Digital Sovereignty Is Impossible Without Big Tech

Prof. Lokke Moerel
Freddy Dezeure, Msc

EU Digital Sovereignty

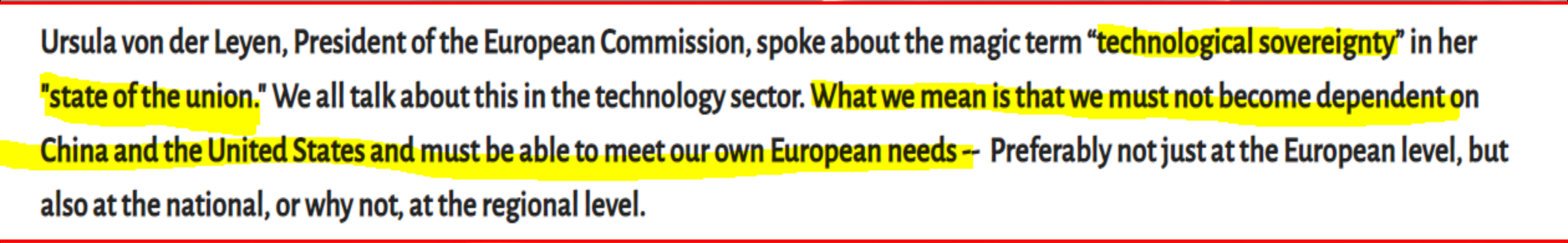
How to navigate the tech cold war without reverting to protectionism

Prof. Lokke Moerel

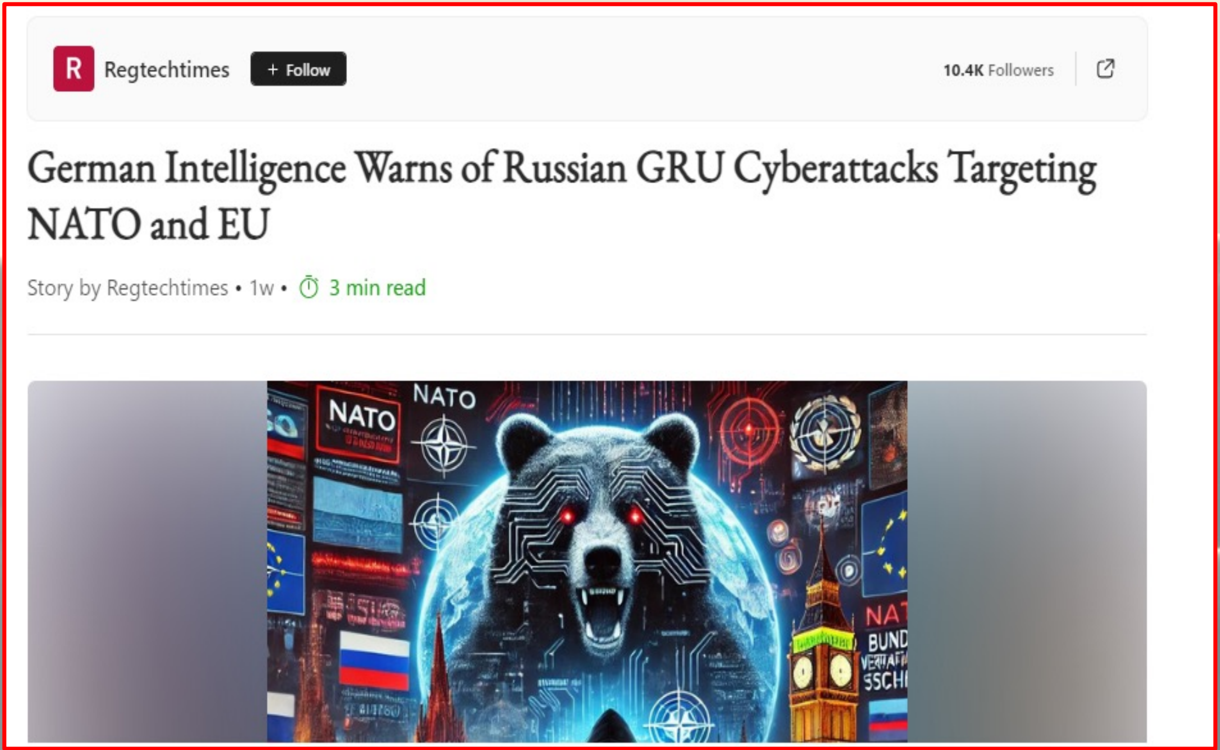
One Conference 2021

Sept. 2021

The magic term "technological sovereignty"



