Verksamheten för strategisk cybersäkerhet

Policy för utveckling och integrering av ny cybersäkerhetsteknologi

Nulägesbild för policyområdet

Nulägesbeskrivning och analys sammanställdes i oktober 2025. Dessa kommer att uppdateras till slutversionen av policyn.

Behov av avancerad teknik för moderna riskhanteringsåtgärder

Sveriges digitalisering har skapat både möjligheter och sårbarheter. Den eskalerade hotbilden under 2025, med ransomware-ökningar på 183%, över 30 miljarder kronor i cyberrelaterade förluster, och ihållande överbelastningskampanjer mot samhällsfunktioner, visar att traditionella säkerhetsåtgärder inte längre räcker. MSB:s statistik bekräftar att nästan hälften av alla incidenter orsakas av mänskliga misstag (22%) och systemfel (27%), och 51% av alla inkomna incidenter uppges ha skett hos en leverantör.

Denna komplexitet kräver avancerade tekniska lösningar som kan automatisera skydd, analysera stora datamängder i realtid, och anpassa sig efter nya mönster. Artificiell intelligens (AI), maskininlärning (ML), stora språkmodeller (LLM), kvantkryptografi, blockkedjeteknologi och Zero Trust-arkitektur representerar en ny generation av riskhanteringsverktyg som kan möta moderna cyberhot.

Ökade satsningar på cybersäkerhet med betydande resurstillförsel under kommande år visar på ett tydligt åtagande att utveckla och integrera avancerad teknik. Sveriges forsknings- och teknikintensiva näringsliv inom cybersäkerhetsområdet ligger i framkant och skapar förutsättningar för både innovation och adoption.

Exempel på avancerad teknik som svar på moderna hot

De mest framträdande hoten 2025 kräver teknikdriven riskhantering och flera avancerade teknologier finns redan idag som adresserar dessa risker:

- AI-förstärkta angrepp kräver AI-baserat försvar: Phishing-as-a-service med AI-genererade meddelanden möts av ML-baserad anomalidetektion som kan identifiera avvikande beteendemönster även när attackerna efterliknar legitim kommunikation.

- Automatiserad upptäckt av ransomware: Med ökning av ransomware kan organisationer inte längre förlita sig på manuell granskning. ML-system kan analysera stora datamängder i realtid och upptäcka tidiga tecken på intrång, vilket möjliggör snabbare respons.
- Zero Trust mot identitetsbaserade hot: Kompromitterade konton och otillräcklig åtkomstkontroll visar behovet av kontinuerlig verifiering. Zero Trust eliminerar implicit förtroende och kräver upprepad autentisering vid varje åtkomstförfrågan.
- Kvantsäker kryptering mot framtida hot: Med EU:s mål om post-kvantumkryptering senast 2030 har Sverige fem år på sig att migrera kritiska system.
- Blockkedjor för transparens i leveranskedjor: Blockkedjebaserade lösningar med Software Bill of Materials (SBOM) och kryptografiska signaturer skapar spårbarhet och förhindrar manipulering.

Sammantaget ser man att hastighet, komplexitet och delade beroenden gör att manuella kontroller inte räcker. Att ungefär hälften av incidenterna orsakas av mänskliga misstag och systemfel understryker behovet av automatisering genom avancerad teknik.

Utveckling och integrering av avancerad teknik i Sverige

Sverige satsar brett på avancerad teknik för att stärka cybersäkerheten.

AI, ML och LLM används för att automatisera riskhantering, där ML analyserar nätverkstrafik i realtid och LLM:er tolkar ostrukturerad information för snabbare incidenthantering. Initiativ från Försvarsmakten, Högskolan i Halmstad och företag som Detectify visar på en stark nationell innovationskraft. Samtidigt utvecklas kvantsäker kryptering genom projekt som National Quantum Communication Infrastructure in Sweden (NQCIS), för att möta framtida hot från kvantdatorer. Tekniker som blockkedjor och Zero Trust stärker strukturell säkerhet där blockkedjor kan användas för att säkra leveranskedjor och identitetsdata, medan Zero Trust-arkitektur möjliggör kontinuerlig verifiering och isolering av potentiella intrång.

Trots att dessa tekniker är beprövade och Sverige som nation ligger i framkant innovationsmässigt är implementeringen ojämn, vilket visar behovet av fortsatt samverkan mellan myndigheter, akademi och näringsliv för att öka apodtionstakten.

