.
- **Radera inte konton –** inaktivera dem istället och ta bort behörigheterna. Raderade konton är svåra att spåra i äldre loggar och kan återanvändas på fel sätt.
- **Prioritera flerfaktorsautentisering för:**
    - System som nås via internet, som intranät, e-post, molntjänster, VPN, RDP och SSH.
    - Information med högt skyddsvärde.
    - Administrativa konton.
- **Administrativa konton bör** skyddas med stark autentisering, exempelvis hårdvaru-nycklar, certifikat eller smartkort.

- **Säkerställ att flerfaktorsautentisering** är korrekt implementerad. Om ett system tillåter åtkomst med enbart lösenord parallellt med flerfaktorsautentisering, är säkerheten fortfarande beroende av lösenordet. För konton där flerfaktorautentisering inte kan användas, ska unika och långa lösenord krävas. Använd ett lösenordshanteringssystem för att undvika att lösenord skrivs ned eller återanvänds mellan olika tjänster.
- **Logga och övervaka** all kontoanvändning. Det är viktigt att loggarna skyddas mot obehörig åtkomst och manipulation, så att organisationen kan lita på dem. Särskilt viktigt är det att uppgifter om användares aktiviteter inte kan förnekas (eng Non-Repudiation).
- **Inför en central** behörighetsfunktion för att effektivt hantera och tilldela behörigheter. Var särskilt uppmärksam på konton med administrativa rättigheter och de som inte hanteras av denna funktion.

Tänk på

- **Se till att alla** konton är personliga och att även systemkonton har en ansvarig person.
- **Använd aldrig samma** konton eller lösenord i utvecklings- och produktionsmiljöer.
- **Ändra alla standardlösenord** innan systemen tas i bruk. Detta gäller applikationer, operativsystem, routrar, brandväggar och andra komponenter.
- **Välj autentiseringsmetoder utifrån** behörighet och behov.

2.4 Begränsa och skydda användningen av höga behörigheter, s.24

Skyddet av administrativa behörigheter är viktigt för att minska säkerhetsrisker i it-miljön. Genom att införa tydliga rutiner för tilldelning och användning av dessa behörigheter kan organisationer skydda sina system och data. Använd separata konton för administrativa behörigheter och begränsa dessa till specifika uppgifter, roller och delar av it-miljön. Tilldela aldrig vanliga användare administrativa behörigheter. Behörigheter ska tilldelas restriktivt och konton ska kunna spåras till en specifik person eller ett system.

Risker med höga behörigheter

Ju fler användare och konton med höga behörigheter, desto större är risken att autentiseringsuppgifter (som lösenord) kan komma i orätta händer. En angripare kan lättare dölja sig bland många administratörskonton.

Om en användare med höga behörigheter oavsiktligt kör skadlig kod, kan konsekvenserna bli allvarligare än om koden körs på ett konto med lägre behörighet. Många system kräver konton med specifika behörigheter, men dessa är ofta dåligt dokumenterade av leverantören. Det gör att konton tilldelas för höga behörigheter för att säkerställa systemets funktion, vilket kan utnyttjas av angripare.

Att ha konton med högre behörigheter än nödvändigt ökar risken för allvarliga misstag, såsom radering av information eller ändringar av systeminställningar.

Rekommenderat arbetssätt, s.25

- **Det är viktigt** att noggrant kartlägga vilka konton som har höga behörigheter och hur dessa används, särskilt när det gäller konton som hanterar känslig information. Grundregeln bör vara att ju högre behörighet ett konto har, desto mer restriktiv ska användningen vara. Inget konto ska ha fler behörigheter än vad som är absolut nödvändigt för dess funktion.
- **För att säkerställa** att användningen av höga behörigheter är kontrollerad och dokumenterad bör organisationer vidta flera åtgärder. Viktigast är att använda separata konton för olika typer av uppgifter, som administration av användare, servrar och klientdatorer. Varje konto måste ha unika autentiseringsuppgifter för att minska risken för obehörig åtkomst.
- **Administrativa behörigheter bör** också delas upp efter specifika funktioner. T ex bör ett konto som kan skapa nya användare inte ha möjlighet att ändra loggar, vilket minskar risken för missbruk. Det är också viktigt att använda olika konton för höga behörigheter i olika delar av it-miljön, så att ett kompromitterat konto inte kan ge fullständig åtkomst till hela systemet.
- **Använd alltid flerfaktorautentisering** när det är möjligt. Speciella arbetsstationer för administrativa uppgifter rekommenderas, isolerade från andra nätverk som internet och begränsade till endast den programvara som behövs.