Ursula von der Leyen, President of the European Commission, spoke about the magic term “technological sovereignty” in her "state of the union." We all talk about this in the technology sector. What we mean is that we must not become dependent on China and the United States and must be able to meet our own European needs -- Preferably not just at the European level, but also at the national, or why not, at the regional level.



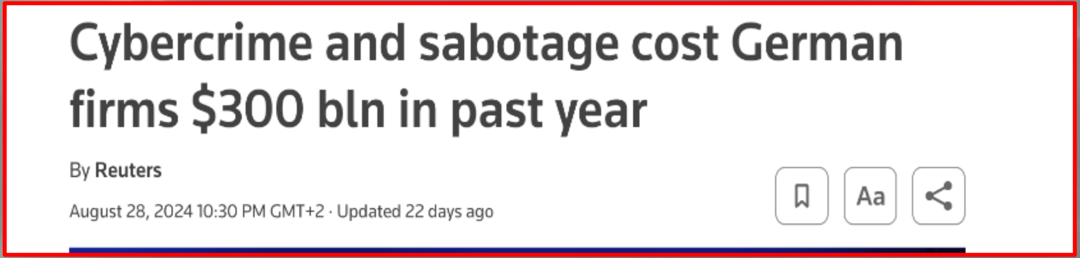
Regtechtimes + Follow 10.4K Followers

German Intelligence Warns of Russian GRU Cyberattacks Targeting NATO and EU

Story by Regtechtimes • 1w • 3 min read

Sept. 2024

August 2024

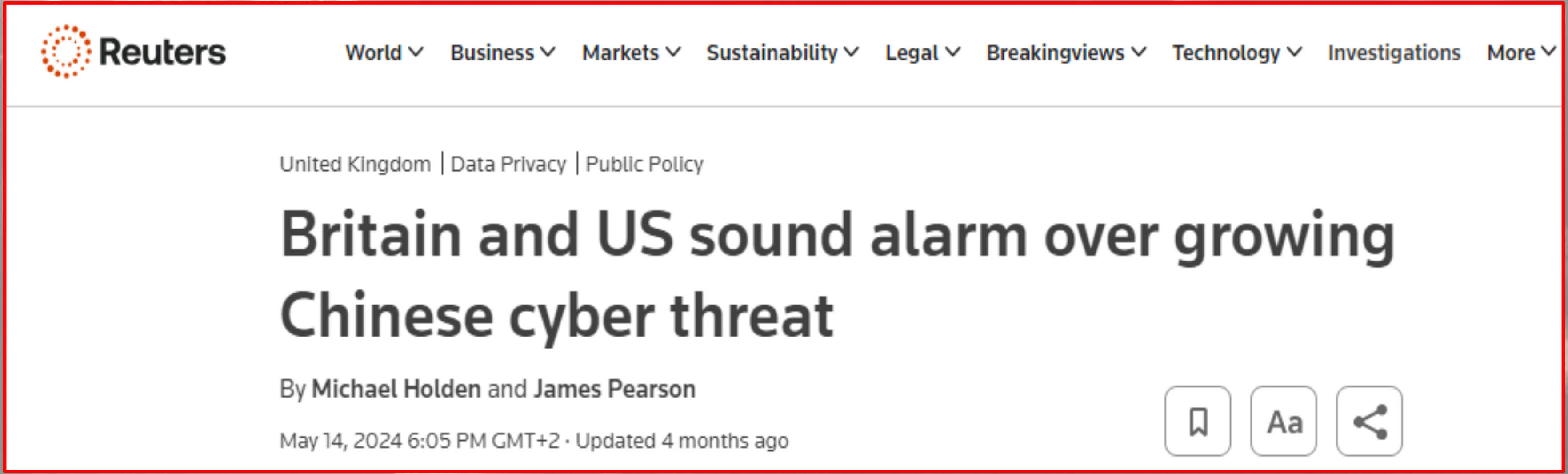


