# Cybersäkerhet

## I SVERIGE 2024

# Innehåll

# Förord

**Cybersäkerhet är något** för alla verksamheter att hantera, lika självklart som man har fysisk säkerhet i form av ett lås i ytterdörren och att alla ens mest värdefulla ägodelar inte ligger på köksbordet. Att man har ett brandlarm och vet att larmnumret är 112. Parallellen kan dras längre om man vill.

**Trots att behovet** av cybersäkerhet varit uppenbart i decennier, har många verksamheter ännu inte tagit tag i ämnet på det allvar som krävs. Pliktskyldiga åtgärder utan systematik är helt enkelt inte tillräckliga. Först med ett systematiskt informationssäkerhetsarbete får man underlag för att veta vilka åtgärder som är motiverade, och en bas för att implementera dem. Den här broschyren är tänkt som en kickstart för de som känner på sig att de kanske inte kommit igång med det arbetet som de borde.

**Broschyren kan också** tjäna som inspiration för verksamheter som redan kommit långt i sitt cybersäkerhetsarbete, och vill ha ett material för att introducera nya kolleger eller verksamhetsledningar i ämnet. På runt 40 sidor får man en grund att stå på, för att sedan diskutera vad ens egen verksamhet har för behov. Vi går kortfattat igenom hur hotet ser ut, några vanliga metoder för angrepp, saker att observera rörande sina nätverk och till sist tio konkreta råd. Det ersätter inte ett systematiskt informationssäkerhetsarbete, utan ska locka just till att sätta igång med ett sådant, eller aktualisera utvärdering av redan gjorda insatser.

**Nationellt cybersäkerhetscenter är** sedan november 2024 del av FRA. Inom centret samarbetar flera myndigheter med kompetens och uppgifter inom cybersäkerhet, samt näringslivet. Under kommande år planeras verksamheten att byggas ut och bli en central plats för svensk cybersäkerhet. Varje verksamhet har dock ett eget ansvar för att ta hand om sin säkerhet – den här broschyren är utgiven som ett stöd för det.

Den här produkten är en gemensam bild av cybersäkerhet i Sverige 2024 som 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.

# Hotaktörer

Sverige står inför komplexa cyberhot från statliga aktörer, kriminella nätverk och ideologiskt motiverade grupper. Dessa aktörer agerar med olika syften – från underrättelseinhämtning och sabotage till ekonomiska vinster och påverkan. Med avancerade metoder och hög anonymitet hotar de både samhällsviktig infrastruktur, nationell säkerhet och ekonomisk stabilitet.

# Vilka hotar oss?

**De cyberhot som** riktas mot Sverige är mångfacetterade och kan kopplas till flera olika typer av hotaktörer. I huvudsak utgörs dessa av statliga aktörer, kriminella och i viss omfattning även av ideologiskt motiverade aktörer, såsom hacktivister.

Statliga aktörer genomför cyberangrepp mot Sverige i syfte att exempelvis inhämta information som kan gynna det egna landets utrikes- och säkerhetspolitiska intressen eller i syfte att stärka det egna landets ekonomi och företag genom företagsspionerі.

Cyberkriminalitet syftar i de allra flesta fall till att tjäna pengar. De ideologiskt motiverade aktörerna agerar i enlighet med sina egna formulerade agendor.

Metoder och verktyg för cyberangrepp utvecklas ständigt och hotaktörernas spelplan förändras i takt med teknikutvecklingen. Hotaktörerna använder sig ofta av enklast möjliga metod för att uppnå önskat resultat och i många fall krävs inte att man använder sig av avancerade metoder.

Att skydda sig mot cyberangrepp från kvalificerade hotaktörer är en nationell angelägenhet. Samhällsviktig infrastruktur är mål för främmande makt, som strävar efter att kunna påverka den. Avsikten kan vara att påverka beslutfattande i fred, skapa oro i ett krisläge eller försvåra våra försvarsansträningar i krig.

Datorer i Sverige angrips också i syfte att i sin tur kunna användas i cyberangrepp mot mål i andra länder.

## Svårigheter med att identifiera en hotaktör på cyberområdet

Förutsättningarna för anonymitet är goda på cyberområdet och en identifiering av en hotaktör är ofta förenad med osäkerhet. Identifiering, eller attribuering, kräver ofta att flera olika informationsunderlag läggs samman och bedöms.

Det händer att olika hotaktörer komprometterar varandras infrastruktur, stjäl verktyg från varandra eller till och med tar över varandras mål.

En hotaktör kan även använda sig av ombud, proxys. Det kan vara kriminella nätverk som får uppdrag och i vissa fall även tekniska hjälpmedel att utföra dem. ●

# Statliga aktörer

**De statliga aktörerna** utgörs i de flesta fall av nationella underrättelse- och säkerhetstjänster samt grupperingar med kopplingar till dessa.

Dessa aktörer använder cyberangrepp för att uppfylla olika nationella intressen. Det kan handla om att ge det egna landet utrikes- och säkerhetspolitiska fördelar, gynna det egna landets forskning och utveckling och skapa konkurrensfördelar för inhemska företag. Det kan också vara fråga om att skaffa underlag för senare påverkansoperationer. Det kan även handla om angrepp i förberedelse för att vid ett senare tillfälle kunna orsaka skada på samhällsviktig infrastruktur.

Vissa statliga aktörer är mycket kvalificerade och genomför cyberangrepp storskaligt, systematiskt, uthålligt och globalt för att tillgodose det egna landets intressen. Cyberangrepp erbjuder goda möjligheter till anonymitet.

Cyberangrepp från statliga aktörer mot svenska mål sker hela tiden, en del med framgångsrikt resultat.

Aktörerna utvecklar sin metodik och sina verktyg och de blir allt mer sofistikerade. Samtidigt fortsätter de att använda sig av äldre kända metoder så länge dessa fortsatt ger resultat.

Statliga aktörer benämns ofta som Advanced Persistent Threat (APT) i dessa sammanhang. De är resursstarka i form av pengar, personal och expertis, har stor långsiktighet och påtaglig uthållighet.

## Utrikes- och säkerhetspolitiska intressen

För att tillgodose sitt eget lands utrikes- och säkerhetspolitiska intressen använder statliga aktörer cyberangrepp mot varierande mål. Olika syften ger olika effekter.

Cyberangrepp från statliga aktörer i syfte att inhämta underrättelser pågår ständigt. De angriper bland annat verksamheter som hanterar känslig eller skyddsvärd information som rör Sveriges säkerhet, men även öppen information är av intresse. Syftet är att ge den egna staten större handlingsfrihet och inflytande i utrikes- och säkerhetspolitiska frågor.

Vissa cyberangrepp genomförs för att försvaga den man angriper. Allt ifrån stulen information som används för att misskreditera makthavare och splittra landet, till angrepp som syftar till att slå ut samhällsviktig infrastruktur, skada tilliten till svenska institutioner, eller på annat sätt försvaga effektivt svenskt beslutsfattande.

Statliga aktörer genomför även angrepp för att få åtkomst till personlig information. Angreppen sker i syfte att få fram uppgifter som kan användas i utpressningssyfte mot personer i maktposition eller som har tillgång till information som aktören vill åt. Det kan

även ske i syfte att bedriva flyktingspionage för att kontrollera inhemska oppositionella eller tysta opinioner utomlands. Angrepp riktas ofta mot individers personliga it-utrustning, vilket gör dem särskilt sårbara. Om en stor mängd av dessa uppgifter är samlade på annat håll, exempelvis i centrala databaser, kan angriparna istället välja att rikta sina attacker dit för att få tillgång till samma information i större skala.