Lärdomar från incidenter och teknikens roll

Transparens och automatiserad verifiering i leveranskedjor. Incidenter som CrowdStrike (8,5 miljoner enheter), XZ Utils-bakdörren (CVE-2024-3094) och 3CX-kaskadangreppet visar att leveranskedjor är en primär attackyta. MSB:s statistik bekräftar att 21% av incidenterna 2024 uppgavs ha skett hos leverantörer och ofta med okänd orsak hos leverantören. Blockkedjebaserade SBOM och kryptografiska signaturer skapar spårbarhet och automatiserad verifiering av programvaruintegritet kan upptäcka manipulering innan distribution.

Zero Trust mitigerar identitetsangrepp

Snowflake-kampanjen (165 företag), Sportadmin (2 miljoner drabbade) och DDoS mot BankID visar att komprometterade identiteter och bristande MFA är kritiska sårbarheter. Zero Trust-arkitektur med kontinuerlig verifiering, MFA, beteendeanalys och mikrosegmentering eliminerar implicit förtroende och begränsar skador vid intrång.

Avancerad teknik som komplement till mänskliga processer

MSB:s it-incidentrapport 2024 (mars 2025) visar att hälften av 319 rapporterade incidenter orsakades av misstag eller systemfel vid uppdateringar och konfigurationer. Med ransomware-ökningar på 183% och cyberrelaterade förluster på över 30 miljarder kronor är manuella processer otillräckliga. AI/ML-baserad automation för konfigurationshantering, prediktiv analys för sårbarhetsidentifiering, och automatiserad incidentrespons minskar beroendet av manuella kontroller.

Integrerad övervakning av kritisk infrastruktur

DDoS-kampanjer mot SVT, banker och BankID samt energisektorns incidenter visar att kritisk infrastruktur måste skyddas med integrerad ot/it-övervakning. ML-driven anomalidetektion i realtid, automatiserad nätverkssegmentering och AI-baserad trafikanalys kan identifiera och isolera angrepp innan de påverkar tjänster.

Regelverk och initiativ

Nationell regleringsram och strategi

Sverige har etablerat en tydlig regleringsram genom föreskrifter om säkerhetsåtgärder i informationssystem för statliga myndigheter, och NIS2-direktivet införs i svensk rätt genom Cybersäkerhetslagen Med detta ställs krav på riskanalys, incident-, kontinuitets- och krishantering, säkerhet i leveranskedjor, personalsäkerhet och utbildning, kravställning vid förvärv, utveckling och underhåll av system samt åtkomstkontroll, autentisering och kryptografi. Med AI-förordningen skapas förutsägbarhet kring styrningen av AI-användning i säkerhetskritiska processer. Fokus på systematiskt och effektivt cybersäkerhetsarbete, utvecklad kunskap och kompetens samt förmåga att förebygga och hantera incidenter kräver alla avancerad teknik för att uppnås i praktiken. Betydande resurstillförsel under kommande år skapar förutsättningar för detta arbete.

EU-gemensamma standarder

EU:s ramverk för cybersäkerhetscertifiering skapar gemensamma standarder för digitala produkter och tjänster. I Sverige har Försvarets materielverk (FMV) utsetts till nationell myndighet för cybersäkerhetscertifiering och ansvarar för att samordna och stödja införandet av EU:s cybersäkerhetscertifieringssystem. Från 2025 kan certifieringar utfärdas enligt EUCC (European Union Common Criteria-based cybersecurity certification scheme).

Cyberresiliensförordningen (CRA) ställer nya krav på cybersäkerhet i produkter med digitala inslag och betonar bland annat vikten av Software Bill of Materials (SBOM) som

ett verktyg för att identifiera och hantera sårbarheter i leveranskedjor och mjukvarukomponenter. Dessa initiativ stärker både tilliten till digitala lösningar och förmågan att hantera framtida cyberhot.

EU har tagit fram en färdplan för övergång till kvantsäkrad kryptografi och lanserade i maj 2025 ett samordnat initiativ för att säkerställa att alla medlemsländer övergår till post-kvantumkryptering för kritisk infrastruktur senast 2030. Standardiserade algoritmer inkluderar NIST FIPS 203, 204, 205.

Pågående svenska initiativ

Samordnad och säker statlig it-drift (2024) utgör en förordning för moderna, säkra och kostnadseffektiva it-verktyg. Interoperabilitetsutredningen föreslår koordinerade skyddsnivåer för att underlätta säkerhetskrav vid datadelning. Sveriges digitala infrastruktur (Ena), som samordnas av Digg, byggs utifrån gemensamma standarder och hög säkerhet och NCSC:s nationella modell utgör en gemensam plattform för systematiskt informationssäkerhetsarbete.

