Det svenska cyberhotlandskapet

Nationell rapport om antagonistiska cyberhot



2026/2027

NATIONELLT CYBERSÄKERHETSCENTER
En del av FRA

Nationellt cybersäkerhetscenter (NCSC) har i uppdrag att stärka Sveriges förmåga att förebygga, upptäcka och hantera cyberhot, och som en del av FRA bidrar vi till ett mer motståndskraftigt Sverige.

I den verksamhet som bedrivs inom ramen för centret samverkar Försvarets materielverk, Försvarets radioanstalt, Försvarsmakten, Myndigheten för civilt försvar, Polismyndigheten, Post- och telestyrelsen och Säkerhetspolisen.

FMV FRA FÖRSVARSMAKTEN Myndigheten för civilt försvar

Polisen PTS Säkerhetspolisen



04.

FÖRORD
John Billow, chef för NCSC, om varför cybersäkerhet behöver få en högre prioritet.



06.

HOTBILDEN 2026
En komplex och förstärkt hotbild med fler sårbarheter, stärkt förmåga genom AI, ett skärpt geopolitiskt läge och risk för hybridangrepp.



12.

TRE TYPER AV HOTAKTÖRER
Cyberkriminella, hacktivister och statsaktörer: deras motiv, metoder och hur olika angrepp kan gå till.



28.

FYRA OMRÅDEN SOM PÅVERKAR HOTBILDEN
AI, sårbara leveranskedjor, OT-system och kvantdatorer är fyra områden som kan vara extra relevanta för er hot- och riskanalys.



38.

ÅTGÄRDER FÖR ATT STÄRKA MOTSTÅNDSKRAFTEN
Skydd mot intrång, försvar i flera lager och ledningens ansvar enligt cybersäkerhetslagen.

Översikt

Uppmärksammade cyberangrepp
Sida 10

Så kan ett angrepp gå till, steg för steg
sida 15, 19, 22

Cyberangrepp under de senaste åren
Sida 23

Ledningens ansvar
Sida 47

Hot- och riskanalys
Sida 48

Ordlista
Sida 52

Kontakt
Sida 54

Gemensamma insatser för ett säkrare Sverige

Välkommen till den första utgåvan av NCSC:s årliga öppna rapport om det svenska cyberhotlandskapet, med fokus på antagonistiska cyberhot. Rapporten är skriven för dig som arbetar med cybersäkerhet, oavsett om du sitter i en ledningsgrupp eller arbetar med tekniska frågor varje dag. Men den är också till för dig som vill förstå mer om cyberhoten i Sverige.

VI PÅMINNS STÄNDIGT om att konsekvenserna av cyberangrepp kan bli betydande, i form av avbrott i kritiska funktioner för verksamheter och samhället, förlust av känslig information, ekonomiska förluster, viten och förtroendeskador. Angreppen får inte sällan konsekvenser även utifrån ett personuppgiftsperspektiv, med en ökad risk för att individer drabbas av integritetsskada och bedrägerier.

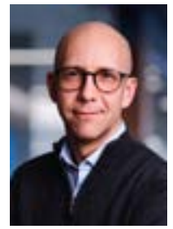
HOTBILDEN är komplex och har förstärkts under det senaste året. Det finns en generell avsikt från vissa statliga hotaktörer att genomföra cyberangrepp i och mot Sverige.

CYBERSÄKERHETSFRÅGOR behöver få en ökad prioritet, inte minst i ledningen hos både privata och offentliga verksamheter. Denna rapport avser att utgöra ett underlag för att bättre förstå de cyberhot som finns i och mot Sverige.

NCSC HAR DET SENASTE ÅRET samlat krafter inom cybersäkerhetsområdet och utvecklar vårt arbete inom analys och proaktiva åtgärder löpande, för att kunna leverera enligt vårt breda nationella uppdrag att stödja och stärka cybersäkerheten i hela samhället. Det utförs inom ett fördjupat samarbete mellan flera myndigheter med nationella uppdrag inom säkerhet och försvar.

RAPPORTEN SKA KUNNA BIDRA till fler insikter och ökad kännedom om cyberhotlandskapet, men även bidra till ökat fokus i svenska verksamheter. Det är våra gemensamma insatser som bidrar till att stärka cybersäkerhetsförmågan och höja motståndskraften. På så sätt gör vi Sverige mer cybersäkert och motståndskraftigt.

November 2026



John Billow
Chef för Nationellt cybersäkerhetscenter

”Hotbilden är komplex och har förstärkts under det senaste året. Därför behöver cybersäkerhetsfrågor få en ökad prioritet, inte minst i ledningen hos både privata och offentliga verksamheter.”

FOTO: JANNI LIPKA

EN KOMPLEX OCH FÖRSTÄRKT HOTBILD

NCSC:s bedömning är att hotbilden gällande cyberangrepp mot svenska intressen har förstärkts under de senaste 12 månaderna. Det beror inte minst på grund av den starkt ökade volymen av identifierade tekniska sårbarheter i system samt hotaktörers ökade förmåga genom AI. Det geopolitiska läget, med varningar om ökade risker för hybridangrepp mot Natoländer, bidrar även till den förstärkta hotbilden.

Det här kapitlet beskriver utvecklingen bakom den förstärkta hotbilden och behovet av ökat fokus på hot- och riskanalys, samt tre typer av hotaktörer och fyra aktuella fokusområden. Längre fram beskrivs respektive typ av hotaktör och fokusområde, samt hur cybersäkerheten kan stärkas för att möta hoten.

FOTO: PANUMAS NIKHOMKHAI / SHUTTERSTOCK.COM

Utvecklingen ställer nya krav på hot- och riskanalys

Utvecklingen inom AI och det geopolitiska läget förstärker hotbilden. Samtidigt agerar hotaktörer i olika skepnader och det blir mer utmanande att ha en tydlig bild av det aktuella hotet.

Det senaste året har AI fått en allt mer framträdande roll inom cybersäkerhet och cyberangrepp. Inte minst har tempot ökat dramatiskt gällande antalet sårbarheter och säkerhetsbrister som upptäcks till följd av utvecklingen inom AI-modeller. Det innebär ökade utmaningar för verksamheter i arbetet med systemuppdateringar.

Konsekvenserna av AI-utvecklingen riskerar att leda till längre ledtider för att genomföra säkerhetsuppdateringar, vilket ger hotaktörer ökade möjligheter att dra nytta av tekniska sårbarheter i system. AI-utvecklingen har även bidragit till att hotaktörer fått en ökad förmåga att genomföra angrepp, vilket kan leda till bredare angrepp där fler verksamheter blir drabbade, och att angreppen genomförs i en snabbare takt.

Finansiellt motiverade angrepp bedöms fortsatt vara det hot som kan drabba en större bredd av verksamheter i Sverige, där angrepp sker mot verksamheter oavsett storlek och sektor. Inom finansiellt motiverade angrepp är bedrägerier, kontostölder och utpressningsangrepp exempel på ofta återkommande typer av angrepp. Viljan från ett antal statliga aktörer att påverka och skapa störningar i vårt samhälle kvarstår, och flera länder har under året varnat för att hybridangrepp mot Natoländer kan komma att öka framöver. Det kan få påverkan på verksamheter i Sverige. Hotaktörerna utvecklas, tar stöd av AI och agerar i ekosystem där olika grupperingar har specialiserade roller. De kan samtidigt ha flera skepnader och flera motiv för angrepp, vilket bidrar till utmaningen att ha en tydlig bild av det aktuella hotet. Därför ökar behovet för verksamheter att ta del av fortlöpande hotinformation och att analysera vilka hot som den egna organisationen bör vara förberedd på att kunna hantera.

Tillsammans med riskanalyser gällande vilka system och tjänster som är kritiska att skydda, bidrar aktuella hotanalyser till inriktning för att stärka cybersäkerheten. Både utifrån verksamhetens perspektiv, och i förlängningen också samhällets.

FYRA AKTUELLA FOKUSOMRÅDEN

AI-utvecklingen – Ställer högre krav på verksamheters cybersäkerhetsarbete.

Leveranskedjeangrepp – Ökade sårbarheter via leverantörer och i systemutvecklingsmiljöer.

Angrepp mot OT-system – Styrsystem i operativ teknik är allt oftare uppkopplade och integrerade med övriga it-system. De blir därmed mer sårbara för angrepp.

Kvantsäker kryptografi – Kvantdatorer kan på sikt försvaga skyddet för dagens krypterade information. Övergången till kvantsäker kryptografi behöver planeras redan nu.

Läs mer om om hotaktörerna på s. 12–27, om hur ni stärker skyddet på s. 38–47 och om hot- och riskanalys på s. 48–49.

Tre huvudtyper av hotaktörer



Cyberkriminella
Finansiellt motiverade hotaktörer som genomför opportunistiska angrepp. Kan drabba de flesta verksamheter.

Hacktivister
Ideologiskt motiverade hotaktörer som vill störa verksamheter och samhället genom riktade angrepp.





Statsaktörer
Bedriver uthålligt industri- och statsspionage samt har förmåga att genomföra sabotage mot kritiska mål.

GRÄNSERNA MELLAN cyberkriminella grupper, hacktivister och statsaktörer är inte alltid tydliga. Det är inte ovanligt att statsaktörer använder hacktivister eller cyberkriminella grupper för att uppnå sina mål, eller att hacktivister och cyberkriminella grupper samarbetar.

UPPMÄRKSAMMADE CYBERANGREPP

Företag, organisationer, myndigheter, kommuner och lärosäten. Under de senaste 12 månaderna har flera cyberangrepp fått konsekvenser för verksamheter som samhället är beroende av.

