16.01.2025

HEIDELBERG

Have you noticed the QR codes?

Haben Sie die QR-Codes bemerkt?

SECURITY MASTERS

Cyberattacks on the Printing Industry Market
Cyberangriffe auf den Druckereimarkt

SECURITY MASTERS

Damian Wróblewski

Currently:

- Owner of SECURITY MASTERS (Poland & Ireland branch) – +10 employees, over 300 clients, more than 100 official references.
- Ethical Hacker
- 16+ years of experience in the IT industry, specializing in Microsoft 365 & Cybersecurity
- Microsoft 365 MVP

Historically:

- Former employee at Microsoft Poland & Microsoft Ireland
- Representative of management boards in public and private sector companies for cybersecurity & Microsoft affairs.

MVP Microsoft® Most Valuable Professional

Microsoft Certified Trainer – Microsoft MCT – Trainer – 2021 - 2022

Microsoft Certified Professional – Microsoft MCSA – Office 365 – Earned 2016

Microsoft Certified Professional – Microsoft MCSE – Productivity – Earned 2016

Microsoft 365 Certified – Security Administrator Associate


WI-FI
WI-Fi
OFFICE
OFFUCE
ROUTER
SEUIGE
ROUTER

Example Always Comes from the Top – If, as company leaders, we lack good habits and understanding in the area of cybersecurity, how can we expect our employees to take care of it as well?

Our Statistics on the results of controlled cyber attacks in Europe

+100 organization from 1 – 100.000 employes

SECURITY® MASTERS

Potential consequences of such an attack for the Organization:

- Encryption of all computers and documents
- Loss of access to all organizational systems
- Daily losses amounting to hundreds of thousands of PLN – approximate total losses in the millions* (depending on the organization's size)
- Blackmail & ransom demands
- Leakage of employee and client data, including sensitive information
- PR damage
- Loss of trust among clients
- Loss of critical contracts, impact on P&L
- Opportunity costs, downtime, layoffs, and reduction in staff and salaries
- Potential bankruptcy of the company

SECURITY® MASTERS

Potential consequences of such an attack for the Board member, IT director

In the Polish Penal Code, liability for failure to fulfill duties by board members or IT employees may arise from several provisions, depending on the nature and consequences of the negligence…

SECURITY® MASTERS

Potential consequences of such an attack for the Board member, IT director

Article 296 of the Penal Code – Offense of Breach of Trust:

This provision applies to individuals responsible for managing financial matters or business activities who, by abusing their authority or failing to fulfill their duties, cause significant financial harm.

Scope: Board members and other individuals responsible for the company's financial matters.

Sanctions: Imprisonment from 3 months to 5 years.

Conditions of liability: Causing significant financial harm (exceeding 200,000 PLN) as a result of abusing authority or failing to fulfill duties.

SECURITY® MASTERS

Potential consequences of such an attack for the Board member, IT director

Article 296 of the Penal Code – Offense of Breach of Trust:

This provision applies to individuals responsible for managing financial matters or business activities who, by abusing their authority or failing to fulfill their duties, cause significant financial harm.

Scope: Board members and other individuals responsible for the company's financial matters.

Sanctions: Imprisonment from 3 months to 5 years.

Conditions of liability: Causing significant financial harm (exceeding 200,000 PLN) as a result of abusing authority or failing to fulfill duties.

SECURITY MASTERS

Penalties for Board Members under NIS-2

Financial Penalty

Maximum amount:
600% of the monthly salary

Ban on Holding Board Positions

- **Maximum duration**:
  5 years – for serious violations.
- **Minimum duration**:
  1 year – for less severe violations
  (depending on the assessment of the supervisory authority or court).

SECURITY MASTERS

Client Stories…

Extracts of data from three selected completed reports on Microsoft 365 Environment Audit & Risk Assessment

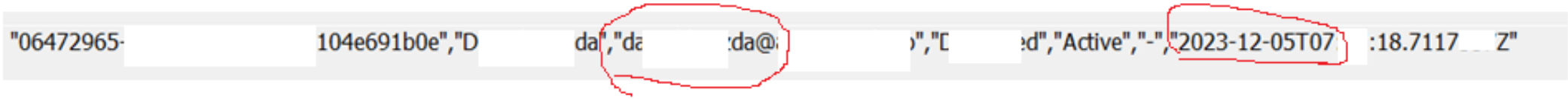
COMPANY No. 1: Microsoft 365 Environment Audit after a Breach

