Using Lightweight Audit Approaches to Identify Real Security Gaps

GOhack25

Nathan Séville & Dimitri Stanojevic
07.11.2025

adnovum

adnovum.com

Introduce ourselves

Séville Nathan
Security Consultant
nathan.seville@adnovum.ch

Stanojevic Dimitri
Security Consultant
dimitri.stanojevic@adnovum.ch

adnovum

And your digital business works

Massnahmen ergriffen

Cyberkriminelle nehmen KIS-Anbieter Cistec ins Visier

Betrieb läuft normal weiter

Ransomware-Gruppe greift Ascoms Ticketing-System an

RANSOMWARE NEWS

Ransomware Group qilin Hits:

Communication | Published on 18 July 2023

Xplain data leak

The hacker group Akira has intensified its activities in Switzerland. Around 200 companies have fallen victim to ransomware attacks. The damage currently amounts to several million francs and several hundred million dollars worldwide.

October 16, 2025 - 12:05 3 minutes

Cyberat
Adminis

30.06.2025 - The foundation Radix has been targeted by a ransomware attack, during which data was stolen and encrypted. Radix's customers include various federal offices. The data has been published on the dark web and will now be analysed by the relevant offices.

~ 30 total employees

Team of engineers and developers. No security team. CTO, no CISO

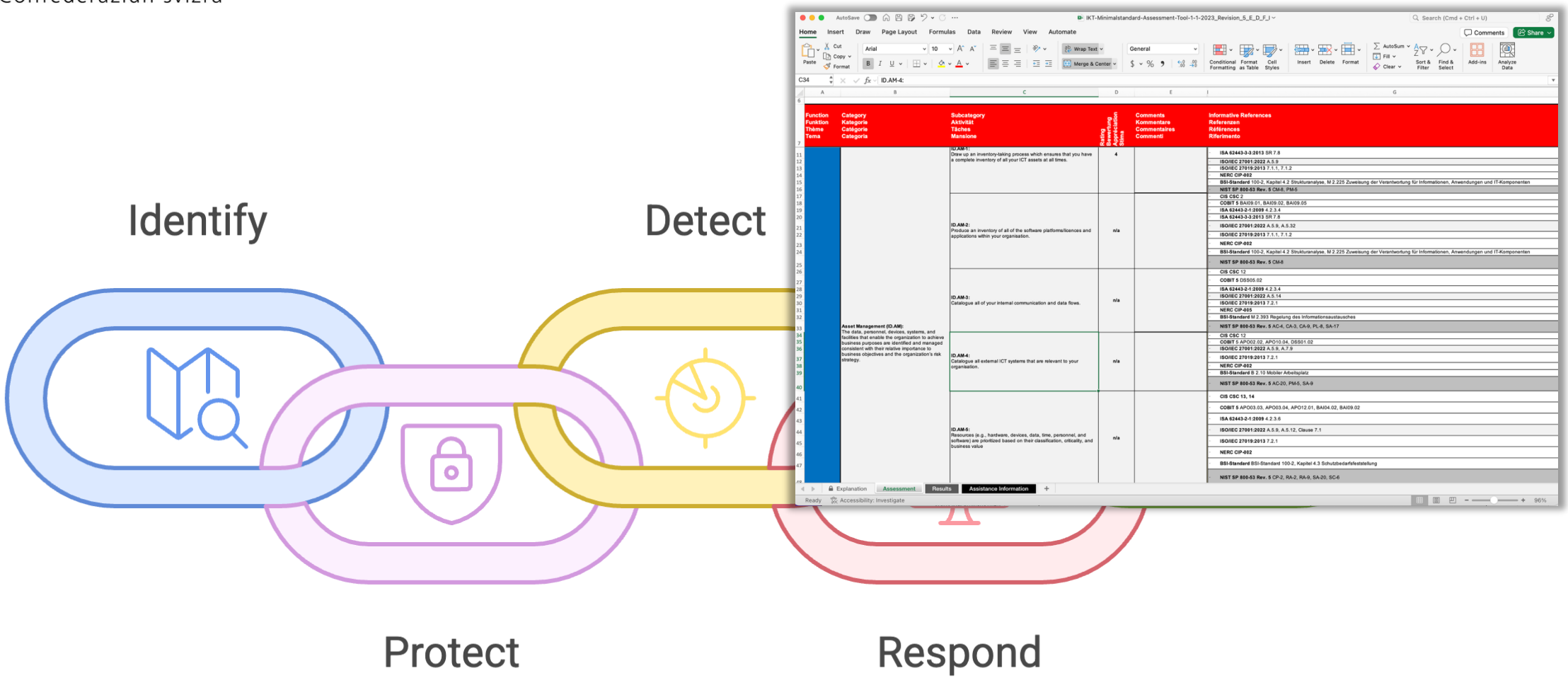
Headquarters in Zurich, Switzerland On-Premise

ll hospitals 20 clinics

Core SaaS platform, backend data storage, integration, internal systems

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

ICT Minimum Standards



A few questions from the assessment tool that can unveil security gaps

ID.AM-1

Draw up an inventory-taking process which ensures that you have a complete inventory of all your **ICT assets** at all times.