Ett urval:

Dataintrång mot Svenska kraftnät, som driver det svenska stamnätet för el. Elförsörjningen påverkades inte.

Angrepp mot ett kraftvärmeverk i Karlskrona. Driften kunde fortsätta.

Överbelastningsangrepp mot myndigheter, politiska organisationer och företag. I november 2025 pekades ett femtiotal svenska verksamheter ut som mål. Detta kan ha haft koppling till ett riksdagsmöte om Krim som hölls i Stockholm vid samma tid.

Dataintrång mot it-leverantören CGI, vilket påverkade flera myndigheters tjänster.

Utpressningsangrepp mot kommuner i Västerbotten.

Utpressningsangrepp mot Instructure, företaget bakom lärplattformen Canvas. Ett stort antal svenska universitet och högskolor påverkades.

Dataintrång mot sårbara instanser av Citrix NetScaler, som drabbade ett flertal verksamheter.

Utpressningsangrepp mot en kommun i Skåne.

Angrepp mot styrsystem i kyl- och frysutrustning hos ett flertal svenska matvarubutiker, kyllager och restauranger.

2026

Den 15 januari började cybersäkerhetslagen (2025:1506) att gälla. Den ställer krav på verksamheter i 18 sektorer, bland annat att ledningen ansvarar för cybersäkerheten och måste utbilda sig.



FOTON: SHUTTERSTOCK.COM OCH JOHNÉR BILDBYRÅ

Finansiellt motiverade hotaktörer

Cyberkriminella är ofta opportunistiska och står för de angrepp som drabbar flest verksamheter i Sverige. Både privata och offentliga organisationer, stora som små, drabbas.

Finansiellt motiverade angrepp drabbar alla typer av verksamheter i Sverige, både privata företag och offentlig sektor, oavsett storlek. Bedrägerier står för de flesta av polisanmälningarna gällande it-relaterade brott. Samtidigt har kontostölder blivit en allt mer specialiserad del av den kriminella hotaktörskedjan, där vissa grupperingar enbart ägnar sig åt att stjäla inloggningsuppgifter i stor skala och sälja dem vidare till andra hotaktörer som genomför cyberangrepp.



ILLUSTRATION: JOHAN ISAKSSON

Så kan ett *utpressnings-angrepp* gå till

Angriparen tar sig ofta in i system med hjälp av konton som stulits genom nätfiske eller skadlig kod som spionprogram, *infostealers*.

IBLAND ÄR DET OLIKA HOTAKTÖRER inblandade, de som stjäl konton och de som sedan genomför själva angreppet i flera steg. Andra metoder för intrång kan vara att utnyttja sårbarheter i system som är exponerade mot internet, till exempel vpn-tjänster eller brandväggar.

Väl inne i systemet försöker angriparen skaffa sig fler behörigheter, till exempel genom att utöka rättigheter för konton, skapa nya konton och använda inloggnings-uppgifter som finns sparade i systemet. Hotaktören kan också utnyttja legitima inbyggda systemverktyg, så kallad *living-off-the-land*, för att förflytta sig i systemmiljön, identifiera kritiska filer och system samt sprida skadlig kod. De inbyggda systemverktygen kan även användas för att inaktivera säkerhetsfunktioner för att undvika upptäckt. Angreppet fortsätter sedan genom att hotaktören stjäl känslig information och för ut den till sin egen infrastruktur.

I slutskedet förstör hotaktören ofta backupmöjligheter och distribuerar skadlig kod i form av ett utpressnings-virus, *ransomware*, för att kryptera filer. Avslutningsvis lämnas ett meddelande med krav på lösensumma till den drabbade verksamheten. Hotaktören kräver sedan ersättning för att tillhandahålla en dekrypteringsnyckel. Det är även vanligt att hotaktören hotar att publicera den stulna informationen offentligt, vilket innebär att offret utsätts för dubbel utpressning.

En del hotaktörer erbjuder så kallad *ransomware-as-a-service (RaaS)* till andra hotaktörer, vilket ökar möjligheten för mindre kunniga hotaktörer att genomföra angrepp.

Om hotaktörer

- Arbetar ofta i ekosystem där olika aktörer har olika uppgifter, från kontostöld till utpressning.
- Utpressning sker ofta både genom stulen information och krypterade system.
- Kan genomföra angrepp i kampanjer, till exempel när en ny teknisk sårbarhet blivit känd.
- Erbjuder ibland plattformar för utpressnings-angrepp till andra kriminella, så kallad *ransomware-as-a-service*.
- Har genomfört flera angrepp i Sverige under det senaste året, både mot offentlig sektor och mot ett stort antal privata företag i olika branscher.

Om hotbilden

- Hotaktörer slår till där deras metoder fungerar, mot både privata och offentliga verksamheter, stora som små.
- Ökad risk för verksamheter med sårbara system som är exponerade mot internet.
- Ökad risk för verksamheter som fått konto-uppgifter stulna.
- Ökad risk för verksamheter som tidigare varit utsatta för angrepp.

Kontakta oss för mer information till er hotanalys.
Se kontaktinformation på sidan 54.

STEG FÖR STEG



TIDEN MELLAN STEG ETT OCH TVÅ kan variera från timmar till flera månader. De resterande stegen i angreppet tar ofta några veckor. Att betala lösensumma är ingen garanti för att få tillbaka information eller fungerande system, och ofta sker utpressningen i flera steg. En kritisk faktor för att hantera just utpressningsangrepp är att säkerhetskopior regelbundet testas, skyddas genom lämplig segmentering från den ordinarie systemmiljön och att åtkomst till säkerhetskopiorna regleras av lämplig behörighets- och åtkomststyrning, så att inte angriparen kan förstöra dem.

UNDER DE SENASTE ÅREN har utpressningsangreppen utvecklats. Det har blivit vanligare att angrepp inte omfattar kryptering av data utan endast informationsstöld, med utpressningshot om att offentligt publicera information som stulits från de system som angripits.

Så skyddar ni er – läs mer på sidorna 38–46.

Ideologiskt motiverade hotaktörer

Hacktivisternas målsättning är att störa verksamheter och samhället genom angrepp som skapar avbrott i system och tjänster.

De flesta angrepp från ideologiskt motiverade angripare är överbelastningsangrepp, där en webbplats eller tjänst belastas av så mycket trafik att den slutar fungera. Även intrång och påverkan på hur system fungerar är exempel på angrepp. Hacktivisternas angrepp kommer ofta i vågor under kortare perioder och bedöms i de allra flesta fall ha koppling till geopolitiska frågor, till exempel Sveriges medlemskap i Nato och stödet till Ukraina. Det är inte ovanligt att hacktivistgrupperingar i det dolda arbetar på uppdrag av statliga aktörer.

50

I slutet av november 2025 pekade hotaktörer ut ett femtiotal svenska verksamheter som mål för överbelastningsangrepp. Angreppen kan ha haft koppling till ett riksdagsmöte om Krim som hölls i Stockholm vid samma tid.



Olika typer av angrepp

Överbelastningsangrepp
till exempel för att slå ut webbplatser och digitala tjänster.

Sabotage
till exempel mot styrsystem för infrastruktur som är exponerade mot internet.

Intrång
till exempel på webbplatser för att ändra innehåll eller funktioner.

Informationspåverkan
till exempel falska och polariserande budskap i sociala medier.

ILLUSTRATION: JOHAN ISAKSSON

Så kan ett *hacktivist-angrepp* gå till

HACKTIVISTER KAN GENOMFÖRA INTRÅNG i system för att orsaka störningar, men de flesta angrepp som uppmärksammas är överbelastningsangrepp. De genomförs ofta med hjälp av ett botnät med ett stort antal datorer och andra uppkopplade enheter. Vid ett botnät-angrepp kan de anslutna enheterna få information om vilka mål som ska angripas från en central server. Sedan skickar enheterna samordnat trafik mot målen, till exempel en webbplats eller en digital tjänst, för att överbelasta den.

Förutom överbelastningsangrepp har även sabotage, till exempel angrepp mot OT-system, med styr- och kontrollsystem, blivit en del av hacktivisternas taktik.

Vissa angripare söker efter system som är exponerade mot internet och har svagare skydd. Denna typ av angrepp har fått begränsad påverkan på system i flera nordiska länder de senaste åren. Till exempel har vattenreningsverk, övervakningskameror och småskaliga energianläggningar drabbats av angrepp.

Kontakta oss för mer information inför er hotanalys. Se kontaktinformation på sidan 54.

Om hotaktörer

- Använder vanligtvis överbelastningsangrepp som metod, men även sabotage förekommer.
- Samarbetar ofta med likasinnade grupper, ibland i större allianser.
- Arbetar inte sällan i det dolda på uppdrag av statliga aktörer.
- Gör ofta reklam för sina angrepp och uppmanar andra att delta via sociala medier, till exempel Telegram.
- Har tagit på sig ansvar för flera angrepp i Sverige under det senaste året, mot offentlig sektor, politiska organisationer och privata företag.

Om hotbilden

- Ökad risk för verksamheter som har ett symbolvärde för Sverige.
- Ökad risk för offentlig sektor, politiska organisationer och medier.
- Ökad risk för organisationer med koppling till geopolitiska frågor, som stödet till Ukraina.
- Ökad risk för samhällsviktiga verksamheter med styrsystem som är åtkomliga från internet, till exempel inom energi och infrastruktur.