Tänk på

- **Leverantörsdokumentation kan ange** att systemkonton ska ha höga behörigheter. Kontrollera alltid vad som faktiskt krävs.
- **Återkalla höga behörighete**r när de inte längre behövs.
- **Dokumentera vem som** godkänt och utfört ändringar i behörigheter samt när de ska återkallas

2.5 Inaktivera oanvända tjänster och protokoll – härda system, s.26

För att skydda informationssystem från hot är det viktigt att stänga av funktioner som inte behövs för systemets drift. Genom att använda rätt säkerhetsåtgärder minskar risken för att systemet utsätts för attacker. Endast de tjänster, protokoll och nätverkskopplingar som är nödvändiga för systemets funktion ska vara aktiva. Allt annat ska inaktiveras eller tas bort.

Riskerna med exponerade tjänster

Informationssystem exponerar ofta flera tjänster mot de nätverk de är anslutna till, där varje tjänst använder mjukvara och protokoll för att fungera. Eftersom all mjukvara har potentiella sårbarheter, ökar angreppsytan och risken för attacker ju fler tjänster och protokoll som är aktiva.

System som är exponerade externt, som webb-, DNS- och mejlservrar, är särskilt utsatta och måste härdas noggrant. Standardinstallationer har ofta fler aktiva tjänster än vad som behövs, vilket ökar risken.

Många tjänster och protokoll är bakåtkompatibla med äldre system, men efter uppgraderingar bör dessa inaktiveras, även om arbetsinsatsen är hög, eftersom äldre versioner ofta är mer sårbara.

Rekommenderat arbetssätt, s.27

- **Härdning innebär att** operativsystem, programvaror, nätverkskomponenter och applikationer i ett informationssystem konfigureras så säkert som möjligt. Det görs genom att inaktivera eller ta bort tjänster, funktioner och äldre protokoll som inte längre behövs i it-miljön.
- **Aktivera lokala brandväggar på** både klientdatorer och servrar och tillåt bara den nätverkstrafik som är nödvändig. Följ leverantörernas rekommendationer för härdning och säker konfiguration. Större leverantörer har ofta riktlinjer för detta, men kvaliteten kan variera.

Tänk på

- **Genomför regelbundna säkerhetstester** och granskningar för att upptäcka sårbarheter, både från interna system, som klientdatorer, och från externa källor som internet.
- **Säkerställ att härdningsåtgärder** inte återställs vid uppdateringar.
- **Alla system i** it-miljön behöver härdas: klientdatorer, nätverksenheter, servrar, skrivare, molntjänster och ip-telefoner

2.6 Säkerhetskopiera. Testa återställning av information, s.28

Att skapa och testa säkerhetskopior är viktigt för att skydda information och system mot informationsförlust. Genom regelbundna säkerhetskopior kan organisationer snabbt återställa data och minimera störningar vid incidenter. För att kunna återställa förlorad eller ändrad information måste organisationen ha säkerhetskopior och förmågan att återställa data från dessa. Detta gäller både enskilda filer och hela system.

Riskerna med att inte ha säkerhetskopior

Om säkerhetskopior saknas riskerar organisationer att förlora viktig information vid angrepp eller misstag. Ett angrepp med en utpressningstrojan kan kryptera delar av eller hela systemet, vilket gör information otillgänglig. Ett annat exempel är att hårdvarufel kan leda till att ett lagringssystems filer blir korrupta.

Säkerhetskopior är också sårbara om de inte hanteras rätt. Om de lagras osäkert kan obehöriga få åtkomst till eller förstöra dem. Speciellt filbaserade säkerhetskopior, som är åtkomliga via nätverket, riskerar att påverkas av skadlig kod som kan radera data på alla skrivbara enheter.

Återställning kan försvåras beroende på hur och var säkerhetskopiorna sparas. Om säkerhetskopieringssystemet uppdateras kan äldre kopior vara svåra eller omöjliga att återställa.

Vid angrepp med utpressningstrojaner är det viktigt att först identifiera och ta bort hotet innan data återställs. Annars kan skadlig kod fortfarande finnas kvar i systemet och orsaka nya problem.

