knowit

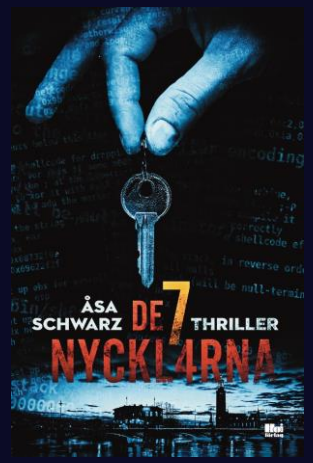
Cybersäkerhet - hur säkrar vi Sverige tillsammans?

SOI ÅRSKONFERENS 2024

ÅSA SCHWARZ, CYBERSÄKERHETSSPECIALIST OCH FÖRFATTARE

knowit

Åsa Schwarz



- Affärsutvecklingschef, Knowit Cybersecurity & Law
- Styrelseledamot, Precise Biometrics & Enea
- 25 års erfarenhet av Cybersäkerhet
- Författare av spänningslitteratur

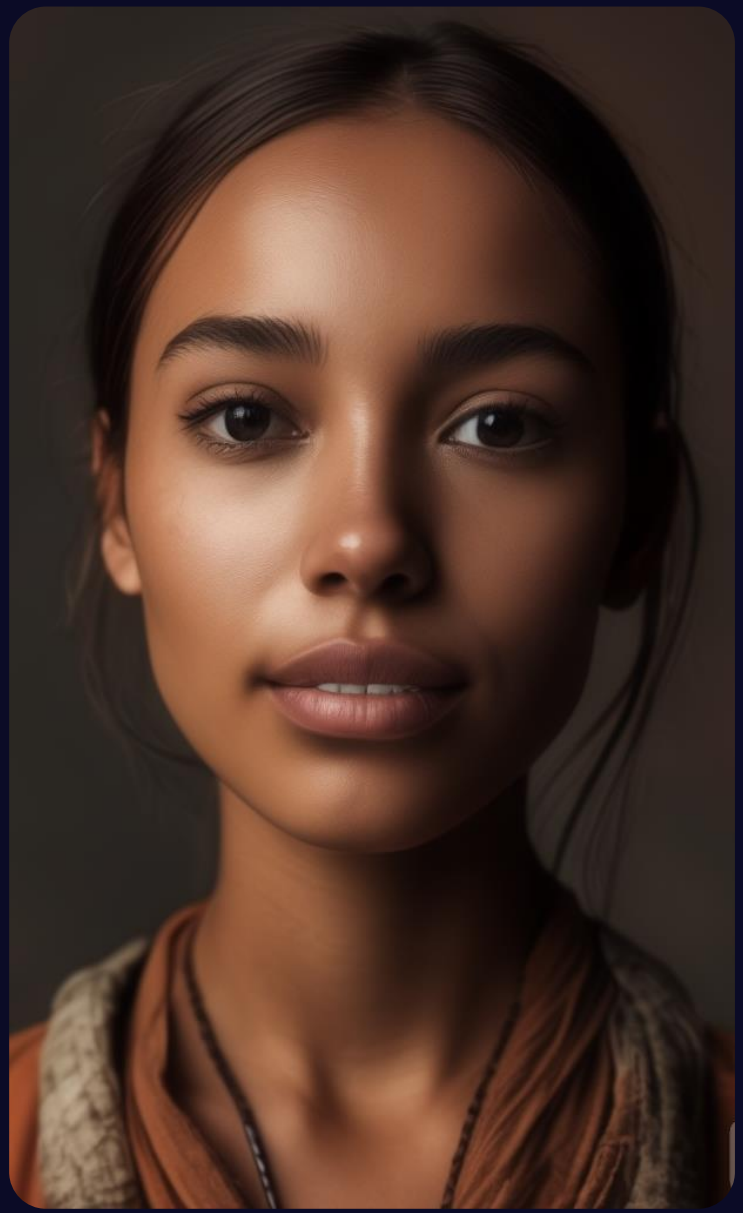
Agenda

En av de viktigaste delarna i delarna i trygga våra digitala infrastruktur är att upphandla säkra och trygga tjänster och system. Men vilka är det som försöker ta sig in i våra system och vad kan man göra som inköpare för att minska risken?

- Vad är cybersäkerhet?
- Sverige
- Världen: Komplex digitalisering, deskriptiv teknik och tredjepartsrisker
- Världen: Vilka är angriparna?
- Vad kan hända?
- Omfattande ny lagstiftning (NIS2 , AI-förordningen etc)
- Standarder och certifieringar förenklar upphandling
- Optimera/minska kostnaden för säkerhet
- Praktiska tips

Imagine AI Art

”peaceful human”



knowit

Vad är cybersäkerhet?