## Militär förmåga

Statliga aktörer bedriver underrättelseinhämtning mot bland annat svensk försvarsindustri och myndigheter i syfte att kartlägga Sveriges försvarsförmåga och sårbarheter. I detta söker man information från öppna källor, men även genom att skaffa sig tillgång till skyddade system via cyberangrepp. Många länder utvecklar dessutom en förmåga att kunna genomföra avancerade cyberoperationer, bland annat offensiva cyberangrepp.

I konflikter mellan stater är cyberoperationer ett av de medel som kan användas för att minska ett lands försvarsvilja. De kan stödja påverkansoperationer där information som stjäls genom cyberangrepp sedan kan manipuleras och publiceras för att påverka opinionen. Stater kan även genomföra angrepp som stör samhällsviktiga eller försvarsrelaterade funktioner i syfte att minska ett lands förmåga att stå emot ett kommande militärt angrepp eller försvaga ett lands motståndskraft mot påtryckningar. Genom att välja vilka mål hotaktören inriktar sig mot och hur stor effekt som ska uppnås, finns möjlighet för en statlig aktör att operera under fredsförhållanden där krigets lagar inte är tillämpliga. Problematiken kring attribuering stärker denna möjlighet.

Effekterna av ett cyberangrepp kan få motsvarande konsekvenser för samhällsviktiga funktioner och kritiska it-system som ett konventionellt väpnat angrepp.

Takten i den tekniska utvecklingen är hög och det upptäcks kontinuerligt nya sårbarheter som sedan åtgärdas. Det pågår således en ständig kapplöpning mellan medel och motmedel. Därför krävs det ett konstant utvecklingsarbete för att upprätthålla en förmåga att stå emot avancerade cyberoperationer.

## Ekonomiska intressen

Vissa stater stjäl företagshemligheter från privata företag systematiskt och förser egen industri med dessa uppgifter för att öka sin konkurrenskraft. Brister eller gap i det egna landets innovationsförmåga vägs upp genom industrispionage som möjliggörs genom cyberangrepp.

Cyberangrepp i syfte att genomföra industrispionage mot svenska mål är numera en del av vardagen. Angreppen får som resultat att innovativa svenska företag konkurreras ut av sina egna lösningar som stulits av statliga aktörer.

Kunskap och innovationer är stöldbegärliga för stater som vill ta genvägar i sin egen teknikutveckling. Många svenska företag och lärosäten har stora mängder forskningsresultat, utvecklingsprojekt och patentsökningar och dessa representerar enorma värden. För Sverige som är ett land beroende av utrikeshandel är det viktigt att vara en säker marknadsplats. Cyberhotet från statliga aktörer som drivs av ekonomiska intressen är över tid mycket allvarligt för Sveriges fortsatta välstånd och förtroende i omvärlden.

Ytterligare ett mål för sådana stater som använder cyberoperationer är att skaffa sig monetära tillgångar, exempelvis genom att angripa banker för att stjäla pengar eller kryptovaluta. Genom att infektera verksamheter med skadlig kod (ransomware) får dessa aktörer möjlighet till ekonomisk utpressning. I tider av sanktioner kan cyberangrepp för att stjäla pengar vara en lockande lösning för de stater som är föremål för sanktionerna. ●

# Ideologiskt motiverade aktörer

**Med ideologiskt motiverade** hotaktörer avses organisationer, enskilda individer eller grupper vars handlingar är drivna av ideologiska skäl. Det finns flera sådana aktörer som betraktar angrepp mot svenska mål som legitima.

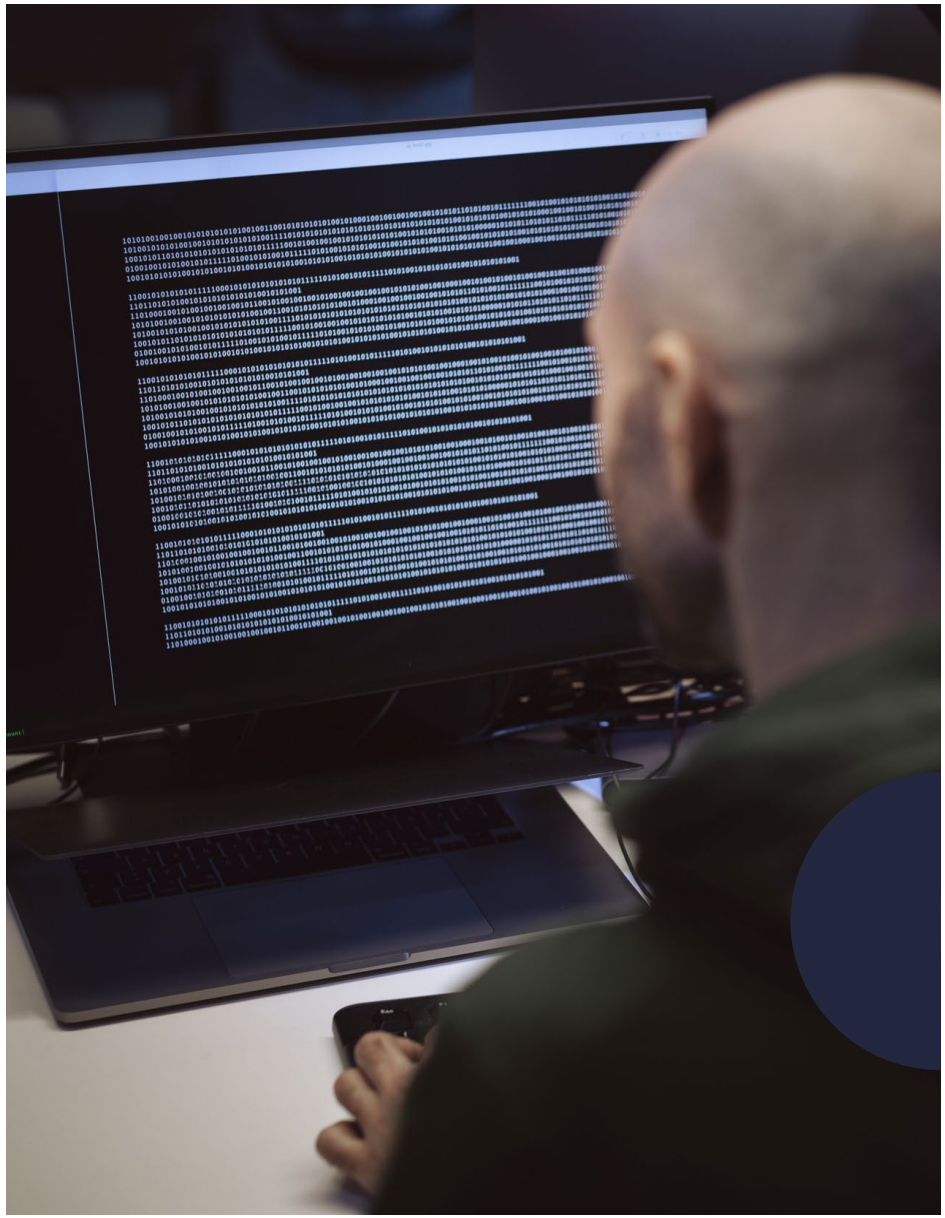
Den generella förmågan att utföra cyberangrepp är ofta mindre utvecklad än ambitionen att genomföra sådana. Försök till cyberangrepp med enklare tekniska medel och metoder kommer att fortsätta, såsom kapade webbplatser eller distribuerade överbelastningsattacker (DDoS). ●

# Kriminella aktörer

**Cyberkriminalitet är en** gränsöverskridande verksamhet som genomförs för att tjäna pengar. Kriminella tar minsta möjliga risker för att erhålla största möjliga avkastning.