Rekommenderat arbetssätt, s.29

- **Diskutera med informationsägaren** eller motsvarande hur ofta säkerhetskopior ska tas och hur länge de behöver sparas.
- **Ta dagliga säkerhetskopior** för ny eller ändrad information, inklusive systemdokumentation, loggar och konfigurationsinställningar.
- **Se över behovet** av att säkerhetskopiera applikationer, operativsystem, virtuella maskiner och containrar.
- **Lagra säkerhetskopior offline** eller på en säker plats som inte är åtkomlig via nätverk, för att skydda mot obehörig åtkomst och skadlig kod.
- **Skydda säkerhetskopior mot** brand och vattenskador. Bestäm hur många versioner som ska sparas genom en riskbedömning.
- **Testa säkerhetskopior minst** årligen eller vid större ändringar i it-miljön. Testa både delvis och fullständig återställning.

Tänk på

- **Ett system som** visar att säkerhetskopior är intakta kan vara missvisande. Testa alltid att de kan återställas.
- **Säkerhetskopiera även systemkonfigurationer,** användarkonton och behörigheter. Också licenser och certifikat kan behöva återställas.
- **Öva på att** återställa till ett nyinstallerat system, inte bara till ett befintligt. Vid vissa angrepp kan hela it-miljön behöva ominstalleras.
- **Förstå hur beroenden** mellan olika system påverkar hur säkerhetskopior tas och återställs.

2.7 Segmentera och kontrollera åtkomst i nätverket, s.30

För att skydda organisationens it-miljö är det avgörande att segmentera nätverket för att begränsa och övervaka trafikflödena mellan olika delar av systemet. Det är också viktigt att säkerställa att endast godkänd utrustning tillåts ansluta. Genom att kombinera dessa två åtgärder minskas risken för intrång, spridning av skadlig kod och obehörig åtkomst.

Nätverket bör delas upp i olika segment där trafiken mellan segmenten noggrant kontrolleras och filtreras. Det gör det möjligt att skydda it-miljön mot både interna och externa hot och att begränsa skadorna om en angripare lyckas ta sig in. Samtidigt måste organisationen se till att endast godkänd utrustning ansluter till nätverket. Obehörig utrustning måste identifieras och blockeras, för att förhindra åtkomst till organisationens system och tjänster.

Risker med otillräcklig segmentering och otillåten utrustning

Organisationers nätverk sträcker sig ofta utanför kontorslokalen. IT-system kan varav utkontrakterade, att det trådlösa nätverket når utanför byggnaden, eller genom VPN-uppkopplingar. När it-miljön ansluts till internet eller externa nätverk ökar risken för attacker.

Om nätverket inte segmenteras korrekt kan en angripare röra sig från den plats där de tagit sig in till andra känsligare delar av it-miljön. Detta gör det lättare för dem att kartlägga system och skaffa högre behörigheter. Utan segmentering blir det även enklare att sprida skadlig kod mellan klientdatorer och servrar, särskilt om all trafik tillåts fritt inom samma nätverkssegment.

Om otillåten utrustning ansluts till nätverket, till exempel via ett oskyddat trådlöst nätverk eller ett nätverksuttag, kan angripare få tillgång till systemet och använda det som en språngbräda för vidare attacker. Bristen på övervakning av både inkommande/ utgående trafik kan förvärra situationen, då angriparna kan använda organisationens nätverk för att kommunicera med externa servrar oupptäckt.

Rekommenderat arbetssätt, s.31

- **Skydda nätverket genom** att segmentera det fysiskt och logiskt, baserat på informations-systemens funktion och känslighet. Använd brandväggar, switchar och routrar för att begränsa trafiken mellan segmenten och övervaka denna noggrant. Endast nödvändig trafik bör tillåtas och klient-till-klienttrafik bör undvikas där det inte behövs. Systemadministration bör utföras från särskilt skyddade segment och utvecklingsmiljöer ska hållas separerade från produktionsmiljön.
- **Tillåt endast godkänd** utrustning att ansluta till nätverket och utbilda personalen om vikten av detta. Använd både aktiva och passiva åtgärder, som 802.1X, för att identifiera och övervaka ansluten utrustning. Skapa en lista över alla nätverksanslutna enheter och minska möjliga angreppspunkter genom att stänga av oanvända nätverksportar och skydda nätverksutrustning med lås och loggar.

Tänk på

- **Det är lika** viktigt att hålla obehörig utrustning borta från nätverket som att hålla obehöriga personer borta från lokalerna.
- **Privata enheter kan** utgöra en risk och bör endast tillåtas i avskilda nätverksdelar.
- **Dokumentera trafikflöden och** brandväggsregler samt revidera dessa regelbundet.
- **Trafik från betrodda** partners måste övervakas och filtreras för att undvika att deras system används för attacker.

