Myndigheten
för civilt försvar

# Allmänna villkor
## Skanning från CERT-SE på begäran

## Innehållsförteckning



## Versionshantering

| Version | Datum | Vad | Vem (initialer) |
|---|---|---|---|
| 1.0 | 2026-01-22 | Version 1.0 | DE |
| | | | |

## Introduktion

Myndigheten för civilt försvar (MCF) förvaltar och utvecklar tjänsten ”Skanning från CERT-SE på begäran” (Skanning). Genom tjänsten uppfyller myndigheten de krav som ställs i lag om att landets nationella CSIRT ska tillhandahålla en proaktiv skanning på begäran till NIS-entiteter.

Skanning är en tjänst som tillhandahålls till alla svenska verksamheter, både offentliga och privata, oavsett om verksamheten omfattas av bestämmelserna i NIS-regleringen eller inte. Tjänsten möjliggör för verksamheter att skapa en fördjupad förståelse av deras angreppsyta på internet och därigenom ges förutsättningar till proaktiv riskhantering.

Tjänsten är kostnadsfri.

Syftet med detta dokument är att tydliggöra de regler och villkor som gäller för både den organisation som önskar använda tjänsten och de som utför tjänsten.

## Definitioner

**Skanning:** Att med tekniska hjälpmedel undersöka och fastställa nätverks- och informationssystems faktiska beskaffenheter.

**Den beställande organisationen, beställaren:** Den organisation som beställer tjänsten.

**Utförare:** CERT-SE (vid Myndigheten för civilt försvar).

**Kritiska iaktagelser:** Upptäckt av sårbarheter av direkt systemhotande karaktär eller tecken på redan fullföjda intrång i systemet.

**Inkräktande aktiviteter:** Att med olika systemanrop eller genom att sända data till system verifiera misstänkta sårbarheter.

## Syfte och målsättning med Skanning

Skanning ska syfta till att exponering av icke nödvändiga angreppspunkter minimeras samt att nödvändiga angreppspunkter exponeras på ett tillförlitligt sätt, utan kända brister i mjukvara och utan bekräftat osäkra konfigurationer. Det övergripande syftet är att stärka samhällets motståndskraft och minska effekterna av cyberangrepp som riktas mot det svenska samhället. Målsättningen med skanning är att upptäcka säkerhetsmässigt negativa omständigheter så att dessa kan åtgärdas innan en angripare lyckas nyttja desamma.

# Grundläggande villkor

För att Skanning ska kunna genomföras på ett sätt som realiserar dess syfte, dess övergripande syfte samt dess mål behöver utföraren tillåtelse från den beställande organisationen att utföra vissa av de aktiviteter som ingår i tjänsten. Utan denna tillåtelse kan resultatet inte nå en verkshöjd som försvarar resursförbrukningen hos utföraren.

Dessa villkor förklarar vilket godkännande den beställande organisationen ger till utföraren genom att godkänna dessa villkor. Villkoren **ska** godkännas av den beställande organisationen.

## Metodbeskrivning

Den metodik som CERT-SE tillämpar följer en modell som börjar med ett klarläggande av vilka exponeringar som finns för att därefter undersöka om dessa är problematiska ur ett cybersäkerhetsmässigt perspektiv. De efterföljande stegen i metoden utformas av resultat av de föregående stegen enligt nedan. Målet för en proaktiv skanning är alltid enheter som kan nås via allmänt tillgängliga kommunikationsnät (i praktiken innebär det att enheterna är nåbara direkt från internet).

Inledningsvis genomförs anslutningsförsök mot alla i uppdraget specificerade IP-adresser i syfte att klarlägga vilka portar och protokoll som går att ansluta till. Dessa förtecknas som tillgängliga tjänster och portar och utgör mottagarens möjliga angreppspunkter.

Därefter genomförs aktiviteter mot mottagarens möjliga angreppspunkter i syfte att klarlägga om och i så fall vilka tjänster som svarar på dessa. I detta steg genomförs också aktiviteter för att så långt som möjligt fastställa vilken typ av programvara och dess version som svarar utan att utföra inkräktande aktiviteter.

Därefter genomförs kompletterande aktiviteter vid behov mot tjänster där det inte gått att klarlägga vilken typ av programvara och version som svarat i syfte att fastställa vad dessa tjänster är. Dessa aktiviteter kan avvika från hur standardanrop till de berörda typerna av tjänster görs.

Därefter matchas identifierade programvaror, versioner, funktioner och konfigurationer mot kända sårbarheter. Om någon bedöms som potentiellt sårbar förtecknas denna för fortsatt utredning.