STEG FÖR STEG

01 Skanning efter till exempel styr- och kontrollsystem som är exponerade mot internet, ofta via publika tjänster.

02 Intrång, främst i system utan åtkomstskydd eller med svag autentisering.

03 Dokumentation av tillgång till system samt eventuell påverkan på system.

04 Publicering av information för att bevisa åtkomst till system, till exempel i form av skärminspelning.

TIDSRAMARNA FÖR ANGREPPEN varierar, där vissa angrepp genomförs direkt och marknadsförs av angriparen relativt omgående. I andra fall har hotaktören säkrat åtkomst till system och genomför systempåverkan vid ett tillfälle då angreppet kan få extra stor uppmärksamhet.

Åtgärder för att motverka den här typen av angrepp är att undvika att exponera OT-system mot internet om det inte är nödvändigt, samt att stärka säkerheten kring OT-system.

Så skyddar ni er – läs mer på sidorna 34–35 och 42.

Statsaktörer – *hög förmåga* och *uthållighet*

Statsaktörer är resursstarka, agerar långsiktigt och har hög teknisk kompetens. Angreppen kan handla om både spionage och störningar, och konsekvenserna kan även bli kännbara utanför den digitala världen.

Det finns en generell avsikt från vissa statliga hotaktörer att genomföra cyberangrepp i och mot Sverige. Syftet är bland annat att inhämta information som rör svensk säkerhet, politiska beslut eller myndighetsutövning, eller för att störa viktiga samhällsfunktioner. Statliga aktörer, likt andra hotaktörer, utnyttjar även infrastruktur i Sverige för att genomföra cyberangrepp mot mål i och utanför Sverige. Avsikten ska ses utifrån att Sverige är en del av väst och medlem i både EU och Nato. Ryssland, Kina och Iran är fortsatt de stater som utgör de tydligaste säkerhetspolitiska hoten mot Sverige, vilket också gäller på cyberarenan.

Cyberangrepp från statliga aktörer kan riktas mot myndigheter, kritisk infrastruktur och skyddsvärda industrier och utgörs av exempelvis spionage och sabotage. Cyberangrepp kan därmed få konsekvenser både i den digitala sfären och den fysiska, genom exempelvis avbrott eller störning av kritisk infrastruktur. Ur hotaktörens perspektiv är det ett effektivt sätt att i det dolda försöka påverka en stat eller befolkning.

Statliga cyberhotsaktörer är generellt sett resursstarka med en hög teknisk kompetens samtidigt som de agerar långsiktigt och strategiskt. Liksom flera andra hotaktörer är de opportunistiska på så sätt att de utnyttjar de tillfällen som ges och de sårbarheter som finns. Statliga aktörer är även opportunistiska gällande vilka aktörer de samarbetar med eller utnyttjar för att nå sina strategiska mål. Vissa statliga aktörer agerar förnekbart genom ombud eller drar nytta av handlingar utförda av aktörer med liknande ideologiska, finansiella eller geopolitiska målsättningar.

De senaste åren har Ryssland generellt blivit allt mer riskbenäget, vilket också återspeglas inom cyberområdet. Tidigare har cyberangrepp mot väst i huvudsak varit avgränsade till digitala miljöer, men flera internationella exempel tyder på en ambition att nu också orsaka konsekvenser i den fysiska miljön.



ILLUSTRATION: JOHAN ISAKSSON

SÅ KAN ETT SPIONAGEANGREPP GÅ TILL

STEG FÖR STEG

1. **Riktat nätfiske**
   Till exempel med skräddarsydda meddelanden till användare med rätt behörigheter.
2. **Intrång i system**
   Till exempel genom en skadlig länk i ett bifogat dokument.
3. **Långvarig åtkomst**
   Till exempel genom skadlig kod som skapar bakdörrar till system.
4. **Dölja spår av närvaro**
   Till exempel genom modifiering av loggfiler och utnyttjande av legitim inbyggd programvara *(living-off-the-land binaries* eller *lolbins)*.
5. **Exfiltrering av information**
   Till exempel genom legitima tjänster och komprimerade filer.
6. **Fortsätta dölja spår av aktivitet**
   Till exempel genom ändrade inställningar i övervakning och logg över trafik.

ANGREPPEN ÄR OFTA relativt komplexa när det kommer till att dölja intrång och närvaro i system. De genomförs därför stegvis och i en takt som minskar risken för upptäckt. Det är inte ovanligt att hotaktören har en lång period, ibland flera år, av åtkomst till system och känslig information.

En viktig åtgärd för att undvika den här typen av angrepp är att stärka övervakning och klientskydd, speciellt i klienter där användaren har tillgång till känslig information.

Så skyddar ni er – läs mer på sidorna 40–46.

Cyberangrepp de senaste åren

Exempel på angrepp med koppling till statliga aktörer de senaste åren.

POLEN

Samordnade angrepp mot energisystemet

Den 29 december 2025 utsattes Polens energiinfrastruktur för flera parallella cyberangrepp. Bland annat utnyttjades skadeprogram för att radera information i it-miljön, *wipers*. Angreppen riktades mot fler än 30 vind- och solcellsparker, ett tillverkningsföretag och ett stort värmeverk.

Enligt Polens digitaliseringsminister tydde allt på ryskt sabotage. Angreppen i Polen orsakade inga störningar i leveransen av el till kunder men blev uppmärksammade till följd av angreppens destruktiva utformning.



FOTO: SHUTTERSTOCK.COM

DANMARK OCH NORGE

Angripare tog över vattensystem

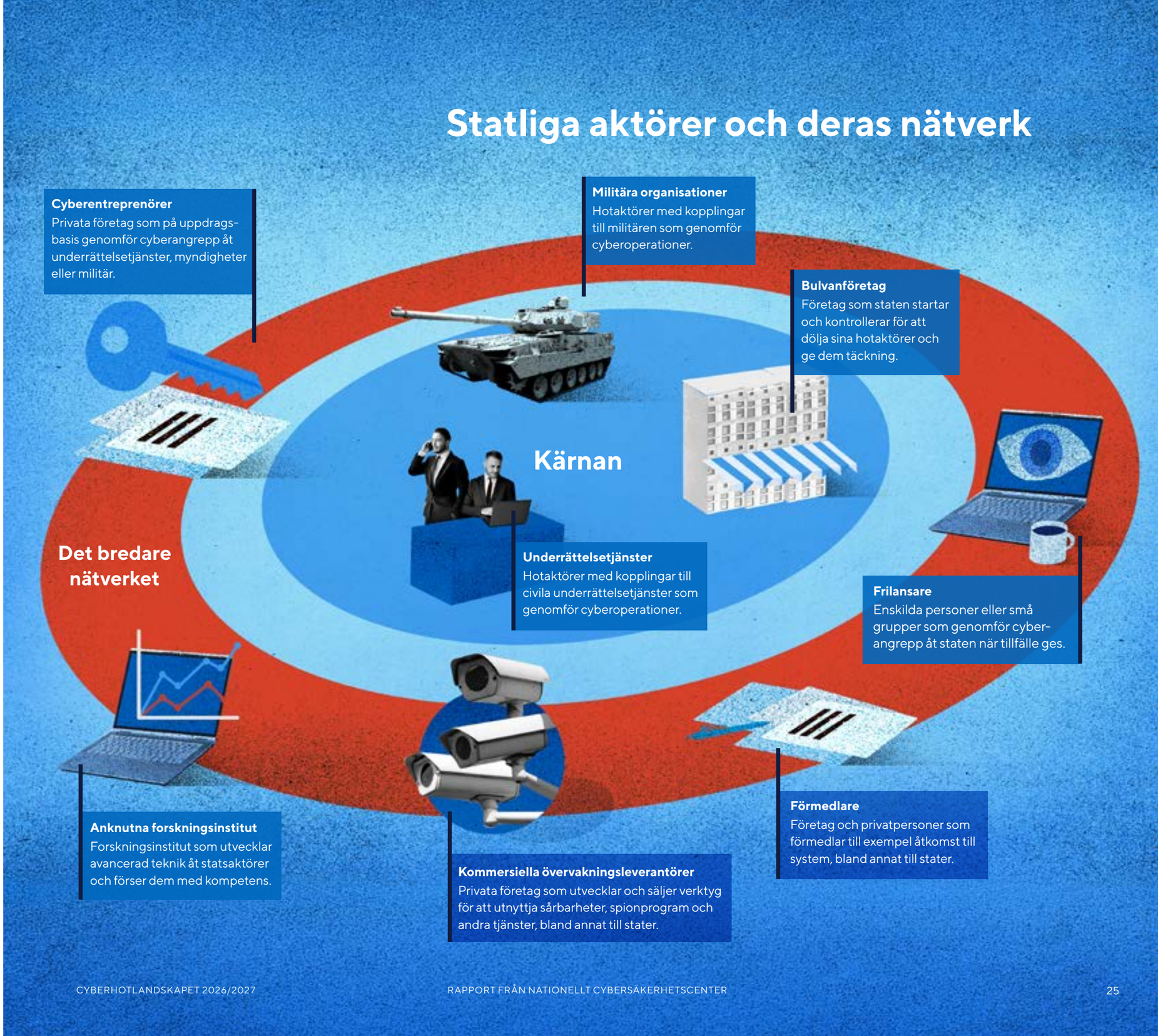
Flera fall har uppmärksammats i Norge och Danmark där proryska hotaktörer genom cyberangrepp tagit kontroll över system kopplade till vattentillförsel. År 2024 genomförde en prorysk hotaktör ett angrepp mot ett danskt vattenkraftverk genom att kompromettera dess OT-system och därefter manipulera vattentrycket. Enligt norska myndigheter genomförde en prorysk hotaktör 2025 ett cyberangrepp mot en damm i Bremanger. Hotaktören tog kontroll över dammens styrsystem och öppnade ventiler, så att stora mängder vatten strömmade ut under flera timmar.

