Tio rekommendationer för bättre It-säkerhet

NATIONELLT CYBERSÄKERHETSCENTER

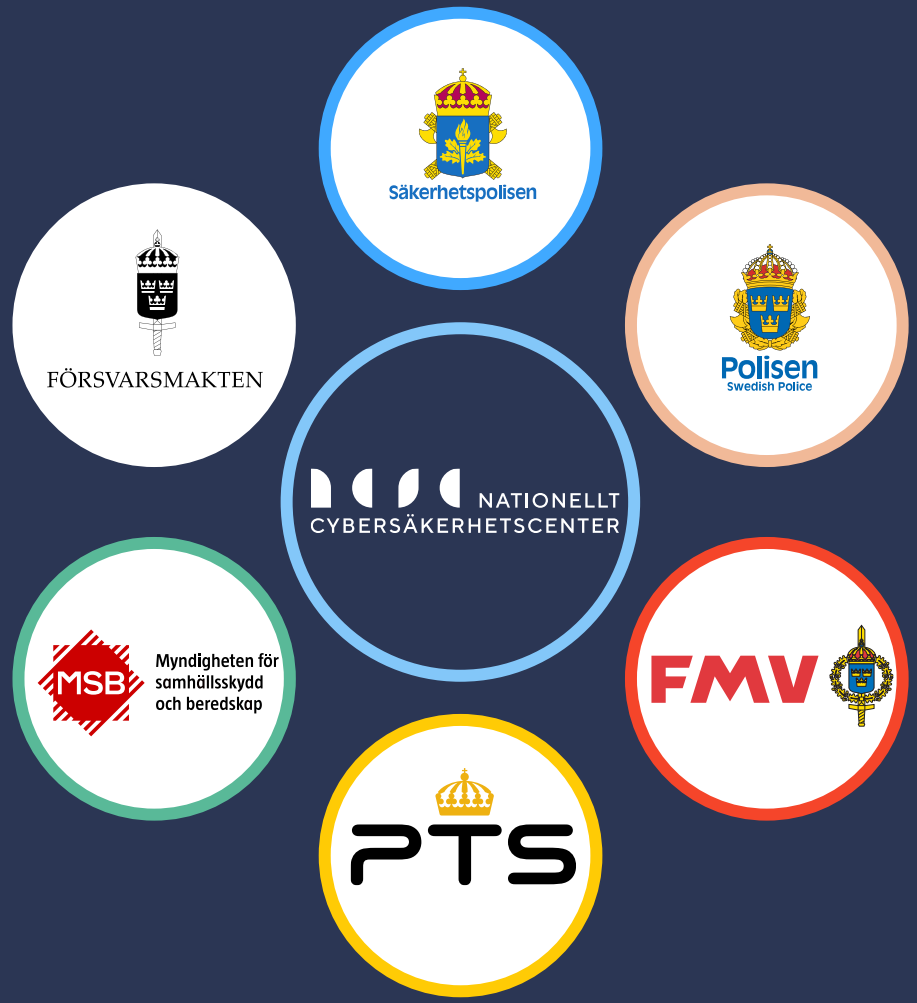
Introduktion NCSC

Nationellt cybersäkerhetscenter (NCSC) ska utvecklas till ett nav för svensk cybersäkerhet och verka för en generell höjning av cybersäkerhet och motståndskraft i samhället.

Det nationella cybersäkerhetscentret

Den nya förordning om det nationella cybersäkerhets-centret vid FRA, anger att NCSC ska:

- Utveckla och stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera antagonistiska cyberhot och andra it-incidenter.
- Vara en mötesplats för samverkan och informationsutbyte mellan privata och offentliga aktörer, och en kontaktpunkt i frågor som rör cybersäkerhet.
- Bidra till att samordna och harmonisera det nationella cybersäkerhetsarbetet.
- Ta fram samlade lägesbilder av antagonistiska cyberhot och andra it-incidenter till privata och offentliga aktörer
- Lämna råd och stöd till privata och offentliga aktörer om cybersäkerhet kopplat till hot, sårbarheter, risker samt vid it-incidenter.
- Genomföra utbildningar, övningar och andra kompetenshöjande insatser inom cybersäkerhetsområdet



NATIONELLT
CYBERSÄKERHETSCENTER

1 Säkerställ förmågan att upptäcka säkerhetshändelser

Varför det är viktigt: Bristande övervakning möjliggör oupptäckta intrång och långvariga attacker. Incidenter upptäcks ofta först när skadan redan är skedd.