Cybercrime and sabotage cost German firms $300 bln in past year

By Reuters

August 28, 2024 10:30 PM GMT+2 · Updated 22 days ago

May 2024



United Kingdom | Data Privacy | Public Policy

Britain and US sound alarm over growing Chinese cyber threat

By **Michael Holden** and **James Pearson**

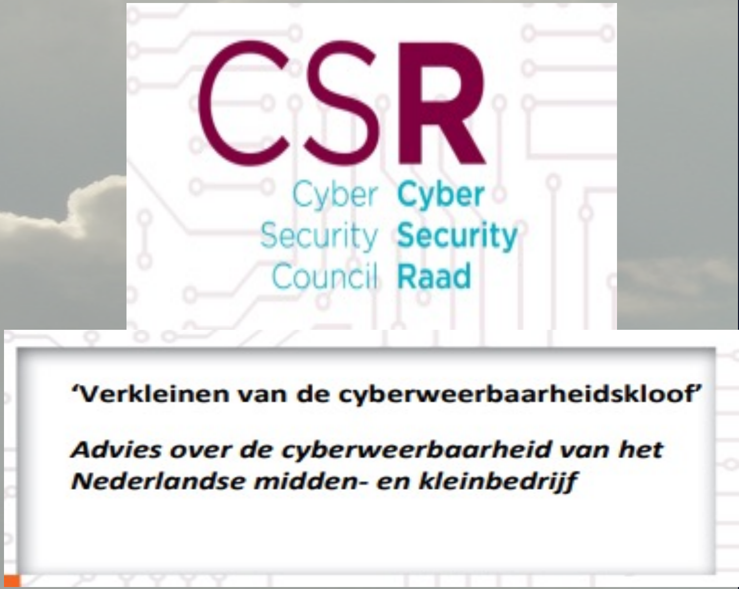
May 14, 2024 6:05 PM GMT+2 · Updated 4 months ago

Dutch Cyber Security Council

June 2024

Advice cyber resilience SME

“SME lack knowledge about cyber risks as well as about what adequate measures are”



CSR

Cyber Security Council

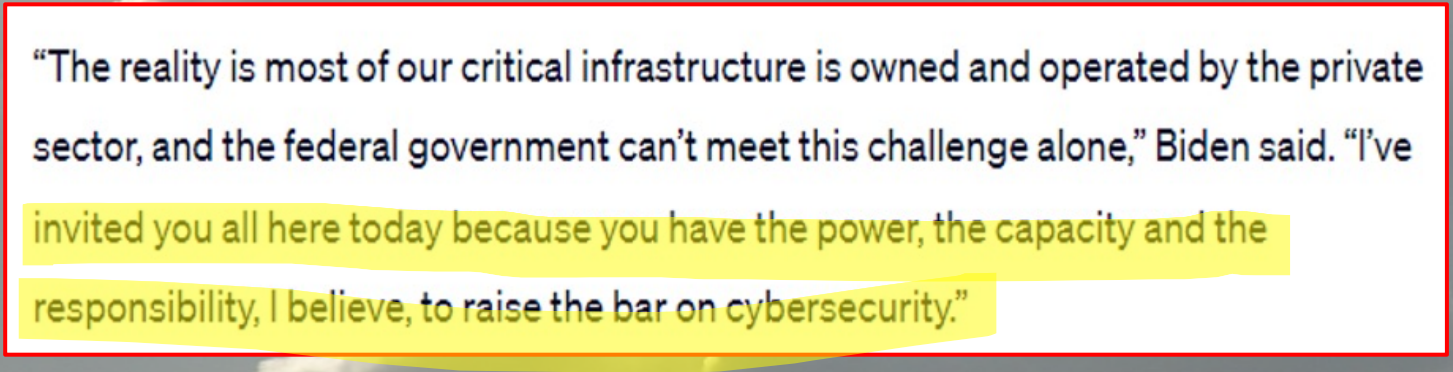
Cyber Security Raad

‘Verkleinen van de cyberweerbaarheidskloof’