500

LITER I SEKUNDEN
strömmade ut under ungefär fyra timmar när hotaktörer tog kontroll över en damm i Bremanger i Norge i april 2025.

Hotaktörer *samarbetar* och *etablerar* ekosystem

Gränserna mellan de olika hotaktörerna som redogjorts för har till viss del blivit mer otydliga de senaste åren. Finansiellt motiverade hotaktörer och hacktivister kan agera enligt statliga aktörers agenda och utföra angrepp till deras förmån. Statliga hotaktörer arbetar ofta i någon form av ekosystem med utkontrakterade roller.



Från aktörer som vill visa *förmåga* till *missnöjda* medarbetare

Utöver tidigare nämnda cyberhot förekommer även andra typer av antagonistiska hot och risker. Det kan till exempel röra sig om angrepp från enskilda personer eller mindre grupperingar som vill visa upp sin förmåga gällande skadlig kod, eller missnöjda medarbetare som värvats eller inspirerats av utomstående antagonister.

En annan relativt vanlig typ av angrepp är att enheter blir infekterade av skadlig kod, vilket kan leda till att enheten blir del i ett större botnät som används i hotaktörers angrepp.

Även AI-modeller som av olika skäl agerar utanför sin tänkta uppgift kan nämnas som ett framväxande, potentiellt cyberhot. Så kallad skugg-it, *shadow IT*, och nu även skugg-AI, alltså it-tjänster och AI-verktyg som medarbetare använder utan att organisationen godkänt dem, utgör en växande säkerhetsrisk som måste hanteras. Det gäller inte minst hur medarbetare hanterar känslig information och använder AI-agenter. Även om dessa hot och risker inte är de högst prioriterade för de flesta verksamheter bör de vara en del av diskussionen och utvärderingen i samband med att hot- och riskanalys genomförs.

Läs mer om hot- och riskanalys på sidan 48.



FOTO: SHUTTERSTOCK.COM

FYRA OMRÅDEN SOM PÅVERKAR HOTBILDEN

Hotbilden påverkas av utvecklingen inom teknik och metoder. AI, sårbara leveranskedjor, operativ teknik och kvantdatorer är fyra områden som kan vara extra relevanta för er hot- och riskanalys.

AI förändrar förutsättningarna och ger hotaktörer en starkare förmåga. Angrepp via leverantörer gör att säkerheten är beroende av många andra verksamheter. System kopplade till operativ teknik blir ett tydligare mål för angripare i takt med att de blir mer uppkopplade och integrerade. Utvecklingen av kvantdatorer gör att övergången till kvantsäker kryptografi behöver planeras redan nu.

För varje område beskriver vi utvecklingen, hur det påverkar cybersäkerhetsarbetet samt NCSC:s rekommendationer och metodstöd.

FOTO: NATALAYA YUDINA / SHUTTERSTOCK.COM

Nya möjligheter för både *angrepp* och *försvar*

Den snabba utvecklingen inom AI innebär nya möjligheter till angrepp och stärkta förmågor hos hotaktörer. Men AI kan också ge verksamheter verktyg för att stärka cybersäkerheten.

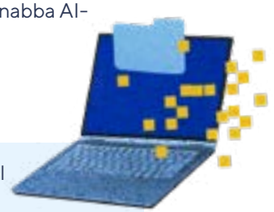
Specialiserade AI-modeller för att identifiera tekniska sårbarheter i system har utvecklats mycket snabbt under det senaste året. Det innebär en ökad utmaning för många verksamheter att prioritera och hantera den ökade volymen av säkerhetsuppdateringar från leverantörer. Utan rätt riskbedömning, resurser, processer och verktyg på plats, ökar risken att ledtiden förlängs, vilket ger hotaktörer större möjligheter att genomföra angrepp. AI-utvecklingen stärker även hotaktörers förmågor genom hela angreppskedjan samt skapar möjligheter att genomföra mer autonoma cyberangrepp. Detta kan leda till fler och snabbare genomförda angrepp samt en generellt förstärkt hotbild, framför allt när tillgången till kommersiella och öppna AI-modeller ökar.

Likt övriga typer av hotaktörer utvecklar och utnyttjar även statliga aktörer AI för att nå sina strategiska målsättningar. Utvecklingen kring AI kan därför även vävas in i ett geopolitiskt sammanhang genom den kapacitetshöjning AI kan erbjuda till en statlig aktör i konkurrens med andra stater. AI utnyttjas generellt men kan även komma att höja specifika staters kapacitet att agera, bland annat inom cyberdomänen.

Ett fenomen som växt fram under året är att AI-modeller tar sig utanför de tänkta testmiljöerna, agerar utanför ramarna för sitt uppdrag och genomför cyberangrepp. Flera sådana angrepp har fått stor uppmärksamhet under 2026 och har ökat kraven på reglering av säkerheten kring AI-modeller. Den bristande säkerheten bedöms kunna leda till fler fall av självständiga angrepp från AI-modeller framöver.

AI innebär också nya möjligheter i cybersäkerhetsarbetet. Verksamheter börjar dra nytta av nischade AI-modeller i sitt säkerhetsarbete för att till exempel göra prioriteringar och öka hastigheten i hanteringen av säkerhetsuppdateringar, hantera larm i SOC-verksamheter (*security operations centre*) och för att analysera angrepp.

NCSC har arbetat fram rekommendationer för hur verksamheter kan hantera utmaningarna som kommer med den snabba AI-utvecklingen.



Läs mer och ta del av metodstöd på **ncsc.se/cyberhotlandskapet**



FOTO: SHUTTERSTOCK.COM

När *vägen* in går via leverantören

Angrepp där leverantörer drabbas, och i förlängningen de samhällsviktiga verksamheter de levererar till, är ett återkommande problem och visar på utmaningen med cybersäkerhet kopplat till leveranskedjor.

I ett leveranskedjeangrepp drabbas först en initial verksamhet, vars tillgångar senare kan utnyttjas för att driva angreppet vidare. Leverantörer som har en avgörande roll i driften av samhällsviktiga tjänster, eller som hanterar känslig information, måste därför ingå i översynen och det löpande arbetet med att säkerställa ett starkt skydd mot angrepp. Organisationer behöver ställa rätt kravbild mot leverantörer och säkerställa att kraven uppfylls fortlöpande. Leverantören har ett ansvar att ge relevant information om säkerhet, sårbarheter och åtgärder, till exempel genom att rapportera aktivt utnyttjade sårbarheter och allvarliga incidenter enligt EU:s cyberresiliensförordning *(Cyber Resilience Act, CRA)*.

I takt med att det digitala ekosystemet växer, ökar också mängden beroenden som verksamheter behöver förhålla sig till. Under de senaste åren har det skett en ökning av angrepp via leveranskedjor mot utvecklingsplattformar, där en hotaktör kompromitterar en leverantörs tjänst eller system för att sprida skadlig kod till de produkter eller tjänster som levereras till slutkunden. Hotaktörer tenderar även att utnyttja tilliten till automatiserade uppdateringar, installationer och skript.

NÄSTAN HÄLFTEN
av samtliga inkomna incidentrapporter under 2025 gällde incidenter hos leverantörer.

EXEMPEL

Så spreds skadlig kod via Trivy och npm

Hotaktörer kan utnyttja att verksamheter litar på automatiska uppdateringar, installationer och skript. Eftersom processerna är automatiserade kan skadlig kod spridas utan mänsklig inblick.



Våren 2026 drabbades säkerhetsföretaget Aqua Security av ett angrepp mot företagets sårbarhetsskanner Trivy, och skadlig kod skapad för att stjäla kontouppgifter samt skapa bakdörrar distribuerades.

Angreppet fortsatte sedan i flera steg. Bland annat spred hotaktören en självspridande skadlig kod som på kort tid tog sig in i ett stort antal programpaket i det öppna programbiblioteket npm, som används av systemutvecklare.

Paketen laddades sedan ned av många verksamheter och kunde användas för att stjäla känslig information i stor skala.

ÖPPEN KÄLLKOD kan innebära ökade risker när det kommer till leveranskedjeangrepp. Vid installation av ett paket byggt med öppen källkod hämtas samtliga beroenden, och angreppsytan ökar. Organisationer bör därför vara extra uppmärksamma på paket som inte underhålls på rätt sätt, där sårbarheter kan upptäckas men tillförlitliga säkerhetsuppdateringar uteblir. Även välkända och tidigare pålitliga paket kan kompromitteras om en hotaktör, till exempel genom social manipulation, kommer över underhållsprivilegier. Det förekommer också att hotaktörer genom bedrägliga domännamn lurar utvecklare att ladda ner paket som verkar legitima men innehåller skadlig kod.

NCSC har tagit fram rekommendationer för hur verksamheter kan kartlägga riskerna kopplade till leveranskedjor och stärka cybersäkerheten i samarbetet med leverantörer.

Läs mer och ta del av rekommendationerna på ncsc.se/cyberhotlandskapet



FOTO: LARS OVE JONSSON / SHUTTERSTOCK.COM

Cyberangrepp riktade mot fysiska system

Styr- och kontrollsystemen bakom till exempel el, vatten och värme blir allt mer uppkopplade och integrerade, vilket skapar nya angreppsytor för hotaktörer.