Där det finns pengar att stjäla kommer även de kriminella att befinna sig. Vilket mål aktören väljer är oftast inte intressant, utan det viktigaste är vilken vinst man kan räkna med. Ransomware, bedrägerier, stölder och liknande kriminella aktiviteter drabbar inte enbart företag utan även myndigheter, och privatpersoner. Det innebär att detta kan drabba även verksamheter med höga skyddsvärden.

En tillbakablick på inträffade händelser visar att hotaktörer har en tendens att använda de verktyg som fungerar för stunden. Istället för att använda nya och avancerade metoder väljer de att förfina existerande metoder och det blir allt svårare för användare att upptäcka förfalskningar och bedrägerier. ●



# Angreppsmetoder

Cyberangrepp tar många former och utnyttjar såväl tekniska sårbarheter som mänskliga svagheter. Från lösenordsattacker och nätfiske till avancerade angrepp via tredjepartsleverantörer och mobila enheter – hotbilden utvecklas ständigt. Genom att kombinera olika metoder kan angripare manipulera system, stjäla känslig information och orsaka stor skada för både individer och organisationer.

# Lösenordsattacker

**Angripare har gissat** lösenord sedan datorsystem kunde kopplas upp med modem på det sena 1980-talet. Lösenordens kvalitet är ofta låg, vilket gör att många kan forceras med beräkningskraften hos en vanlig bärbar dator. Återanvändning av lösenord är ett särskilt stort problem, eftersom angripare ofta kan använda läckta lösenord från tidigare intrång.

# Angrepp via e-post

**E-post används ofta** som attackvektor i nätfiske (phishing) eller, om angreppet är riktat mot specifika individer, i riktat nätfiske (spearphishing). Angripare skickar e-postmeddelanden som verkar legitima för att lura mottagaren att klicka på länkar, öppna bifogade dokument eller tillåta hämtning av innehåll från internet. Genom sådana åtgärder kan angriparen stjäla lösenord, kreditkortsuppgifter eller installera skadlig kod.

Nätfiske och riktat nätfiske utnyttjar mänskliga svagheter som nyfikenhet, men också bristfällig implementation av tekniska skydd.

## Nätfiske

Nätfiske riktar sig mot en bred målgrupp och saknar ofta personliga detaljer. Angripare försöker träffa så många offer som möjligt genom generiska meddelanden som påstår sig vara från betrodda aktörer.

## Riktat nätfiske

Riktat nätfiske går mot specifika individer eller organisationer och inkluderar detaljer som namn eller information om mottagaren. Detta kräver att angriparen kartlägger målet i förväg. Riktat nätfiske används ofta av statliga aktörer och kriminella, särskilt vid riktade trojan-angrepp där några få offer är målet.

# Webbangrepp

**Webbapplikationer består ofta** av komplexa konstruktioner med flera lager av kod och abstraktioner, vilket skapar potentiella sårbarheter. Angripare kan exempelvis injicera skadlig kod via ett webbformulär, som sedan körs i databasen. Detta kan leda till att känslig information exponeras, att data ändras, eller att obehöriga får åtkomst till systemet.

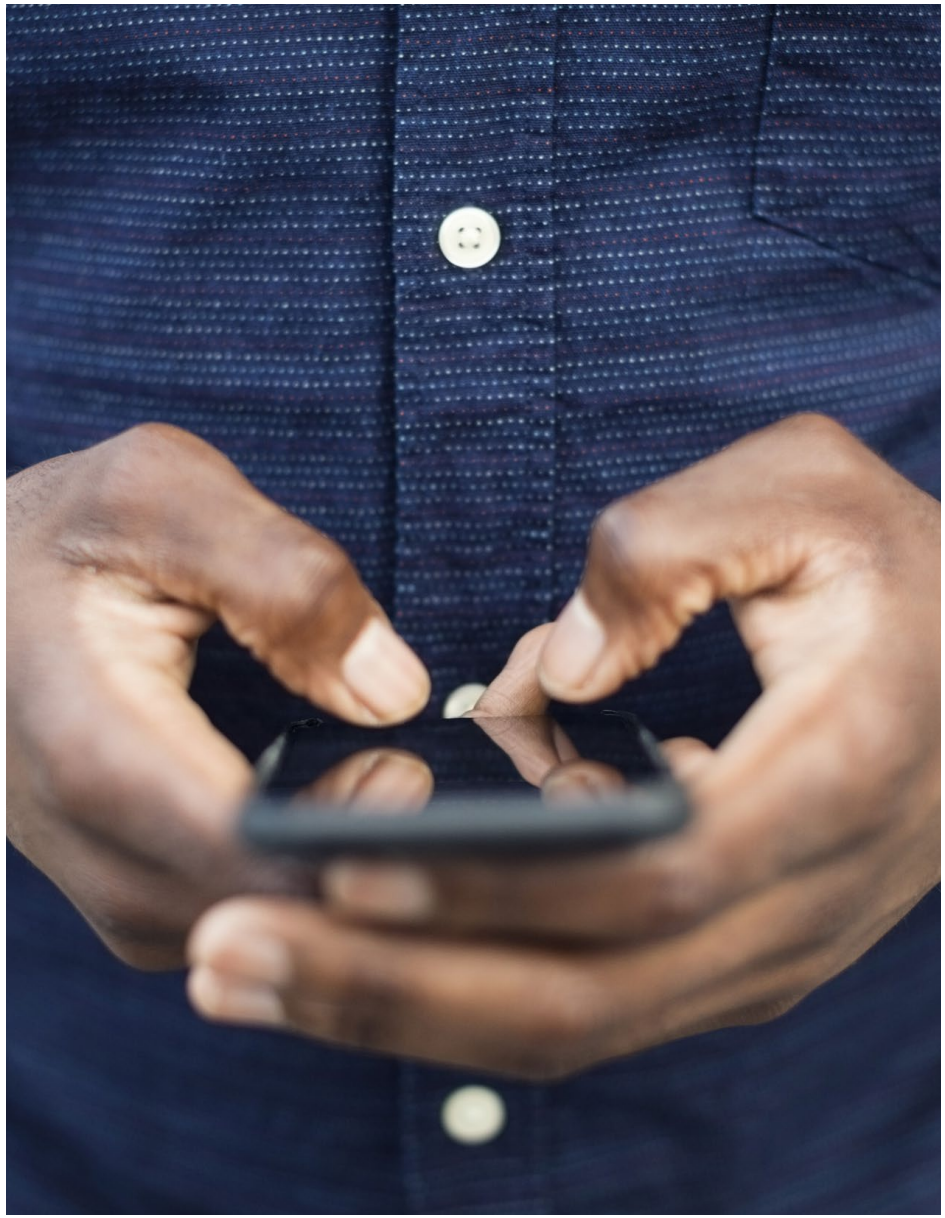
# Vattenhålsangrepp

**Vattenhålsangrepp skiljer sig** från nätfiske genom att angriparen inte kontaktar offret direkt. Istället placeras skadlig kod på en webbplats som är av intresse för målgruppen, exempelvis branschsidor eller lokala nyhetssajter. När användare besöker webbplatsen laddas koden ned till deras system, ofta utan deras vetskap. Detta kan ske genom att utnyttja sårbarheter i webbplattformen eller genom att manipulera tredjepartsinnehåll, såsom annonser.