- Tillgänglighet
- Riktighet
- Konfidentiell

- Informationssäkerhet / It-säkerhet

Sverige är:

nr 2 på Global Innovation Index

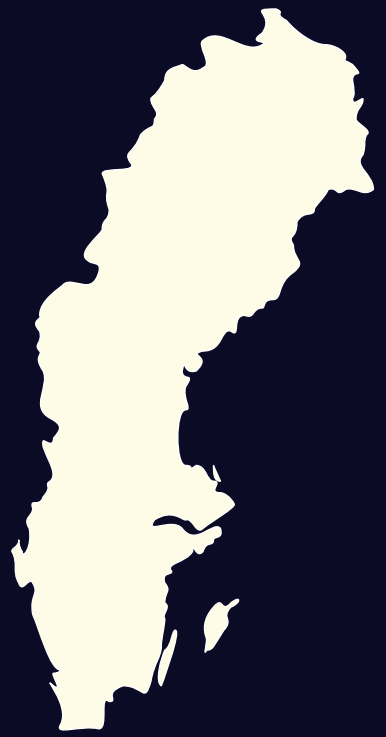
nr 3 på listan över mest digitala länder i Europa (DESI)

nr 16 (26, 32) plats på Global Cybersecurity Index (GCI).

* Flest lönsamma start ups per capita efter Sillicon Valey.
* Vann Locked Shields 2021 + 2023

knowit

Det här ska fungera varje dag



- 21 regioner
- 290 kommuner
- 458 myndigheter, varav 249 är statliga förvaltningsmyndigheter
- 7 Polisregioner
- 45 flygplatser som möjliggör ca. 367 000 landningar, med ca. 36 miljoner passagerare
- Ca. 1200 vårdcentraler och ca. 90 sjukhus med omkring 13 miljoner vårdbesök
- Ca.1,6 miljarder påstigningar i kollektivtrafiken

- 1 200 106 företag
- Ca. 140 elbolag som möjliggör svenskarnas elförbrukning om 15MWh per invånare och år
- Ca. 600 teleoperatörer som bl.a tillhandahåller ca. 13,5 million internetabonnemang
- Ca. 2400 finansbolag och ca. 3 miljarder kortköp på årlig basis
- Ca. 1750 vattenverk som förser varje invånare med 60 liter vatten per dygn
- Ca 160 dagstidningar, 340 minuters mediekonsumtion per person och dag

knowit

Gartner Top 10 Strategic Technology Trends 2024

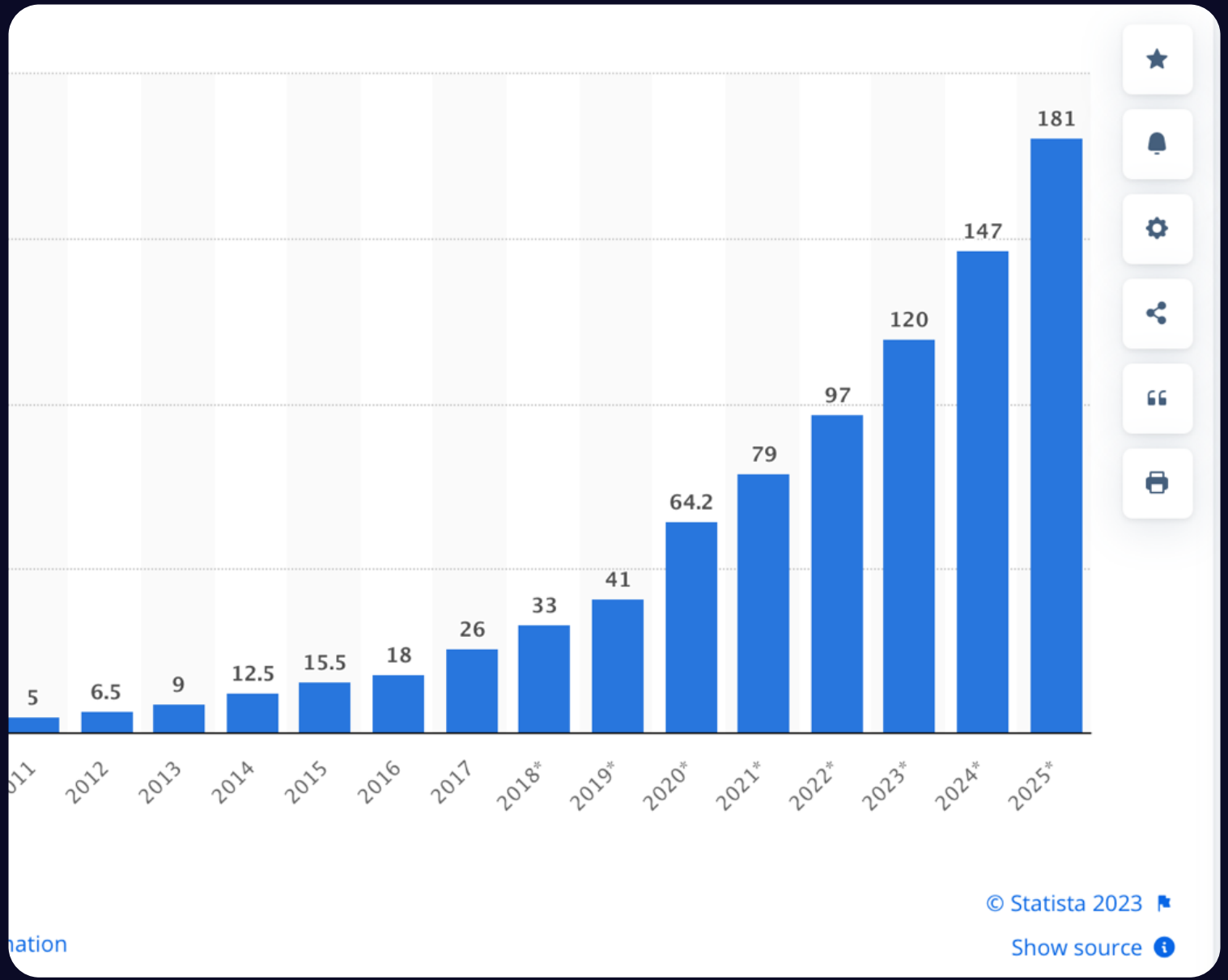
1. AI as Partner: AI Trust, Risk and Security Management (AITRiSM)

