

Välkomna till Griffel

– en förmiddag om digital säkerhet

Griffeldagen

- Vilka deltagare?
 - Besitter kunskap
 - Har kunskapsbehov
 - Har intresse
- Innehåll?
 - Få/ta till sig kunskap
 - Dela tankar och erfarenheter genom samtal



Agenda

9.15 Griffel hälsar välkomna

9.20 Sharp

9.35 ALSO

9.50 Clavister

10.00 Mingel med Griffel och våra samarbetspartners

11.00 Föreläsning Max Villman

12.00 Lunch

SHARP

SHARP

Be Original.



Sharp och Griffel



Sharp Sverige

Vi är specialister på digitala arbetsplatser. Vårt mål är att göra er digitala arbetsplats enklare, säkrare och effektivare.



Finns över hela landet,
huvudkontor i Stockholm.



200 medarbetare i Sverige
med kontor på 9 orter.



Starkt nätverk av partners
över hela landet.



Jobbar med alla olika
branscher och storlekar på
företag både inom privat-
och offentlig sektor.



Konsulterar, levererar,
installerar och utbildar i
verktyg för den digitala
arbetsplatsen.



Den digitala arbetsplatsen

SHARP
Be Original.

Skrivare och kopiatorer

Vi har rätt verktyg och expertis för att hjälpa er till effektivare och säkrare dokumenthantering.



Underlätta för moderna och digitala arbetssätt med rätt hård- och mjukvara



Support och servicetjänster



Integration direkt mot molntjänster som Teams, Exchange, OneDrive och Google Drive.



Branschledande inom säkerhetsfunktioner

200 Canon Printer Models May Expose Wi-Fi Connection Data

Aug 2023

Windows Print Spooler Vulnerabilities Increasingly Exploited in Attacks

MAY 2022

Lexmark warns of RCE bug affecting 100 printer models, PoC released

Jan 2023

HP prepping firmware update to fix critical security vulnerability in LaserJet printers

April 2023

Hackers have carried out over 65,000 attacks through Windows' Print Spooler exploit

May 2022

Russia State-Sponsored Hackers Used Misconfigured MFA to Breach NGO

FBI and CISA warn of attack on multifactor authentication account to exploit "PrintNightmare"

March 2022

BLACK BASTA RANSOMWARE ACTORS TAKE AIM AT PRINTNIGHTMARE FLAW

JULY 2022

Hackers have carried out over 65,000 attacks through Windows' Print Spooler exploit

May 2022

PaperCut vulnerabilities exploited using LockBit and ClOp ransomware – Microsoft

The flaws in the popular print management software could help criminals gather data for secondary attacks

April 2023

Sensitive submarine documents found in Wetherspoons pub

Official documents pertaining to a Royal Navy submarine were reportedly discovered in the restroom of a Wetherspoons pub.

April 2023

Data Leak Hits Thousands of NHS Workers

We hijacked 28,000 unsecured printers to raise awareness of printer security issues

October 2022

PaperCut Software Flaw Sparks Ransomware Attacks, CISA Warns

May 2023

Child takes patient records to school to use 'as drawing paper'

A child arrived at their primary school with printed records containing details of 150 patients to use as "drawing paper", the trust involved has admitted. May 2023

Vad är Digital Signage och varför ska vi ha det?

Affärsområdeschef Visual Solutions



Effektiv informationsdelning och samarbete med digital skyltning och interaktiva displayer.



Kommunicera med din målgrupp via digitala skyltar i alla miljöer.



Ökad synlighet med flexibla LED-lösningar.



Intuitiv mjukvara för enkel uppdatering.

Kassasystem och betallösningar

Våra betalsystem och kassor ger dig kontroll på försäljning samtidigt som dina kunder får en bra upplevelse.



Kassor och betalösningar för alla typer av branscher och företagsstorlek.



Molnbaserade lösningar för smidig hantering och större flexibilitet.



Enkelt, användarvänligt gränssnitt.



Backoffice och analysverktyg för att förstå och öka dina affärer.

SHARP
Be Original.

ALSO



Security, Cyber Threats & Solutions – 2025

Danny Rahmani – Cloud Sales MW + Security
@ALSO



Dagens Agenda:



Hotlandskapet i världen



Marknadstrender & Insikter



Ökningen av techscams & phishing



Sårbarhet hos SMB

Utmaningar för organisationer...

Hur kan vi jobba smartare?



Hybridarbete – anställda jobbar från olika platser.

Obeskyddade nätverk och osäkra inloggningar gör företag sårbara.

Ökad risk för **nätfiske** och **identitetskapning**.

Hur kan vi bibehålla säkerheten?



Företagsägda och privata enheter används i arbetet.

Bristande kontroll över enheter skapar **säkerhetsluckor**.

Ökad risk för **dataförlust, intrång** och **spridning av skadlig kod**.

Hur kan vi minska kostnaderna & arbeta proaktivt?



