Pressbriefing om läget på cyberområdet

Minister för civilt försvar, Carl-Oskar Bohlin
Chef Nationellt cybersäkerhetscenter (NCSC), John Billow

Stockholm, 10 november 2026

Komplexiteten tilltar i cyberdomänen

Hotbilden skärps

- Ryssland är mer riskbenäget och har försökt genomföra förstörande cyberangrepp mot flera länder inkl. Sverige
- Främmande makt riktar in sig på system som styr el, vatten och värme

AI gör det lättare att angripa

- AI hittar säkerhetshål i ett mycket snabbare tempo än tidigare
- Antalet kända säkerhetshål har nästan fördubblats på ett år

Tiden att agera krymper

- Säkerhetshål utnyttjas inom några dagar efter att de blir kända
- Den som inte uppdaterar riskerar att bli ett lätt byte.

Uppmärksammade incidenter

PHP-sårbarheten, oktober

- Allvarligt säkerhetshål programspråket som en stor del av världens webbplatser bygger på
- Miljontals försök att utnyttja det inom ett dygn

Kylsystem, oktober–november

- Angrepp mot butiker i Frankrike, Sverige och sex andra europeiska länder
- System stod öppna mot internet, med svaga lösenord och kända säkerhetshål

Omfattande reformer på cyberområdet

- Samlat NCSC vid FRA, navet i Sveriges cybersäkerhetsarbete
- Ny nationell cybersäkerhetsstrategi med årlig handlingsplan
- Historiska satsningar: drygt 1 miljard kronor 2026–2028 till bland annat NCSC, kommuner och regioner
- Ny cybersäkerhetslag
- Uppdrag till NCSC att samordna frågor om avancerade AI-modeller
- Uppdrag till FRA och Försvarsmakten att utveckla en AI-stödd cybersäkerhetsförmåga

Lägesbild från NCSC

- Flera tusen sårbara enheter exponerade mot internet, fler än i något annat nordiskt land
- Kylangreppen: främst äldre system från samma tillverkare, med svaga lösenord
- Riktade varningar till berörda verksamheter före angreppen
- Stöd till drabbade via CERT-SE
- Samordning nationellt och i EU:s cyberkrisnätverk

Rekommenderade åtgärder

1. Inventera uppkopplade enheter
2. Begränsa exponeringen mot internet
3. Skydda systemen i flera lager
4. Ha en plan för incidenter och kontinuitet

Tiden att agera är nu

- Grundläggande cyberhygien är ett minimum
- Vet vad er verksamhet ska leverera, och säkerställ att den kan göra det även under störda förhållanden
- **Cybersäkerhet är inte fritt valt arbete**
- **Agera nu och agera uthålligt**