Arkitekturgillet

30.3.2026

Digital säkerhet

Innehåll

Arkitekturgillet

30.3.2026

Vad är digital säkerhet

Syftet med **digital säkerhet**, eller digisäkerhet, är att säkerställa att den digitala verksamhetsmiljön är tillförlitlig, säker och tillgänglig. Detta förutsätter att olika aktörer kan förbereda sig på hot mot den digitala verksamhetsmiljön, att de tål störningssituationer och kan återhämta sig från dem så bra och snabbt som möjligt. Även tryggandet av vardagliga funktioner kräver omfattande samarbete, delade verksamhetsmodeller och en vilja att utveckla dem.

Områdena för genomförande av digital säkerhet sträcker sig också utanför den digitala världen. Digital säkerhet är alltså inte en helhet som är separat från organisationens eller samhällets övriga funktioner, men en väsentlig del av all verksamhet.

Den digitala säkerheten inom den offentliga förvaltningen har fem tyngdpunkter som är gemensamma för alla aktörer och nödvändiga för att producera kontrollerad digital säkerhet. Dessa tyngdpunkter är ledning och riskhantering, kontinuitetshantering, datasäkerhet, dataskydd och cybersäkerhet.[1]

Bild 1 Digital säkerhet

[1] Vad är digital säkerhet? | Myndigheten för digitalisering och befolkningsdata (dvv.fi)

1.1 Arkitekturen för digital säkerhet

Arkitekturen för digital säkerhet är i första hand ett verktyg som underlättar planeringsarbetet och med vilket den digitala säkerheten kan utvecklas och struktureras. Arkitekturen skapar en uppfattning om organisationens egendom och verksamhetsmiljö som ska skyddas samt de hot och risker som de utsätts för. Den inkluderar dessutom en förståelse för de krav och strategiska riktlinjer som påverkar organisationen, samt de byggstenar för digital säkerhet som genomför dessa.

Med arkitekturen för digital säkerhet strävar man alltså efter att planera och gestalta den digitala säkerheten, som är en omfattande helhet i ständig förändring, genom att fästa särskild uppmärksamhet vid hur den föränderliga miljön och de krav den ställer påverkar de val och lösningar som gjorts för den digitala säkerheten.

Med arkitekturen för digital säkerhet strävar man efter att uppnå bland annat följande mål:

- Förståelse för behoven av organisationens verksamhet och fastställande av mål för den digitala säkerhetens verksamhetssätt och tekniska lösningar med hjälp av dem.
- Upprättande av en beskrivning av den digitala säkerhetens strukturer som en del av organisationens övergripande arkitektur.
- Anpassning av lösningar för den digitala säkerheten till organisationens övriga verksamhet, till exempel genom att beakta dem i organisationens övergripande arkitektur.
- Fastställande av ett målläge för den digitala säkerheten som man vill nå genom målmedveten utveckling.

Ramverket som sådant är alltså inte en uppsättning kriterier eller en katalog över säkerhetskontroller, utan den innehåller konkreta åtgärder och exempel på hur den digitala säkerheten kan förbättras.

För vem?

Ramverket är avsett för alla aktörer inom den offentliga förvaltningen som verktyg för att planera och gestalta den digitala säkerheten som helhet.

Ramverket tar inte ställning till med vilka metoder eller med vilka verktyg den digitala säkerheten borde beskrivas eller dokumenteras i organisationen, eftersom en metod som fungerar i en organisation kanske inte nödvändigtvis fungerar alls i en annan. Organisationen bör utnyttja ramverket på det sätt den anser vara ändamålsenligt. Att göra visuella och strukturella beskrivningar gör det dock betydligt lättare att gestalta omfattande helheter.

2 Ramverk

Ramverket för arkitekturen för digital säkerhet grundar sig på det internationellt vida kända Cybersecurity Framework som utarbetats av det amerikanska National Institute of Standards and Technology (NIST). Ramverket sammanställer praxis från flera olika standarder

och består av sex nyckelfunktioner: hantera, identifiera, skydda, upptäcka, svara och återhämta.