SMB-organisationer drabbas i allt större utsträckning av cyberattacker.

Attacker kan leda till driftstopp, dataläckor, stora ekonomiska förluster.

Kostnaden för en cyberattack är i snitt 4,88 miljoner USD (2024)¹.

Digitala miljöer blir allt mer komplexa och attackerna vanligare



600

Miljoner identitetsattacker dagligen

99%

Av identitetsattacker är lösenordsbaserade

2,75x

Ökning i mänskligt utförda ransomware attacker

90%

Av organisationer är exponerade för minst en attackväg

61%

Av attackvägar leder till ett känsligt användarkonto



Hotlandskapet i världen

Identity attacks in perspective: Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than 99% of identity attacks are password attacks

Breach replay

Password spray

Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1% of attacks



MFA attacks

SIM swapping

MFA fatigue

AitM

Post-authentication attacks

Token theft

Consent phishing

Infrastructure compromise

Source: Microsoft Threat Intelligence

" I takt med att organisationer flyttar till molnet har identitetsrelaterade attacker ökat där motståndarna använder komprometterade autentiseringsuppgifter för att komma åt kritiska resurser.

Microsoft Entra-data visar att lösenordsbaserade attacker utgör över **99 % av 600 miljoner identitetsattacker per dag**. Under det senaste året har **Microsoft blockerat 7 000 lösenordsangrepp per sekund** vilket visar på hur ihärdiga och utbredda de här hoten är." ¹

SMB är en stor målgrupp av cyberattacker

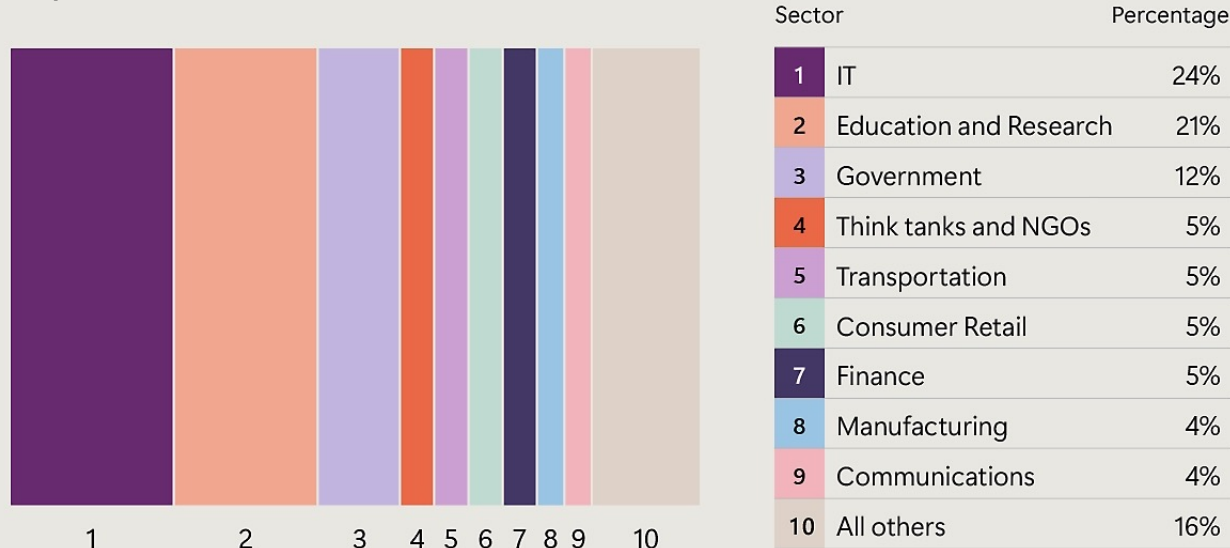


33% av alla cyberattacker riktar sig mot SMB.²

Microsoft 365 säkerhet skyddar mot dessa hot genom:

- **Proaktivt skydd** som minskar attackytan och stoppar hot i realtid.
- **Automatiserad hotrespons** – Identifierar och neutraliserar avancerade attacker utan manuell insats.
- **Integration med Microsofts säkerhetsekosystem** – Sömlöst skydd över identitet, enheter och moln.