Vad som krävs: En kombination av manuella, automatiserade och tekniska metoder – i en säker och central logghanteringslösning.

Rekommendationer:

- Logga händelser som inloggningar, behörighetsändringar och åtkomst till känslig data.
- Använd en fristående logghanteringstjänst med synkroniserad tid och rätt skydd.
- Etablera en SOC (internt eller externt) med god förståelse för verksamhetens system och användning.

Tips: Övervakning handlar inte bara om loggar – nätverkstrafik, beteendeanalys och incidentrapporter är lika viktiga.

2 Installera säkerhetsuppdateringar skyndsamt

Varför är det viktigt: Angripare letar aktivt efter kända sårbarheter – sårbarheter kan utnyttjas bara timmar efter att en uppdatering har släppts.

Vad som krävs: Inventera alla system som kräver säkerhetsuppdateringar. Etablera rutiner för att snabbt upptäcka, verifiera och installera uppdateringar. Använd automatiserade lösningar där det är möjligt.

Rekommendationer

- Prioritera system som är internetexponerade eller verksamhetskritiska.
- Använd CVSS-skalan och hotinformation för att prioritera kritiska uppdateringar.
- Kombinera tekniska verktyg som sårbarhetsskanning med manuell omvärldsbevakning.

Tips: Håll dig uppdaterad om relevanta sårbarheter och tillgängliga patchar. Även "vanliga" uppdateringar kan innehålla viktiga förbättringar – installera dem också.

3 Förvalta behörigheter och använd stark autentisering

Varför det är viktigt: Angripare utnyttjar ofta gamla, dåligt skyddade eller övergivna konton för att ta sig in i it-miljöer. Svaga lösenord, återanvända inloggningar och brist på spårbarhet är vanliga svagheter.

Vad som krävs: För att minska risken krävs full kontroll över alla konton, minimal behörighet, och stark autentisering – helst flerfaktor.

Rekommendationer

- Använd unika konton för alla användare och tjänster
- Alla användare bör använda flerfaktorsautentisering eller smartkort
- Administrativa konton ska skyddas med stark autentisering, som hårdvarunyckel, certifikat eller smartkort
- Separera test- och produktionsmiljöer
- Använd lösenordshanterare där flerfaktor inte är möjligt

4 Begränsa och skydda användningen av höga behörigheter

Varför det är viktigt: Konton med höga behörigheter utgör en stor säkerhetsrisk – särskilt om de används brett, delas mellan användare eller saknar spårbarhet.

Vad som krävs: Ett komprometterat administratörskonto kan ge angripare full åtkomst till känsliga system. Därför krävs strikt segmentering, minimal tilldelning och flerfaktorsautentisering.

Rekommendationer

- Använd separata konton för olika administrativa uppgifter
- Minimera och dokumentera alla höga behörigheter
- Använd alltid flerfaktorsautentisering
- Begränsa administrativ åtkomst till särskilda arbetsstationer

Tips: Kontrollera alltid om höga rättigheter verkligen krävs

5 Inaktivera oanvända tjänster och protokoll

Varför det är viktigt: Alla aktiva tjänster och protokoll i ett system ökar angreppsytan – särskilt om de är gamla, onödiga eller bakåtkompatibla.

Vad som krävs: Härdning handlar om att inaktivera eller ta bort det som inte behövs. Det gäller alla delar i it-miljön – från klienter till servrar och molntjänster.

Rekommendationer

- Inaktivera alla tjänster, protokoll och funktioner som inte behövs
- Följ leverantörers härdningsguider och dokumentera ändringar
- Säkra att härdning kvarstår efter uppdateringar
- Kontrollera även äldre system – avveckla stöd för sårbara protokoll som SMBv1

Tips: Glöm inte att härda även skrivare, IP-telefoner och nätverksenheter

6 Säkerhetskopiera och testa återställning av information

Varför det är viktigt: Utan fungerande säkerhetskopior riskerar organisationer total informationsförlust vid angrepp, fel eller misstag.