Advies over de cyberweerbaarheid van het Nederlandse midden- en kleinbedrijf

President Biden to CEOs Big Tech

August 2021



"The reality is most of our critical infrastructure is owned and operated by the private sector, and the federal government can't meet this challenge alone," Biden said. "I've invited you all here today because you have the power, the capacity and the responsibility, I believe, to raise the bar on cybersecurity."

U.S. National Cybersecurity Strategy

2023

"We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us."

https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/

Digital Sovereignty

Should the EU be worried?

The future of European competitiveness

Part B | In-depth analysis and recommendations

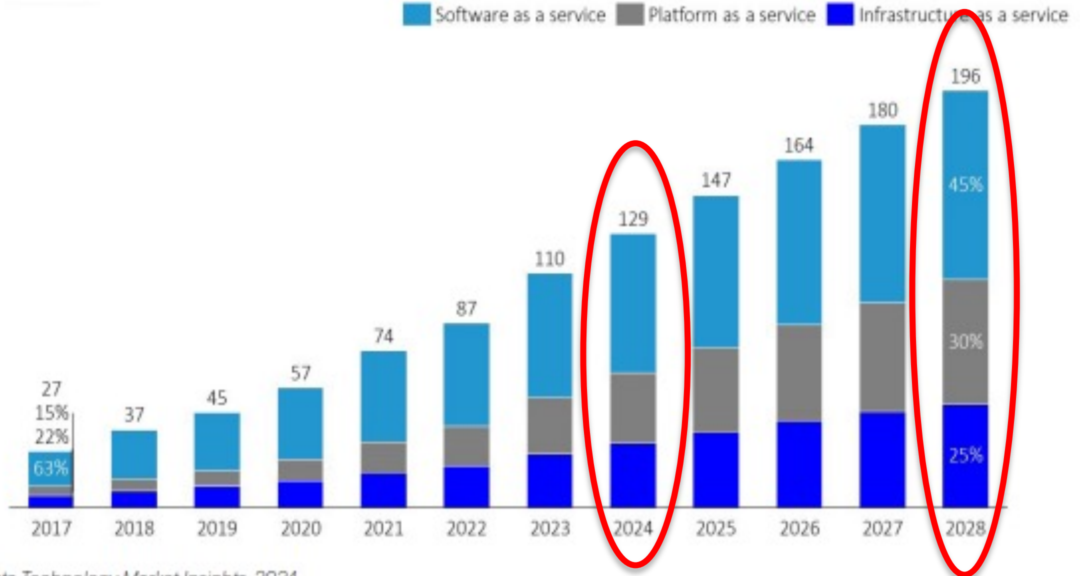
SEPTEMBER 2024

Sept. 2024

FIGURE 6

EU cloud market size

EUR billion



Source: Statista Technology Market Insights, 2024.

The future of European competitiveness

Part A | A competitiveness strategy for Europe

SEPTEMBER 2024

Sept. 2024

- 3 main action areas, incl. increasing security & reducing dependencies
- Too late for EU to develop systemic challengers to US cloud providers

  > “the investments needed are too large and would divert resources away from sectors and companies where the EU’s innovative prospects are better”

- Need to collaborate between EU/US cloud providers to increase security

Managing the world's infrastructure

Cloud (IAAS): 70% market share

Office automation (SAAS): 100% market share

CapEx: 100 $bn/year (2024)