Top 10 mest drabbade sektorerna i världen



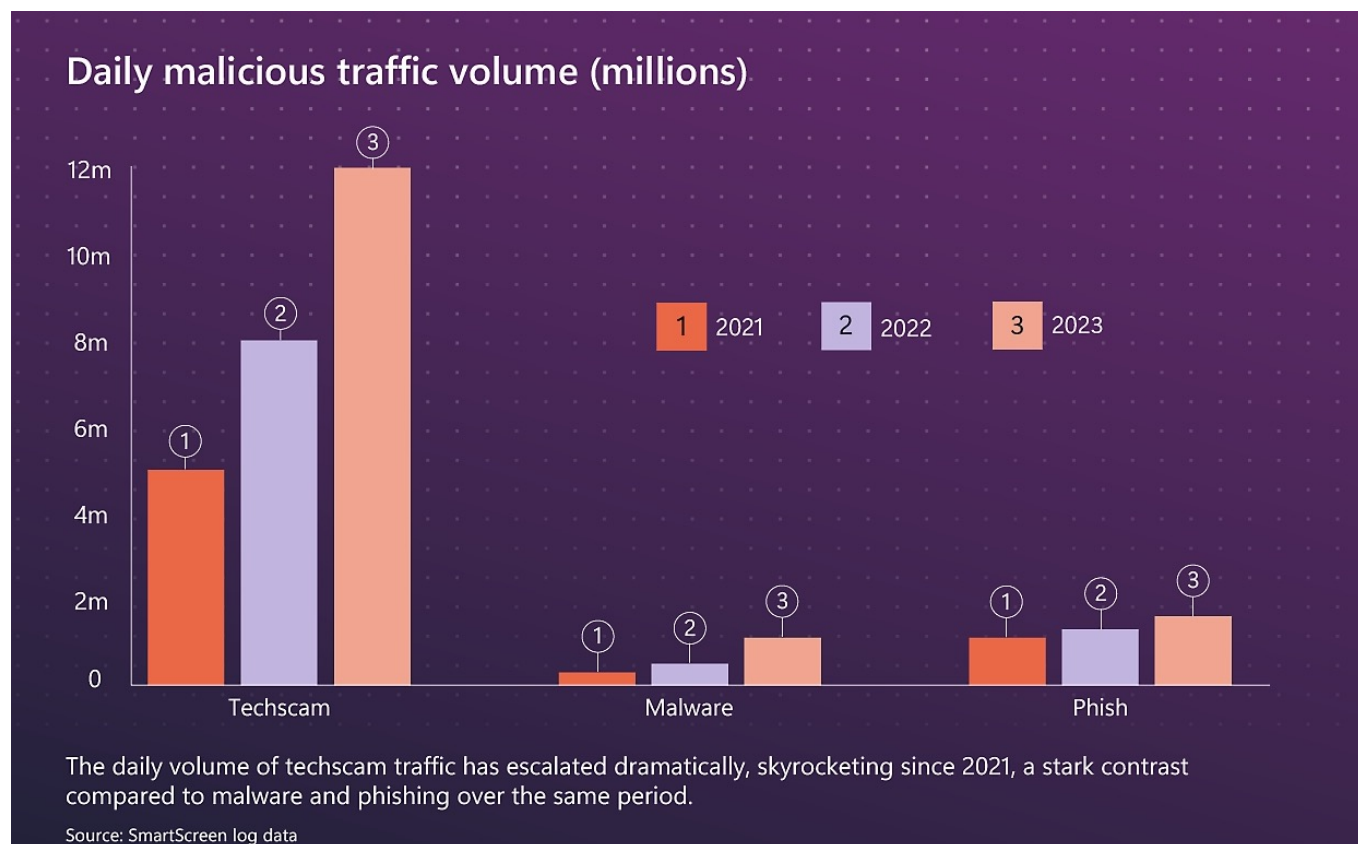
Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Source: Microsoft Threat Intelligence, nation-state notification data

¹ Source: Microsoft Security Exposure Management
The Microsoft Digital Defense Report 2024

² Source: ABCNews

Ökningen av tech scams



Nätfiske har **ökat från runt 1 miljon år 2021 till 2 miljoner 2023.**¹

Cyberkriminella använder alltmer sofistikerade metoder, inklusive bluffannonser och falska tekniska supporttjänster, för att lura användare och stjäla känslig information.

Microsoft 365 säkerhet skyddar mot dessa hot genom:

Stoppar bluffmejl och misstänkta länkar innan de når användaren.

Säkra Länkar & Säkra Bilagor –

Förhindrar att användare klickar på skadliga länkar eller öppnar skadliga bilagor.

Med Microsofts inbyggda säkerhetsfunktioner kan företag **proaktivt minska risken för teknikbedrägerier och skydda sina anställda från att luras.**

¹ Source: Microsoft Security Exposure Management
The Microsoft Digital Defense Report 2024