Ramverket gör det möjligt att systematiskt planera och dokumentera kraven och principerna för digital säkerhet och de förmågor som betjänar dessa i enlighet med organisationens mål. Ramverkets nyckelfunktioner och målen för dem beskrivs kort i detta dokument. Själva åtgärderna är indelade i kategorier under de sex funktionerna, som tillsammans bildar ramverkets struktur.

Cybersecurity Framework

Ramverket för arkitekturen för digital säkerhet grundar sig på det internationellt vida kända *Cybersecurity Framework* som utarbetats av amerikanska *National Institute of Standards and Technology (NIST)*. Ramverket samlar praxis från flera olika standarder och består av sex nyckelfunktioner: **hantera, identifiera**, **skydda**, **upptäcka**, **svara** och **återhämta**. I ramverket är funktionerna indelade i flera underkategorier som vidare delas in i mer detaljerade åtgärder och de **förmågor** som dessa bildar.

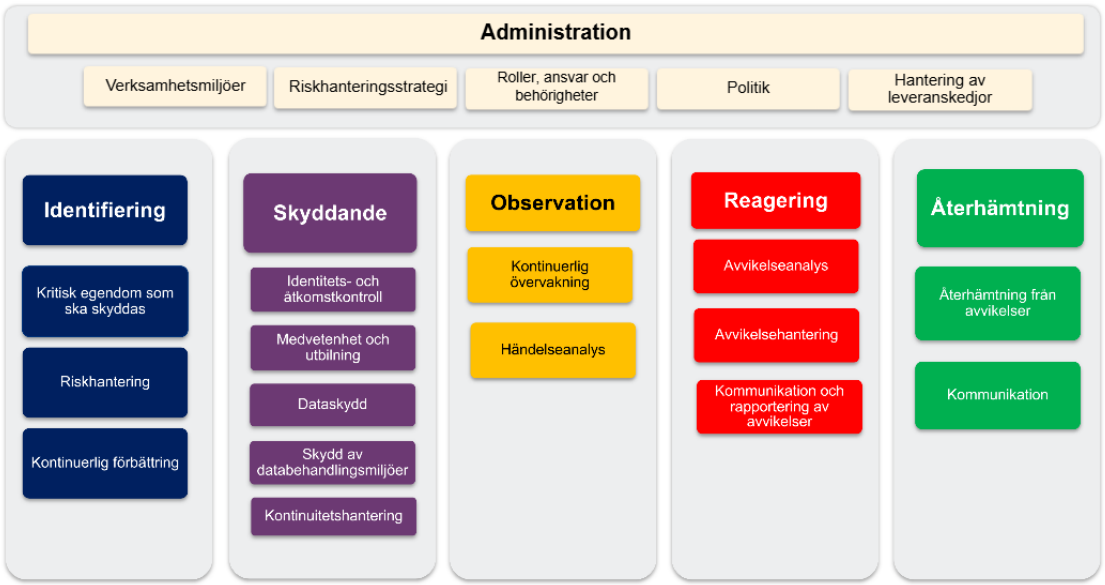
Bild 2 Cybersecurity Framework | NIST

The NIST Cybersecurity Framework (CSF) 2.0

Presentation av ramverket

Utarbetandet av arkitekturen för digital säkerhet inleds genom identifiering av faktorer i den egna verksamhetsmiljön, såsom digitala objekt som ska skyddas, infrastruktur, författningar och andra krav. När faktorer och krav i anslutning till digital säkerhet har identifierats kan denna information användas som hjälp för att planera de lösningar som används för skydd och observation. Syftet med de huvudsakliga faserna i anvisningarna är dessutom att hjälpa till att bygga omfattande strukturer för att reagera i undantagssituationer, återhämta sig från dessa situationer samt utnyttja insamlade lärdomar och erfarenheter i den fortsatta utvecklingen.

Bild 3 Ramverket för arkitekturen för digital säkerhet



2.1 Hantera – Hur vi hanterar digital säkerhet

Målet för administration är att organisationen har administrativa strukturer och processer för hantering av den digitala säkerheten.