Därefter sker noggrant utvalda aktiviteter i syfte att klarlägga om de potentiella sårbarheterna faktiskt utgör sårbarheter. I detta skede vidtas inkräktande aktiviteter som bedömts att de under normala omständigheter inte ska störa systemets funktion. I detta skede testas också vanligt förekommande användarnamn och lösenord mot tjänster som har allmänt tillgängliga autentiseringsmöjligheter (inloggningsmöjligheter). Vidare prövas att skicka förfrågningar som tjänster normalt sett inte ska svara på i syfte att identifiera säkerhetsmässigt tillåtande eller sårbara konfigurationer. Om inkräktande aktiviteter lyckas sker inga vidare inkräktande aktiviteter i systemet. Det betyder exempelvis att det inte kommer förekomma försök att ta sig längre in i miljön eller försök att extrahera information.

Slutligen sammanställs iakttagelser som gjorts under skanningen och sänds till mottagaren.

Under genomförandet av skanning är CERT-SE beredda att omedelbart eskalera kritiska iakttagelser till den av beställaren utpekade motparten.

### Villkor för genomförandet av Skanning

Beställaren ger utföraren tillåtelse att mot deras system genomföra

- Inkräktande aktiviteter om dessa i normalfallet inte kan förväntas störa systemets funktion.
- Inloggningsförsök med kända kombinationer av användarnamn och lösenord.

Tillgång till system som utföraren erhåller genom inkräktande aktiviteter eller lyckade inloggningsförsök får inte nyttjas för:

- vidare inkräktande aktiviteter mot aktuellt eller omkringliggande system
- att extrahra information ur aktuellt eller bakomliggande system

Beställaren utser en kontaktpunkt (person/funktionsbrevlåda/beredskap/etc) i den egna organisationen som utföraren ska kunna nå under genomförandet av Skanning.

Utföraren rapporterar utan onödiga dröjsmål till beställaren om kritiska iaktagelser görs vid genomförandet av Skanning.

Beställaren förbinder sig till att vara aktiverad i CERT-SE:s system för automatiska notifieringar om tekniska sårbarheter (ANTS) under minst ett års tid efter genomförd skanning. Detta säkerställer möjlighet till strukturerad uppföljning och ger ingångsvärden till förbättringar av skanningstjänsten.

Resultatet av skanningen sparas vid CERT-SE under motsvarande tid för att möjliggöra uppföljning. Resultatet av skanningen kan också komma att nyttjas inom CERT-SE för att producera allmänt tillämpliga råd. Innehållet i dessa råd kommer inte gå att koppla till unika händelser eller organisationer.

I och med att resultatet överlämnas till mottagaren upphör utförarens rätt att genomföra inkräktande skanningar mot mottagarens system och skanningsuppdraget är därmed slutfört.

## Avsteg

Avsteg från dessa villkor kan inte göras och samtidigt erhålla tjänsten.

## Finansiering

Skanning från CERT-SE genomförs utan kostnad.

## Behandling av personuppgifter

Då MCF inte ges tillträde till personuppgifter hos uppdragsgivarens kommer personuppgifter inte att behandlas av MCF vid utförande av Skanning.

Insamling och behandling av personuppgifter är nödvändigt för MCF:s administration av beställningar av tjänsten. De uppgifter som kommer att samlas in är namn och andra kontaktuppgifter för kontaktpersoner. MCF är personuppgiftsansvarig för behandlingen och den rättsliga grunden är att uppgiften är nödvändig för ett allmänt intresse. De medarbetare på MCF som kommer att ta del av uppgifterna behöver det för att utföra sina arbetsuppgifter. Informationen kommer inte att delas med någon utomstående. MCF kommer att behandla personuppgifterna i detta syfte så länge som den registrerade är kontaktperson för Skanning.

Som registrerad har du rätt att få en kopia av de personuppgifter som MCF har om dig. Om du anser att något i uppgifterna är felaktigt eller ofullständigt har du rätt att begära att vi rättar eller kompletterar dem. Du kan också begära att vi ska begränsa behandlingen av, eller radera, dina personuppgifter, men detta sker endast om så är möjligt.

Om du anser att MCF behandlat dina uppgifter felaktigt har du rätt att invända mot vår behandling. Vänd dig i första hand till cert@cert.se. Du har också möjlighet att kontakta vårt dataskyddsombud genom att maila dso@mcf.se och/eller att lämna in ett klagomål till Integritetsskyddsmyndigheten.

## Ändring av dessa villkor

MCF har rätten att ändra dessa villkor. Ändringar får dock inte ske i en befintlig beställning, det vill säga mellan det att beställaren godkänt villkoren till det att utföraren sänt resultatet av genomförd verksamhet till beställaren.

## Godkännande av villkor

I och med att beställaren fullföljer sin beställning av tjänsten ”Skanning från CERT-SE på begäran” godkänner beställaren de i detta dokument förtecknade villkoren.