Microsoft Security



- Omfattande säkerhets och produktivetslösning



Samarbeta i realtid



Aktivera säker åtkomst
och skydda identiteten



Försvara dig mot
cyberhot och
dataförlust



Skydda och hantera
enheter på ett enkelt
sätt

Fördelarna med Microsoft Security



Omfattande och enkel att använda

En lösning för produktivitet och säkerhet

Molnplattform förenklar driftsättning

Får dig igång snabbt



Minskar kostnaderna

Eliminerar kostnader för flerpunktslösningar

Minskar kostnaderna för helpdesk

Underlättar licensieringskomplexiteten



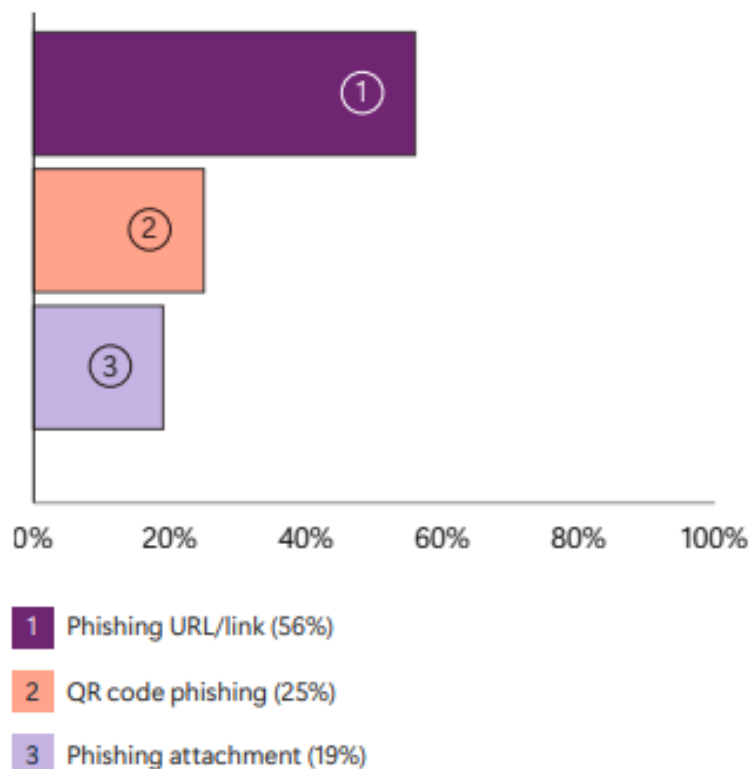
Teknik i företagsklass

Avancerad säkerhet som går att lita på

AI-driven hotinformation

Topprankad säkerhetsleverantör

Top email phishing-typer



Source: Microsoft Defender Threat Experts notifications



Cyberkriminella använder allt mer sofistikerade phishing-metoder, inklusive **QR-kods-baserat nätfiske** som växer snabbt.

Microsoft 365 Säkerhet, skyddar mot dessa hot genom:

- **AI-driven e-postsäkerhet** – Identifierar och blockerar skadliga länkar i realtid.
- **Säkra Länkar & Säkra bilagor** – Förhindrar att användare klickar på skadliga länkar eller öppnar skadliga bilagor.
- **Automatiserad hotrespons** – Isolerar misstänkta e-postmeddelanden innan de når inkorgen.

Med **Microsofts inbyggda säkerhet** kan företag **proaktivt skydda sig mot phishing och minska risken för intrång**.

SMBs blir alltmer sårbara för cyberattacker

+1070%

- Ransomware-attacker senaste året
- Mer än 50% riktade mot småföretag¹



33%

1/3 av alla cyberattacker riktar sig mot småföretag.²

61%

av småföretag som nyligen utsattes för en cyberattack kunde inte fortsätta.³

60%

SMBs saknar kompetens att hantera cyberattacker⁴

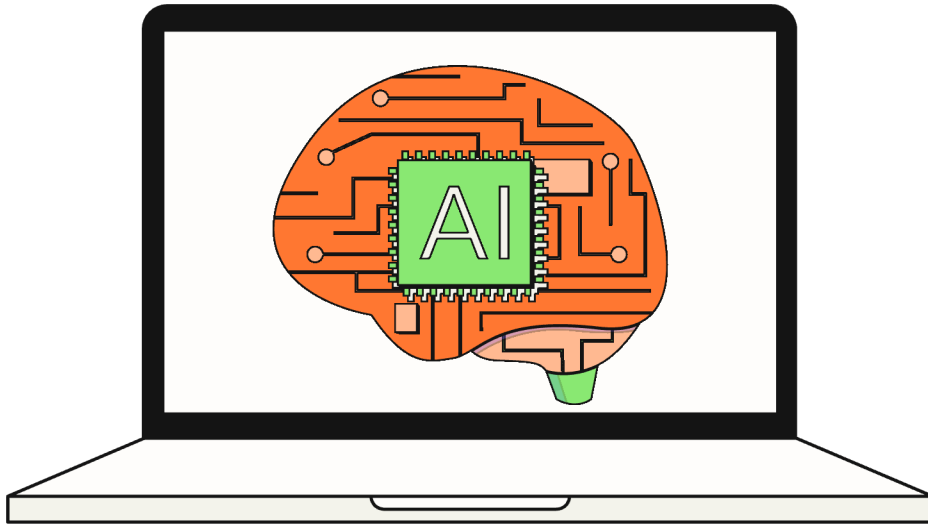


\$108K

genomsnittlig kostnad för ett SMB-dataintrång.⁵

1. [Homeland Security Secretary Alejandro Mayorkas, 06 May 2021 ABC report](#)
2. [Introduction to the 2020 DBIR | Verizon Enterprise Solutions](#)
3. [Microsoft commissioned Forrester Research](#)
4. [Underserved and Unprepared: The State of SMB Cyber Security in 2019](#)
5. [Kaspersky Global Corporate IT Security Risks Survey, 2019](#)