COMPANY No. 2: Microsoft 365 Environment Audit after a Breach

COMPANY No. 3: Microsoft 365 Environment Audit during a Breach

SECURITY® MASTERS

Company 1


"06472965-
104e691b0e","D
da","da
:da@
","[
ed","Active","-","2023-12-05T07
:18.7117
Z"

Company 1

Atakujący sprawdzał zawartość takich witryn jak:

- https://[redacted]my.sharepoint.com/personal/d[redacted]/_layouts/15/filebrowser.aspx
- https://[redacted]-my.sharepoint.com/personal[redacted]
- https://[redacted].sharepoint.com/sites[redacted]/
- https://[redacted].sharepoint.com/sites[redacted]/Shared Documents/Forms/AllItems.aspx
- https://[redacted].sharepoint.com/sites[redacted]/_layouts/15/listhost.aspx
- https://[redacted].sharepoint.com/sites[redacted]/
- https://[redacted].sharepoint.com/sites[redacted]/Shared Documents/[redacted].xlsx
- https://[redacted].sharepoint.com/sites/[redacted]/Shared Documents/Client[redacted]credentials (2).docx

  Dostępy do kont administracyjnych wszystkich serwisów!!!
- https://[redacted]s.sharepoint.com/sites/[redacted]/Shared Documents/[redacted]map.xlsx

  Zmapowane projekty z danymi wrażliwymi klientów
- https://[redacted]sharepoint.com/sites/[redacted]Shared Documents/Requirements/S[redacted]723[redacted]-1.pdf
- https://[redacted]om/sites/[redacted]/_layouts/15/online/handlers/[redacted]Links.ashx
- https://[redacted]sharepoint.com/sites[redacted]/Shared Documents/[redacted]oking
- https://[redacted]s.sharepoint.com/sites/[redacted]/Shared Documents/Requirements/client-self-ser[redacted]xlsx
- https://[redacted]sharepoint.com/sites[redacted]ganization

Atakujący sprawdzał zawartość całej poczty, plików wysłanych i otrzymanych oraz kontaktów e-mail. Następnie atakujący wysyłał głównie dwa typy wiadomości:

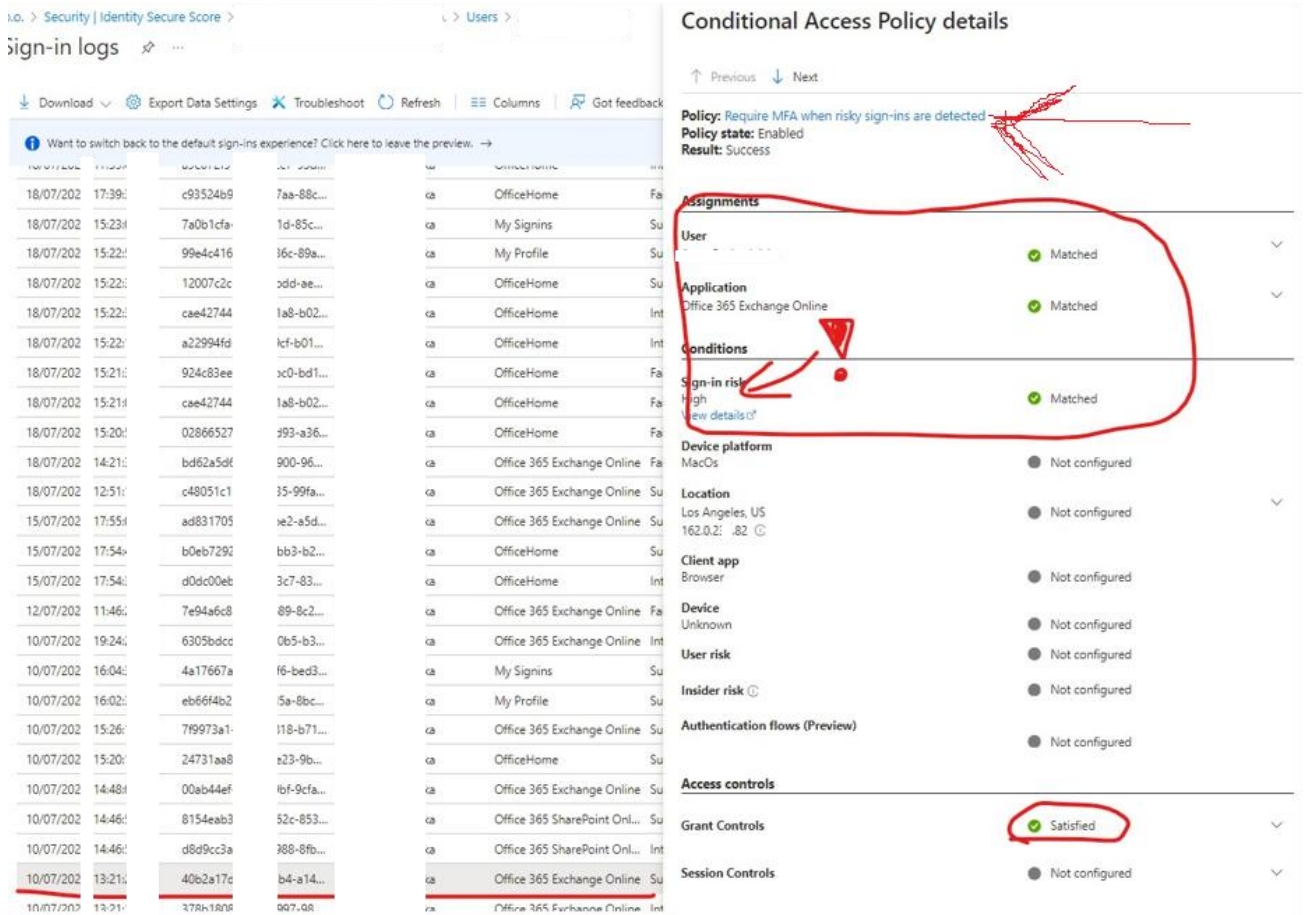
SECURITY MASTERS

Company 1

Atakujący sprawdzał zawartość całej poczty, plików wysłanych i otrzymanych oraz kontaktów e-mail. Następnie atakujący wysyłał głównie dwa typy wiadomości:

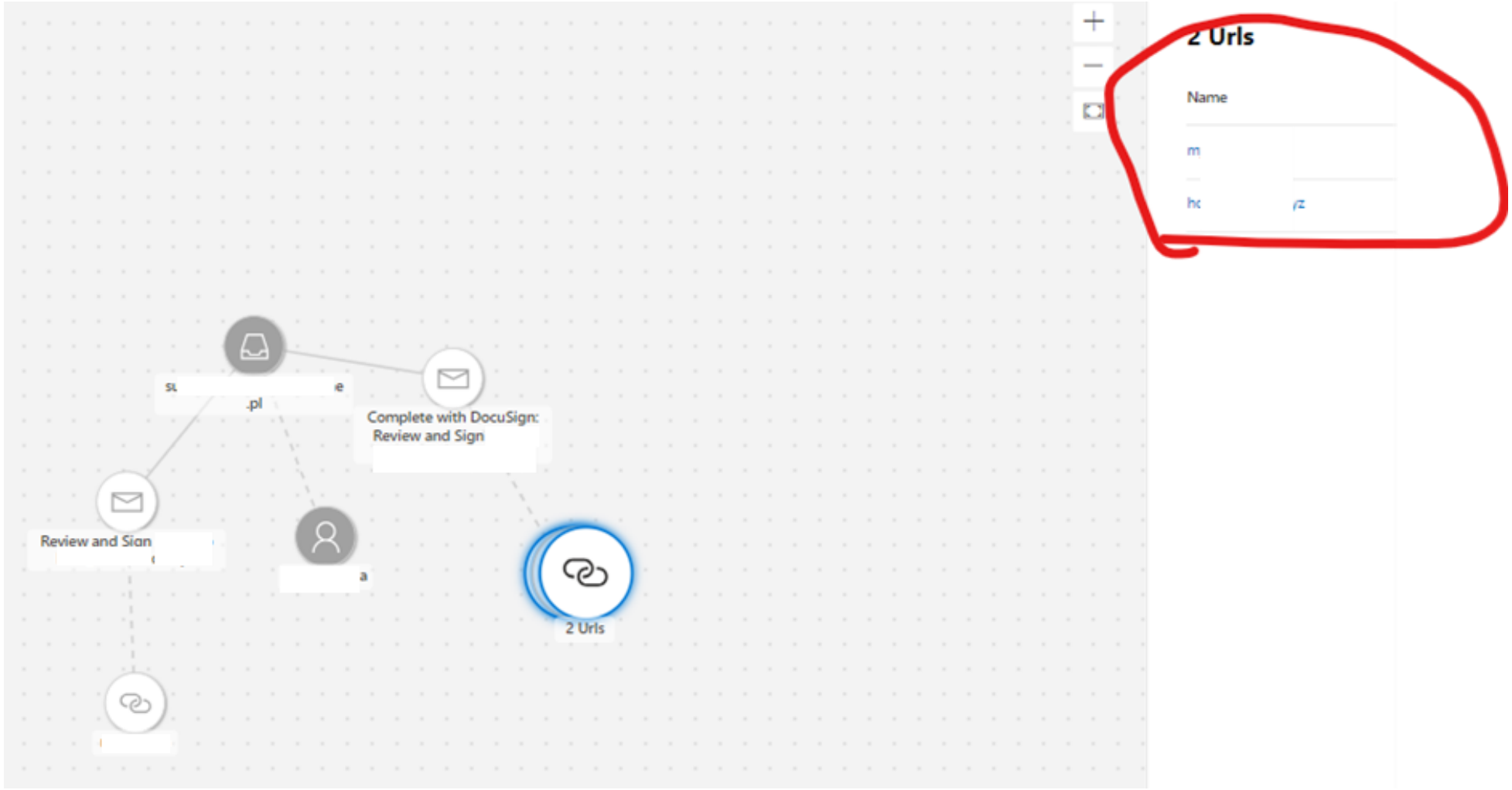
- **Do klientów firmy wysyłając plik PDF informujący o zmianie numer konta bankowego „Subject"":**
  - ""Re: URGENT: IBAN Changes" dokument: Bunq Account Details pdf
  - Subject"":""Re: Payment for outstanding invoices
  - ""Subject"":""Re: Correction to New Bank Details""
  - "Re: Overdue invoices"
  - Subject"":""Revised invoices
  - Subject"":""Credit Note for INV 282""
  - Subject"":""Re: Unpaid invoices"
  - Subject"":""ODP: Invoices"
  - sp. z o.o. Payments
  - Subject"":""Hi What is going on with all the account changes?
    I sent 3 payments to the old account (BUNQ A,..NI 101 5090 32) You informed me that all 3 payments should be transferred back to us because that IBAN was connected to your Polish Zloty ac..."
    - Ten email jest z lutego 1 :3
- **Do pracowników firmy ze złośliwym oprogramowaniem**
  - Np.: Subject"":" Internal daily
  - Subject"":""Wage Increment Form for all Employee -(2\/24
  - ""Subject"":""We noticed a new login to your Todoist account"
  - ""Subject"":""Approved: Salary Ammendment and Benefit Plan for All 2024 -

Company 2



SECURITY® MASTERS

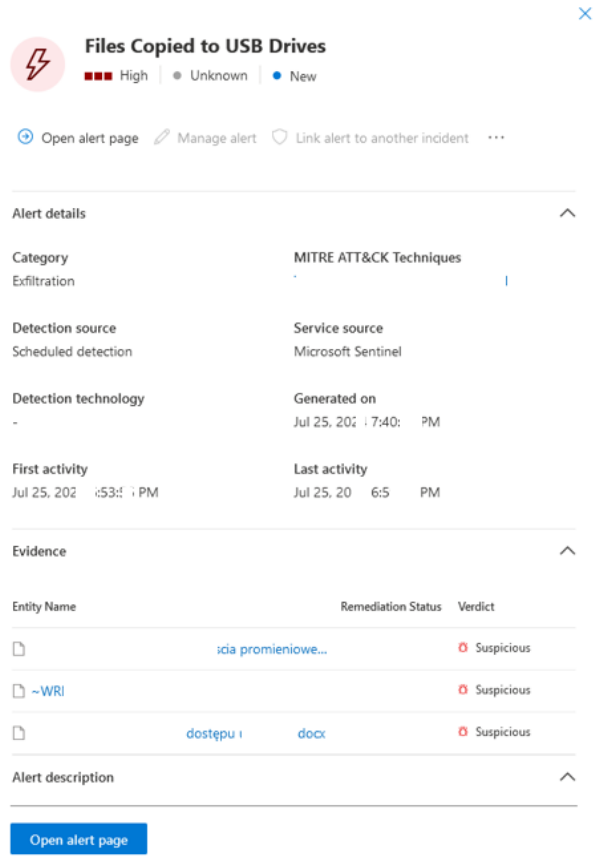
Compromise of a DocuSign account and signing of documents!



