NCSC-SE

Karl Selin

NATIONELLT CYBERSÄKERHETSCENTER

Det nationella cybersäkerhetscentret

Operativ- och strategisk cybersäkerhet

Säkerhetsskydd

Huvudman, cybersäkerhet

Brottsförebyggande och utredning

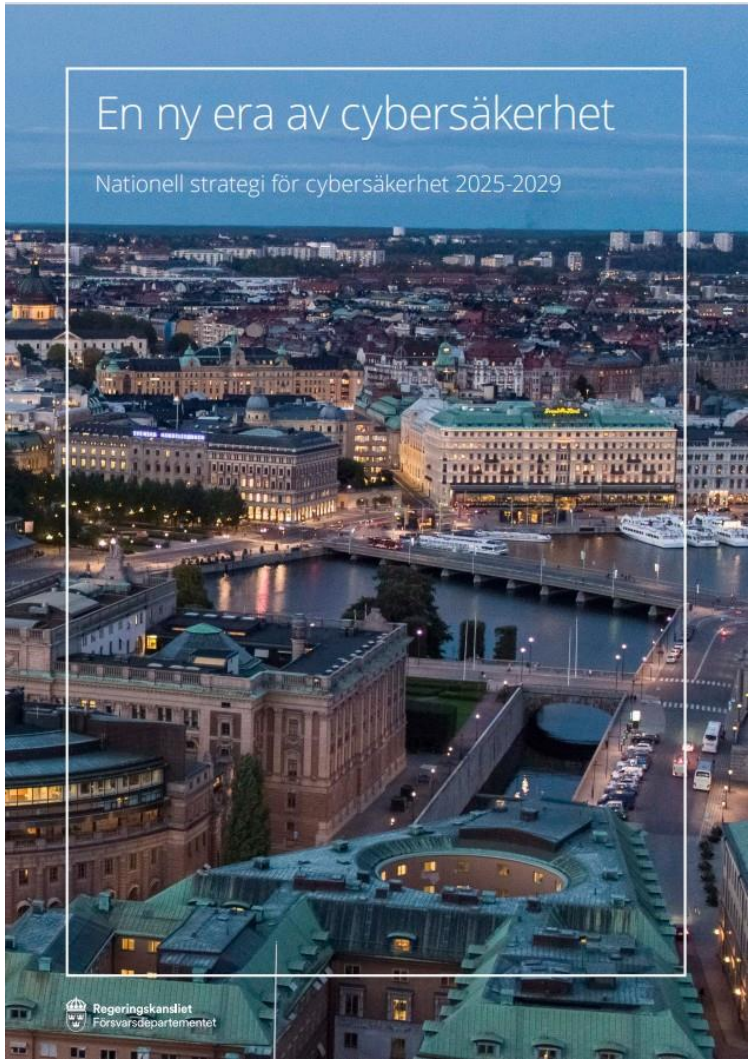
Cybersäkerhetscertifiering

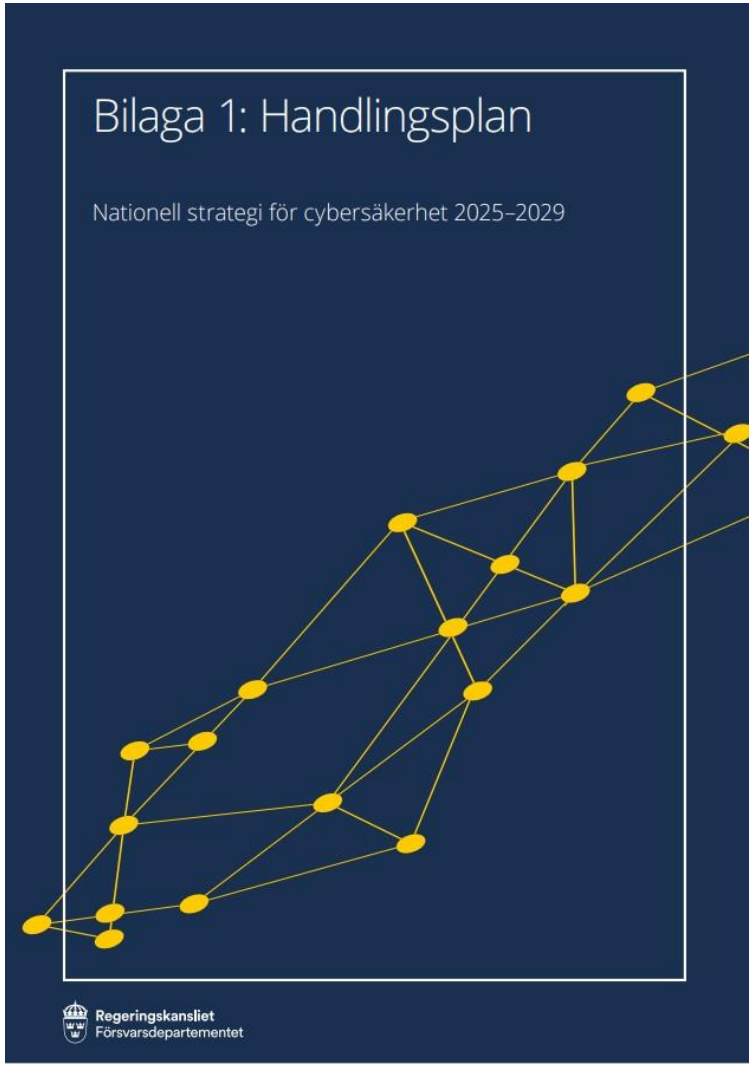
Telekom och internet

Sveriges försvar

NATIONELLT CYBERSÄKERHETSCENTER

Nationell cybersäkerhetsstrategi 2025





NATIONELLT CYBERSÄKERHETSCENTER

Nationell cybersäkerhetsstrategi

Systematiskt och effektivt cybersäkerhetsarbete

Utvecklad kunskap och kompetensutveckling inom cybersäkerhet

Förmåga att förhindra och hantera cybersäkerhets-incidenter

NATIONELLT CYBERSÄKERHETSCENTER

Verksamhet

Lägesbilder

Koordinering

Publikationer

Samverkan

Övning

Konferens

NATIONELLT CYBERSÄKERHETSCENTER

Planen framåt

NATIONELLT CYBERSÄKERHETSCENTER

Vad händer nu?