Bring Your Own AI (BYOAI)

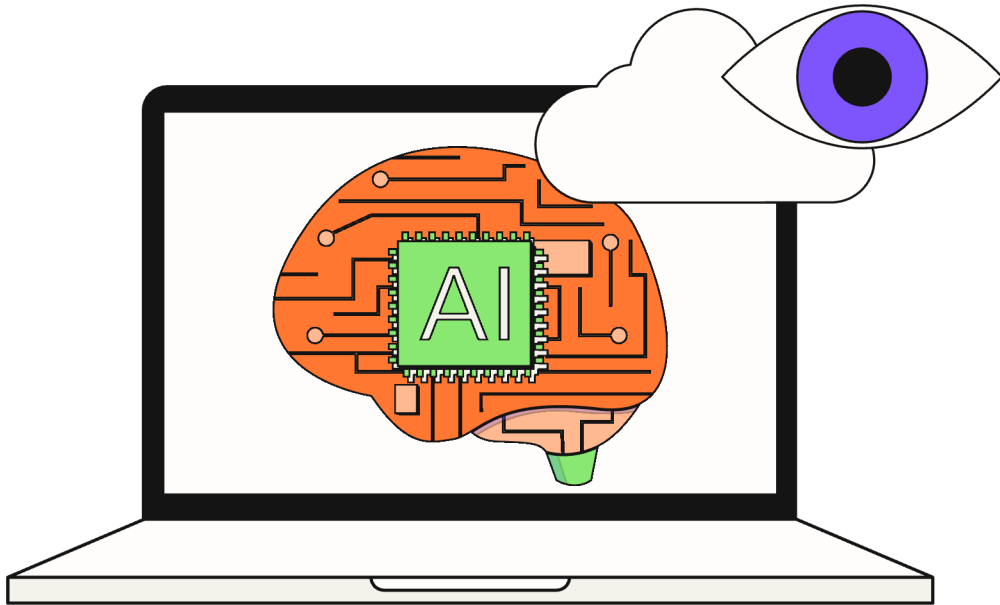


En projektledare på Northwind Traders kopierar kunddata från ett skyddat dokument och klistrar in det i en tredjeparts-AI-app för att skapa en rapport. Appen är inte godkänd av IT, och datan laddas upp till en osäker plattform, vilket riskerar läckage av känslig information och bryter mot regelverk.



86% av svenska informationsarbetare tar med sin egen AI till arbetet (BYOAI).¹

Kontrollera & skydda mot BYOAI



Med Microsoft 365 Säkerhet kan Northwind Traders stoppa otillåten AI-användning genom:

- Identifierar och blockerar oönskade AI-tjänster som ChatGPT, Claude eller Perplexity i realtid.
- Skapar policies för att begränsa åtkomst till tredjeparts-AI-appar.
- Övervakar enheter i realtid och stoppar otillåten datadelning.



63%

av svenska "information workers" använder generativ AI på arbetsplatsen idag.¹

Tack för oss!



danny.rahmani@also.com

CLAVISTER



VI LEVER I EN OSÄKER TID

**Cyberkriget
har redan börjat.
Och hotet är på allvar.**

En värld i förändring



KRIG I EUROPA



HYBRIDKRIGFÖRING MOT KRITISK
INFRASTRUKTUR



GEOPOLITISK INSTABILITET

VÅRT UPPDRAG ÄR ATT CYBERSÄKRA EUROPA

**Clavister levererar svensk-
tillverkade cybersäkerhetslösningar
till samhällskritisk verksamhet.**



Digital suveränitet ur två perspektiv



Det legala perspektivet

Vem har tillgång till din data?



Infrastrukturperspektivet

Vem har tillgång till din infrastruktur?

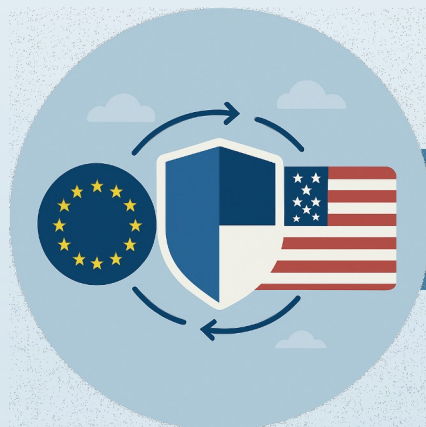
Adekvansbesluten

EN TIDSLINJE



Safe Harbor

2000



**Privacy
Shield**

2015



**Data Privacy
Framework**

2020

2023



Data Privacy Framework (DPF)

Nytt försök att rätta till brister i tidigare ramverk, framförallt:

**Massövervakning av EU-medborgare
av amerikanska myndigheter.**

**Avsaknad av rättsmedel
för EU-medborgare.**

Godkändes av EU-kommissionen i juli 2023
som nytt ramverk.