2. Be Safe: Continuous Threat Exposure Management (CTEM)

3. Protect the Future: Sustainable Technology

4. Developer-Driven Self-Service: Platform Engineering
5. Accelerate Creation: AI-Augmented Development
6. Tailor Your Tailor's Work: Industry Cloud Platforms
7. Optimize Decision - Making: Intelligent Applications
8. Power AND Responsibility: Democratized Generative AI
9. Push the Pioneers: Augmented Connected Workforce
10. Buyers With Byte(s): Machine Customers

knowit



Data skapad, sparad, kopierad, och konsumerad i hela världen*

*in zettabytes from 2010 to 2020, with forecasts from 2021 to 2025

← All Open Letters

Pause Giant AI Experiments: An Open Letter

We call on all AI labs to immediately pause for at least 6 months the training of AI systems more powerful than GPT-4.

Signatures
33709

Add your signature

Published
March 22, 2023

OCTOBER 30, 2023

FACT SHEET: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence

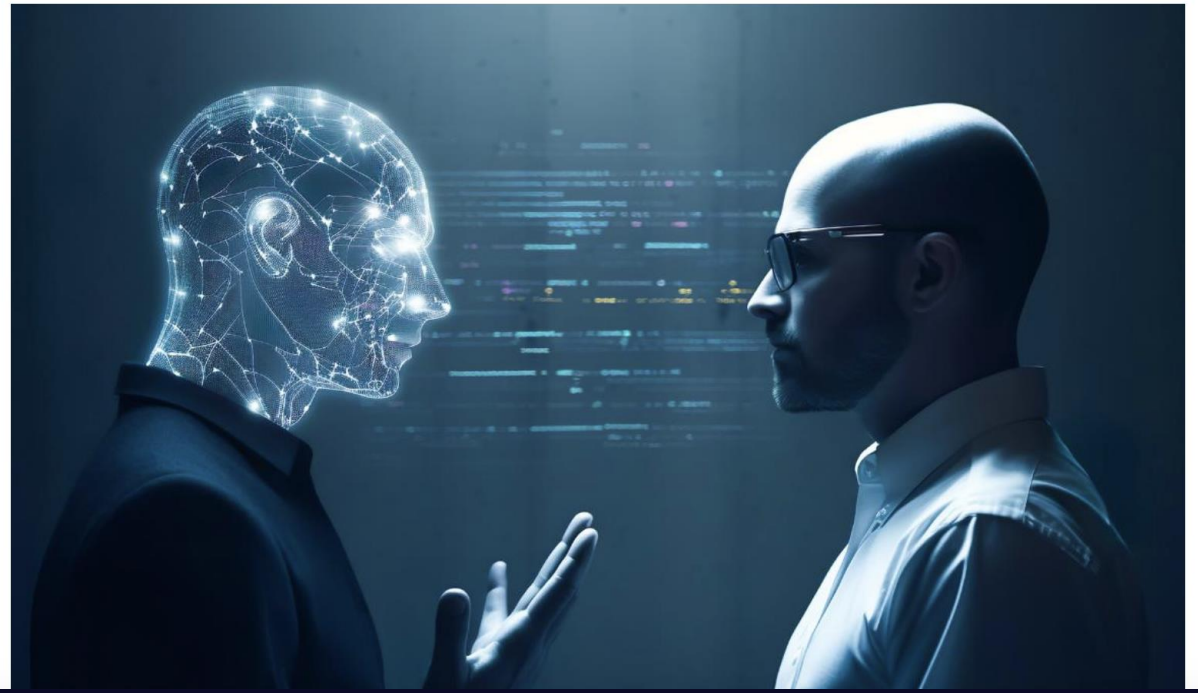
BRIEFING ROOM › STATEMENTS AND RELEASES

European Parliament

EU AI Act: first regulation on artificial intelligence

Society Updated: 14-06-2023 - 14:06
Created: 08-06-2023 - 11:40

The use of artificial intelligence in the EU will be regulated by the AI Act, the world's first comprehensive AI law. Find out how it will protect you.