# Angrepp mot tredjepartsleverantörer

**Tredjepartsleverantörer spelar en** central roll i många organisationers leveranskedjor, och angripare utnyttjar detta genom så kallade supply chain-angrepp. Detta innebär att angriparen komprometterar en leverantörs system eller tjänster för att injicera skadlig kod i produkter eller tjänster som levereras till slutkunden. När kunden använder eller uppdaterar produkten sprids den skadliga koden direkt in i organisationen.

Exempelvis kan angripare manipulera öppen källkod eller utvecklingsverktyg som används av leverantören. Andra metoder innefattar kompromettering av programuppdateringar, integrationslösningar eller tredjepartssystem.



# Angrepp mot mobila enheter

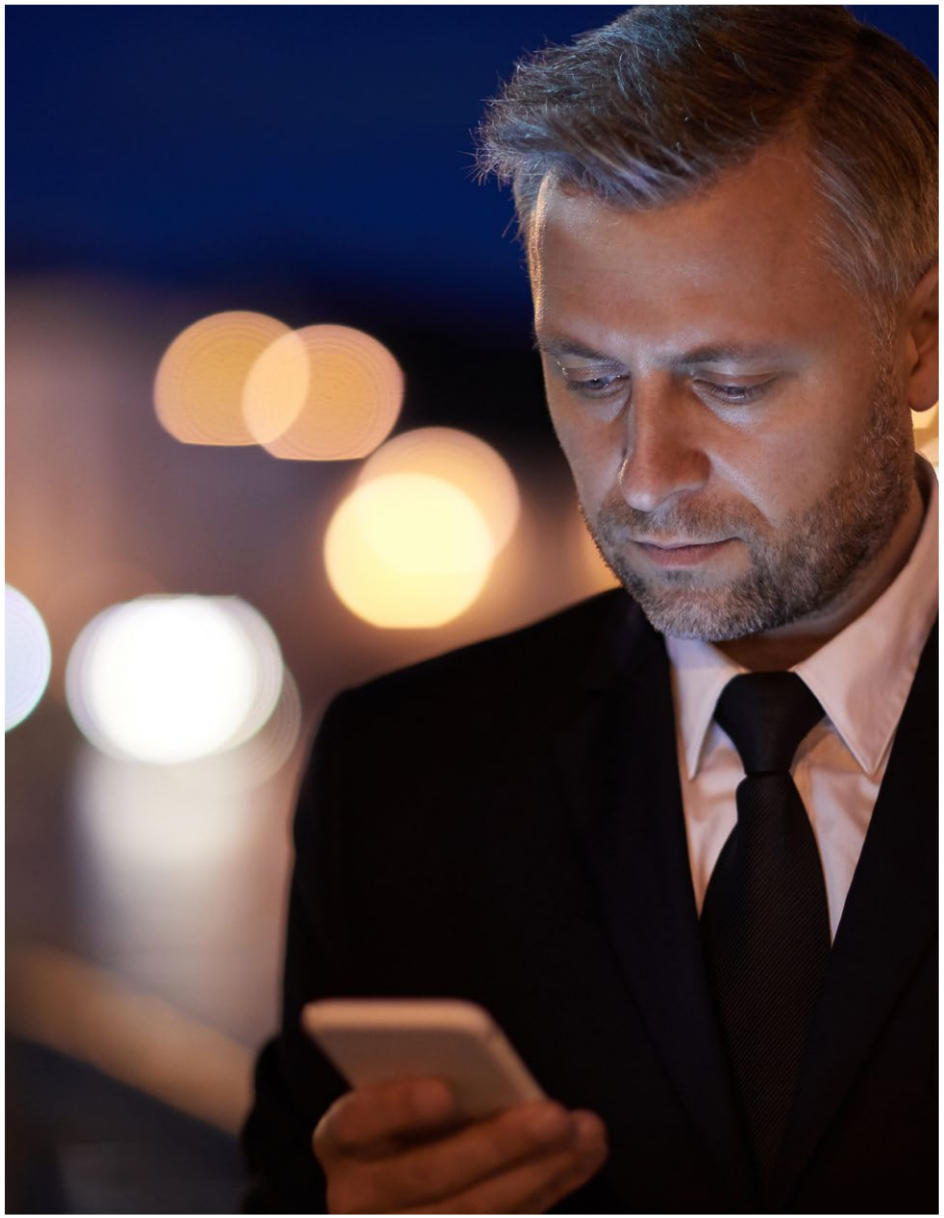
**Mobiltelefoner och andra** bärbara enheter är sårbara plattformar som kan utnyttjas i cyberangrepp för att samla in information. Om de infekteras kan angripare få åtkomst till en mängd känsliga uppgifter, såsom e-post, kreditkortsinformation, planerade resor, bilder, meddelanden, kontaktlistor och GPS-positioner. Dessutom kan mobiltelefonens mikrofon användas för att avlyssna samtal och omgivande ljud.

# Fysisk åtkomst

**Fysisk åtkomst utgör** ett annat hot, där en individ kan utnyttja åtkomst till nätverk som är svåra att nå via internet för att införa skadlig kod.

Ett exempel är användning av USB-stickor som innehåller skadlig kod. Dessa kan spridas på sätt som gör att personer oavsiktligt ansluter dem till organisationens nätverk, vilket kan leda till infektion.

Ett annat exempel är insiderhot, där en person inom organisationen, antingen rekryterad av angriparen eller en missnöjd anställd, injicerar skadlig kod eller avslöjar känslig information. Insiderhot kan också skapas genom att utnyttja individens personliga situation, exempelvis ekonomiska svårigheter eller utpressning.



# Brister och beroende

Ett starkt cybersäkerhetsarbete kräver struktur, kompetens och tydliga prioriteringar – men många verksamheter kämpar med brister som kan få allvarliga konsekvenser. Från otillräcklig kravställning vid upphandling till svårigheter att hantera molntjänster och kompetensbrist, visar sig riskerna på flera nivåer. Samtidigt ökar hoten, vilket understryker vikten av ett systematiskt, dynamiskt och långsiktigt säkerhetsarbete som inkluderar både tekniska lösningar och organisatoriska insatser.

# Avsaknad av ett strukturerat säkerhetsarbete

**Cybersäkerhet är en** central del av allt säkerhetsarbete i dagens digitaliserade samhälle. Nästan alla verksamheter förlitar sig på digital information och tjänster, men arbetet med cybersäkerhet är ofta otillräckligt i förhållande till de hot och risker som finns.

# Bristande säkerhetsarbete innebär risktagande

**Ett bristande säkerhetsarbete kan** få allvarliga konsekvenser. Röjande av känslig information kan skada individer, medan manipulation eller skador på system kan hota hela verksamheten. Säkerhetsarbetets framgång avgörs i hög grad av ledningens inställning. Det är avgörande att ledningen inte bara tar ansvar utan även stödjer och följer upp säkerhetsåtgärderna. Detta ansvar måste tydliggöras på alla nivåer inom organisationen.