Vad som krävs: Kopior räcker inte – återställning måste fungera i praktiken. Därför krävs både tekniska skydd och regelbundna tester.

Rekommendationer

- Säkerhetskopiera dagligen ny/ändrad informationmen även konfigurationer, konton och certifikat
- Skydda kopior mot obehörig åtkomst, brand och skadlig kod
- Lagra säkerhetskopior offline eller isolerat från nätverk
- Testa återställning minst årligen – både delvis och fullständigt

Tips: Dokumentera återställningsplaner och tydliggör vem som ansvarar för vad. Se också till att förstå beroenden mellan system, så att återstarten sker i rätt ordning och med minimal störning.

7 Segmentera och kontrollera åtkomst i nätverket

Varför det är viktigt: Utan nätverkssegmentering och åtkomstkontroll kan angripare röra sig fritt och sprida skadlig kod.

Vad som krävs: Genom att dela upp nätet och styra vilken utrustning som får anslutas, minskar risken för incidenter – även inifrån.

Rekommendationer

- Segmentera efter funktion och känslighet – separera utveckling från produktion
- Begränsa och övervaka trafik mellan segment med brandväggar och switchar
- Aktivera lokala brandväggar och tillåt endast nödvändig trafik
- Skydda nätverksutrustning fysiskt och logga åtkomst
- Tillåt bara godkänd och identifierad utrustning
- Behandla otillåten utrustning som ett intrång – isolera privata enheter

Tips: Dokumentera och uppdatera trafikflöden och brandväggsregler, även för betrodda externa parter.

8 Säkerställ att endast godkänd mjukvara får köras – vitlistning

Varför det är viktigt: Otillåten mjukvara är en vanlig spridningsväg för skadlig kod och kan orsaka dataläckor, driftstopp och attacker.

Vad som krävs: Genom att vitlista mjukvara tillåts endast godkända program köras, vilket kraftigt begränsar angriparens möjligheter.

Rekommendationer

- Inför vitlistning på klienter och servrar
- Förhindra att användare installerar program själva
- Använd signaturkrav och moderna operativsystem
- Starta med inlärningsläge, aktivera skarpt läge när klart
- Övervaka även godkänd mjukvaras beteende
- Svartlistning räcker inte – kombinera med vitlistning

Tips: Skadlig kod kan gömma sig i oväntade filformat. Se till att säkerhetsregler täcker fler än bara vanliga körbara filer. Begränsa makrokörning till betrodda källor och miljöer.

9 Uppgradera mjuk- och hårdvara

Varför det är viktigt: Föråldrad mjuk- och hårdvara saknar ofta säkerhetsuppdateringar och support, vilket gör systemen sårbara. Angripare utnyttjar gamla produkter för att få fotfäste i nätverk.

Vad som krävs: Upprätta en plan för livscykelhantering där du regelbundet byter ut eller uppgraderar mjuk- och hårdvara innan support upphör.

Rekommendationer:

- Planera för utbyte av it-utrustning i god tid
- Aktivera inbyggda säkerhetsfunktioner efter uppgradering
- Härda systemen direkt vid införande
- Undvik produkter som inte kan uppdateras
- Isolera gammal utrustning i separata nätverkssegment

Tips: Begränsa användningen av enklare enheter som saknar uppgraderingsmöjligheter.

10 Kontrollera internetåtkomst

Varför det är viktigt: Direkt internetåtkomst gör det möjligt för angripare att fjärrstyra system och föra ut data utan att upptäckas. Utan tydliga kontroller och loggning kan skadlig trafik passera obemärkt, vilket ökar risken för intrång.

Vad som krävs: All internettrafik ska gå via kontrollerade och övervakade kanaler, aldrig direkt ut från interna system.

Rekommendationer:

- Använd en dedikerad, härdad webbläsare med godkända tillägg och håll säkerhetsinställningarna uppdaterade.
- Implementera lokala brandväggsregler för att säkerställa att endast den härdade webbläsaren har tillgång till internet via en webbproxy
- Analysera proxyloggar kontinuerligt för att upptäcka misstänkt aktivitet

Tips: Glöm inte att utbilda användare i säker internetanvändning

Varför det är viktigt: Bristande övervakning möjliggör oupptäckta intrång och långvariga attacker. Incidenter upptäcks ofta först när skadan redan är skedd.