Hotbilden gällande OT-system, operativ teknik, som är en del av cyberfysiska system, har hamnat mer i blickfånget de senaste åren. Ett flertal uppmärksammade angrepp i vår omvärld där styr- och kontrollsystem har påverkats har fått konsekvenser för till exempel vattenkraftverk, vattenrenings- och energianläggningar. Inte minst har vi sett angrepp mot styrsystem inom kyl- och frysutrustning i Sverige och Europa, som haft en direkt påverkan på ett stort antal verksamheter.

OT-system är en central del i samhällets infrastruktur och funktionalitet. De återfinns i allt från fastighetsautomation och ventilation till vattenförsörjning och industriell utrustning. Från ett totalförsvarsperspektiv kan angrepp mot OT-system påverka samhället på ett mycket kännbart sätt, och OT-systemen kan därför vara ett prioriterat mål för till exempel statliga hotaktörer.

En ökad integration mellan it- och OT-miljöer innebär att angreppsytan utvidgas. Lösningar för fjärradministration, datainsamling och verksamhetsintegration kan skapa nya möjligheter för hotaktörer, där en initial kompromettering av ett it-system i förlängningen också kan påverka fysiska processer. Att stärka säkerheten kring OT-system är samtidigt utmanande då de ofta har långa livscykler, äldre komponenter och begränsade möjligheter till säkerhetsuppdateringar utan att driften och tillgängligheten i systemen påverkas.



FOTO: SHUTTERSTOCK.COM

OT-system bör därför så långt det är möjligt inte vara direkt exponerade mot internet. Sett till omfattningen av exponerade system i Sverige, bedömer NCSC att verksamheter behöver se över och stärka skyddet. Om ett verksamhets- eller samhällskritiskt system måste vara exponerat mot internet behöver det skyddas i flera lager. Det kan till exempel vara säkra uppkopplingar via vpn, särskilda brandväggar, löpande övervakning och larm gällande konton och nätverkstrafik, segmentering av nätverk och säker inloggning med multifaktorautentisering. Dessutom krävs rutiner för att löpande identifiera och åtgärda säkerhetsbrister samt en beredskap för incidenter som tar hänsyn till kravet på säker och oavbruten drift.

Viktigt, speciellt i större organisationer, är att samordna processer gällande drift och säkerhetsarbete i integrerade system, samt att säkerställa hur samordningen mellan verksamheten och it-leverantörer fungerar vid en störning.

NCSC har tagit fram rekommendationer för hur verksamheter kan öka säkerheten kring OT-system.

Läs mer och ta del av metodstöd på ncsc.se/cyberhotlandskapet



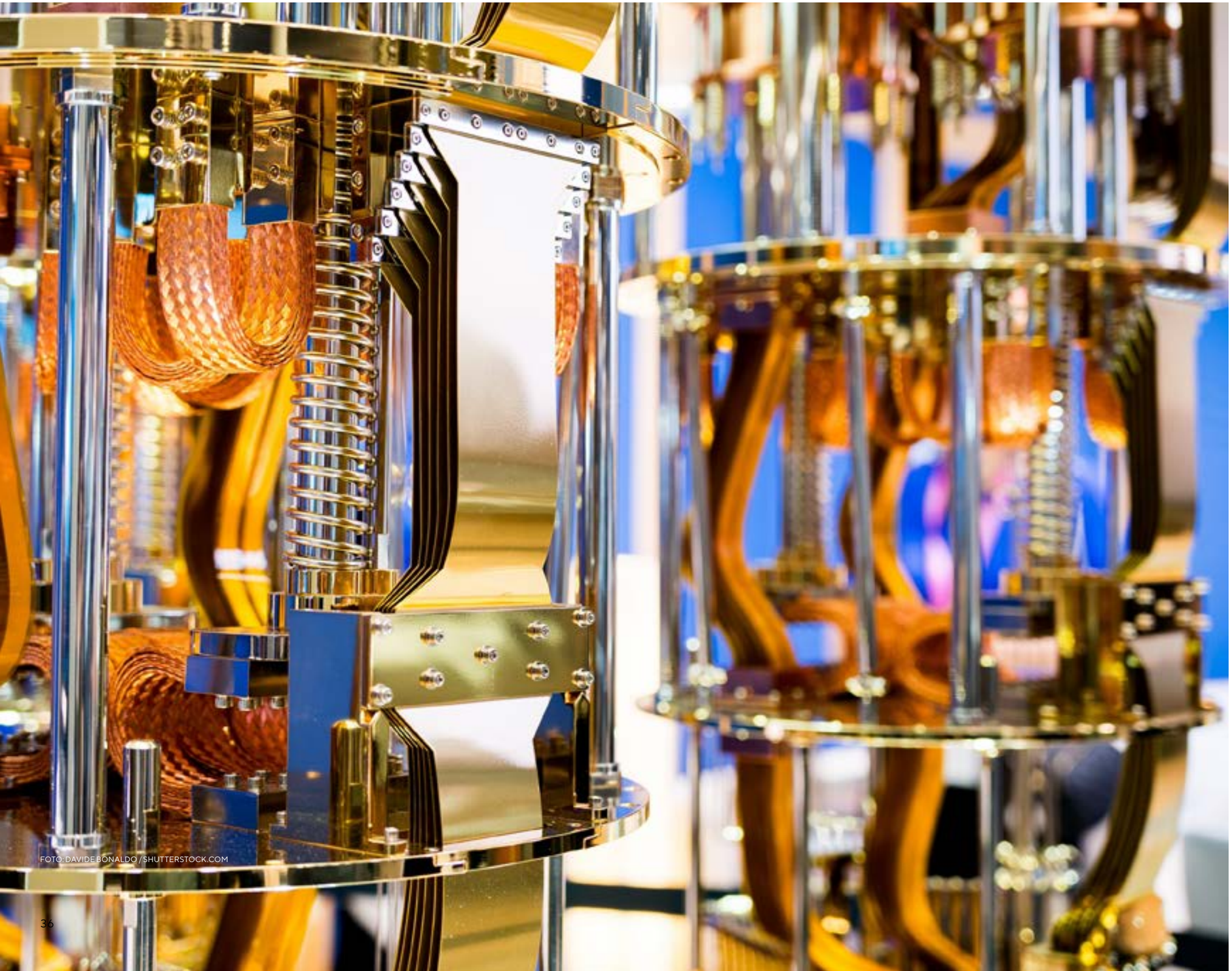


FOTO: DAVIDE BONALDO / SHUTTERSTOCK.COM

2030

Senast då bör särskilt skydds-värda verksamheter ha gått över till kvantsäker kryptografi. För övriga verksamheter är målet 2035.

Läs mer och ta del av metodstöd på **ncsc.se/cyberhotlandskapet**

Övergång till kvantsäkra system

Kvantdatorer kan på sikt försvaga skyddet för dagens krypterade information. Därför behöver övergången till kvantsäker kryptografi planeras redan nu.

Det digitala samhället bygger på kryptering, för att göra information otillgänglig för obehöriga. Den skyddar allt från bankärenden och e-post till samhällsviktig infrastruktur och offentliga tjänster. Men utvecklingen av kvantdatorer gör att delar av dagens kryptering på sikt inte ger det skydd som avsetts. Då skulle angripare kunna komma åt känslig information och system. NCSC har tagit fram övergripande rekommendationer för när och hur övergången till kvantsäkra lösningar bör ske. Målet är att övergången ska vara klar senast 2035, och för särskilt skyddsvärda verksamheter redan 2030.

ÅTGÄRDER FÖR EN STÄRKT MOTSTÅNDSKRAFT

Det går att göra mycket för att minska risken att drabbas av angrepp. Här beskrivs hur ni försvårar för angriparen, skyddar system i flera lager och hur ledningen tar sitt ansvar för cybersäkerhetsarbetet. Vi beskriver också hur ni kan utveckla arbetet inom hot- och riskanalys.

I avsnittet går vi igenom hur ni kan stärka skyddet, steg för steg. Vi börjar med skydd mot vanliga metoder för intrång; läckta eller stulna inloggningsuppgifter, sårbarheter i system som är exponerade mot internet och nätfiske. Därefter beskrivs metoder för att bygga skydd i flera lager, så att ett intrång inte gör hela systemmiljön sårbar. Till sist tar vi upp ledningens ansvar enligt cybersäkerhetslagen och hur hot- och riskanalys hjälper er att prioritera insatserna där de gör störst nytta.

FOTO: SHUTTERSTOCK.COM



FOTO: AFDIN ADIN / SHUTTERSTOCK.COM

Skydda verksamheten: *initial åtkomst*

Bredare kampanjer för att stjäla kontouppgifter, effektivare utnyttjande av sårbarheter i system och nätfiske som blir allt mer sofistikerat, gör att det är avgörande att stärka skyddet mot hotaktörers initiala åtkomst till system.

Vanliga metoder för att en hotaktör ska kunna få initial åtkomst till ett system är att använda läckta eller stulna inloggningsuppgifter, utnyttja sårbarheter i system som är exponerade mot internet och att skicka nätfiskemeddelanden som lurar användaren att avslöja känslig information eller som innehåller skadliga länkar eller bifogade filer. En framväxande metod är *clickfix*-angrepp där användaren luras att installera skadlig kod via manipulerade webbplatser och program. AI används av hotaktörer för att effektivisera metoderna gällande initial åtkomst, vilket bidrar till ökade krav på att stärka skyddet.

Skydd för konton

FÖR ATT SKYDDA ER mot att hotaktörer missbrukar läckta eller stulna inloggningsuppgifter, rekommenderas att implementera kontoövervakning för att snabbt upptäcka misstänkt eller felaktigt användande av konton. Det kan till exempel gälla kontoanvändning på oväntade tider och platser, oväntat skapande av nya konton samt oväntat utökande av ett kontos behörigheter. Vid misstanke om att ett konto är komprometterat bör det isoleras, aktiva sessioner upphävas och lösenord bytas ut.