Analys av nuläget

Tillfredsställande omständigheter för utveckling av avancerad teknik

Analysen visar en tydlig paradox i Sveriges arbete med avancerad teknik för cybersäkerhet: tekniken finns tillgänglig, regleringen är på plats och resurser allokeras – men implementeringen släpar efter hotbilden.

Stark regleringsram och strategisk resurstillförsel

Sveriges regleringsram (bland annat myndighetsföreskrifter, Cybersäkerhetslagen/NIS2, AI-förordningen och CRA) skapar tydliga krav på riskanalys, incidenthantering, leveranskedjor och kryptering driver på utveckling och integrering av avancerad teknik.

Särskilt betydelsefullt är de ökade satsningarna på cybersäkerhet med betydande resurstillförsel under kommande år. För att effektivt uppnå systematik, kompetens och incidenthantering i praktiken är avancerad teknik nödvändigt. Detta skapar både efterfrågan och finansieringsmöjligheter för teknikutveckling och innovation.

Hög politisk prioritet driver teknikadoption

Regeringens satsningar på området i närtid visar att cybersäkerhet adresseras på högsta politiska nivå. Detta skapar förutsättningar för investeringar i avancerad teknik som annars skulle kunna anses för dyra eller experimentella. Inom organisationer ser man att ledningens engagemang korrelerar med högre teknikadoption, vilket även bör vara fallet på nationell nivå, vilket skapar momentum. Nu måste detta omsättas från strategi till praktisk teknikadoption.

Sveriges teknikintensiva näringsliv samt samverkan mellan akademi och industri skapar ett starkt innovativt svenskt teknologiskt försprång.

Otillfredsställande omständigheter för teknikutveckling och integrering

Gap mellan tillgänglig teknik och faktisk implementation

Analysen visar ett gap i Sveriges arbete med avancerad teknik för cybersäkerhet: tekniken finns tillgänglig, regleringen är på plats, och resurser allokeras – men implementeringen släpar efter hotbilden. Den eskalerade hotbilden möts inte med motsvarande ökning av teknikadoption. Upprepade högprofilerade incidenter minskar medborgarnas tillit till digitala system och kan bromsa nödvändig digitalisering.

Detta innebär att potentiell och realiserad nytta blir policyproblemets kärna oavsett vilken avancerad teknik som för tillfället visar sig vara mest potent som riskhanteringsåtgärd. Inom lagstiftningsområdet såsom CSL/NIS2, AI-förordningen, PQC-migrering och CRA ställer krav som förutsätter avancerad teknik, men verktygen och processerna för att uppfylla kraven saknas ofta.

Generellt finns ett antal förutsättningar som påverkar inom policyområdet. Nationell standardisering av tekniska lösningar saknas och organisationer väljer egna implementationslösningar, vilket försvårar interoperabilitet och kunskapsdelning. Äldre system är inte designade för integration med avancerad teknik och migrering kräver ofta fullständig ombyggnation. Därtill saknas ofta både budget och specialistkompetens samt strategisk ledningsförmåga för långsiktiga åtaganden för kontinuerlig drift, modellträning och integration med befintliga system.

Värdering av centrala tekniker

AI/ML/LLM som riskhanteringsverktyg

AI/ML/LLM representerar ett paradigmskifte för cybersäkerheten.

ML-algoritmer kan analysera terabyte av nätverkstrafik i realtid och identifiera avvikelser som skulle ta människor veckor. LLM:er kan sammanfatta tusentals incidentrapporter på sekunder och ge kontextualiserade rekommendationer för åtgärder. Detta möjliggör proaktiv riskhantering snarare än reaktiv incidentrespons.

MSB:s årsrapport 2024 visar att hälften av incidenter orsakas av mänskliga misstag vid uppdateringar och konfigurationer. Detta trots att AI/ML-baserad automation för konfigurationshantering, prediktiv sårbarhetsanalys och automatiserad incidentrespons finns tillgänglig. Trots den akuta hotbilden arbetar de flesta organisationer fortfarande manuellt och spenderar resurser på att "släcka bränder", vilket är ineffektivt när hotaktörer använder AI-förstärkta automatiserade angrepp.

Många organisationer använder molnbaserade AI/ML-verktyg utan adekvat datastyrning. Forskning visar att små mängder manipulerad träningsdata kan ha oproportionell påverkan ("dataförgiftning"), men rigorösa kontroller av datakällor och modellövervakning saknas ofta. AI/ML-system riskerar att generera falskt positiva/negativa larm eller manipuleras av hotaktörer.