Microsoft

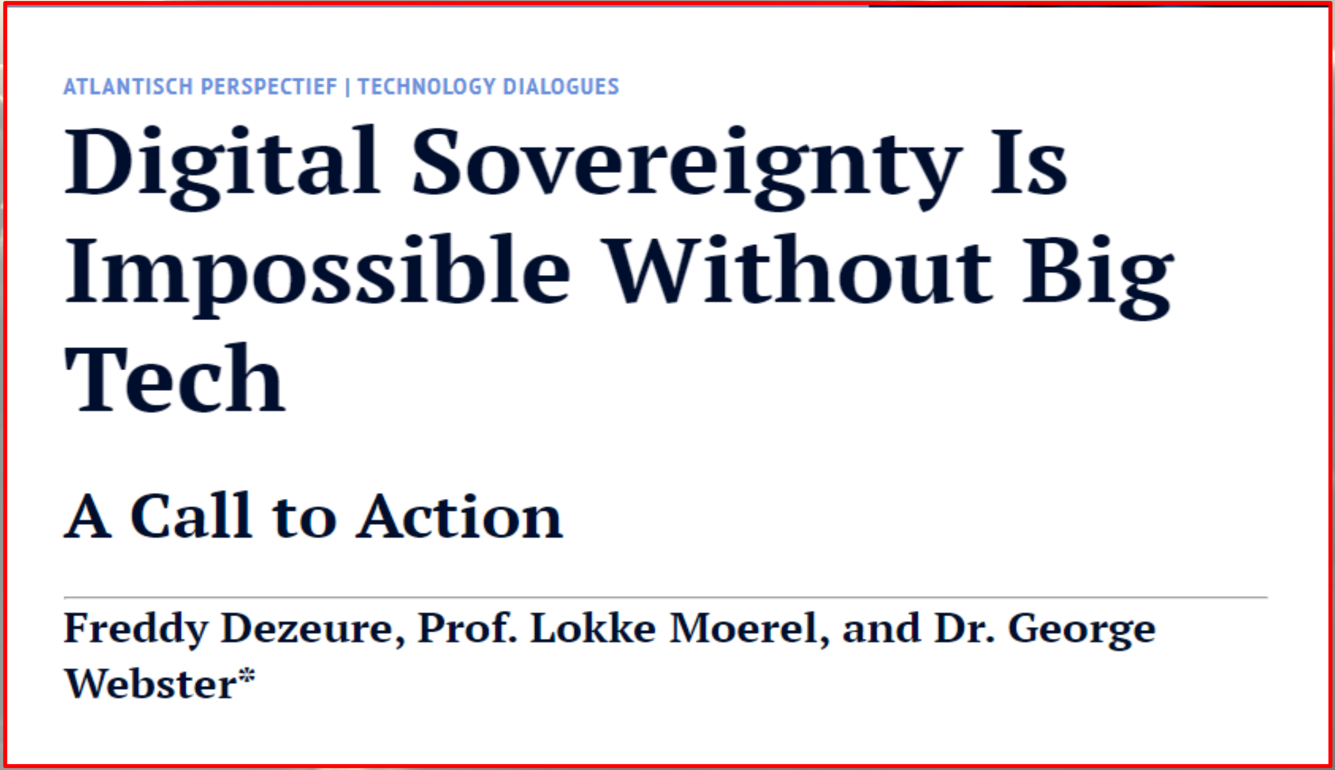
aws

Google Cloud

[Gartner Says Worldwide IaaS Public Cloud Services Revenue Grew 16.2% in 2023]()

[Tech giants pour billions into cloud capacity in AI push]()