## Ett systematiskt förhållningssätt

Ett systematiskt säkerhetsarbete börjar med att identifiera verksamhetens skyddsvärden, analysera hot och risker, och fastställa nödvändiga åtgärder. Säkerhetsarbetet måste vara kontinuerligt, eftersom verksamheter och hotbilder förändras över tid. Detta innebär att säkerhet inte är en engångsinsats, utan en dynamisk process som kräver regelbunden uppföljning och anpassning.

## Hantera nya teknologier

Utvecklingen av ny teknik ställer krav på verksamheter att förstå och bedöma dess påverkan på säkerheten. Teknik introduceras ofta gradvis, vilket gör det svårt att fastställa exakt när säkerhetsanalyser behövs. Därför är det viktigt att kontinuerligt granska tekniska förändringar och deras inverkan på tidigare säkerhetsbedömningar.

## Regelverk och säkerhet

Lagstiftning ställer krav på cybersäkerhet och skapar enhetlighet i tillämpningen. Eftersom lagar måste vara generella för att passa många verksamheter är det organisationens ansvar att tolka och implementera dessa krav i enlighet med sina unika förutsättningar.

# Kravställning vid upphandling och utkontraktering

**En tydlig och** välformulerad kravställning är en förutsättning för en lyckad upphandling. Att kravställa cybersäkerhet kräver kompetens, både när det gäller anskaffning av varor och tjänster samt vid utkontraktering av it-infrastruktur.

Med rätt kravställning kan utkontraktering vara en säkerhetshöjande åtgärd, särskilt för verksamheter som inte själva har möjlighet att upprätthålla tillräcklig kompetens eller resurser. Många svenska verksamheter, både offentliga och privata, utkontrakterar därför delar av sin it-infrastruktur till externa tjänsteleverantörer.

Om flera leverantörer eller underleverantörer delar på ansvaret för den utkontrakterade it-infrastrukturen kan det bli svårare att säkerställa en kontinuerlig och enhetlig säkerhetsnivå. Tydliga avtal och hänvisningar till etablerade standarder och regelverk, kan underlätta både för kunder och leverantörer att uppfylla säkerhetskrav.

## Molntjänster – möjligheter och utmaningar

Molntjänster är en vanlig form av utkontraktering där verksamheter hyr resurser istället för att själva investera i hårdvara och mjukvara. Detta kan omfatta allt från enskilda applikationer till hela it-infrastrukturer.

Användningen av molntjänster innebär ofta att verksamheten överlåter kontroll över system och data till leverantören, vilket kan begränsa insynen och försvåra övervakning av säkerhetsåtgärder. Samtidigt har molnleverantörer ofta hög kompetens inom säkerhet och tillgång till avancerade lösningar som kan vara svåra att upprätthålla inom en egen organisation.

Med rätt analys, kravställning och kontroll kan molnlösningar bedömas som både attraktiva och säkra, beroende på verksamhetens behov. Det är dock avgörande att tydligt definiera säkerhetskrav, följa upp leverantörens arbete och säkerställa att insyn och kontroll inte går förlorade. ●

# Säkerställa relevant kompetens inom cybersäkerhet

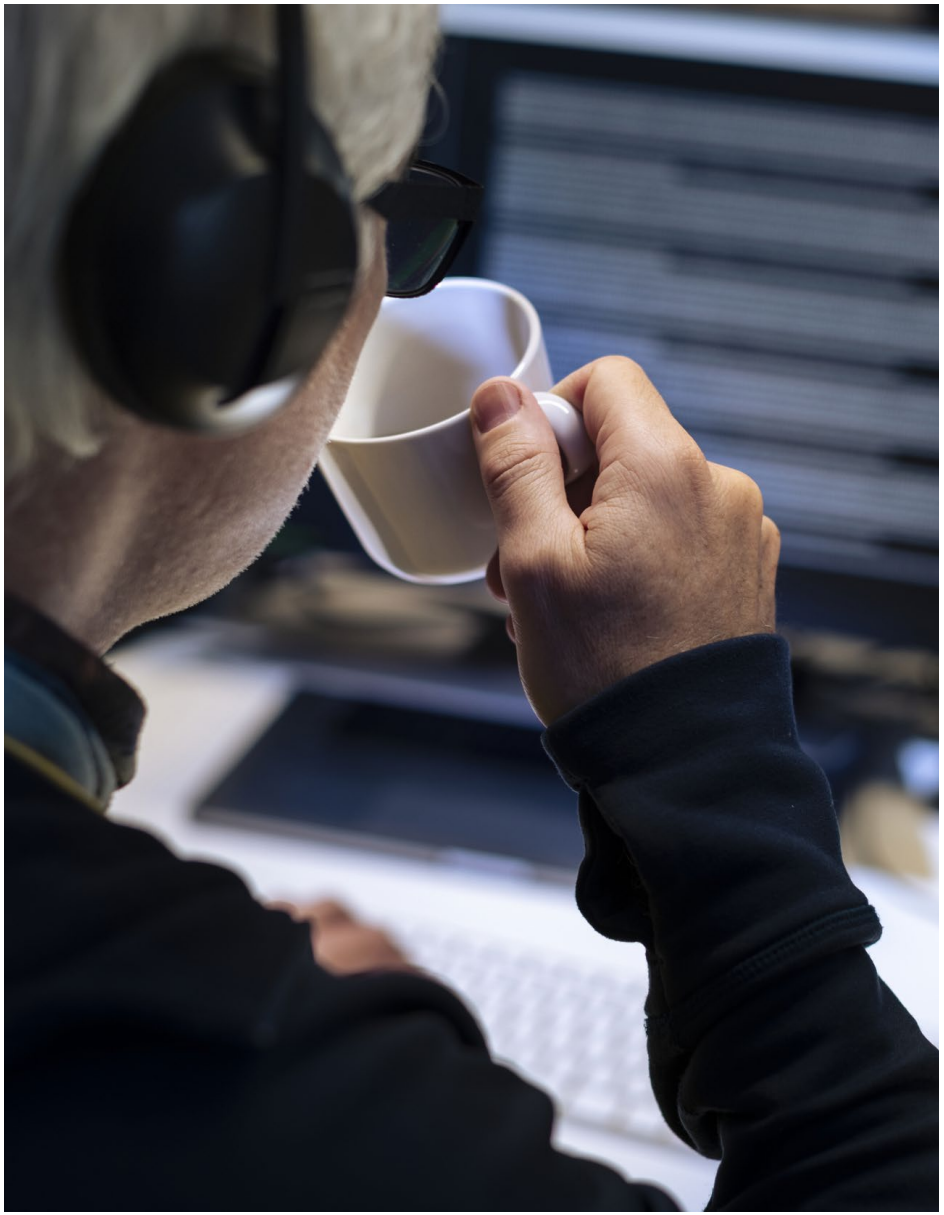
**Det råder stor** brist på kompetens inom cybersäkerhetsområdet. I Sverige finns högt tekniskt kunnande, men det är inte tillräckligt för att möta behovet. Det innebär att arbetsgivare behöver öka sina insatser för att rekrytera, utveckla och behålla personal med denna kompetens. Att utveckla egna utbildningsprogram, eller köpa utbildningar, och att kontinuerligt upprätthålla kompetensen för att följa teknikutvecklingen är kostsamt men nödvändigt.