SECURITY MASTERS

Company 3

25 lipca o godzinie 18:53 doszło do incydentu. Incydent został wykryty przez Sentinel (jak na obrazku poniżej w „service source”



26 lipca o godzinie 8:41 rano ponownie doszło do incydentu z tej samej kategorii. Doszło do wycieku pliku " .doc".

SECURITY® MASTERS

Client Case No. 1

Number of employees: 50

Industry: HR company

STEP 1: Completed 1-hour free consultation – analysis of the Microsoft 365 environment

STEP 2: Received a thank-you note from the company

STEP 3: Thank-you for the security offer – no agreement for implementation.

SECURITY MASTERS

Approximately 3 months later…

Attack carried out: Man-in-the-Middle (MITM)

STEP 1: Breach into the company and encryption of everything (including backups)

STEP 2: Ransom payment of $30,000 – a "discount" (initial demand: $60,000)

STEP 3: Conflict with cybercriminals

STEP 4: Re-encryption and demand for another ransom!

STEP 5: Incident reported to the police...

STEP 6: Workforce reduction to approximately 18 employees...

SECURITY MASTERS

Client Case No. 2

Number of employees: Approximately 500

Industry: Logistics

STEP 1: Completed 1-hour free consultation – analysis of the Microsoft 365 environment

STEP 2: Received a thank-you note from the company

STEP 3: Thank-you for the security offer – no agreement for implementation…

SECURITY MASTERS


Approximately 2 months later...

Attack carried out: Man-in-the-Middle (MITM)

STEP 1: Breach into the company and sending altered invoices to clients for 22 days, while employees received ransomware!
STEP 2: Financial losses exceeding 2 million PLN (paid invoices sent to fraudulent bank accounts!).
STEP 3: Incident reported to the police and legal firms, which initiated lawsuits – Clients involved.
STEP 4: Loss of a key client, accounting for 10% of the company's total revenue!
STEP 5: Workforce reduction of approximately 35 employees – layoffs including the IT Director and a board member!

Client Case from the Enterprise Segment

(International Corporation)

Number of employees: Approximately 15,000

Industry: Consumer Electronics & Home Appliances

- STEP 1: Completed 1-hour free consultation – analysis of the Microsoft 365 environment in **February 2023!**
- STEP 2: Received a thank-you note from the company
- STEP 3: Thank-you for the security offer – They agreed to a full Microsoft 365 environment audit but wanted to implement the report's findings themselves without assistance from any external company.

SECURITY® MASTERS

Approximately 18 months later…

Attack carried out: Man-in-the-Middle (MITM)