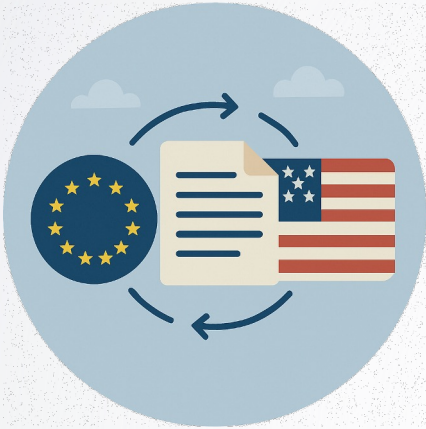


Begränsning av övervakning

Presidentorder 14086 utfärdad 2022 av president Joe Biden.

Begränsar amerikanska myndigheters inhämtning av persondata – får
enbart ske om det är **”nödvändigt och proportionerligt”**.





Ny tillsyns- myndighet

DPRC (Data Protection Review Court) där EU-medborgare kan klaga om de misstänker att data hanterats felaktigt av amerikanska myndigheter.

DPRC är tänkt att vara oberoende, med möjlighet att ge bindande beslut (inklusive att radera data).

Efter kritik från EU kring oberoendefrågan står DPRC under tillsyn av PCLOB (Privacy and Civil Liberties Oversight Board).



**U.S. PRIVACY AND
CIVIL LIBERTIES
OVERSIGHT BOARD**





Självcertifiering

Enbart amerikanska företag som är **självcertifierade** får ta emot personuppgifter från EU enligt DPF.

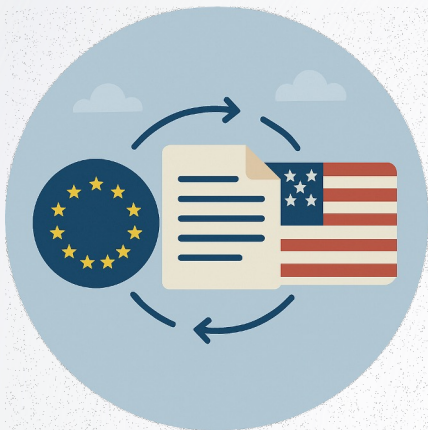
Certifieringen bygger på **ansökan hos DoC**,
intygande att man **följer DPF-principerna**,
publicering av **sekretesspolicy** samt **interna regler**
för efterlevnad.





Allt är väl grönt
ljus då, eller...?

Nja.



Presidentordrar är svaga

EO 14086 kan **upphävas** med omedelbar
verkan genom en **ny presidentorder**.

Därmed skulle DPF sannolikt **inte**
längre ha adekvat skyddsnivå.

Samtliga EU-verksamheter som lagrar persondata i
amerikanska molntjänster skulle därmed **bryta mot GDPR**.





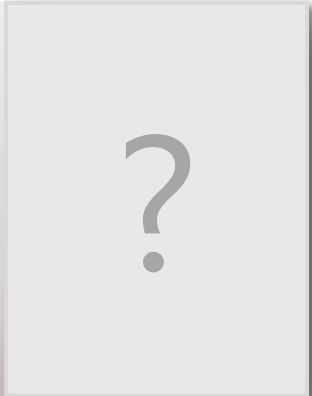
Men tillsyns- myndigheten då?



U.S. **PRIVACY AND
CIVIL LIBERTIES**
OVERSIGHT BOARD



Beth A.
Williams (R)



Sharon
Franklin (D)



Edward W.
Felten (D)



Veronica
LeBlanc (D)



Vacant

Risker

Just nu rättslig och strategisk osäkerhet.

En "Schrems III"-dom kommer att göra överföringar olagliga.

Höga sanktionsavgifter och rättsliga följder.

Risk för brott mot säkerhetsskyddslagen
vid hantering av skyddsklassad information.

Rekommendationer

Riskinventera – ställ uppsidan av icke-europeiska molntjänster mot de rättsliga och finansiella riskerna.

Utvärdera alternativa lösningar – det finns fler kompetenta och kostnadseffektiva europeiska lösningar än man kanske tror.