Slutresultatet är att följande aspekter som gäller organisationens digitala säkerhet är i linje med organisationens verksamhet och att de utvecklas regelmässigt.

- Strategier
- Praktiker
- Processer
- Resurser

På så sätt styrs organisationen kring vad den ska göra för att uppnå och prioritera målen för och förväntningarna på ramverkets övriga fem nyckelfunktioner. Ledningsfunktionerna är centrala för att inkludera cybersäkerheten och den digitala säkerheten i organisationens övergripande riskhanteringsstrategi.

I hanteringen ingår att förstå organisationens verksamhet; fastställa cybersäkerhetsstrategin och riskhanteringen i leveranskedjan, fastställa roller, ansvar och behörigheter, policyskapande samt hantering av leveranskedjor.

Det väsentliga är att man fastställer, kommunicerar och följer upp organisationens riskhanteringsstrategi, förväntningar och policy för cybersäkerheten och den digitala säkerheten.

2.2 Identifiera – Vad vi har som måste skyddas

Målet med identifieringsfasen är att organisationen har identifierat sin egen verksamhetsmiljö samt kritiska objekt och tillgångar i anslutning till verksamhetens kontinuitet som möjliggör verksamheten och som ska skyddas. Dessutom har organisationen identifierat hot och risker som riktar sig till dessa samt deras eventuella inverkan på verksamheten.

Identifiering av den egna verksamhetsmiljön och de objekt som ska skyddas är det första steget för att skapa en arkitektur för digital säkerhet. Åtgärder såsom att skydda objekt eller observera avvikelser kan göras endast om man känner den egna miljön tillräckligt väl.

Slutresultatet av identifieringen är en beskrivning av den egna organisationens digitala miljö, såsom

- System, datalager, anordningar och den information de innehåller
- Verksamhetsmiljön och de faktorer som styr verksamheten, såsom lagstiftningen
- Modellen för hantering av digital säkerhet, såsom praxis och planer
- Hot, risker och metoder för att hantera dem i den digitala miljön

Det är väsentligt för arkitekturen för digital säkerhet att man i synnerhet i identifieringsskedet kan definiera de objekt som kräver särskilda skydds-, observations-, reaktions- eller återhämtningsåtgärder.

2.3 Skydda – Hur vi skyddar oss mot hot

I skyddsfasen är målet att organisationen skyddar identifierade objekt, såsom datasystem, datalager och uppgifter, mot de hot och risker som identifierats med hjälp av riskhanteringen. I praktiken innebär detta bland annat planering och genomförande av identitets- och åtkomstkontroll, säkerhet i datanät, informationssäkerhet och informationssäkerhetsteknologi i förhållande till identifierade risker samt dokumentering och beskrivning av dessa åtgärder.

Med tanke på skyddsåtgärderna är det viktigt att beakta olika krav och informationssäkerhetslösningar i alla skeden av livscykeln för informationssystem, tjänster och infrastruktur som stöder dessa, från utveckling till underhåll och beslut.

Eftersom datasäkerhets- och dataskyddskraven för de objekt som ska skyddas varierar enligt den information som behandlas, och enligt verksamhetsmiljön, är det särskilt viktigt att identifiera kraven på den egna organisationens verksamhet och information i punkten identifiering i ramverket.

De skyddsåtgärder som presenteras i ramverket är åtgärder som härletts från internationella standarder för informationssäkerhet, cybersäkerhet och digital säkerhet och som gör det möjligt för organisationen att bygga upp sina skyddsåtgärder som en helhet, i stället för som separata lösningar.

2.4 Upptäcka – Hur vi upptäcker avvikelser

Målet med observationsfasen är att organisationen utvecklar förmågan att observera störningar som påverkar den digitala säkerheten. I praktiken innebär detta att processen för avvikelsehantering definieras och genomförs så att organisationen har fastställt basnivån för den digitala säkerheten och tagit i bruk en process och metoder för att upptäcka händelser som påverkar den digitala säkerheten, och kan förbättra observationsförmågan.