Samtidigt finns ett behov av att höja grundkompetensen och medvetenheten om cybersäkerhet hos alla medarbetare. Även ledningsgrupper behöver kompetens för att prioritera och driva arbetet med hänsyn till cybersäkerhet. Bristen på kompetens inom cybersäkerhet är dock inte ett svenskt fenomen – det är globalt.

## En föränderlig hotbild

Metoder och verktyg för cyberangrepp utvecklas kontinuerligt, och angripare använder sig ofta av de enklaste metoder som kan uppnå önskat resultat. I många fall är avancerade metoder onödiga, eftersom många mål fortfarande har grundläggande säkerhetsbrister. Exempelvis kan nätfiske, lösenordsangrepp och utnyttjande av okorrigerade sårbarheter vara tillräckliga för att angriparen ska lyckas.

Den nuvarande säkerhetsbilden kan liknas vid att många organisationer har ”låsta entrédörrar men olåsta källarfönster.” Detta illustrerar behovet av ett holistiskt säkerhetsarbete där alla nivåer av organisationen bidrar till att minska sårbarheter och stärka skyddet. ●



# 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.

## 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. ●

# 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. 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.

## Exempel från verkligheten

Under en cyberattack drabbades ett stort detaljhandelsföretag av ett intrång som resulterade i att betalningsinformation för cirka 40 miljoner kunder stals. Angriparna utnyttjade en sårbarhet hos en tredjepartsleverantör för att få tillgång till företagets it-system. Där installerade de skadlig programvara i kassasystemet, som samlade in kundernas kortinformation under den hektiska julhandeln.

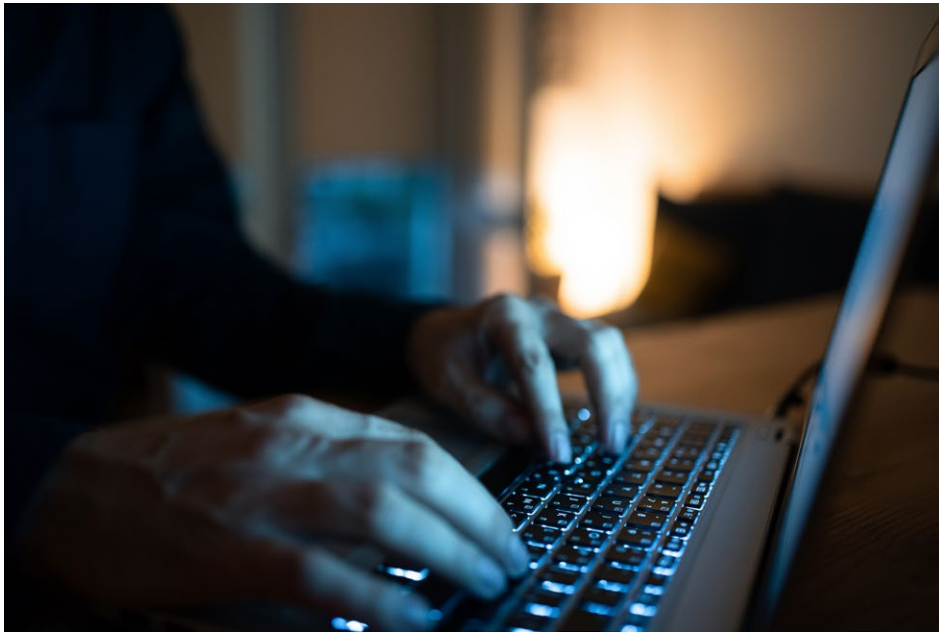
Trots att företagets säkerhetssystem hade larmat om ovanlig aktivitet vidtogs inga åtgärder i tid. Den bristande uppföljningen av varningarna och ineffektiv säkerhetsövervakning gjorde att attacken pågick i flera veckor innan den upptäcktes. Resultatet blev en stor läcka av kredit- och betalkortsinformation, vilket orsakade betydande ekonomiska och ryktemässiga skador för företaget. ●

# Rekommenderat arbetssätt

- ☐ **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 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.

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.

## Exempel från verkligheten

En organisation drabbades av intrång via en sårbarhet i sin VPN-funktion. Leverantören hade publicerat en uppdatering några dagar innan, men angriparna hade redan börjat utnyttja sårbarheten. Organisationen installerade uppdateringen två veckor senare, men vid det laget hade angriparna redan tagit sig in i nätverket. Detta visar hur viktigt det är att installera säkerhetsuppdateringar snabbt. Även om en organisation inte är ett prioriterat mål, kan intrång ske när fler blir medvetna om sårbarheten. ●

# Rekommenderat arbetssätt

- ☐ **Gör en inventering av** alla informationssystem och deras behov av säkerhetsuppdateringar. 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.

# 3

# Förvalta behörigheter och använd stark autentisering

**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.

## Exempel från verkligheten

En anställd skapade flera extrakonton utöver sitt vanliga konto. Dessa konton hade VPN-åtkomst och tillgång till ett centralt system. Efter att personen slutade fortsatte denne att använda både sitt gamla konto och extrakontona för att få tillgång till systemet. Det berodde på tre brister:

- Användarens konto inaktiverades inte efter att anställningen avslutades.
- Skapandet av extrakonton upptäcktes inte.
- VPN-åtkomst kunde ske med bara användarnamn och lösenord.

# Rekommenderat arbetssätt

- ☐ **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 hårdvarunycklar, 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.

# 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.

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.

## Exempel från verkligheten

Ett stort kreditföretag drabbades av en allvarlig dataläcka, där miljontals personuppgifter exponerades. Angriparna utnyttjade en sårbarhet i en webbapplikation som företaget inte hade uppdaterat i tid. Genom denna sårbarhet fick de åtkomst till företagets nätverk och kunde sedan utnyttja höga behörigheter för att obemärkt ta sig runt i systemet.

Administrativa konton hade tilldelats för breda behörigheter utan att begränsas till specifika uppgifter, vilket gav angriparna tillgång till stora delar av företagets känsliga data. Bristen på övervakning och loggning gjorde det dessutom möjligt för dem att extrahera data under flera månader utan att upptäckas.