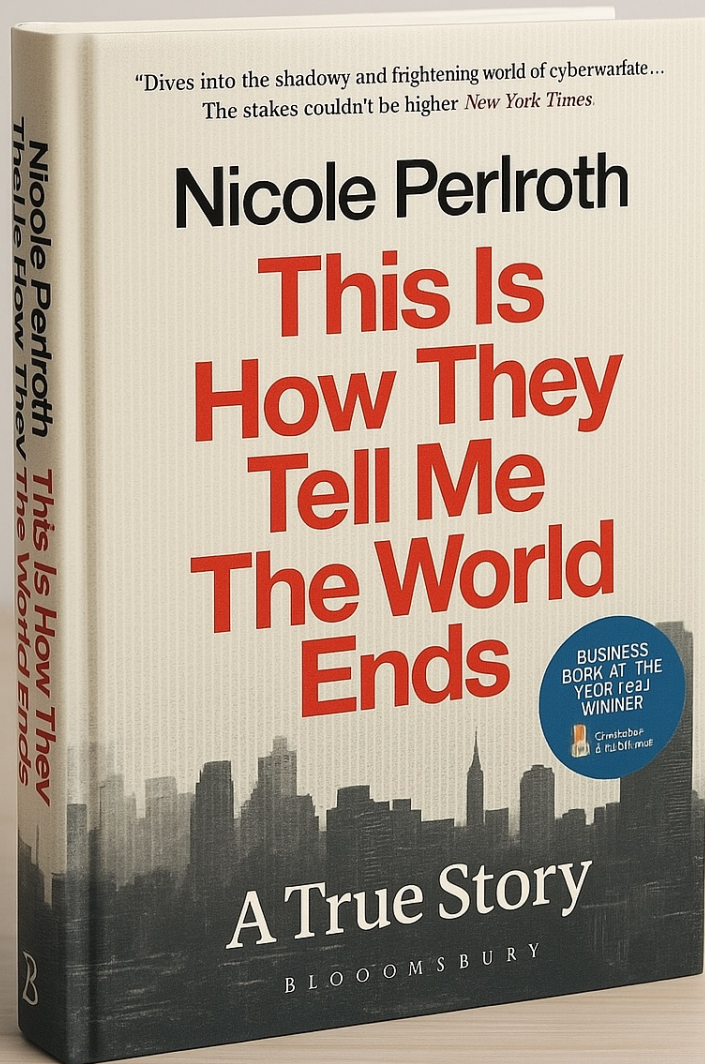
Vem har tillgång till
din infrastruktur?

CLAVISTER®



CLAVISTER®





Regeringar, inklusive den amerikanska, har en lång tradition av att **förvärva** och **använda** s.k. "zero-day"-sårbarheter som ett led i sina **offensiva cyber-operationer**.

Ett axplock

Stuxnet

2009-2010

Utförare: USA (NSA) +
Israel (Unit 8200)

Zero-days: MS Windows,
Siemens SCADA

Användes mot: Irans
urananrikningsprogram

EternalBlue

-2017

Utförare: USA (NSA)

Zero-days: MS Windows,

Användes av: WannaCry,
NotPetya

QUANTUM / FOXACID

-2013

Utförare: USA (NSA)

Zero-days: Firefox, Internet
Explorer

Användes för: Bred
övervakning

iOS Zero-Days

2017

Utförare: USA (FBI, NSA)

Zero-days: Apple iOS

Användes för: Bred
övervakning och aktiva
cybervapen

TURBINE / TURMOIL

Utförare: USA (NSA)

Zero-days: Misc

Användes för: Injicering av
malware globalt

SolarWinds

2020

Utförare: Ryssland (APT29)

Zero-days: SolarWinds
Orion

Användes för: Spioneri på
amerikanska myndigheter

MS Exchange

2021

Utförare: Kina (Hafnium)

Zero-days: MS Exchange
Server

Användes för: Infiltration
av 30 000 amerikanska
organisationer

ArcaneDoor

2023-2024

Utförare: Kinesiska
statsfinansierade aktörer

Zero-days: Cisco ASA

Användes för: Infiltration
av myndighetsnätverk

iOS Zero-Days

April 2025

Utförare: Statlig aktör

Zero-days: Apple Core
Audio, Pointer
Authentication

Användes för: Övervakning
av specifika användare

Tänkvärt

Om man som **svensk organisation** bygger sin nätverksinfrastruktur med aktiva komponenter från icke-europeiska tillverkare, lägger man *de-facto* hela sin **tillgänglighet** och **dataintegritet** i händerna på aktörer som står helt **utanför EU-lagstiftningen**.

Ett urval av europeiska initiativ

The Digital Europe Programme



EU-finansiering (8+ md. €)
för att bygga digital
suveränitet.

European Alliance for Industrial Data, Edge and Cloud



Offentlig-privat samverkan
för att bygga en suverän,
konkurrenskraftig europeisk
digital infrastruktur.

GAIA-X



Initiativ för att skapa
en öppen, säker
och suverän digital
infrastruktur.

EUCC



EU-ramverk för
cybersäkerhets-
certifiering av produkter,
tjänster och processer.