Artificiell intelligens

Arbetsgivarna uppskattar att ca 44% av medarbetarnas kunskaper kommer att behöva förändras kraftigt.
/The Future of Jobs Report 2023

Nya medarbetare

Ny organisationer

Ny teknik

Nya metoder

Nya risker

= Helt ny input till säkerhetsarbetet

knowit

Vilka är angriparna?

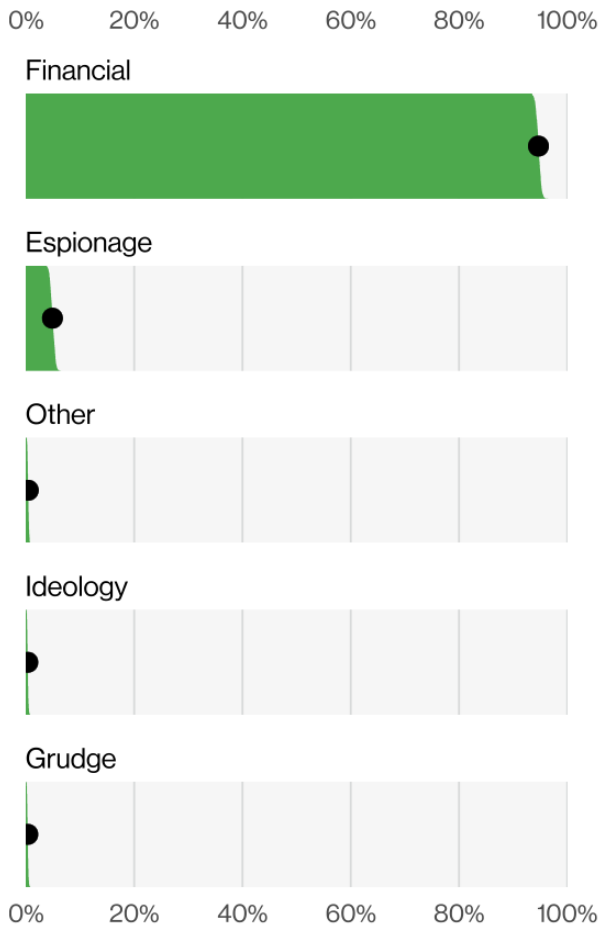


Figure 12. Threat actor Motives in breaches (n= 2,328)

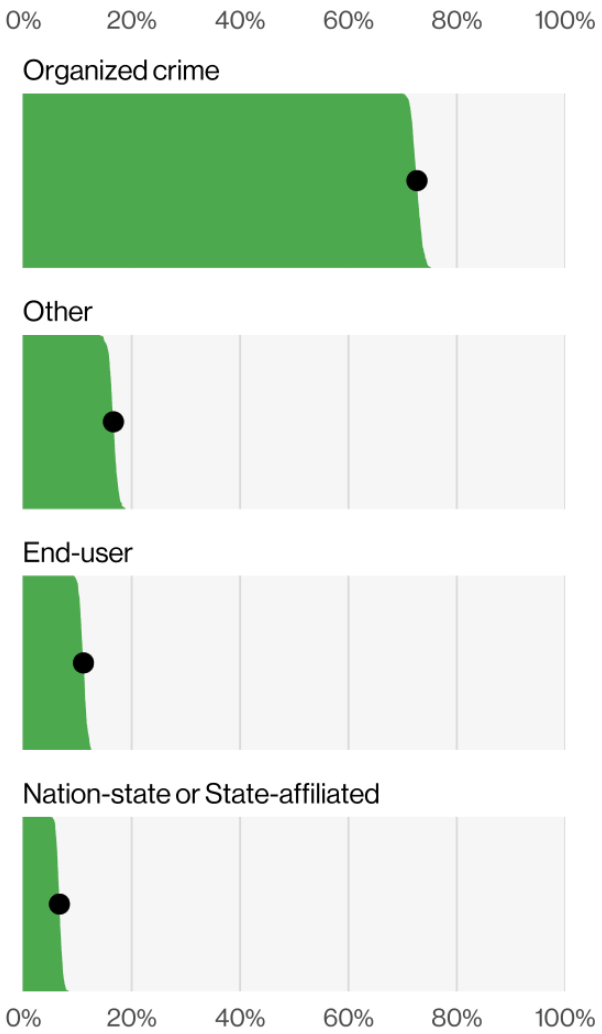


Figure 13. Threat actor Varieties in breaches (n=2,489)