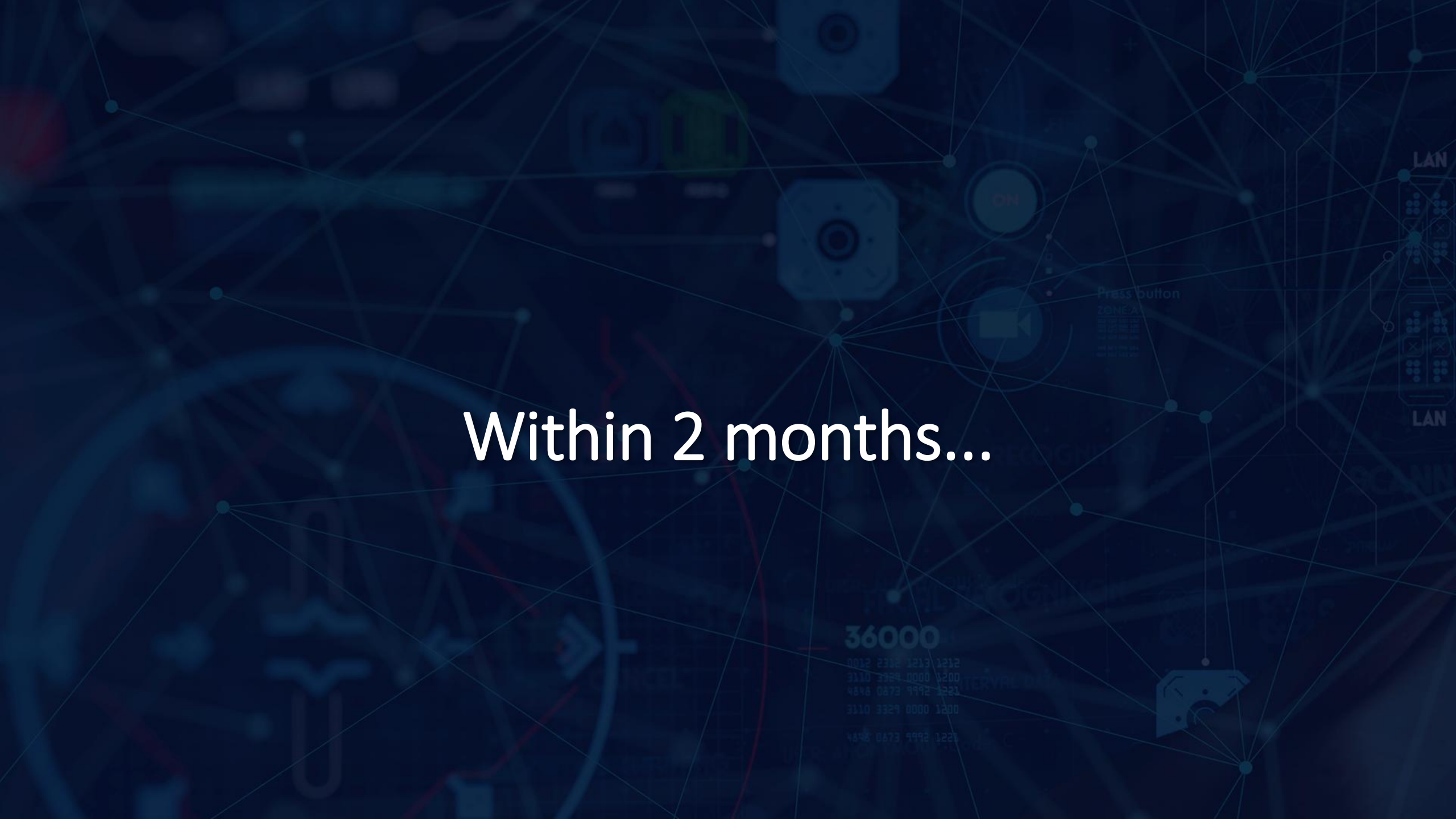
- **STEP 1:** Breach into the company and sending altered invoices to clients for 26 days, while employees received ransomware! Partial encryption of employee computers.
- **STEP 2:** Estimated losses exceed $20 million, plus stolen know-how (paid invoices sent to fraudulent bank accounts!). Ransom payment of $4 million.
- **STEP 3:** It was additionally revealed that company employees did not implement the recommendations, citing other priorities, and what was done for formality contained configuration errors.
- **STEP 4:** The attacker had access for two weeks, starting from a "minor incident" that was dismissed and marked by the MS 365 security team as a false positive (based on internet advice!).
- **STEP 5:** Loss of key clients accounting for 2% of the company's total revenue.
- **STEP 6: Stock market** valuation dropped by approximately 8% in one day.
- **STEP 7:** Workforce reduction of around 200 employees – layoffs across the entire **management tier of the cybersecurity and IT departments.**

SECURITY® MASTERS

A positive story of a 350-employee company

- **STEP 1:** Completed 1-hour free consultation – analysis of the Microsoft 365 environment
- **STEP 2:** Received a thank-you note from the company
- **STEP 3:** Thank-you for the security offer – They agreed!

SECURITY MASTERS


Within 2 months...

STEP 1:

Conducted a **Microsoft 365 Environment Audit & Risk Assessment**

STEP 2:

Implemented the **recommended plan** - MDM system integrated with Identity - strong MFA (Yubico)

STEP 3:

Connected the company to daily, one-time log analysis and monitoring by an administrator, and provided support for Microsoft 365 to IT workers and business employees, all under a subscription plan valued at €999 per month with no hidden costs (**Cheaper than extra hiring an IT employee**).

SECURITY® MASTERS

Just 3 days after completing the implementation!....

STEP 1: The company owner downloaded an application from the internet (he requested less restrictive policies and the ability to act as an IT administrator – this was not recommended).

STEP 2: He downloaded the application and began installing it from a "trusted source."

STEP 3: He dismissed the Windows warning advising against installing the application.

STEP 4: It was a virus! And the trouble began…

STEP 5: …The security measures we implemented, along with support, activated and blocked everything, with the help of 5 team members from our company, who analyzed the situation throughout the weekend.