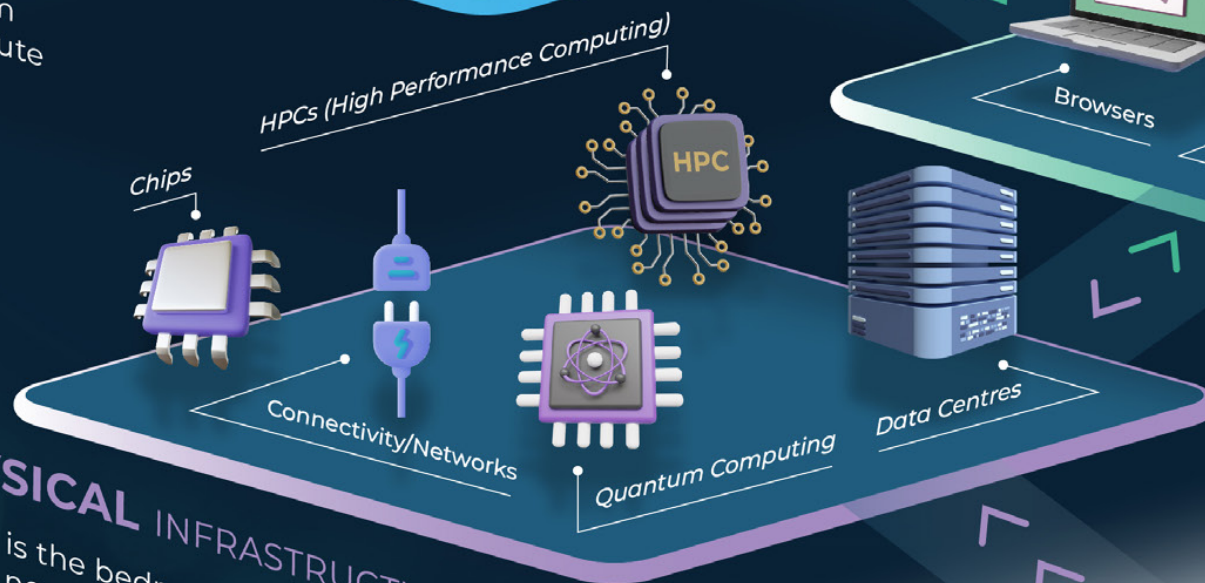
INTERMEDIATION

Connecting ecosystem participants to distribute value to those who build on EuroStack.



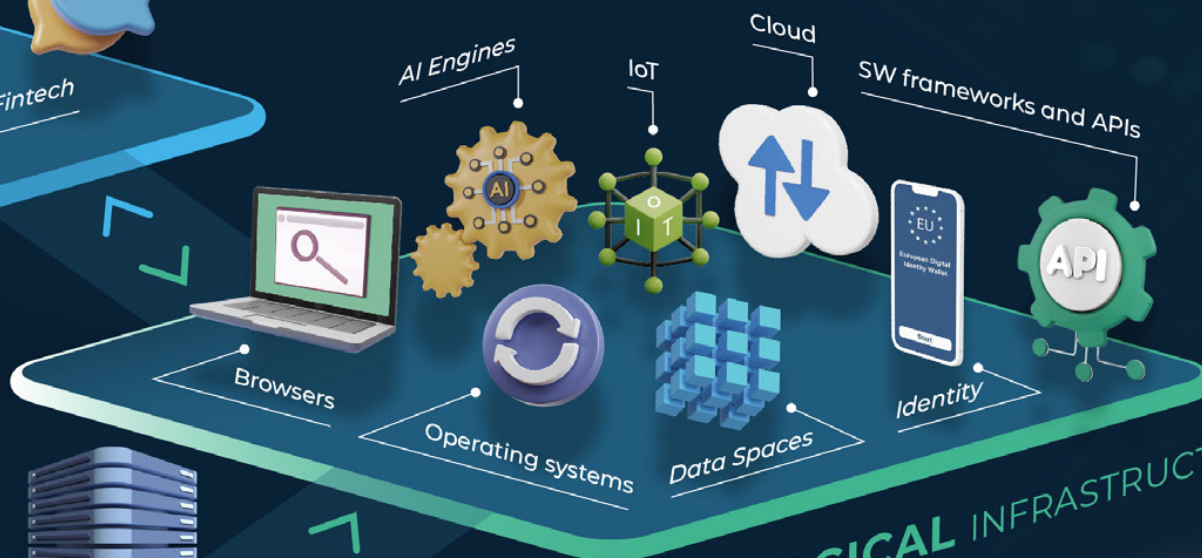
HARD/PHYSICAL INFRASTRUCTURE

Physical capacity is the bedrock of EuroStack and needs to include chips, compute, communications.



SOFT/LOGICAL INFRASTRUCTURE

Software and services, interoperable and reusable to be assembled into products.



Partnerskap för säkerhet och beredskap

Ingen bygger säkerhet ensam.

Vi måste skapa ett europeiskt ekosystem där teknik, kunskap och förtroende går hand i hand.

Genom partnerskap mellan myndigheter, industrin och akademien – och genom att lyfta fram nordisk innovation – stärker vi hela vår motståndskraft.

Clavister är en stolt del av detta ekosystem – och vi vill se fler svenska och europeiska aktörer i kritiska roller.

TACK