2.8 Säkerställ att endast godkänd mjukvara får köras- vitlistning, s.32

Endast tillåten mjukvara ska köras i it-miljön. Genom att använda vitlistning kan organisationen skydda sina system och information genom att förhindra att otillåten mjukvara används.

För att skydda it-miljön från otillåten mjukvara bör vitlistning användas. Detta innebär att endast godkända program kan köras, vilket minskar risken för att skadlig mjukvara infiltrerar systemen. Använd också ett modernt operativsystem som kräver att mjukvara och skript är signerade för att förstärka skyddet.

Riskerna med otillåten mjukvara

Otillåten mjukvara kan leda till skadlig kod och orsaka stora problem, till exempel:

• **Dataläckage:** Känslig information kan hamna i orätta händer.

• **Dataförlust:** Viktig information kan gå förlorad eller bli otillgänglig.

• **Avbrott i system:** Verksamhetskritiska system kan störas eller sluta fungera.

Skadlig mjukvara kan också ge angripare tillgång till it-miljön, vilket kan leda till att obehöriga får åtkomst till information, manipulerar data eller använder organisationens resurser till skadliga syften, som att beräkna kryptovalutor eller skicka skräppost.

Rekommenderat arbetssätt, s.33

- **Inför vitlistning för** att endast tillåta körning av godkänd mjukvara och skript på både servrar och klientdatorer. Detta försvårar för angripare att använda otillåtna verktyg. Samtidigt bör övervakning införas för att kontrollera hur godkända program används. På så sätt kan misstänkt aktivitet upptäckas i ett tidigt skede.
- **Tillåt inte användare** att själva installera mjukvara på sina klientdatorer och mobil-telefoner.
- **En bra start** är att aktivera vitlistning i ett inlärningsläge för att identifiera vilka program som behöver blockeras eller godkännas. När systemet är intrimmat, aktiveras det skarpa läget för att stärka skyddet.
- **Svartlistning, det vill** säga blockering av känd skadlig kod, är inte tillräckligt för att skydda mot ny skadlig kod och är därför inte en optimal säkerhetsmetod.

Tänk på

- **Skadlig kod sprids** ofta via e-postbilagor eller webb läsare. Användarna luras då att aktivera makron i dokument som ser ofarliga ut.
- **Konfigurera systemen så** att makron från okända källor inte får köras. Tillåt bara makron från betrodda källor om makron är nödvändiga.
- **Exekverbar kod kan komma** i många olika format, inte bara ”.exe”. Se till att alla typer av kod och makron hanteras av säkerhetsreglerna.

2.9 Uppgradera hård- och mjukvara, s.34

Byt ut och ersätt gammal mjuk- och hårdvara för att minska sårbarheter och säkerställa att systemen fungerar som de ska och har tillräcklig säkerhet.

För att minska sårbarheter i organisationens it-system bör man använda mjuk- och hårdvara som fortfarande får uppdateringar och support från leverantören. Om man använder föråldrad utrustning ökar risken för sårbarheter i systemen.

Risker med gammal mjuk- och hårdvara

All mjuk- och hårdvara blir sämre över tid, både när det gäller funktion och säkerhet. Det kan bero på att sårbarheter inte längre kan åtgärdas eller att leverantören slutar ge support och uppdateringar. Det gäller alla typer av it-system som klienter, servrar, nätverksutrustning och IoT-enheter.

Om en organisation bygger sin digitalisering på gamla produkter uppstår risker. För att undvika detta måste system bytas ut eller uppgraderas regelbundet. När nya system kopplas ihop med äldre, osäkra it-lösningar blir informationssäkerheten svårare att upprätthålla.

Ibland kan det vara svårt att uppgradera system, till exempel på grund av risker för störningar eller beroenden till andra system. Men angripare bryr sig inte om dessa problem utan utnyttjar sårbarheter i gamla system.