Feb. 2024



ATLANTISCH PERSPECTIEF | TECHNOLOGY DIALOGUES

Digital Sovereignty Is Impossible Without Big Tech

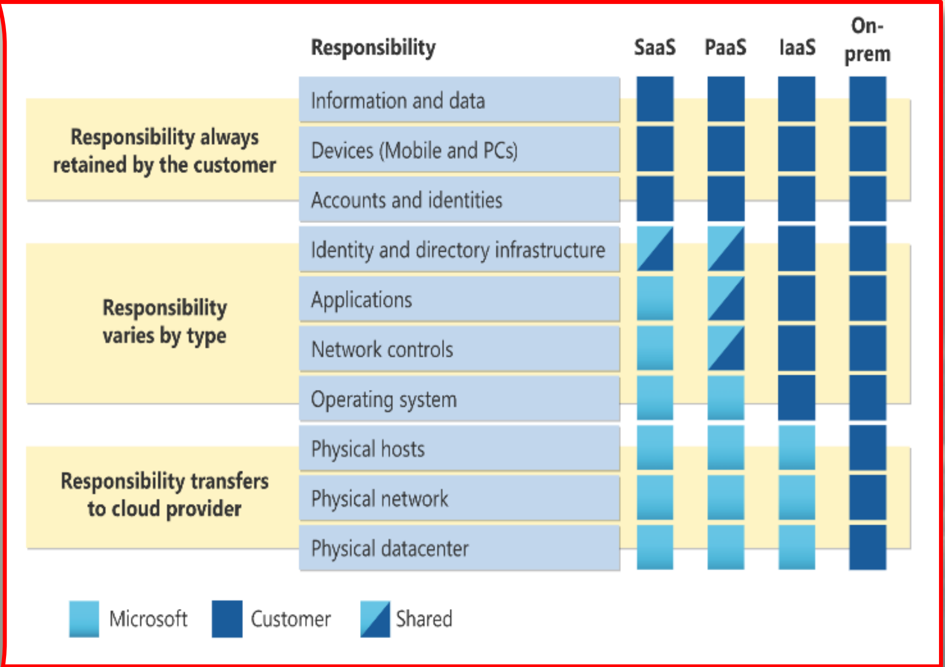
A Call to Action

Freddy Dezeure, Prof. Lokke Moerel, and Dr. George Webster*

What is the issue?

“Shared Responsibility Model”

- CSPs rely on customers to implement secure settings
- Customers lack capacity and expertise
- Most organizations are not / will never be secure
- Thriving economy of criminals hacking our infrastructure and vendors promising to protect it



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

Vendor guidance

https://learn.microsoft.com/en-us/microsoft-365/security/
https://www.microsoft.com/en-us/security
https://aws.amazon.com/security/
https://cloud.google.com/security
https://workspace.google.com/security/

Government guidance

SCuBA

FR
FedRAMP

CyberFundamentals

ASD's Blueprint for Secure Cloud

CIS_Microsoft_365_Foundations_Bench...
Page 1 of 417

CIS. Internet Security®

CIS Benchmarks

CIS Microsoft 365
Foundations Benchmark

v3.1.0 - 04-29-2024

Users

Individual efforts to harden infrastructure:

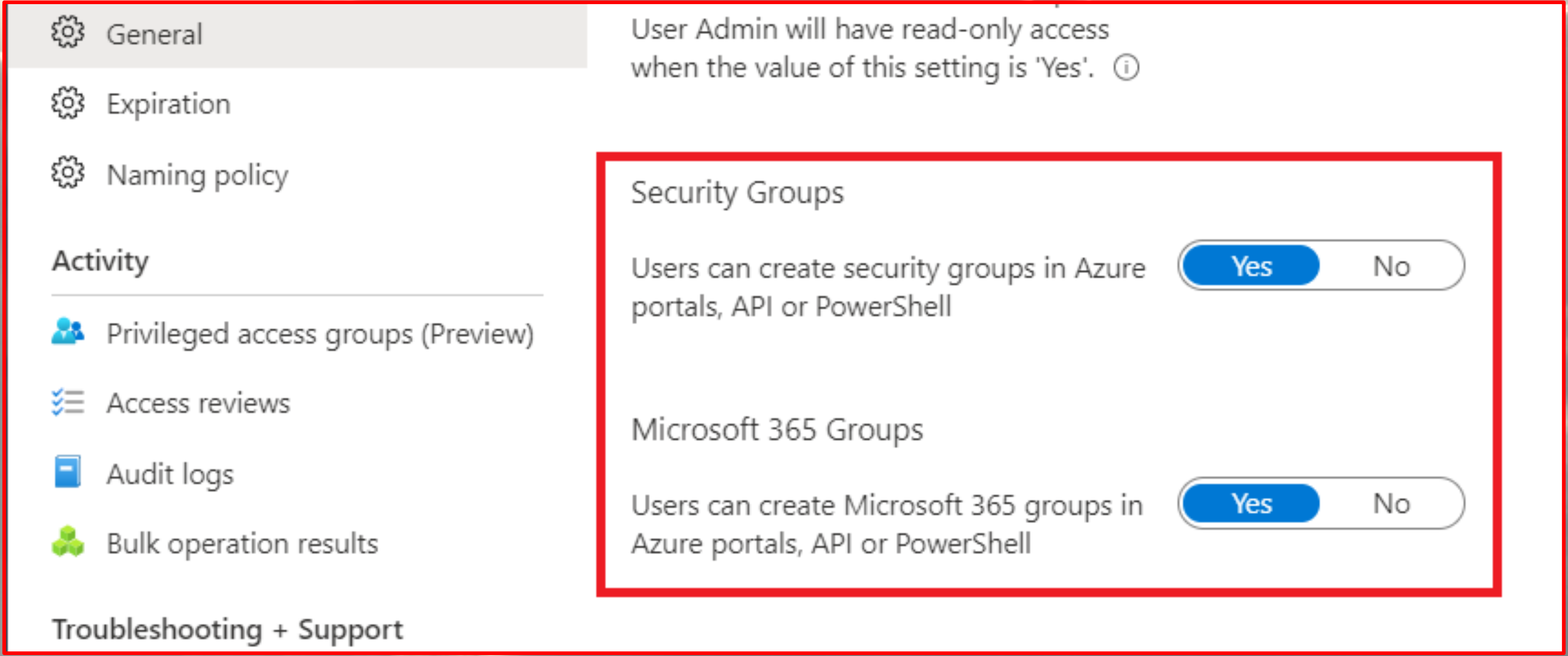
- Internal expertise
- Paid vendor support
- Specialised consultancy