Vad som krävs: En kombination av manuella, automatiserade och tekniska metoder – i en säker och central logghanteringslösning.

Rekommendationer:

- Logga händelser som inloggningar, behörighetsändringar och åtkomst till känslig data.
- Använd en fristående logghanteringstjänst med synkroniserad tid och rätt skydd.
- Etablera en SOC (internt eller externt) med god förståelse för verksamhetens system och användning.

Tips: Övervakning handlar inte bara om loggar – nätverkstrafik, beteendeanalys och incidentrapporter är lika viktiga.

1

Säkerställ förmågan att upptäcka säkerhetshändelser

2

Installera säkerhetsuppdateringar skyndsamt

Varför är det viktigt: Angripare letar aktivt efter kända sårbarheter – sårbarheter kan utnyttjas bara timmar efter att en uppdatering har släppts.

Vad som krävs: Inventera alla system som kräver säkerhetsuppdateringar. Etablera rutiner för att snabbt upptäcka, verifiera och installera uppdateringar. Använd automatiserade lösningar där det är möjligt.

Rekommendationer

- Prioritera system som är internetexponerade eller verksamhetskritiska.
- Använd CVSS-skalan och hotinformation för att prioritera kritiska uppdateringar.
- Kombinera tekniska verktyg som sårbarhetsskanning med manuell omvärldsbevakning.

Tips: Håll dig uppdaterad om relevanta sårbarheter och tillgängliga patchar. Även "vanliga" uppdateringar kan innehålla viktiga förbättringar – installera dem också.

Varför det är viktigt: Angripare utnyttjar ofta gamla, dåligt skyddade eller övergivna konton för att ta sig in i it-miljöer. Svaga lösenord, återanvända inloggningar och brist på spårbarhet är vanliga svagheter.

Vad som krävs: För att minska risken krävs full kontroll över alla konton, minimal behörighet, och stark autentisering – helst flerfaktor.

Rekommendationer

- Använd unika konton för alla användare och tjänster
- Alla användare bör använda flerfaktorsautentisering eller smartkort
- Administrativa konton ska skyddas med stark autentisering, som hårdvarunyckel, certifikat eller smartkort
- Separera test- och produktionsmiljöer
- Använd lösenordshanterare där flerfaktor inte är möjligt

3

Förvalta behörigheter och använd stark autentisering

4

Begränsa och skydda användningen av höga behörigheter

Varför det är viktigt: Konton med höga behörigheter utgör en stor säkerhetsrisk – särskilt om de används brett, delas mellan användare eller saknar spårbarhet.

Vad som krävs: Ett kompromitterat administratörskonto kan ge angripare full åtkomst till känsliga system. Därför krävs strikt segmentering, minimal tilldelning och flerfaktorsautentisering.

Rekommendationer

- Använd separata konton för olika administrativa uppgifter
- Minimera och dokumentera alla höga behörigheter
- Använd alltid flerfaktorsautentisering
- Begränsa administrativ åtkomst till särskilda arbetsstationer

Tips: Kontrollera alltid om höga rättigheter verkligen krävs

Varför det är viktigt: Alla aktiva tjänster och protokoll i ett system ökar angreppsytan – särskilt om de är gamla, onödiga eller bakåtkompatibla.

Vad som krävs: Härdning handlar om att inaktivera eller ta bort det som inte behövs. Det gäller alla delar i it-miljön – från klienter till servrar och molntjänster.

Rekommendationer

- Inaktivera alla tjänster, protokoll och funktioner som inte behövs
- Följ leverantörers härdningsguider och dokumentera ändringar
- Säkra att härdning kvarstår efter uppdateringar
- Kontrollera även äldre system – avveckla stöd för sårbara protokoll som SMBv1

Tips: Glöm inte att härda även skrivare, IP-telefoner och nätverksenheter

5

Inaktivera oanvända tjänster och protokoll

6

Säkerhetskopiera och testa återställning av information

Varför det är viktigt: Utan fungerande säkerhetskopior riskerar organisationer total informationsförlust vid angrepp, fel eller misstag.