Det är viktigt att observera att det med tanke på den digitala säkerheten inte räcker med att enbart skydda sig mot identifierade risker och hot. Utöver det behövs en uppfattning om vad som är normal verksamhet och vad som är verksamhet som avviker från det normala i digitala miljöer. Observationen av avvikande verksamhet kan genomföras effektivt om man är tillräckligt förtrogen med de objekt som skyddas och deras användningsändamål och verksamhetsmiljö.

Det finns flera olika tekniska lösningar för att genomföra observation, men det räcker inte med att endast förlita sig på tekniska lösningar, utan det måste finnas processer och verksamhetsmodeller för att hantera och korrigera avvikelserna.

Även användarnas anmälningar fungerar som stöd för observation av den digitala säkerheten. Därför är det viktigt att organisationen har en verksamhetsmodell för rapportering och mottagning av anmälningar.

Följande punkter handleder i hur man på ett systematiskt sätt kan bygga upp observationsförmågan så att verksamhetsmodellerna och de valda tekniska lösningarna stöder varandra så bra som möjligt.

2.5 Svara – Hur vi hanterar avvikelser

Målet med responsfasen är att organisationen ska ha förmåga att reagera på observerade avvikelser i den digitala säkerheten så snabbt som möjligt i enlighet med processen för avvikelsehantering. I praktiken innebär detta att processen för avvikelsehantering genomförs så att personalen och intressentgrupperna känner till sin uppgift och roll i reaktionsåtgärderna, så att praxis för kommunikation, samordning och rapportering har definierats och att störningar i den digitala säkerheten hanteras och inverkan av dem lindras.

Responsen på avvikelser i den digitala säkerheten sker oftast antingen på grund av avvikelser som observerats med tekniska medel eller som meddelats av användarna.

Med tanke på responsen är det viktigt att man redan på förhand har tänkt på avvikande situationer och att planerna för kommunikation, återhämtning och kontinuitet är uppdaterade och att nödvändiga personer känner till dem.

Analys av situationen och att utreda orsakerna till avvikelsen samt att vidta nödvändiga reparationsåtgärder är en del av responsen på avvikande situationer.

Det rekommenderas att man regelbundet övar på att svara på avvikande situationer, antingen genom att ordna interna och riktade övningar eller genom att delta i en övning som ordnas av en utomstående aktör.

2.6 Återhämta – Hur vi kan fortsätta verksamheten

Målet med återhämtningsfasen är att organisationen ska ha förmåga att återhämta sig från störningar orsakade av den digitala säkerheten och återgå till det normala verksamhetsläget. I praktiken innebär detta att man skapar och utvecklar återhämtningsplaner för kritiska system som ska skyddas. Detta görs utifrån erfarenheter av återhämtning efter störningssituationer, och dessutom gör man upp planer för att korrigera eventuella olägenheter för anseendet som störningen i den digitala säkerheten orsakar.

Åtgärderna för funktionell återhämtning fungerar dessutom som input för kontinuerlig förbättring, dvs. **identifiering** av nya krav, behov och förmågor (fas 1).

3 Utvärdering av den digitala säkerheten

3.1 Metoder för informationssäkerhetsauditering

Detta dokument sammanställer de vanligaste referensramarna och metoderna för informationssäkerhetsauditering samt ger praktiska anvisningar om valet av en lämplig kombination för att säkerställa den administrativa och tekniska informationssäkerheten. Betoningen ligger på auditeringspraxis: vad som egentligen granskas, med vilka bevis och med vilka verktyg.

Vad innebär informationssäkerhetsauditeringen i praktiken

Auditering kan innebära mycket olika saker. I praktiken delas den in på tre frågor:

1) Är det lednings- och styrsystem som krävs på plats? (administrativ informationssäkerhet)

2) Förverkligas kontrollerna i vardagen och är de mätbara? (operativ verksamhet)

3) Är det tekniska genomförandet och konfigurationen i linje med kraven? (teknisk datasäkerhet)

En bra auditering kombinerar både administrativ och teknisk informationssäkerhet (bl.a. konfigurationer, loggar, testresultat, sårbarheter, kodkontroller).