Kvantteknik

Utveckling av kvantteknik och kraftfulla kvantdatorer gör vissa kryptografiska algoritmer alltmer sårbara. Genom cyberangrepp och avlyssning kan kvalificerade hotaktörer lagra krypterade data i syfte att forcera dem när kvanttekniken utvecklats – den så kallade "harvest now, decrypt later"-strategin. Organisationer har goda förutsättningar att skydda säkerhetsskyddsklassificerade uppgifter genom godkända kryptografiska system som redan är kvantdatorsäkra. Under 2025 har konkreta insatser gjorts: National Quantum Communication Infrastructure in Sweden (NQCIS)-projektet och det svenska konsortiet (Ericsson, KTH, Chalmers, Linköping, Stockholm) visar att Sverige går från planering till handling genom att arbeta aktivt med implementation.

Med EU:s mål om post-kvantumkryptering senast 2030 har Sverige fem år på sig att migrera kritiska system. Utan accelererad implementation riskerar känslig information som lagras idag att kunna dekrypteras i framtiden.

Blockkedjor för leveranskedjor och identitet

Blockkedjeteknologi adresserar två av de mest kritiska riskområdena i nulägesbilden: leveranskedjor (21% av incidenter) och identitetssäkerhet (Sportadmin, Snowflake). Organisationer saknar transparens i sina leveranskedjor och kan inte verifiera programvaruintegritet automatiserat.

Decentraliserad lagring gör manipulation möjlig att upptäcka identitetsdata minskar risken för massexponering, kryptografiska signaturer verifierar autenticitet, och smarta kontrakt automatiserar säkerhetskontroller. Blockkedje-baserade SBOM skapar oföränderlig historik av programvarukomponenter, vilket möjliggör snabb sårbarhetsanalys. Tekniken kryptografiska signaturer och spårbar proveniance finns tillgängliga men integration pågår endast gradvis.

Zero Trust som fundamental riskhanteringsmodell

Zero Trust ("never trust, always verify") är inte bara en säkerhetsåtgärd utan en fundamental riskhanteringsmodell för en verklighet där perimeterförsvar inte längre fungerar. Incidenter visar att kompromitterade identiteter är en primär attackvektor som kräver kontinuerlig verifiering. Mikrosegmentering begränsar lateral rörelse vid intrång. Kontextbaserad åtkomst med MFA kombinerat med beteendeanalys och riskbedömning stoppar kompromitterade identiteter. Implementeringen är ojämn trots att tekniken är beprövad.

Referenslista

- Anthropic (2024), A small number of samples can poison LLMs of any size
- MSB (2025), MSB-rapport visar: många it-incidenter orsakas fortfarande av systemfel eller misstag
- NCSC (2024), Cybersäkerhet i Sverige 2024
- IMY (2023), Granskning klar av 1177-incident
- EU (2025), Securing Europe's digital future: The EU's strategy for quantum technologies and post-quantum cryptography
- NQCIS (2025), National Quantum Communication Infrastructure in Sweden
- IQT (2025), IQT Nordics 2025 to Spotlight Quantum Technology Applications and Industry Growth
- NIST (2024), FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard
- NIST (2024), FIPS 204: Module-Lattice-Based Digital Signature Standard
- NIST (2024), FIPS 205: Stateless Hash-Based Digital Signature Standard
- CISA (2024), Reported Supply Chain Compromise Affecting XZ Utils (CVE-2024-3094)
- Microsoft (2024), FAQ and guidance for XZ Utils backdoor
- Diesec (2025), An Analysis of Sweden's Cyber Threat Landscape
- Chambers (2025), Cybersecurity 2025 - Sweden: Trends and Developments
- World Economic Forum (2025), Cybersecurity awareness: AI threats and cybercrime in 2025
- Mandiant/Google Cloud (2024), UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion
- The Hacker News (2024), Snowflake Breach Exposes 165 Customers' Data
- CyberScoop (2024), As many as 165 companies potentially exposed in Snowflake-related attacks
- Healthcare Dive (2024), 7 of the biggest healthcare cyberattack and breach stories of 2024
- Mandiant/Google Cloud (2023), 3CX Software Supply Chain Compromise
- CISA (2023), Supply Chain Attack Against 3CXDesktopApp
- NETSCOUT (2024), Sweden Continues to be a Prime DDoS Target as They Join NATO
- Infosecurity Magazine (2024), Hackers Target New NATO Member Sweden with Surge of DDoS Attacks
- Cybernews (2023), Denmark hit with largest cyberattack on record
- The Hacker News (2023), Russian Hackers Linked to Largest Ever Cyber Attack on Danish Critical Infrastructure