Fortsatt arbete med nuvarande uppdrag

Verksamheten utvecklas

Kulturresa FRA

Rekrytering

Nya lokaler

Stärkt samverkan

NATIONELLT CYBERSÄKERHETSCENTER

NATIONELLT CYBERSÄKERHETSCENTER

hotAKTÖRER

- Stater
- Kriminella
- Hacktivister
- *Terrorister*
- *Insiders*
- *Inga klara gränser!*

Trender, statsaktörer

- Gör ingen skillnad på militära och civila mål, genomför mycket sofistikerade angrepp
- Mycket uthålliga, kan vänta länge och arbetar mycket metodiskt
- För att skydda sig: Alltid alla rätt, ett fel gör att angreppet kan lyckas

Trender, CYBERKRIMINELLA

- Förfinade ”affärsmodeller” och professionella organisationer
- Enkla mål -> Motivation att betala, alla kan drabbas
- Kryptovalutor en katalysator
- Ransomware & Publicering

Trender, hacktivister

- Försöker påverka stater eller organisationer genom cyberangrepp
- Ofta löst sammansatta utan tydlig ledning
- Exempel: Frivilliga Ukrainska cyberarmén
- Har genomfört sofistikerade angrepp

Exempel, typer av cyberangrepp

- Överbelastningsattacker (DDoS, tillgänglighet)
- Dold kartläggning och informationsinhämtning (CNE)
- Förstörande angrepp (CNA, Wipers mm)
- Öppen informationsinhämtning (OSINT)
- Subversion (Defacement, Hack and leak)
- Utpressningsangrepp (Ransomware)

Publiceringar från NCSC

NATIONELLT CYBERSÄKERHETSCENTER

Cybersäkerhet i Sverige 2024

NATIONELLT CYBERSÄKERHETSCENTER

NCSC-SE:s rekommenderade säkerhetsåtgärder

1
Säkerställ förmågan att upptäcka säkerhetshändelser
För att effektivt kunna upptäcka säkerhetshändelser i it-miljön är det viktigt att skapa en förmåga att identifiera dessa så tidigt som möjligt. Det kan göras genom en kombination av manuella, tekniska och automatiserade metoder.

2
Installera säkerhetsuppdateringar skyndsamt
Se till att prioritera uppdateringar för informationssystem som är exponerade mot internet, är verksamhetskritiska, eller har sårbarheter som riskerar att utnyttjas. Målet bör vara att installera säkerhetsuppdateringar så snart de publiceras.

3
Förvalta behörigheter och använd stark autentisering
Kontrollera alla konton i it-miljön och inaktivera de som inte längre används. Tilldela bara nödvändiga behörigheter.

4
Begränsa och skydda användningen av höga behörigheter
Skyddet av administrativa behörigheter är viktigt för att minska säkerhetsrisker i it-miljön. Genom att införa tydliga rutiner för tilldelning och användning av dessa behörigheter kan organisationer skydda sina system och data.

5
Inaktivera oanvända tjänster och protokoll
För att skydda informationssystem från hot är det viktigt att stänga av funktioner som inte behövs för systemets drift. Genom att använda rätt säkerhetsåtgärder minskar risken för att systemet utsätts för attacker.

6
Säkerhetskopiera och testa återställning av information
Att skapa och testa säkerhetskopior är viktigt för att skydda information och system mot informationsförlust. Genom regelbundna säkerhetskopior kan organisationer snabbt återställa data och minimera störningar vid incidenter.

7
Segmentera och kontrollera åtkomst i nätverket
För att skydda organisationens it-miljö är det avgörande att segmentera nätverket för att begränsa och övervaka trafikflödena mellan olika delar av systemet. Det är också viktigt att säkerställa att endast godkänd utrustning tillåts ansluta.

8
Säkerställ att endast godkänd mjukvara får köras – vitlistning
Endast tillåten mjukvara ska köras i it-miljön. Genom att använda vitlistning kan organisationen skydda sina system och information genom att förhindra att otillåten mjukvara används.

9
Uppgradera mjuk- och hårdvara
Byt ut och ersätt gammal mjuk- och hårdvara för att minska sårbarheter och säkerställa att systemen fungerar som de ska och har tillräcklig säkerhet. För att minska sårbarheter i organisationens it-system bör man använda mjuk- och hårdvara som fortfarande får uppdateringar och support från leverantören.

10
Kontrollera internetåtkomst
För att skydda interna system och data från obehörig kommunikation med omvärlden är säker internetåtkomst avgörande. Genom att införa rätt åtgärder förhindrar man att ett angripet system kan missbrukas för fjärrstyrning eller datastöld.

NATIONELLT CYBERSÄKERHETSCENTER

Tillsammans gör vi cybersverige säkrare!

Frågor?

Statsaktörer

NATIONELLT CYBERSÄKERHETSCENTER