Example lack of SbD

Recent Red Team findings

- Ensure 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'
- Ensure That 'Users Can Register Applications' Is Set to 'No'
- Ensure 'User consent for applications' is set to 'Do not allow user consent’ or Ensure 'User consent for applications' Is Set To 'Allow for Verified Publishers'
- Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'
- Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No’

Recent Red Team



User Admin will have read-only access when the value of this setting is 'Yes'.

Security Groups

Users can create security groups in Azure portals, API or PowerShell [✓ Yes] No

Microsoft 365 Groups

Users can create Microsoft 365 groups in Azure portals, API or PowerShell [✓ Yes] No

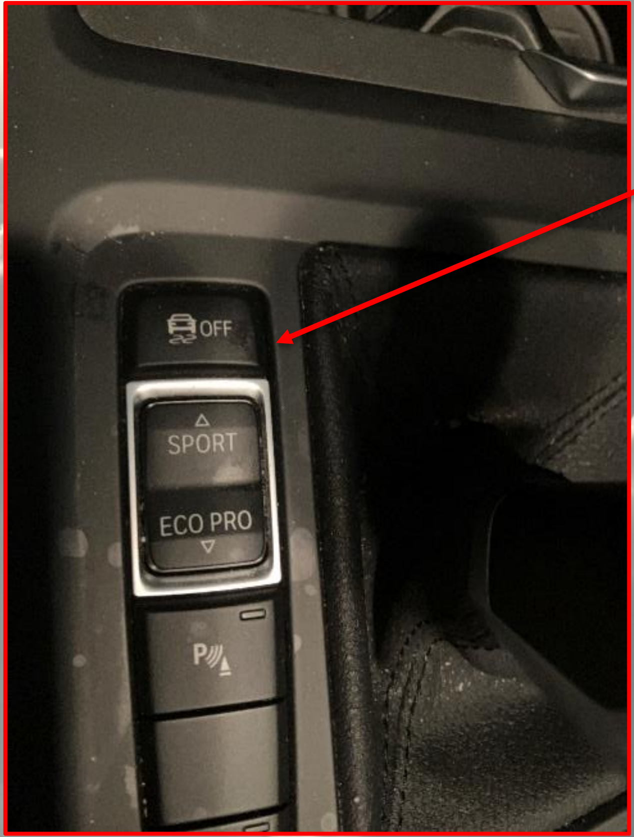
Our call to action

Improving the world’s cyber resilience, at scale
Implementing baseline security by default

