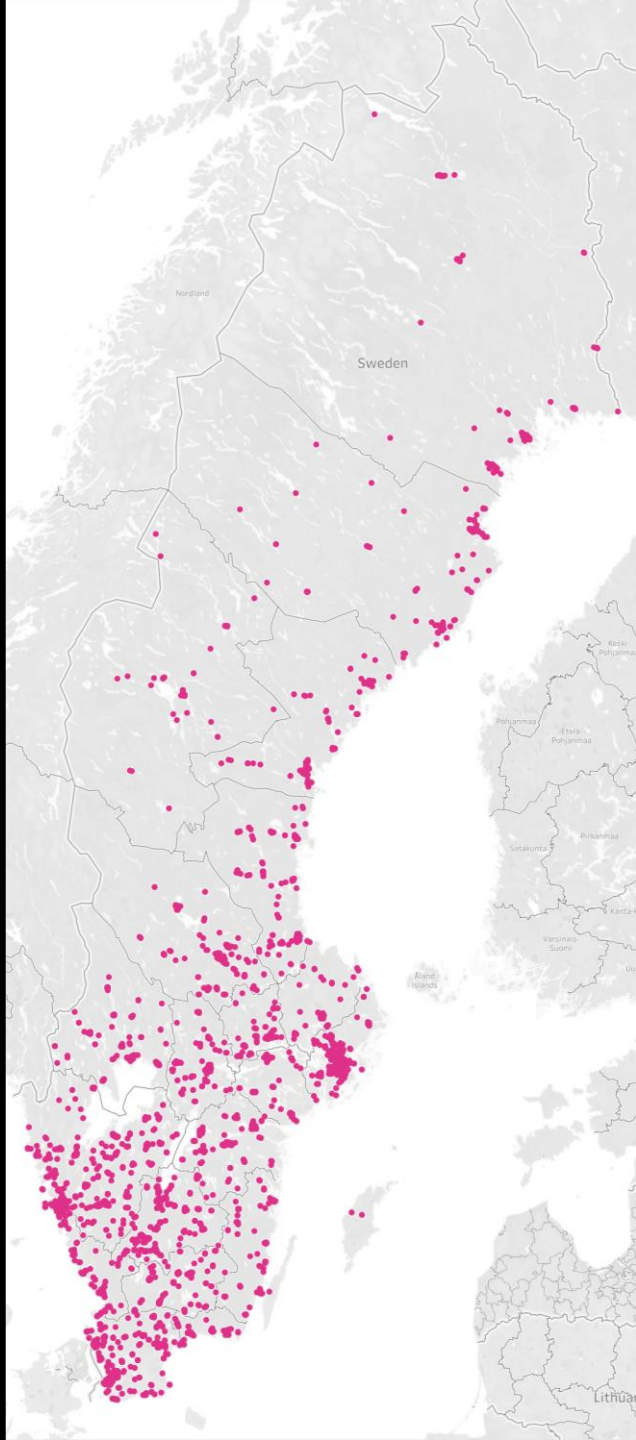


Cybersäkerhet & reglering

- Mycket att hålla koll på, men behöver jag verkligen bry mig?

My Bergdahl





Vilka är Teknikföretagen?

- 4 400 medlemmar inom teknikindustrin
- Står tillsammans för en tredjedel av Sveriges export
- Sysselsätter fler än 800 000 i Sverige
- Vårt uppdrag är att främja våra medlemmars internationella konkurrenskraft och långsiktiga lönsamhet
 - Arbetsgivarfrågor (förhandla kollektivavtal, rådgivning i arbetsrätt, etc)
 - Branschfrågor (påverkansarbete inom näringspolitiska frågor, nationellt / EU + strategiska innovationsprogram)

Sex cyberattacker som skakat världen

ATTACKERNA MOT ESTLAND

När: 2007
Vad: Omfattande överbelastningsattacker och flera databräningar mot estländska banker, tidningar och myndigheter efter en dispyt med grannlandet Ryssland.
Vem: Ryssland har pekats ut som ansvarig för attacken.