Vad som krävs: Kopior räcker inte – återställning måste fungera i praktiken. Därför krävs både tekniska skydd och regelbundna tester.

Rekommendationer

- Säkerhetskopiera dagligen ny/ändrad informationmen även konfigurationer, konton och certifikat
- Skydda kopior mot obehörig åtkomst, brand och skadlig kod
- Lagra säkerhetskopior offline eller isolerat från nätverk
- Testa återställning minst årligen – både delvis och fullständigt

Tips: Dokumentera återställningsplaner och tydliggör vem som ansvarar för vad. Se också till att förstå beroenden mellan system, så att återstarten sker i rätt ordning och med minimal störning.

7

Segmentera och kontrollera åtkomst i nätverket

Varför det är viktigt: Utan nätverks-segmentering och åtkomstkontroll kan angripare röra sig fritt och sprida skadlig kod.

Vad som krävs: Genom att dela upp nätet och styra vilken utrustning som får anslutas, minskar risken för incidenter – även inifrån.

Rekommendationer

- Segmentera efter funktion och känslighet – separera utveckling från produktion
- Begränsa och övervaka trafik mellan segment med brandväggar och switchar
- Aktivera lokala brandväggar och tillåt endast nödvändig trafik
- Skydda nätverksutrustning fysiskt och logga åtkomst
- Tillåt bara godkänd och identifierad utrustning
- Behandla otillåten utrustning som ett intrång – isolera privata enheter

Tips: Dokumentera och uppdatera trafikflöden och brandväggsregler, även för betrodda externa parter.

8

Säkerställ att endast godkänd mjukvara får köras – vitlistning

Varför det är viktigt: Otillåten mjukvara är en vanlig spridningsväg för skadlig kod och kan orsaka dataläckor, driftstopp och attacker.

Vad som krävs: Genom att vitlista mjukvara tillåts endast godkända program köras, vilket kraftigt begränsar angriparens möjligheter.

Rekommendationer

- Inför vitlistning på klienter och servrar
- Förhindra att användare installerar program själva
- Använd signaturkrav och moderna operativsystem
- Starta med inlärningsläge, aktivera skarpt läge när klart
- Övervaka även godkänd mjukvaras beteende
- Svartlistning räcker inte – kombinera med vitlistning

Tips: Skadlig kod kan gömma sig i oväntade filformat. Se till att säkerhetsregler täcker fler än bara vanliga körbara filer. Begränsa makrokörning till betrodda källor och miljöer.

9

Uppgradera mjuk- och hårdvara

Varför det är viktigt: Föråldrad mjuk- och hårdvara saknar ofta säkerhetsuppdateringar och support, vilket gör systemen sårbara. Angripare utnyttjar gamla produkter för att få fotfäste i nätverk.

Vad som krävs: Upprätta en plan för livscykelhantering där du regelbundet byter ut eller uppgraderar mjuk- och hårdvara innan support upphör.

Rekommendationer:

- Planera för utbyte av it-utrustning i god tid
- Aktivera inbyggda säkerhetsfunktioner efter uppgradering
- Härda systemen direkt vid införande
- Undvik produkter som inte kan uppdateras
- Isolera gammal utrustning i separata nätverkssegment

Tips: Begränsa användningen av enklare enheter som saknar uppgraderingsmöjligheter.

10

Kontrollera internetåtkomst

Varför det är viktigt: Direkt internetåtkomst gör det möjligt för angripare att fjärrstyra system och föra ut data utan att upptäckas. Utan tydliga kontroller och loggning kan skadlig trafik passera obemärkt, vilket ökar risken för intrång.

Vad som krävs: All internettrafik ska gå via kontrollerade och övervakade kanaler, aldrig direkt ut från interna system.

Rekommendationer:

- Använd en dedikerad, härdad webbläsare med godkända tillägg och håll säkerhetsinställningarna uppdaterade.
- Implementera lokala brandväggsregler för att säkerställa att endast den härdade webbläsaren har tillgång till internet via en webbproxy
- Analysera proxyloggar kontinuerligt för att upptäcka misstänkt aktivitet

Tips: Glöm inte att utbilda användare i säker internetanvändning

ncsc@ncsc.se
www.ncsc.se
NCSC-SE

NATIONELLT CYBERSÄKERHETSCENTER