Freddy Dezeure, Prof. Lokke Moerel, and Dr. George Webster

https://www.researchgate.net/publication/378213351_Improving_the_world's_cyber_resilience_at_scale_Implementing_baseline_security_by_default

Built-in / opt-out



Tiered approach

- Secure baselines **by default** in the user environment, at no additional cost

- If (1) not possible, implement secure baselines **by workflow**

- If (1) – (2) not possible: offer transparently explained opt-in services (e.g., logging and secure backups)

- Timely warnings if defaults are changed and baseline security is not met

- Higher tiers of protection for specific industries

Community support

Rijksoverheid

National Cyber Security Centre
Ministry of Security and Justice

CENTRE FOR
CYBERSECURITY
BELGIUM

EUROCONTROL

DCSO

ASML

CYBER SECURITY
COALITION.be

etis THE COMMUNITY
FOR TELECOM
PROFESSIONALS

SHARING SINCE 2010 Health-ISAC™
Collaborating for Resilience in Healthcare

cecimo cecimo
European Association of Manufacturing Technologies

Beltug

CIO PLATFORM
NEDERLAND

Cyber
Weerbaarheidscentrum
BRAINPORT

FERM Rotterdam Port
Cyber Resilience

SIEMENS

Allianz

BAYER

thyssenkrupp

AkzoNobel

NN

Henkel

BASF

VOLKSWAGEN
AKTIENGESELLSCHAFT

WÜRTH GROUP

HILTI

Rabobank

FRESENIUS

axel springer_

WACKER

ZF

MCB

KMWE

BYLDIS

Royal
Swinkels

VDL

SCHUBERG
PHILIS

NTS GROUP

TSS total specific solutions
VERTICAL MARKET SOFTWARE

nviso

sata

MATS

MAG
Manchester
Airport

NAV PORTUGAL

Administration de la Navigation Aérienne

Brunel

CANSO

ADR
AEROPORTI DI ROMA

KION
GROUP

Panel Introduction

Marty Smit

ASML

Andreas Rohr

DCSO

Matthijs van Amelsfort

NCSC

Hans de Vries

ENISA

Jack Cable

CISA

Bart Asnot

Microsoft

What are the challenges?

What about

EU laws - NIS2, DORA, CRA?

ENISA Cloud Certification Scheme?

CISA Secure by Design pledge?

MSFT Secure Future Initiative?

CISA's Secure by Design Whitepaper

SECURE BY DESIGN

SHIFTING THE BALANCE OF CYBERSECURITY RISK:

PRINCIPLES AND APPROACHES FOR SECURE BY DESIGN SOFTWARE

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
National Cyber Security Centre
National Cyber Security Centre
CSIRTAmericas Network
NISC
CSA SINGAPORE
certnz
NSM NORWEGIAN NATIONAL CYBER SECURITY CENTRE
National Cyber and Information Security Agency
KISA KOREA INTERNET & SECURITY AGENCY
JPCERT CC

SECURE BY DESIGN

PLEDGE

GOALS

- MULTIFACTOR AUTHENTICATION (MFA)
- DEFAULT PASSWORDS
- REDUCING ENTIRE CLASSES OF VULNERABILITY
- SECURITY PATCHES
- VULNERABILITY DISCLOSURE POLICY
- COMMON VULNERABILITIES AND EXPOSURES (CVE)
- EVIDENCE OF INTRUSIONS

SECURE FUTURE INITIATIVE (SFI)

Secure by design

Security comes first when designing any product or service

Secure by default

Security protections are enabled and enforced by default, require no extra effort, and aren’t optional

Secure operations

Security Controls and monitoring will be continuously improved to meet current and future threats

What is needed (*also from you…*)?

An imperfect market

Vendors

- Profit driven
- Organised by product
- Concerned about legal risks
- Lobbying for status quo

Regulators

- Organised by country/sector
- Slow and static
- Lacking skills
- Influenced by lobbyists

Community

- Mostly representing mature organizations
- Lacking resources

Customers

- Focused on convenience, and cost
- Lacking skills
- Dealing with legacy
- Scattered