Drivkrafter

Verizon DBIR, 2023

knowit

Ett flertal länder genomför cyberangrepp mot Sverige

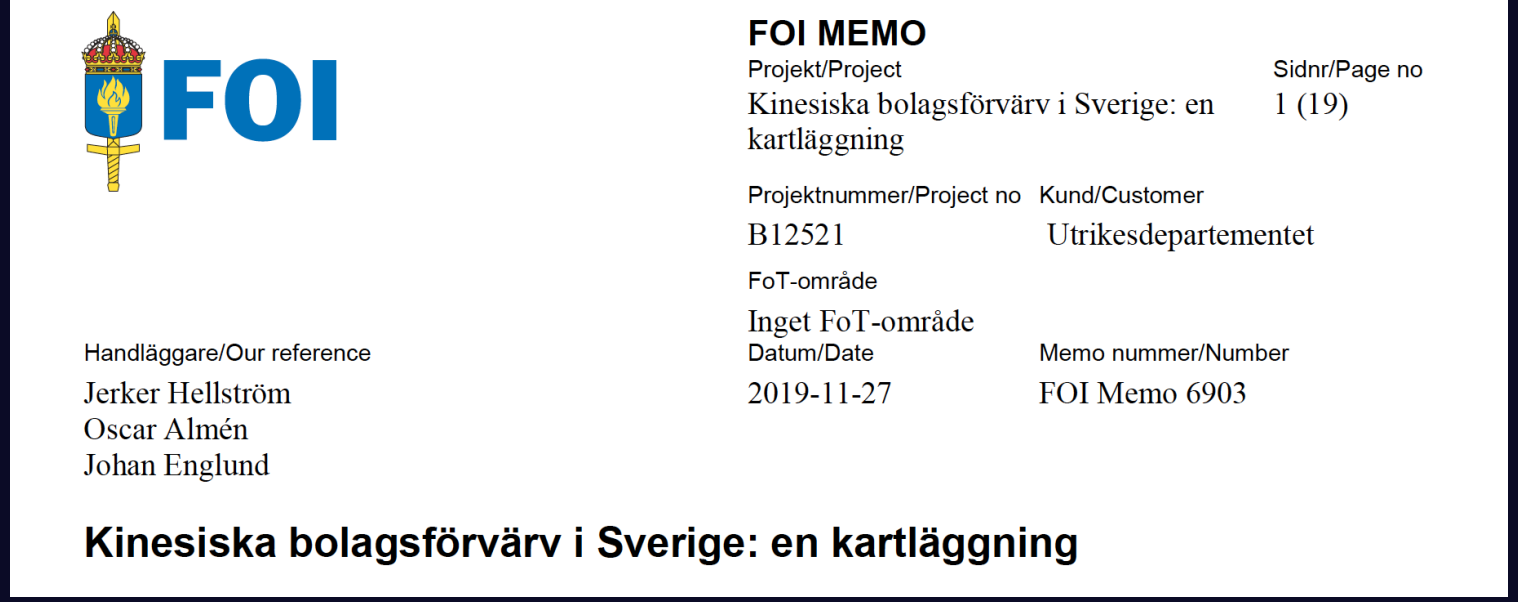
* Säkerhetspolisens årsbok

- Långsiktig agenda
- Information och förberedande arbeten för angrepp
- Flest angrepp: Ryssland och Kina
- Underrättelsetjänster, bolag, universitet
- APT:er = Advanced Persistent Threat

knowit

En av världens största hackerarméer

Det finns andra sätt att kontrollera svensk teknik och innovation.



FOI

FOI MEMO

Projekt/Project
Kinesiska bolagsförvärv i Sverige: en kartläggning

Sidnr/Page no
1 (19)

Projektnummer/Project no
B12521

Kund/Customer
Utrikesdepartementet

FoT-område
Inget FoT-område

Handläggare/Our reference
Jerker Hellström
Oscar Almén
Johan Englund

Datum/Date
2019-11-27

Memo nummer/Number
FOI Memo 6903

Kinesiska bolagsförvärv i Sverige: en kartläggning

knowit

Vet du vilka som äger bolagen som du upphandlar varor och tjänster ifrån?

...och vilka som äger dem som äger dem som äger dem?