ELNÄTSATTACKERNA I UKRAINA

När: 2015 och 2016
Vad: Natten innan julafton 2015 blev över 230 000 ukrainare strömlösa i upp till sex timmar efter en koordinerad cyberattack mot företag som sköter driften av landets elnät. I december året därpå genomfördes en liknande attack mot landets huvudstad Kiev.
Vem: Ryssland pekas ut som ansvarig.

STUXNET-MASKEN

När: 2010
Vad: Stuxnet brukar kallas världens första cybervapen. Det är ett virus som skapades för att slå ut centrallagret för uranrikning i Iran.
Vem: Israel pekas ut som ansvarig för attacken.

CLOUD HOPPER

När: Uppdagades 2013
Vad: Hackare har...



Okat cyberhot mot Sverige inför valet

Efter flera kända cyberattacker mot bland annat Finlands riksdag, slår it-experters fast att även Sverige befinner sig i riskzonen. Nu flaggar de för myndighetssajternas utsatthet med anledning av det stundande valet och landets Nato-ansökan. "Sverige är nu en betydligt mer intressant måltavla", säger it-säkerhetsexperten Mikael Westerlund.

Uppdaterad: 26 augusti 2022, 10:50 Publicerad: 21 augusti 2022, 10:54

Maja-Wera Honkanen Text



Basfakta EU



- Frivilligt samarbete mellan 27 länder – Sverige medlem sedan 1995
- Gemensamma regler inom många områden, OCH - medlemsländerna får där bara stifta lagar när det inte finns en lag från EU som reglerar samma sak
- EU-lagstiftning kan bara föreslås av EU-kommissionen
- EU-lagstiftning beslutas av Europaparlamentet och medlemsstaterna (rådet) gemensamt

Centrala EU-initiativ under denna mandatperiod (2019-2024)



Cybersäkerhets-
akten

ENISA

Cybersäkerhets-
certifiering

Cybersäkerhets-
strategin

NIS

Cyberresiliensakten
(CRA)

Cybersäkerhetsakten

- Stärker ENISA
- Etablerar ramverk för cybersäkerhetscertifiering
- Länk: [L_2019151SV.01001501.xml \(europa.eu\)](#)

ENISA



- EU:s myndighet för cybersäkerhet, baserad i Grekland
- Inrättad 2004 – inledningsvis ganska blygsamt uppdrag, men sedan 2019 en allt större roll och permanent mandat
- Sekretariat för nationella CSIRT-nätverket
- Samarbetar med EU:s övriga institutioner och myndigheter
- Information och kommunikation
- Roll kring cybersäkerhetscertifiering

Cybersäkerhetscertifiering

- Baserat på cybersäkerhetsakten
- ENISA utarbeta förslag på certifieringsordningar (eng: certification scheme)
- Tre områden; molntjänster, 5G och ikt-produkter (generell)
- Frivillig certifiering – men kan komma att bli (de facto) tvingande?
- FMV utpekad som svensk nationell myndighet – har inrättat Inspektionen för cybersäkerhetscertifiering
- Länk: [Cybersecurity Certification \(europa.eu\)](https://europa.eu/cybersecurity-certification)

Swedish Certification Body for IT Security (www.csec.se)



Ärendetyp: 6

Diarienummer: 22FMV8472-8

Dokument ID EP-301



CSEC

Swedish Certification Body for IT Security

301 Certification and Evaluation - EUCC - Overview

Issue: 2.0, 2023-Jun-07

- [301 Certification and Evaluation - EUCC - Overview \(fmv.se\)](https://www.fmv.se/301-Certification-and-Evaluation-EUCC-Overview)

Swedish Certification Body for IT Security
301 Certification and Evaluation - EUCC - Overview