EN ANNAN VIKTIG ÅTGÄRD i det förebyggande arbetet är att införa multifaktorautentisering, MFA, och att ha en genomtänkt lösenordspolicy. Policyn bör innehålla aspekter såsom lösenordssammansättning, giltighetstid, distribution och skyddsåtgärder. En lösenordshanterare kan användas för att underlätta efterlevnad av en lösenordspolicy. Längden på lösenord, minst 15 tecken, och att lösenordet är unikt är viktiga faktorer. Använd gärna lösenordsfraser med slumpmässigt sammansatta ord och tecken, som bildar längre strängar, fortfarande med minst 15 tecken. Använd gärna spärrlistor för lösenord där det är möjligt, så att vanliga eller tidigare lösenord inte kan användas.

ORGANISATIONER rekommenderas också generellt att följa principer som *zero trust* och *least privilege* i sitt säkerhetsarbete, det vill säga att kräva identifiering och autentisering under hela sessionen vid åtkomst till system samt att begränsa en medarbetares tillgång och behörigheter till den lägsta möjliga för att kunna utföra en uppgift. På så sätt kan vidare konsekvenser undvikas, om ett konto skulle kompromettеras.

Använd tidsbegränsade behörigheter, *just-in-time*, för att begränsa administrativ åtkomst med höga privilegier till specifika tidsperioder vid utförandet av administrativa åtgärder. Dessa behörigheter bör granskas innan de tilldelas. Säkerställ också en tydlig separation mellan konton för administrativa uppgifter med höga privilegier och konton för dagligt bruk.



Tips

NCSC rekommenderar verksamheter att prioritera hur ni kan stärka ert skydd utifrån råden i rapporten. Inom vilka områden bör skyddet stärkas och vad bör ni ta tag i först utifrån era hot och risker? Använd gärna etablerade ramverk för cybersäkerhetsarbete.

Läs mer på **ncsc.se/cyberhotlandskapet**

FOTO: SHUTTERSTOCK.COM

Skydd för exponerade system

UTIFRÅN ETT SKYDDSPERSPEKTIV är det viktigt att endast de enheter och program som verkligen behöver vara exponerade mot internet är det, eftersom onödig exponering ger hotaktörer ökade möjligheter att genomföra angrepp genom att till exempel utnyttja tekniska sårbarheter. För system som är exponerade mot internet rekommenderas som regel att applicera säkerhetsuppdateringar direkt och att hantera eventuella driftstörningar kopplade till dessa. Om säkerhetsuppdateringen inte kan genomföras direkt och konsekvenserna bedöms kunna bli allvarliga, behöver överväganden göras om att till exempel isolera systemet från internet. Avvägningar måste här göras mellan konsekvenserna av ett potentiellt intrång och de konsekvenser och eventuella kostnader ett driftstopp innebär. För att kunna arbeta effektivt med cybersäkerhet är det viktigt att ha en kontinuerligt uppdaterad förteckning över den hårdvara och programvara som används i verksamheten, inklusive aktuella versioner, en *asset list*.

DE SYSTEM SOM BEHÖVER vara exponerade mot internet behöver också ett stärkt skydd. Detta kan bestå i vpn-lösningar, specifika brandväggar, kontinuerlig övervakning av konton och nätverkstrafik med regler för detektering och larm gällande avvikelser, segmentering av nätverk samt säkra och multifaktorbaserade lösningar för åtkomst till systemen.

Skydd mot nätfiskeangrepp

UTÖVER VANLIG MULTIFAKTORAUTENTISERING kan så kallad nätfiskeresistent MFA användas för privilegierade konton med höga behörigheter och enheter som behöver extra skydd. Det kan till exempel innebära fysiska säkerhetsnycklar eller smarta kort som kan användas för åtkomst till mer skyddsvärda konton. På enheter som behöver extra skydd kan vissa funktioner stängas av, till exempel möjligheten att öppna länkar i bilagor. Ni kan också använda tillåtelselistning, så att bara godkända program kan användas på enheten.

Gör det enklare för medarbetarna genom att markera e-post som kan innebära högre risk, till exempel meddelanden från externa avsändare. Då blir det också tydligt om en hotaktör försöker använda en intern e-postadress som avsändare för att verka trovärdig.

Ta del av fler råd för att stärka skyddet via ncsc.se/cyberhotlandskapet





Utbilda medarbetare i hur de känner igen och undviker nätfiske. Uppmuntra dem till exempel att:

- Vara vaksamma på e-post och sms från okända och externa avsändare.
- Kontrollera avsändarens e-postadress, inte bara namnet, i misstänkta e-postmeddelanden.
- Vara vaksamma på meddelanden och kontaktförsök från okända nummer eller personer i kommunikationsappar.
- Dela känslig information enbart i skyddade kommunikationskanaler, det vill säga inte i reguljär e-post eller via en vanlig telefonlinje.
- Aldrig dela koder eller lösenord med andra, och inte återanvända koder och lösenord i olika system.
- Inte logga in i systemtjänster vid oväntad begäran, eller kopiera, ladda ned och exekvera kod på uppmaning, till exempel vid besök på webbplatser.
- Genast rapportera om de misstänker att de fått ett nätfiskemeddelande, särskilt om de har klickat på en bilaga eller länk, skannat en qr-kod eller lämnat ut känsliga uppgifter.

FOTO: BENEDEK ALPAR / SHUTTERSTOCK.COM

Stärkt *skydd* i flera lager

Ingen enskild skyddsåtgärd är normalt sett tillräcklig, men med flera lager av skydd kan angrepp försvåras och stoppas upp.

Istället för att förlita sig på enskilda åtgärder bör organisationer skydda sina system med flera lager av skydd som överlappar och kompletterar varandra. Tankesättet *assumed breach*, att utgå från att en angripare redan lyckats ta sig in i organisationens nätverk, används i syfte att skapa skyddsåtgärder som faktiskt kan hantera att ett intrång sker. Säkerhetsåtgärder i flera lager brukar kallas försvar på djupet, *defence in depth*.

Syften med skydd i flera lager

Begränsa och försvåra en angripares möjlighet att utnyttja och röra sig vidare i systemmiljön vid ett intrång. Därmed begränsas skadorna om ett intrång sker.

Skapa flera oberoende barriärer så att ett enskilt fel eller ett enskilt skydd som fallerat inte gör hela systemmiljön sårbar.

Möjliggöra tidigare upptäckt av intrång.

FOTO: AQUILA CHRYSAETOS / SHUTTERSTOCK.COM

Så kan skydd i flera lager se ut

Försvar på djupet kan till exempel implementeras med följande åtgärder:

Nätverkssegmentering
Dela upp nätverket i olika segment för att begränsa åtkomsten mellan olika system och delar av infrastrukturen.

Säker kommunikation mellan segment
Säkerställ att kommunikationen mellan nätverkssegment är autentiserad, validerad och endast tillåten när det finns ett väldefinierat behov av kommunikation.

Säkra brandväggskonfigurationer
Se över brandväggsreglerna och tillämpa tydliga säkerhetspolicys. Trafik bör inte automatiskt betraktas som betrodd bara för att den kommer från organisationens interna nätverk.

Begränsa vilka system som får kommunicera med varandra
Tillåt bara den kommunikation mellan system som är helt nödvändig för verksamheten.

Stärkt klientskydd
Säkerställ ett grundläggande skydd på klientnivå. Detta är särskilt viktigt för enheter som används av medarbetare som hanterar känslig information. Tilldela endast de rättigheter som behövs för en enhet. Kontrollera även dess säkerhetstillstånd innan åtkomst till olika system eller information beviljas. Använd till exempel skydd mot automatisk exekvering av webbaserade filer samt tillåtelselistning av godkänd programvara för klienter, *allow listing*.

Härda servrarna
Säkerställ att servrar är korrekt konfigurerade, uppdaterade och att onödiga tjänster och åtkomstmöjligheter är avstängda.

GENOM ATT KOMBINERA dessa åtgärder skapas flera kompletterande lager av skydd. Om en angripare lyckas ta sig förbi ett säkerhetslager finns ytterligare barriärer som kan hindra angriparen från att ta sig vidare i systemmiljön och utöka angreppet.

Ta del av NCSC:s 10 rekommenderade säkerhetsåtgärder och flera råd för att stärka skyddet via ncsc.se/cyberhotlandskapet

Cybersäkerhet och ledningens ansvar

Cybersäkerhet är inte bara en fråga för it-avdelningen. Enligt cybersäkerhetslagen är det ledningen som bär det yttersta ansvaret och ledningen måste också utbilda sig.

Ledningen ansvarig för cybersäkerhetsarbetet

En engagerad och kunnig ledning är avgörande för ett väl fungerande cybersäkerhetsarbete. Enligt cybersäkerhetslagen (2025:1506) är det ledningen som ytterst ansvarar för att styra organisationens cybersäkerhetsarbete så att det blir systematiskt och riskbaserat. En viktig del i detta är att cybersäkerhetsarbetet ska vara integrerat i organisationens befintliga ledning och styrning, och inte hanteras i ett separat spår. Ledningen ska besluta om mål, inriktning och resurser och se till att organisationen har den kompetens och de resurser som behövs för att nå rätt säkerhetsnivå.