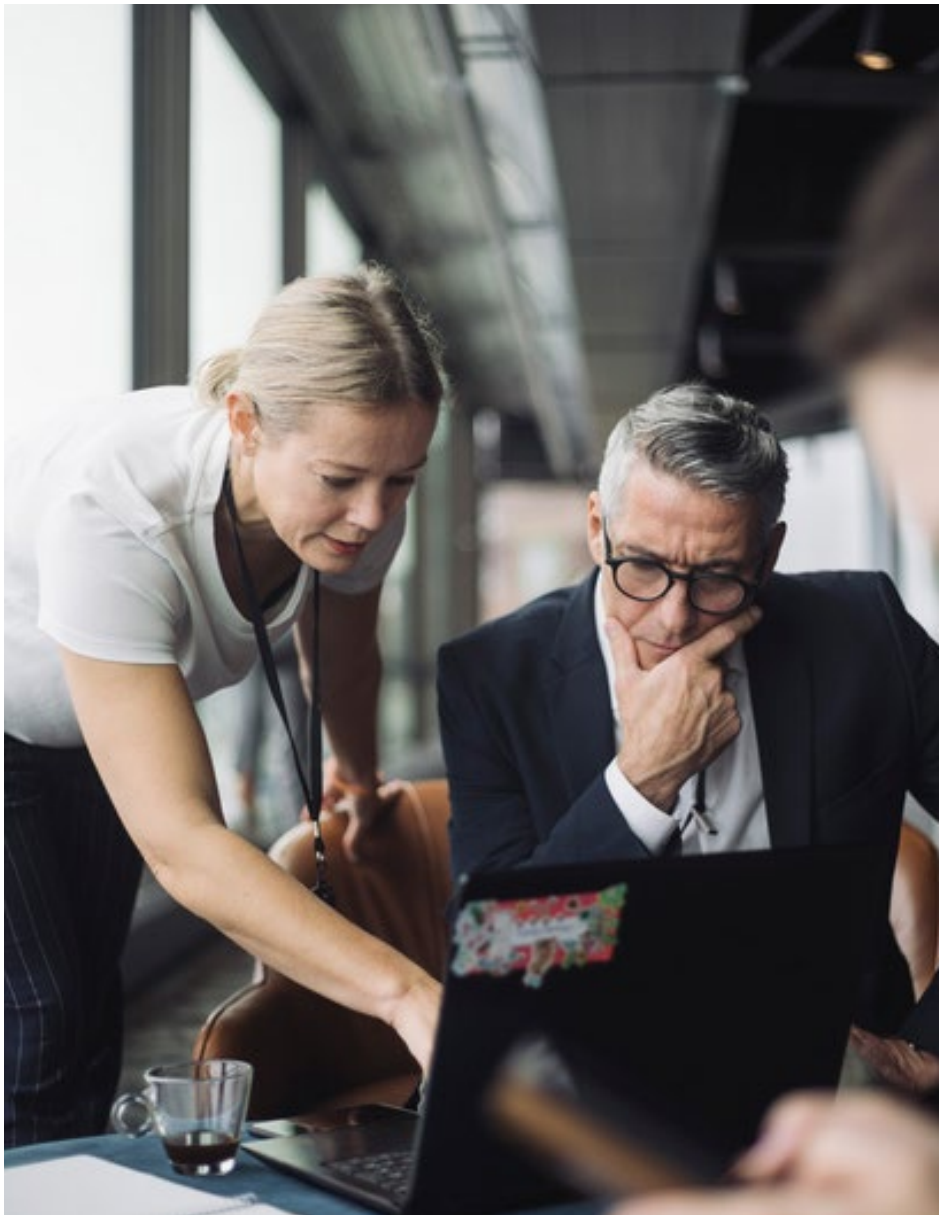
Denna incident belyser vikten av att införa strikta regler för tilldelning av höga behörigheter, att segmentera åtkomsten och att implementera flerfaktorautentisering och effektiv övervakning av kritiska konton. ●

# Rekommenderat arbetssätt

- ☐ **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. Till exempel bör ett konto som kan skapa nya användare inte ha möjlighet att ändra loggar, vilket minskar risken för missbruk. Det är dessutom 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.



# 5

# Inaktivera oanvända tjänster och protokoll – härda system

**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.

## Exempel från verkligheten

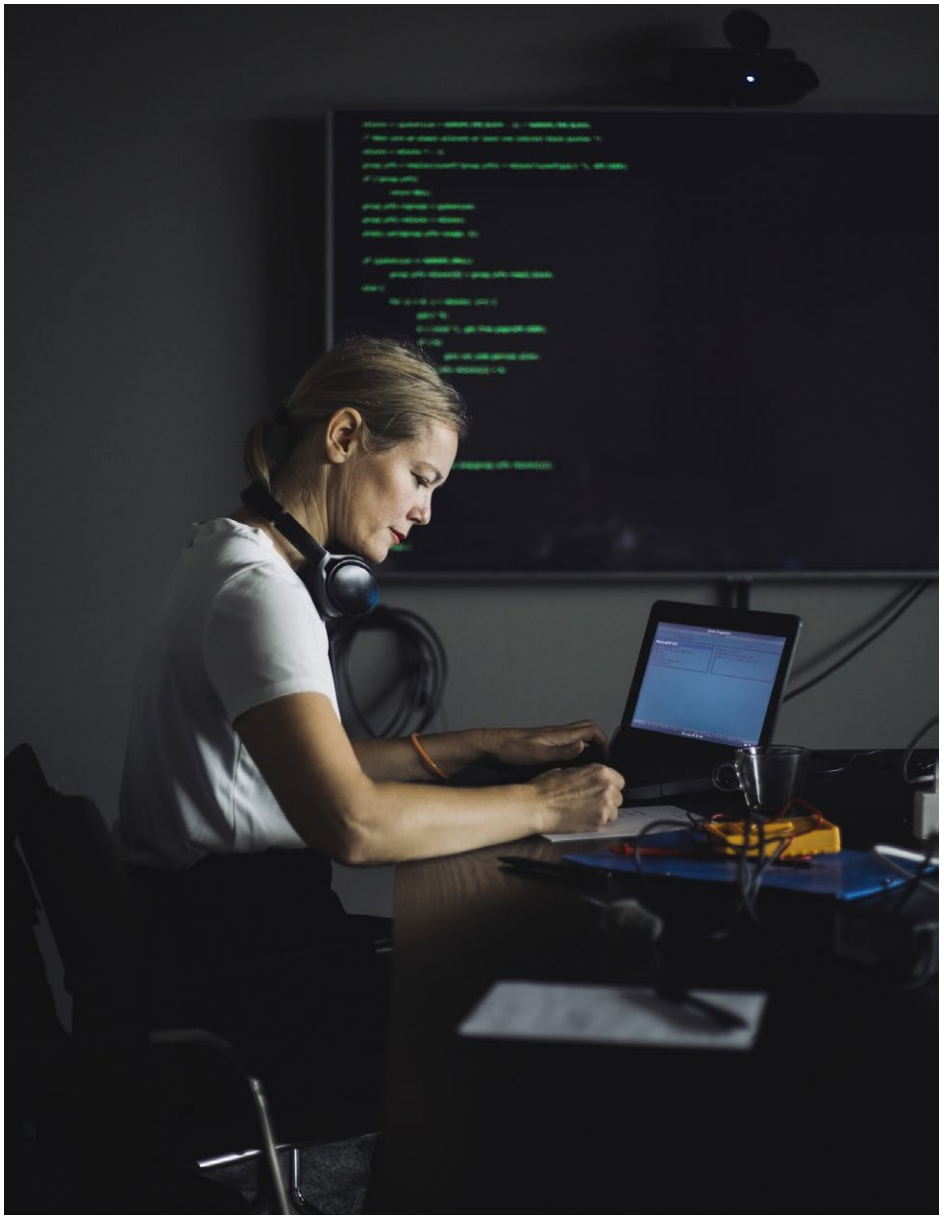
Under den så kallade WannaCry-attacken drabbades en stor europeisk vårdgivare hårt eftersom det föråldrade och sårbara SMBv1-protokollet fortfarande var aktivt i deras system. WannaCry utnyttjade en känd sårbarhet i SMBv1 (EternalBlue), vilket gjorde att en utpressningstrojan (eng Ransomware) snabbt spreds och infekterade flera kritiska system. Denna brist på härdning, genom att inte inaktivera ett onödigt protokoll, ledde till omfattande störningar, inklusive inställda operationer och förlorad åtkomst till patientjournaler. ●

# Rekommenderat arbetssätt

- ☐ **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.



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.

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.