Administrativ vs. teknisk informationssäkerhet

Administrativ informationssäkerhet avser:

- Ledning, olika politikområden, ansvarsområden, riskhantering, hantering av avvikelser, kontinuitet, leverantörshantering, roller, anvisningar, protokoll, leverantörsavtal, kontinuitetsplaner, auditeringsrapporter

Teknisk informationssäkerhet innebär:

- Konfigurationer, hantering av sårbarheter, identitetshantering, nätverkslösning och -segmentering, loggning, tillräcklig härdning, applikationssäkerhet, säkringar, sårbarhetsskanningar, penetrationstestningsrapporter

3.2 Ramverk och standarder – för vad lämpar de sig

Nedan beskrivs de viktigaste auditeringsmetoderna och i vilken roll de i allmänhet används. Det bästa slutresultatet uppstår nästan alltid genom att kombinera ledningssystemet (t.ex. ISO 27001) och den tekniska kontrollkatalogen (t.ex. CIS Controls) samt kravlistan för applikationssäkerhet (OWASP ASVS).

ISO 27001

ISO 27001 är ett ledningssystem som kräver processer för riskbaserad hantering av informationssäkerhet. Lämpar sig utmärkt för extern certifiering och visar att informationssäkerheten leds kontrollerat och när organisationen vill ha en systematisk hanteringsmodell (roller, risker, förbättring) och/eller certifiering.

ISO/IEC 27002 är en bilaga till standarden ISO 27001 och med hjälp av den kan man kontrollera att informationssäkerhetskontrollerna (organisatoriska, personal, fysiska, teknologiska) är tillräckliga. Den lämpar sig särskilt som auditeringskriterium.

CIS (Critical Security Controls)

CIS är en prioriterad teknisk kontrollkatalog för praktiskt cyberförsvar (18 kontroller) och den lämpar sig för situationer där man vill försäkra sig om att ”konfigurationen är rätt”. Den innehåller en genomförande- och åtgärdslista för det tekniska grundskyddet och innehåller även konfigurationshärdningsstandarder (operativsystem, molntjänster, databaser, nätverksutrustning).

OWASP ASVS (Application Security Verification Standard)

OWASP ASVS är en krav- och auditeringsstandard för applikationssäkerhet som definierar de säkerhetskrav för applikationer som ska mätas och verifieras enligt hur kritiska de är (nivåerna L1–L3).

Den används i praktiken som en gemensam uppsättning av kriterier för utveckling, testning och auditering, till exempel som upphandlingskrav, underlag för penetrationstestning och som en uppsättning av kriterier för godkännande av DevSecOps.

NIST SP 800-53

NIST SP 800-53 är en omfattande och detaljerad referensram för informationssäkerhets- och dataskyddskontroller som omfattar administrativa, tekniska och operativa kontroller särskilt i fråga om högsäkerhets- och myndighetsmiljöer.

Den används i praktiken för att fastställa säkerhetskraven för systemen, för auditering och kontinuerlig tillsyn, ofta tillsammans med riskklassificeringen och baselinetänkandet.

4 Mer information

Om du vill bekanta dig närmare med ramverket för arkitekturen för digital säkerhet, bekanta dig med både Myndigheten för digitalisering och befolkningsdatas offentliga Confluence-arbetsyta och eOppiva-kursen om arkitekturen för digital säkerhet och utnyttjandet av den i organisationen.

Arbetsyta: Digitaalisen turvallisuuden arkkitehtuuri - Digitaalisen turvallisuuden arkkitehtuurin julkinen dokumentaatio - DVV external Confluence

Du hittar till kursen i eOppiva: Vad är arkitekturen för digital säkerhet?- Den digitala säkerheten i ordning med hjälp av arkitektur (eOppiva.fi) (Digitaalinen turvallisuus järjestykseen arkkitehtuurin avulla)