

EU-initiativ i korthet

EU-förslag om skydd av kritiska digitala system

BAKGRUND

- **Allt fler viktiga tjänster i EU bygger på digitala system** – affärstransaktioner, hälso- och sjukvård, säkerhets- och trygghetssystem och andra viktiga samhällstjänster.
- **Systemstörningar** – genom riktade IT-attacker (dataintrång och skräppost), naturkatastrofer eller tekniska fel – kan orsaka stor **skada för ekonomi och samhälle**.
- Framför allt IT-attackerna **ökar och blir allt mer sofistikerade**.
- Otillräckligt skydd för viktiga system kan leda till **förlust av personuppgifter eller annan känslig information** och innebär risk för identitetsstöld och andra bedrägerier.
- Ofta saknas medvetenhet om **riskerna**, eller så har man inte analyserat dem tillräckligt.

VAD KAN EU GÖRA?

Syftet är att få alla aktörer i EU att samarbeta i stället för att dra åt olika håll. Tanken är att göra de kritiska systemen tillräckligt **säkra och motståndskraftiga** och att se till att de **fortsätter att fungera**.

EU har satt upp **fyra specifika mål**:

- Överbrygga **skillnaderna mellan medlemsländernas insatser** för säkerhet och motståndskraft i kritiska system.
- Förbättra **EU:s styrning** på området.
- Stärka EU:s kapacitet för **incidenthantering**.
- Stärka Internets motståndskraft och stabilitet.

VAD HANDLAR DET OM I DETALJ?

EU vill lägga fram en plan för omedelbara åtgärder på följande områden:

- **BEREDSKAP OCH INSATSER**
 - Fördjupat EU-övergripande samarbete mellan nationella/statliga **organisationer för incidenthantering**.
 - Ett europeiskt **offentligt-privat partnerskap** för motståndskraft.
 - Ett europeiskt **forum där nationella myndigheter** kan utbyta information och lösningar.
- **UPPTÄCKT OCH INSATSER**
 - Ett nytt EU-system för **informationsutbyte och varning** för allmänheten och små och medelstora företag.

- **SKADEBEGRÄNSNING OCH ÅTERSTÄLLNING**
 - **Nationella beredskapsplaner och övningar** för hantering av nätverksincidenter och katastrofer efter storskaliga säkerhetsincidenter.
 - **EU-omfattande övningar** för storskaliga säkerhetsincidenter i nätverk.
 - Stärkt **samarbete** mellan nationella/statliga organisationer för incidenthantering.
- **INTERNATIONELLT SAMARBETE**
 - Internationella **principer och riktlinjer** för Internets motståndskraft och stabilitet.
 - **Globala övningar** för återställning och skadebegränsning av storskaliga Internet-incidenter.
- **KRITERIER FÖR KRITISKA DIGITALA SYSTEM**
 - Till stöd för EU-direktiv 2008/114 om kritisk infrastruktur.

VARFÖR BÖR EU AGERA?

Kritiska **digitala system** är ofta **kopplade till system i andra länder**, så det räcker inte alltid att ett land förbättrar sitt system.

Ett lands systemsäkerhet är ofta i **hög grad beroende** av skyddsnivån i **andra länder**.

Därför krävs en **samordnad EU-strategi** som förbättrar de befintliga nationella programmen och stärker EU-ländernas bilaterala och multilaterala samarbete.

NÄR TRÄDER FÖRSLAGET I KRAFT?

Under **första halvåret 2009**.

Det fördjupade samarbetet kommer att få omedelbara effekter, men det handlar också om att gradvis och fortlöpande öka människors kunskap och bygga upp deras förtroende.