Obligatoriskt med utbildning för ledningen

Enligt cybersäkerhetslagen är det obligatoriskt för ledningen att genomgå cybersäkerhetsutbildning. Medan verksamhetsutövaren är skyldig att vidta nödvändiga säkerhetsåtgärder. Detta förtydligas närmare i NCSC:s föreskrifter. Det ställs bland annat krav på att utbildningen ska ge ledningen tillräckligt med kunskap och kompetens för att kunna fastställa mål och inriktning för verksamhetsutövarens cybersäkerhet samt upprätthålla en lämplig cybersäkerhetsnivå utifrån identifierade risker.

Systematiskt arbete ger ökad motståndskraft

Syftet med att ledningen får ett mer tydligt uttalat ansvar är att den då kan driva på ett mer systematiskt cybersäkerhetsarbete där rätt kompetens och resurser finns på plats. Det innebär att cybersäkerheten ingår i verksamhetsplanerna och att riskanalyser är en naturlig del av arbetet. Genomförandet kan ske genom implementering av ledningssystem för informationssäkerhet (LIS), standarder och certifiering, vilket ger uttryck för verksamhetens cybersäkerhetsmognad, en hög medvetenhet om hotbilden och därmed konkurrenskraft i upphandlingar. Målet är att organisationen ska bli mer motståndskraftig och samtidigt få ett högre förtroende inom sitt verksamhetsområde.

Läs mer om hot- och riskanalys på nästa sida.



Visste du att...

Ledningens styrning och kontroll är det område där organisationerna oftast uppger att de brister gällande det systematiska cybersäkerhetsarbetet.

65 procent uppger att de saknar den personal som krävs för att förbättra cybersäkerhetsarbetet.

61 procent uppger att deras högsta ledning har det engagemang som krävs för att förbättra cybersäkerhetsarbetet.

Informationen kommer från NCSC:s mätning Cybersäkerhetskollen 2025. Mätningen genomförs vartannat år och visar nivån på verksamheternas systematiska cybersäkerhetsarbete.

Rätt hot- och *riskanalys* är nyckeln

Ingen verksamhet kan skydda alla system fullt ut. Genom att veta vilka system som är viktigast och vilka hot som är aktuella kan ni lägga resurserna där de gör störst nytta.

Prioritera era system och kartlägg hot

För att kunna bygga en motståndskraftig cybersäkerhet är det viktigt att förstå vilka hot och risker som verksamheten står inför.

Börja med att identifiera de delar av verksamheten och de tjänster som måste kunna upprätthållas. Identifiera därefter deras beroenden av information, system och leverantörer. Det är viktigt att förstå vad som är mest kritiskt för er organisation och var ett angrepp skulle få allvarligast konsekvenser, det vill säga var verksamheten och era leveranser skulle bli särskilt påverkade om systemen slutar fungera eller information går förlorad. Undersök sedan hotbilden mot er organisation och er sektor. Omvärldsbevakning, analysverktyg och samarbete inom den egna sektorn för att ta del av information om hot kan bidra till en god förståelse för den aktuella hotbilden.

Genomför systematiska riskanalyser

De hot ni har identifierat är en del av den riskanalys som varje organisation bör göra. Risk kan definieras på olika sätt. Ett vanligt sätt är att väga samman hur sannolikt det är att en oönskad händelse, till exempel ett cyberangrepp, inträffar och hur allvarliga konsekvenserna blir.

För att kunna bemöta riskerna och begränsa konsekvenserna bör riskanalysen göras utifrån en systematisk process. Där sammanställs de risker verksamheten har identifierat, tillsammans med en beskrivning av hur verksamheten ska agera om något händer. Beroende på verksamhet kan det finnas olika lagkrav på hur grundlig analysen ska vara.

I cybersäkerhetslagen ställs det tydligare krav på verksamhetsutövare att ta fram riskanalyser. Verksamhetsutövare ska identifiera, analysera och värdera riskerna utifrån vilka konsekvenser de kan få och hur sannolika de är.

Riskmatris – värdera risker

KONSEKVENS	Låg	Medelhög	Hög	Mycket hög
Allvarlig	M	H	H	MH
Betydande	M	M	H	H
Måttlig	L	M	M	H
Försumbar	L	L	M	M

En riskmatris kan användas för att värdera olika risker mot varandra. Tillsammans med kriterier för riskacceptans är det ett bra verktyg för att välja rätt säkerhetsåtgärder.

Analys med riskmatris

Verksamhetsutövare behöver fastställa kriterier för riskacceptans. En risk med måttliga konsekvenser men hög sannolikhet kan placeras i den röda delen av riskmatrisen, medan en risk med mycket allvarliga konsekvenser men låg sannolikhet kan hamna i den orange delen. Detta kan ge intrycket att den förstnämnda risken är mer allvarlig, trots att konsekvenserna av den senare skulle kunna bli betydligt mer omfattande. Riskmatrisen bör därför kompletteras med tydliga kriterier för riskacceptans för att säkerställa att risker bedöms utifrån sannolikhet, konsekvens och verksamhetens tolerans för risk.

Utgå från relevant informationsklassning, omvärldsbevakning och information om incidenter och tillbud. När hotbilden förändras eller då verksamheten får kännedom om nya sårbarheter ska riskanalysen uppdateras. Riskanalysen ska ligga till grund för valet av säkerhetsåtgärder.

Öva regelbundet

För att upprätthålla er prioriterade verksamhet även under störningar är det viktigt att öva på olika scenarier som skulle kunna bli verklighet och därmed påverka er organisation och era leveranser. Se till att ha reservrutiner och att öva dem regelbundet. Testa era säkerhetskopior och återställningsrutiner samt hur samordningen mellan verksamheten, er it-leverantör, beredskapsfunktioner och andra leverantörer fungerar vid en störning.



Läs mer och ta del av metodstöd på ncsc.se/cyberhotlandskapet

Uppdateringar och metodstöd på nätet

På NCSC:s webbplats hittar ni fördjupningar, rekommendationer och metodstöd som hör till den här rapporten.

Metodstöd för informationssäkerhetsarbete
NCSC:s metodstöd syftar till att förtydliga hur ett systematiskt informationssäkerhetsarbete kan utformas utifrån standarderna om ledningssystem för informationssäkerhet (LIS). Metodstödet innehåller vägledningar, verktyg, tips, mallar och annat stöd och råd. Metodstödet innehåller till exempel en del om riskanalys.
Läs mer på ncsc.se/metodstod

Cybersäkerhetskollen
Cybersäkerhetskollen är samlingsnamnet på NCSC:s cybersäkerhetsmätningar som mäter nivån på verksamheters systematiska cybersäkerhetsarbete. De kan också användas som stöd för att kartlägga och förbättra det systematiska cybersäkerhetsarbetet.
Läs mer på ncsc.se/cybersakerhetskollen

Mognadsdialogen
Mognadsdialogen är ett pedagogiskt verktyg för att följa upp hur effektivt organisationen arbetar med sitt systematiska informationssäkerhetsarbete utifrån behov, krav och förutsättningar.
Läs mer på ncsc.se/mognadsdialogen

Automatiska notifieringar om tekniska sårbarheter (ANTS)
ANTS är en kostnadsfri tjänst från CERT-SE vid NCSC, och som hjälper svenska verksamheter att övervaka sina angreppsytor på internet. Tjänsten skickar notifieringar när brister eller andra företeelser identifieras som kan behöva åtgärdas för att minska risken för cyberangrepp.
Läs mer på ncsc.se/ants

Proaktiv skanning
Proaktiv skanning från CERT-SE vid NCSC hjälper svenska verksamheter att få en bättre förståelse för sin angreppsyta på internet. Tjänsten stödjer organisationer i att identifiera sårbarheter, felkonfigurationer och andra säkerhetsrisker innan de kan utnyttjas av angripare.
Läs mer på ncsc.se/skanning

MISP-SE
MISP-SE är en kostnadsfri tjänst som gör det möjligt för svenska verksamheter att dela och ta del av information om cyberhot. Genom att utbyta hotindikatorer och erfarenheter från cyberincidenter kan organisationer upptäcka, förebygga och hantera cyberangrepp snabbare.
Läs mer på ncsc.se/misp-se

Veckobrev från NCSC:s nationella CSIRT-funktion CERT-SE
Veckobrevet sammanfattar veckans omvärldsbevakning inom cybersäkerhetsområdet i olika öppna nationella och internationella källor, till exempel nyheter, publiceringar och rapporter om veckans it-säkerhetshändelser.
Läs mer på cert.se/prenumerera

Vi har också samlat fördjupningar, rekommendationer och metodstöd som hör till den här rapporten.
Läs mer på ncsc.se/cyberhotlandskapet