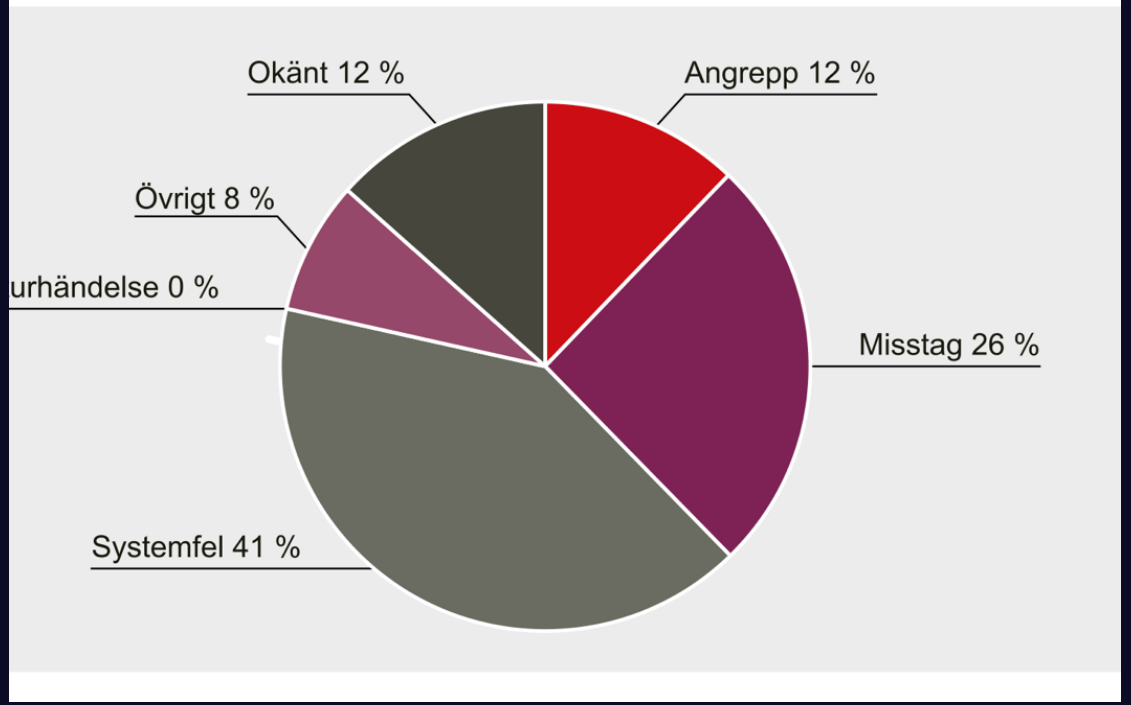
knowit

Vad kan hända?

Orsaker

* Allt är inte bara hackerattacker och antagonister

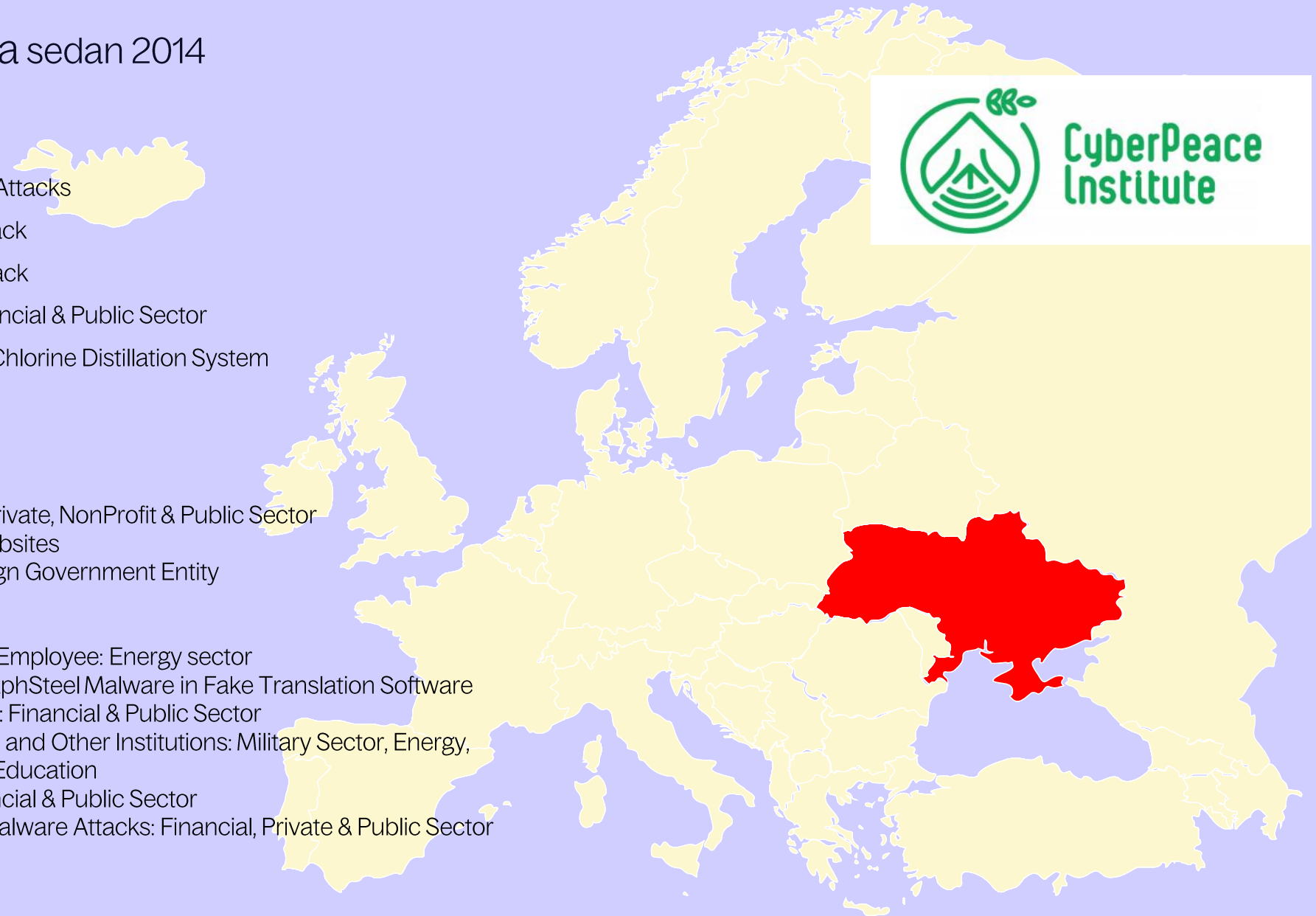
3. Fördelning av inrapporterade orsaker till it-incidenter 2022