ID.AM-2

Produce an inventory of all of the **software platforms/licences** and applications within your organisation.

Inventories can be extended

Confidential information in the wild

ID.AM-3

Catalogue all of your **internal communication** and data flows.

Where is enterprise information exchanged and are there all **secure** ?

No restriction in communication means

How to define which protective measures are relevant

ID.RA-3

Identify and document internal and external cybersecurity threats.

Did you already perform a **threat-analysis** ?

No concrete view of threats

Digital Identities

PR.AC-6

Ensure that digital identities are allocated to **unambiguously** authenticated individuals or processes.

Manage **digital identities** and disable stale ones.

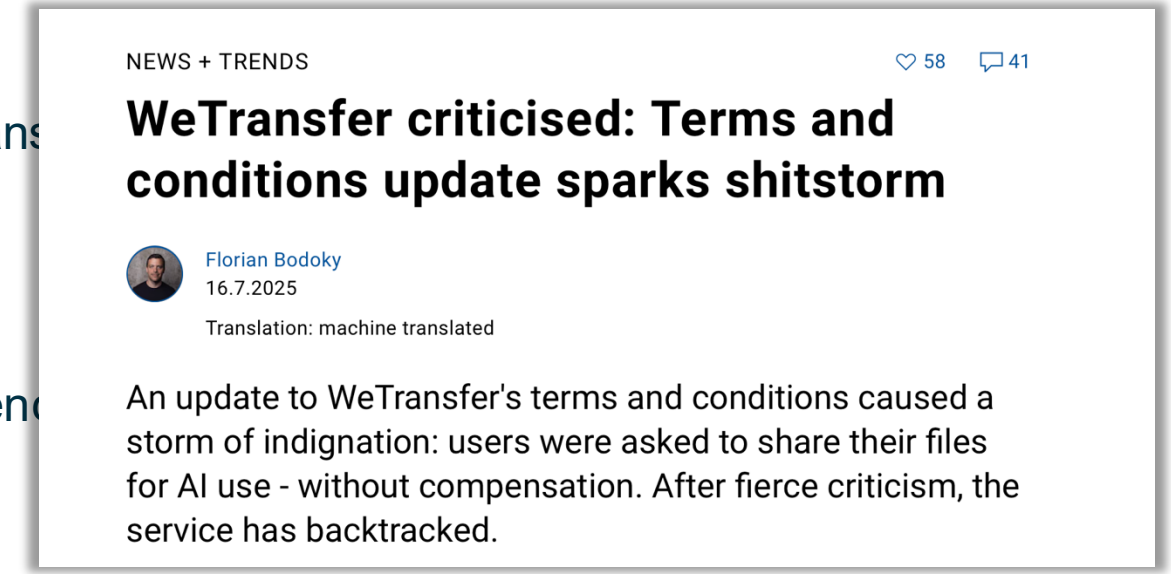
Admin Accounts are shared between employees!

Another example

PR.DS-2

Ensure that data is protected while in trans
availability).

Protect **data in transit** (en



NEWS + TRENDS

58 41

WeTransfer criticised: Terms and conditions update sparks shitstorm

Florian Bodoky
16.7.2025

Translation: machine translated

An update to WeTransfer's terms and conditions caused a storm of indignation: users were asked to share their files for AI use - without compensation. After fierce criticism, the service has backtracked.

Encyrpted VPN, TLS 1.2, internal traffic is encrypted

WeTransfer is not end-to-end encrypted

Questions regarding organisation and responsabilities

DE.DP-1

Define clear roles and responsibilities so that there is no doubt about who is responsible for what, and who holds what authority.

Make sure everyone knows who's **responsible** for what.

Nobody is responsible of checking fishing attempts

Other means of detection

DE.CM-8

Vulnerability scans are performed.

They perform automated scans on their codebase

But not on their internal infrastructure

Incident Response Planning

RS.RP-1

Ensure that the response plan is executed promptly and properly during or after a detected incident.

The incident response plan is five years old and was never battle tested

Incident Recovery

RS.RP-1

Ensure that recovery plans can be executed properly after any cybersecurity incident.

How do you recover your systems after a breach?

System Recovery was never tested

Key Takeaways

- They perform automated scans on their codebase
- Encrypted protocols (VPN, TLS, etc.) are used
- Asset Inventories should be extended
- No restriction on communication mean
- Admin Accounts are shared between employees!
- No vulnerability scans on internal infrastructure
- No overview of potential threats
- Nobody is responsible of checking fishing attempts
- Incident response plan is five years old
- System Recovery was never tested
- WeTransfer is not end-to-end encrypted

Questions ?

adnovum