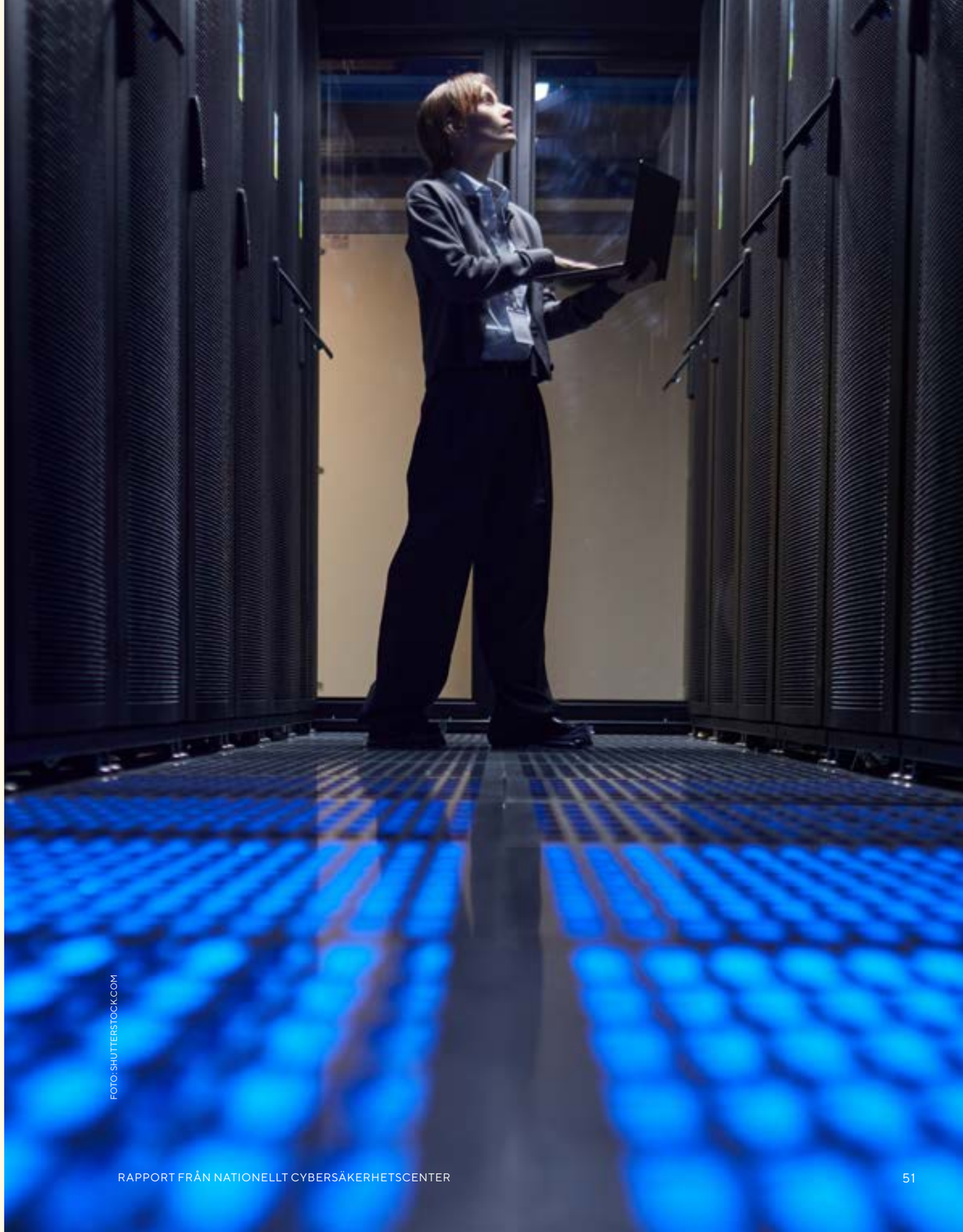


FOTO: SHUTTERSTOCK.COM

Antagonistiska hot
Hot från någon som avsiktligt vill orsaka skada, till skillnad från olyckor eller tekniska fel.

Botnät
Ett nätverk av datorer och andra uppkopplade enheter som styrs gemensamt, ofta utan att ägarna vet om det. Används till exempel för överbelastningsangrepp.

CERT-SE
CERT-SE vid NCSC är Sveriges nationella CSIRT *(Computer Security Incident Response Team)* med uppgift att stödja det svenska samhället i arbetet med att hantera och förebygga it-säkerhetsincidenter.

Clickfix
Angreppsmetod där användaren luras att själv köra skadlig kod, ofta genom falska instruktioner på en manipulerad webbplats.

Cyberfysiska system
Datorsystem som styr och övervakar fysiska processer, till exempel i elnät, vattenverk och industrier. Kallas även industriella styrsystem (ICS) eller operativ teknik (OT).

Dubbel utpressning, *double extortion*
När angriparen både låser offrets filer och hotar att publicera stulen information.

Exfiltrering
När en angripare för ut stulen information från ett system till sina egna servrar.

Försvar på djupet, *defence in depth*
Att skydda system med flera lager av skydd som kompletterar varandra.

Hacktivist
Person eller grupp som genomför cyberangrepp av ideologiska eller politiska skäl.

Hotaktör
Den som ligger bakom, eller kan ligga bakom, ett cyberangrepp – en person, en grupp, en organisation eller en stat.

Infostealer
Spionprogram som stjäl inloggningsuppgifter och annan information från en dator.

Kritisk infrastruktur
Verksamheter och system som samhället inte klarar sig utan, till exempel el, vatten, transporter och betalningar.

Kryptering
Teknik som gör information oläslig för den som inte har rätt nyckel.

Kvantsäker kryptografi
Kryptering som är utformad för att stå emot angrepp även från framtida kvantdatorer.

Leveranskedjeangrepp
Angrepp där angriparen tar sig in hos en leverantör för att nå leverantörens kunder.

Living-off-the-land
När angriparen använder systemets egna, legitima verktyg i stället för egen skadlig kod. Det gör angreppet svårare att upptäcka.

Multifaktorautentisering, MFA
Inloggning i flera steg, till exempel lösenord plus en kod i mobilen. Nätfiskeresistent MFA, till exempel en fysisk säkerhetsnyckel, stärker skyddet ytterligare mot social manipulation.

NCSC
Nationellt cybersäkerhetscenter. En del av Försvarets radioanstalt, FRA.

NPM, *Node Package Manager*
Ett stort, öppet bibliotek med färdiga programpaket som utvecklare använder när de bygger program.

Nätfiske, *phishing*
Bedrägliga mejl, sms eller andra meddelanden som ska lura mottagaren att lämna ut uppgifter, klicka på länkar eller öppna filer. Riktat nätfiske är skräddarsytt för en viss person eller organisation.

Opportunistiska angrepp
Angrepp där en hotaktör slår till där det finns en öppning, snarare än mot ett i förväg utvalt mål.

Ransomware-as-a-service, RaaS
Affärsmodell där kriminella hyr ut färdiga verktyg för utpressningsangrepp till andra kriminella.

Segmentering
Att dela upp ett nätverk i separata delar, så att ett intrång begränsas till en del av nätverket.

Skadlig kod
Program eller kod som är gjord för att skada, stjäla information eller ge en angripare kontroll över ett system.

SOC, *Security Operations Centre*
Säkerhetscentral som övervakar en organisations system och hanterar larm.

Sårbarhet
En säkerhetsbrist i ett program eller system som en angripare kan utnyttja.

Säkerhetsuppdatering, *patch*
Uppdatering från en leverantör som åtgärdar en sårbarhet.

Tillåtelselistning
Att bara tillåta godkända program att köras.

Typosquatting
När angripare använder namn som liknar välkända namn, med avsiktliga stavfel, för att lura användare.

Utpressningsangrepp, *ransomware*
Angrepp där angriparen låser (krypterar) offrets filer och/eller stjäl information och kräver en lösensumma.

VPN, *virtual private network*
En krypterad förbindelse som ger säker åtkomst till ett nätverk över internet.

Wiper
Skadlig kod som raderar eller förstör information.

Zero trust
Säkerhetsprincip där ingen användare, enhet eller trafik automatiskt betraktas som pålitlig, inte ens inom det egna nätverket. Behörigheten kontrolleras vid varje åtkomst.

Överbelastningsangrepp, DDoS
Angrepp där en webbplats eller tjänst belastas av så mycket trafik att den slutar fungera.

Kontakta oss

Har ni frågor om cybersäkerhet eller behöver råd?
Kontakta NCSC på telefon 010-382 80 00 eller
e-post ncsc@ncsc.se.

Cybersäkerhetsrådgivningen
Rådgivningstjänsten vänder sig till alla som deltar i, driver eller ansvarar för cybersäkerhetsarbetet i en organisation. Tjänsten riktar sig i första hand till offentlig sektor samt organisationer som omfattas av cybersäkerhetslagen, men alla typer av organisationer är välkomna att kontakta rådgivningen.
Läs mer på ncsc.se/cybersakerhetsradgivning.

Drabbad av en it-incident?
Rapportera incidenter till NCSC:s cyberportal. För verksamheter som omfattas av cybersäkerhetslagen eller förordningen om statliga myndigheters beredskap, är rapporteringen obligatorisk. Andra kan rapportera frivilligt.
Läs mer på cyberportal.ncsc.se

Mer information om angrepp, metoder och hotaktörer
Vill du veta mer om de angrepp, metoder och hotaktörer som beskrivs i rapporten? Kontakta oss, så berättar vi mer.

Nationellt cybersäkerhetscenter (NCSC) stärker Sveriges förmåga att förebygga, upptäcka och hantera cyberhot.

Vi är navet för Sveriges cybersäkerhet och samordnar hanteringen av allvarliga cyberangrepp som påverkar samhället. Genom stöd och rådgivning hjälper vi organisationer att stärka sin motståndskraft mot hot i den digitala miljön. Vi samverkar med näringsliv, offentlig sektor, civilsamhället, organisationer och akademin. Genom att dela aktuell och relevant kunskap bidrar vi till att höja cybersäkerheten i hela samhället.

FOTO: OLEG ELKOV / SHUTTERSTOCK.COM

Det här är den första utgåvan av NCSC:s årliga öppna rapport om det svenska cyberhotlandskapet med fokus på antagonistiska cyberhot. Rapporten har tagits fram av NCSC med stöd av våra samverkansmyndigheter. Den är skriven för dig som arbetar med cybersäkerhet, oavsett om du sitter i en ledningsgrupp eller arbetar med tekniska frågor varje dag. Men den är också till för dig som vill förstå mer om cyberhoten i Sverige.

NATIONELLT
CYBERSÄKERHETSCENTER
En del av FRA