Rekommenderat arbetssätt, s.35

- **När man köper in** it-utrustning (mjuk- och hårdvara, externa tjänster och infrastruktur) är det viktigt att ha en plan, livscykelhantering, för när utrustningen ska bytas ut. Planen hjälper till att förbereda resurser som pengar och arbetstid, och att identifiera beroenden mellan olika system. Att köpa it-utrustning är inte en engångskostnad, utan en kontinuerlig investering så länge systemen behövs.
- **Nyare versioner av** mjuk- och hårdvara har ofta bättre säkerhetsfunktioner. Dessa kan vara avstängda från början för att undvika kompatibilitetsproblem. Se till att aktivera och använda de säkerhetsfunktioner som passar in i organisationens säkerhetsstruktur. Efter uppgradering bör systemen också härdas.
- **Många leverantörer ger** information om hur länge en produkt förväntas fungera. Det hjälper till att i tid hitta rätt ersättningsprodukt.

Tänk på

- **Vissa enklare produkter,** som vissa IoT-enheter, kan inte uppgraderas eller uppdateras. Dessa bör användas med försiktighet, och om möjligt beaktas vid inköp, placering och drift.
- **Isolera gammal utrustning** som inte kan bytas ut till separata nätverkssegment, skilda från övriga it-miljön, och vidta säkerhetsåtgärder för att minska risken för attacker.
- **Nyare produkter** har ofta inbyggda säkerhetsfunktioner som kan ersätta tredje-partsprodukter. Genom att använda dessa kan man minska komplexiteten i it-miljön.

2.10 Kontrollera internetåtkomst, s.36

För att skydda interna system och data från obehörig kommunikation med omvärlden är säker internetåtkomst avgörande. Genom att införa rätt åtgärder förhindrar man att ett angripet system kan missbrukas för fjärrstyrning eller datastöld.

Säker internetåtkomst handlar om att minimera risken för att komprometterade enheter kan kommunicera med externa servrar eller tjänster. Genom att begränsa och kontrollera hur internet används inom nätverket, kan man hindra att skadlig trafik lämnar organisationen och säkerställa att alla anslutningar är kontrollerade och säkra.

En viktig del av detta är att använda en dedikerad webbläsare som är strikt reserverad för internetåtkomst. Genom att ha en särskild webbläsare kan organisationen härda och begränsa den med godkända tillägg och säkerhetsinställningar, vilket gör den mer resistent mot sårbarheter och attacker. Det minskar även risken att andra applikationer eller tjänster får tillgång till internet på ett osäkert sätt.

Riskerna med direkt internetåtkomst

Direkt åtkomst till internet innebär att en angripare som tagit sig in i ett system enkelt kan kommunicera med externa servrar för att fjärrstyra systemet eller stjäla data. Utan skydd, som en proxy eller en brandvägg, kan skadlig trafik obemärkt skickas ut från det interna nätverket, vilket gör det svårt att upptäcka och stoppa attacker i tid.

Rekommenderat arbetssätt, s.37

- **För att minska riskerna** med direkt internetåtkomst bör en dedikerad och härdad webbläsare användas exklusivt för internetanslutningar. Denna webbläsare ska vara strikt kontrollerad med endast godkända tillägg och säkerhetsinställningar, vilket minimerar risken för sårbarheter och attacker. Det är också viktigt att synkronisering av webbläsarprofiler mellan arbets- och hemmadatorer inte tillåts, då detta kan leda till att känslig information exponeras i mindre säkra miljöer.
- **Lokala brandväggsregler** ska implementeras för att säkerställa att endast den härdade webbläsaren har tillgång till internet via en webbproxy. Detta begränsar åtkomsten för andra program och tjänster, vilket gör det svårare för skadlig trafik att passera obemärkt. Ingen direktrouting av trafik till internet ska tillåtas. All trafik ska hållas lokal eller styras via proxyn för att minska risken för oönskad extern kommunikation.
- **Webbproxyn används** för att filtrera och logga all trafik, vilket säkerställer att endast tillåten kommunikation når internet. Genom att analysera dessa loggar kan man upptäcka och reagera på misstänkt aktivitet i tid. All trafik ska gå via proxyn, och ingen direkt åtkomst till internet ska tillåtas för att minska risken för otillåten eller osäker kommunikation.
- **Om det av någon anledning** inte är möjligt att använda en proxy, bör alternativa lösningar som lastbalanserare eller integrationstjänster användas för att säkerställa att trafiken fortfarande kontrolleras på ett säkert sätt.

Tänk på

- **Uppdatera** brandväggs- och proxyregler regelbundet.
- **Se till** att webbläsaren är härdad och inte tillåter osäkra tillägg.
- **Övervaka** proxyloggar kontinuerligt för att upptäcka avvikelser.
- **Utbilda** användare i säker internetåtkomst.

//