knowit

Attacker mot Ukraina sedan 2014

- Ej fullständig



2014 May - Presidential Election Attacks

2015 December - Power Grid Attack

2016 December - Power Grid Attack

2017 July - NotPetya: Energy, Financial & Public Sector

2018 July - “VPNFilter” Attack on Chlorine Distillation System

2022

<u>January</u>
- “WhisperGate” Wiper Attacks: Private, NonProfit & Public Sector
- Defacement of Government Websites
- Attempt to Compromise a Foreign Government Entity

<u>Feburary</u>
- Spear Phishing Email Targeting Employee: Energy sector
- Cobalt Strike, GrimPlant and GraphSteel Malware in Fake Translation Software
- Large DDoS Attack on Websites: Financial & Public Sector
- Attacks on Ukraine Government and Other Institutions: Military Sector, Energy, Financial, Transport, Healthcare, Education
- DDoS Attack on Websites: Financial & Public Sector
- “HermeticWiper / FoxBlade” Malware Attacks: Financial, Private & Public Sector

Etc....

Leverantörsberoenden

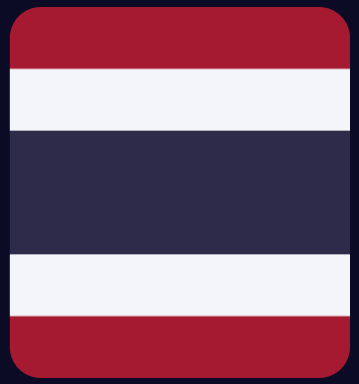
knowit

1177-incidenten

Region Stockholm
Region Sörmland
Region Värmland

Inera AB

Medhelp AB



Medicall Co Ltd

Voice Integrate Nordic

Leverantörsberoenden

knowit

När många är beroende av en

Några exempel på drabbade:

- Anticimex
- Filmstaden
- Granngården
- Loomis
- Mediq
- Munters
- Primula/Statens servicecenter
- Region Blekinge, Sörmland, Uppsala, Västerbotten
- Swedavia
- Vellinge kommun


HACKAD

knowit

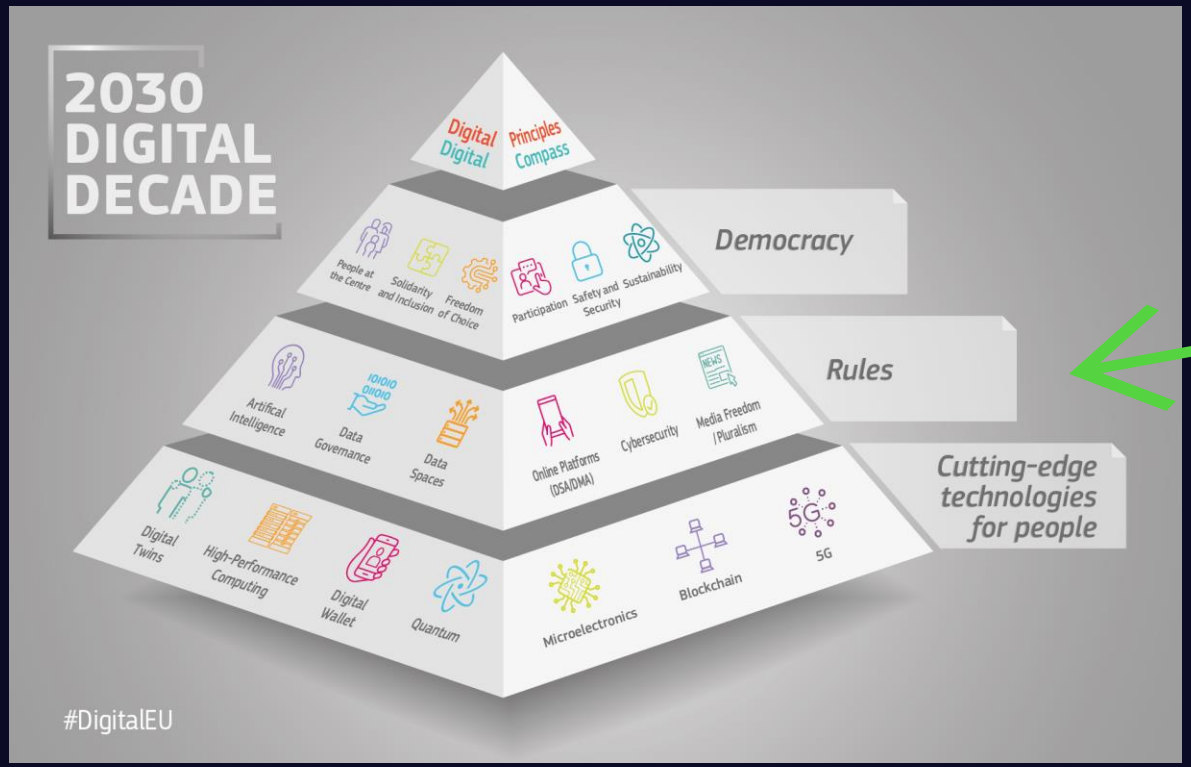
Vet du vilken säkerhet dina leverantörer har?