## Exempel från verkligheten

En större nordisk tjänsteleverantör drabbades av ett angrepp med en utpressningstrojan som ledde till betydande driftstörningar för deras kunder, inklusive statliga myndigheter och företag i Sverige. Trots att företaget snabbt isolerade den drabbade plattformen och påbörjade återställningsprocessen, lyckades de inte återställa alla system tillräckligt snabbt, vilket ledde till förlängda avbrott i kritiska tjänster som lönesystem och verksamhetsapplikationer. Kritiken mot företaget fokuserade på den långsamma återhämtningen och frågetecken kring om deras säkerhetskopior och återställningsstrategi var tillräckligt robusta. ●

# Rekommenderat arbetssätt

- ☐ **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.

# 7

# Segmentera och kontrollera åtkomst i nätverket

**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

Många organisationers nätverk sträcker sig utanför kontorslokalen. Det kan ske genom att informationssystem är 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 och utgående trafik kan förvärra situationen, eftersom angriparna kan använda organisationens nätverk för att kommunicera med externa servrar oupptäckt.

## Exempel från verkligheten

En organisation hade både inpasseringssystem, fastighetsdriftssystem och administrativa system på samma nätverk. Vid en uppdatering i de administrativa systemen slutade nätverket fungera, vilket resulterade i att medarbetarna inte kunde använda sina passerkort. Hade nätverket varit segmenterat skulle denna påverkan ha undvikits och säkerheten ökat, eftersom ett problem i ett system inte hade kunnat sprida sig till andra delar.

# Rekommenderat arbetssätt

- ☐ **Skydda nätverket genom** att segmentera det fysiskt och logiskt, baserat på informationssystemens 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.


**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.

## Exempel från verkligheten

Två statliga organisationer i Europa och Nordamerika fick e-post om en kommande försvars- och säkerhetskonferens. Avsändaren såg ut att vara konferensarrangören och e-posten innehöll en bilaga med ett påstått konferensschema. För att kunna läsa bilagan krävdes att mottagaren aktiverade ett makro.

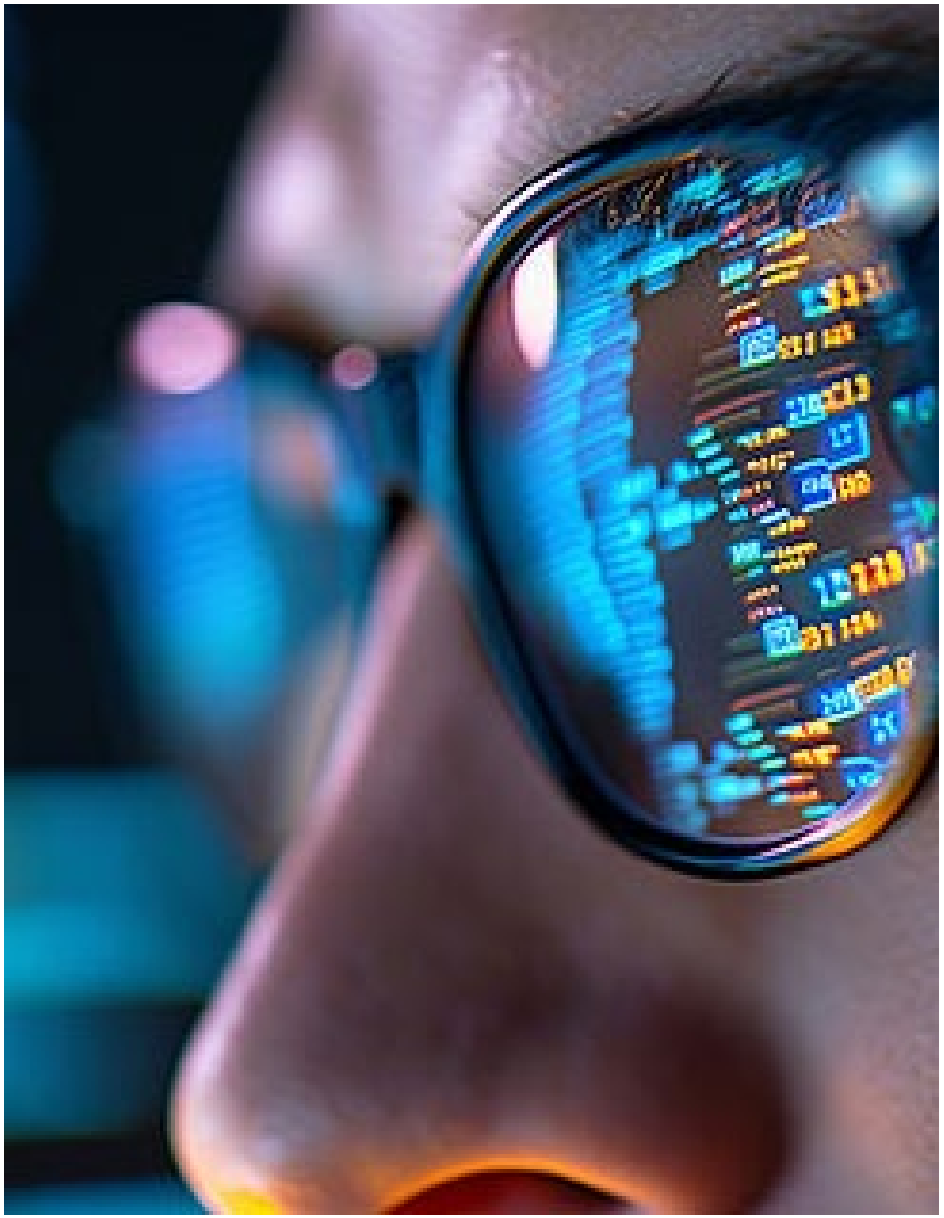
När makrot aktiverades installerades skadlig kod osynligt på datorn. Den skadliga koden gav angriparen tillgång till organisationens it-miljö genom att kommunicera med en server på internet. ●

# Rekommenderat arbetssätt

- ☐ **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 mobiltelefoner.
- ☐ **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 webbläsare. 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.




**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.

## Exempel från verkligheten

Den kinesiska hackergruppen APT31 utförde för en tid sedan, en serie cyberangrepp mot europeiska mål, inklusive Sverige. Gruppen, känd för cyberspionage, använde till en början hyrda virtuella servrar för sina attacker, men bytte sedan till att använda hackade routrar från privatpersoner runt om i Europa. Genom att utnyttja sårbarheter i föråldrad programvara kunde de ta kontroll över dessa routrar och bygga ett distribuerat nätverk för sina attacker, vilket gjorde det svårt att spåra dem. ●

# Rekommenderat arbetssätt

- ☐ **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.

# 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.

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.

## Exempel från verkligheten

En global industrikoncern drabbades av en omfattande attack med utpressningstrojanen LockerGoga, som genom direkt internetåtkomst till en Command and Control (C2)-server tillät angriparna att fjärrstyra och låsa företagets system. Detta orsakade allvarliga störningar i verksamheten och tvingade många delar av företaget att gå över till manuella processer, vilket ledde till stora ekonomiska förluster. Företaget valde att inte betala lösensumman och fokuserade istället på att återställa sina system från säkerhetskopior. Attacken illustrerade vikten av att blockera direkt internetåtkomst och använda säkerhetsåtgärder som nätverkssegmentering och webbproxy för att förhindra obehörig kommunikation med externa servrar. ●

# Rekommenderat arbetssätt

- ☐ **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.

# Sammanfattning

**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 trafikflödena 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.

NATIONELLT CYBERSÄKERHETSCENTER

Den här produkten är en gemensam bild av cybersäkerhet i Sverige 2024 som 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**