SECURITY MASTERS

Summary from the Company Owner after the incident:

Now I understand what I paid for. **I didn’t fully grasp** or appreciate it before...

Outcome?

The company owner requested **not to be included** in IT security exceptions after all. :-)

SECURITY® MASTERS

Rules for Safe Use of Personal and Corporate Devices.

Protecting Against Everyday Attacks: Strong Passwords, Updates, Caution in Public Networks, Password Managers, MFA.

Private Devices

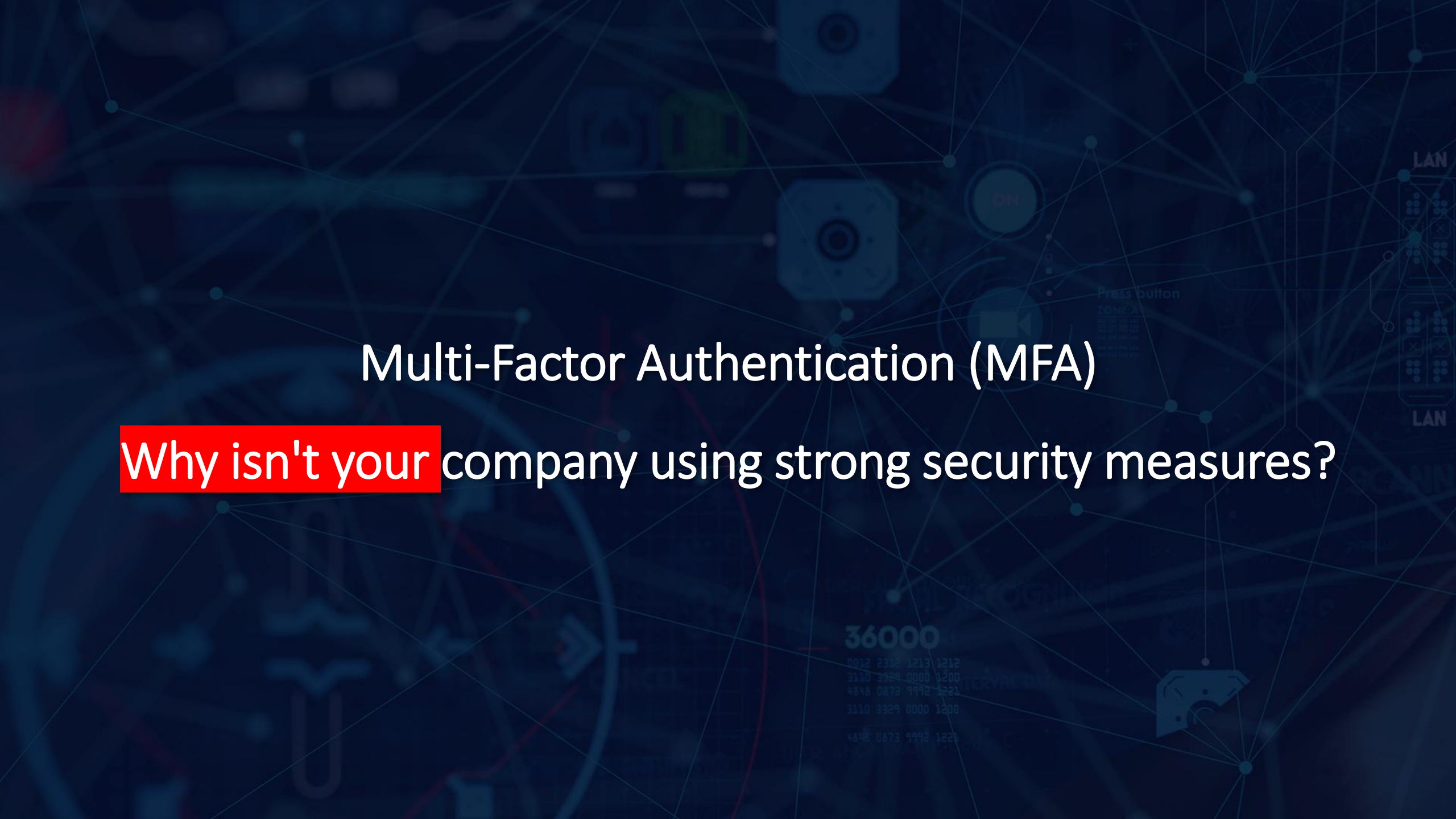
- **Private Laptop** – A portable computer used for personal purposes, such as browsing the internet or working with private documents.
- **Private Desktop Computer** – A computer used at home, e.g., for entertainment or studying.
- **Private Smartphone –** A mobile phone used for personal calls, social media applications, and private tasks.
- **Private Tablet** – A device used for entertainment, social media browsing, watching videos, etc.
- **Private Smartwatch** – A smart watch used for tracking physical activity, receiving notifications, and private messages.
- **Multimedia Devices** – Private Bluetooth speakers, headphones, and media players used in home settings.
- **Gaming Console** – A private device for gaming, which can also connect to the internet.