Table of Contents

1	Preface	3
1.1	Purpose	3
1.2	Terminology	3
2	Introduction	4
2.1	Overview	4
2.2	Brief Description of CSEC EUCC	4
2.3	EUCC scheme	5
2.4	Relevant Legislation, Standards and Regulations	5
2.5	Trademarks	6
2.6	Documentation	6
3	Types of Certifications	8
3.1	ICT Product Certification	8
3.2	Protection Profile Certification	8
4	Roles within CSEC EUCC	9
4.1	Sponsor	9
4.2	Developer	9
4.3	IT Security Evaluation Facility (ITSEF)	9
4.4	Certification Body	9
5	Processes within the CSEC EUCC	10
5.1	Management of Confidential Information	10
5.2	Certification Agreement	11
5.3	Evaluation and Certification Process	11
5.4	Certificate Validity	12
5.5	Compliance monitoring	13
5.6	Assurance continuity	13
5.7	Licensing of Evaluation Facilities	14
5.8	Scheme Notes	14
5.9	Complaints and Appeals	14
Appendix A	16	
A.1	References	16
A.2	Abbreviation	18
A.3	Glossary	19

Cybersäkerhetsstrategi



- Presenterades i slutet av 2020
- Beskriver vad EU bör göra framåt; såväl kring regler som finansiering och samarbeten
- ”Det samordnade genomförandet av denna strategi kommer att bidra till ett cybersäkert digitalt decennium för EU, till skapandet av en säkerhetsunion och till en stärkt global ställning för EU”
- Länk: [IMMC.JOIN%282020%2918%20final.SWE.xhtml.1_SV_ACT_part1_v2.docx \(europa.eu\)](#)

NIS



- NIS (nätverks- och informationssäkerhetsdirektivet) – i kraft i svensk lag juli 2018
 - Omfattar 7 sektorer ; bland annat bankverksamhet, digital infrastruktur, energi m.fl.
 - Krav: arbeta systematiskt och riskbaserat + rapportera incidenter
 - Sektorsansvariga myndigheter
 - MSB nationell kontaktpunkt + har meddelat föreskrifter om vilka aktörer inom resp sektor som är skyldig att anmäla sig samt vägledning för hur anmälan ska gå till

NIS forts.



- NIS2 (åtgärder för en hög gemensam cybersäkerhetsnivå i hela EU)
 - Färdigförhandlades hösten 2022
 - Bredare tag; utökat antalet sektorer + stärkta krav
 - Nya sektorer: avloppsvatten, offentlig förvaltning, rymd, Forskning och utveckling avseende läkemedel, tillverkning av bl.a. farmaceutiska basprodukter och läkemedel, tillverkning av medicintekniska produkter och medicintekniska produkter för in vitro-diagnostik, digitala leverantörer, forskning m.fl.
 - Nya krav: kortare tid för incidentrapportering, ansvar hos ledningen, vidta åtgärder för att hantera risker i bl.a. leverantörskedjor, höga bötesbelopp!
 - Ska vara genomfört och börja tillämpas 18 oktober 2024 (förslag 23 mars 2024)

CRA

- Förslag presenterat i september – förhandlas nu
- Cybersäkerhetskrav för ”produkter med digitala element”
- Bygger på NLF-struktur, dvs standardisering, CE-märkning och marknadskontroll
- Men – för kritiska produkter (enligt bilaga till lagen) krävs tredjeparts-certifiering OCH listan kan komma att utökas
- Ansvar för tillverkare, importörer, distributörer m.fl.
- Böter

.....OSV, OSV, OSV...

- Dataakten
- AI-akten
- Produktansvarsdirektivet
- AI-produktansvarsdirektivet
- Cybersolidaritetsakten
-

Varför viktigt att hålla koll?

- Kommande krav?
- Möjligheter?
- Kan bli dyrt!
- Ständig utveckling!



Tack!



My Bergdahl

my.bergdahl@teknikforetagen.se

www.teknikforetagen.se