...och vilken säkerhet de som levererar till dem som levererar till dem som levererar till dem har?

knowit

Omfattande och ny lagstiftning

The Digital Decade 2020–2030



Källa; EU-kommissionen, https://digital-strategy.ec.europa.eu/en/policies/europes-digital-decade

Ambitiösa mål som ska nås med hjälp av

- *Vägledande principer*
- *Regelverk*
- *Finansieringsprogram*
- *Internationella samarbeten*

knowit

Nya och uppdaterade regelverk

AI Act (AIA)	Data Act (DA)	Data Governance Act (DGA)	General Data Protection Regulation (GDPR)
Digital Operational Resilience Act (DORA)	NIS2	Cyber Resilience Act (CRA)	**Med flera…**

knowit

I blickfånget NIS2

Ökad omfattning*

- Alla kommuner med undantag för kommunfullmäktige
- Samtliga regioner med undantag för regionfullmäktige
- Samtliga myndigheter med vissa undantag.

*Delbetänkande av Utredningen om genomförande av NIS2- och CER-direktiven.

Exempel på förändringar

- Större fokus på styrelse och ledningens ansvar
- Högre krav på säkerhet och rapportering
- Säkerhet för leverantörskedjor och leverantörer

knowit

Verksamhets-ledningssystem

- Vikten av ett ledningssystem (med olika inriktningar)
- Kvalitet, miljö, cybersäkerhet
- Dokumenterade processer och ständiga förbättringar
- Mycket lättare hantera kravbilden
- Cybersäkerhet t ex ISO 27001 + 27002
- Nya lagkrav
- Verksamhets och teknikspecifika standarder
- Både upphandlande verksamhet och leverantör
- Enhetligt språk och kravbild i hela kedjan
- Certifiering?

knowit

Hur sjutton ska jag som inköpare kunna allt?

knowit

Jurister

Inköpare

Leverantörer

Verksamhetsutvecklare

IT

Cybersäkerhet är ett teamarbete!

Ekonomer

Verksamhetsspecialister

Kommunikatörer

Säkerhetsspecialister

Vad driver kostnader?

- För höga säkerhetskrav
- Ej anpassade säkerhetskrav
- För låga säkerhetskrav som resulterar till incidenter och/eller sanktionsavgifter
- Säkerhetskrav ställs efter inköp
- Hitta på egna krav istället för att arbeta med standarder

Ett bra förarbete leder till kostnadseffektiv säkerhet.

knowit

Att tänka på vid upphandling

- Typ av verksamhet?
- Typ av information?
- Lagstiftning?
- Alla intressenter:
  - Leverantörer? (ägare, beroenden)
  - Tillsynsmyndigheter?
- Vilka analyser krävs?
- Ta hjälp av säkerhetsstandarder
  - På verksamhetsnivå ex ISO 27001
  - På produkt eller tjänst, t ex NIST SP 800-82
  - Certifiering?
- Tänk på säkerhet i hela livscykeln
- Hur ska du följa upp att kraven faktiskt fylls?
  - Avtal räcker inte
  - Revision och egna tester
  - Tredje part

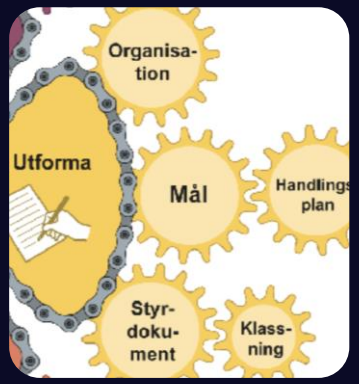
knowit

Ni är en viktig pusselbit i vårt försvar

Vill du veta mer?

knowit

Kostnadsfri rådgivning för systematiskt informationssäkerhetsarbete



Informationssäkerhet.se
Stöd för systematiskt arbete med informationssäkerhet i organisationer

The European Union Agency for Cybersecurity (Enisa)

Svenska institutet för standarder

Säkerhetspodcasten

Facebook: Säkerhetsbubblan

knowit

Cybersäkerhet - hur säkrar vi Sverige tillsammans?

SOI ÅRSKONFERENS 2024

ÅSA SCHWARZ, CYBERSÄKERHETSSPECIALIST OCH FÖRFATTARE

Följ mig gärna på Linkedin!

knowit