Corporate devices

- **Company Laptop** – A portable computer issued by the company for professional work.
- **Office Desktop Computer** – A stationary computer used exclusively for business purposes.
- **Company Smartphone** – A mobile phone designated for making calls, sending emails, and using work-related applications.
- **Company Tablet** – A portable device used for working with documents, presentations, and corporate applications.
- **Peripheral Devices** – Printers, scanners, keyboards, and mice dedicated to business use.
- **Networking Equipment** – Routers, modems, and other devices ensuring secure connections to the company network.
- **Security Keys (Hardware Tokens)** – Devices used for multi-factor authentication (MFA) during login to corporate systems.

What connects them?

- Access to corporate data
- Risk of infection with malicious software (malware)
- Phishing, spoofing, and social engineering attacks
- Lack of proper security measures on personal devices
- Shared use of devices
- Protection against loss or theft
- Connecting to unsecured Wi-Fi networks
- Outdated software
- Management of file permissions
- Lack of backups (OneDrive, external drive)


Multi-Factor Authentication (MFA)
Why isn't your company using strong security measures?


Multi-Factor Authentication
Multi-Factor Authentication
MFA
Tranks so MFA
FAKE
PREVENT

Strong Multi-Factor Authentication (MFA)

SECURITY MASTERS

Darknet – How much are we worth to cybercriminals?

Since 2020, at every conference I attend as a speaker and during industry meetings, I present a single challenge…

SECURITY® MASTERS

If a company owner, CEO, board member, or IT director **believes** their organization is **fully secure** and needs **no** improvements, I propose a controlled cyberattack… ☺

SECURITY® MASTERS

If I fail to breach the company's systems during the test, **I will** invite that person to the **finest restaurant** in their hometown – at my expense, of course.

SECURITY MASTERS

For four years, **I haven’t had the chance to treat anyone...**☹

SECURITY MASTERS

Would your company be the first? 🛡️

If you don’t believe it, test it – write to me at **damian@securitymasters.pl**

SECURITY® MASTERS

HEIDELBERG

As a token of appreciation for your participation in the event organized by Heidelberg, I am offering a complimentary **1-hour** cybersecurity consultation for your company.

The consultation will be conducted personally by me
Damian Wróblewski.

This offer is valid only today, during the conference. Simply come over and leave your **business card**.

SECURITY® MASTERS

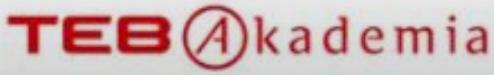
HEIDELBERG

Als Dankeschön für Ihre Teilnahme an der von Heidelberg organisierten Veranstaltung biete ich Ihnen **eine kostenlose** einstündige Beratung im Bereich Cybersicherheit für Ihr Unternehmen an.

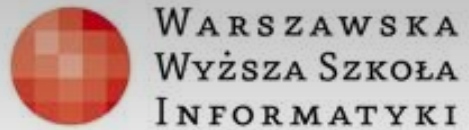
Die Beratung wird persönlich von mir **Damian Wróblewski** – durchgeführt.

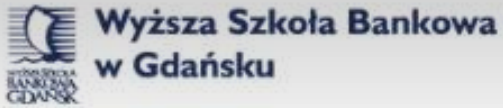
Dieses Angebot gilt nur heute während der Konferenz. Kommen Sie einfach vorbei und hinterlassen Sie Ihre **Visitenkarte.**

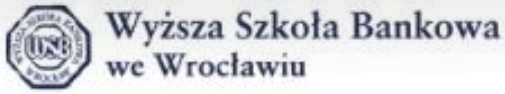
SECURITY® MASTERS



They trusted us.







Thank you!

Contact:

damian@securitymasters.pl

Damian Wróblewski

https://securitymasters.pl