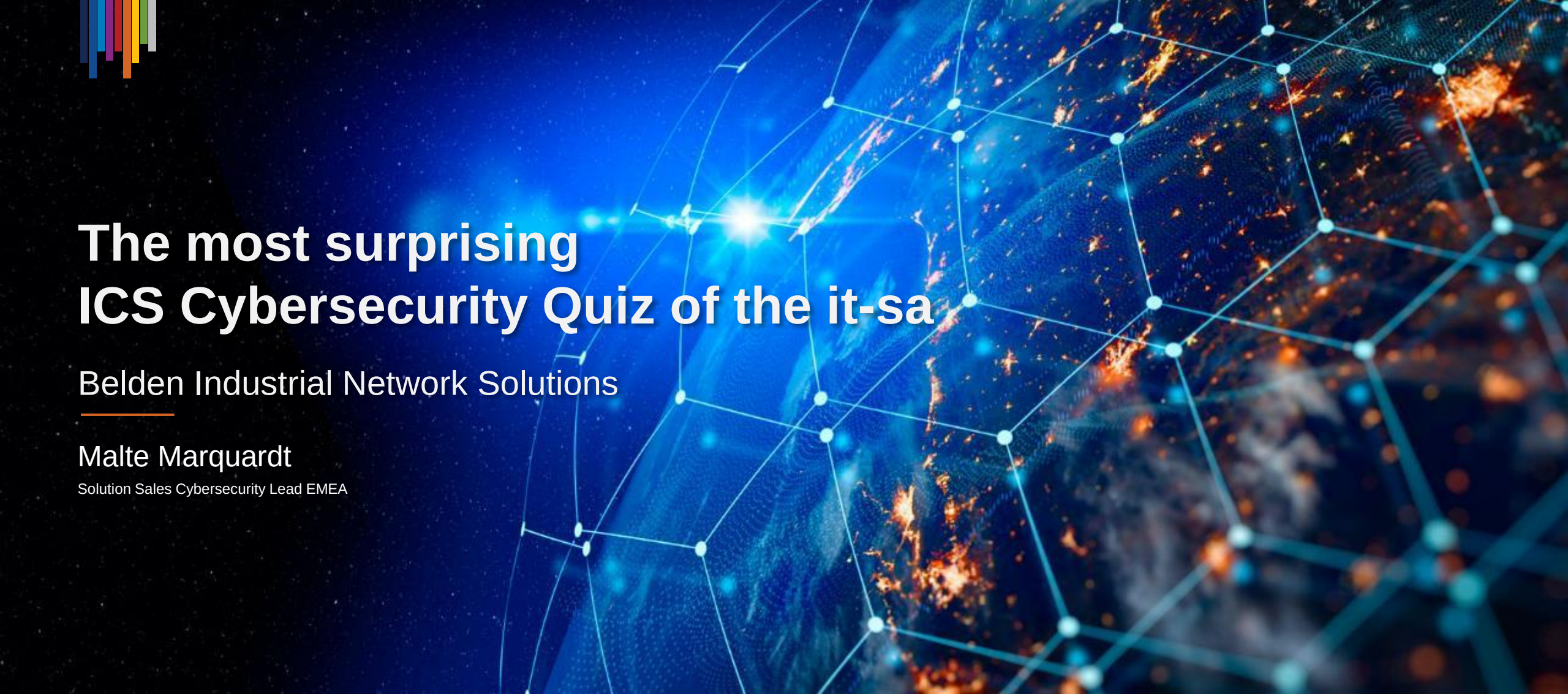

The most surprising ICS Cybersecurity Quiz of the it-sa

Belden Industrial Network Solutions

Malte Marquardt

Solution Sales Cybersecurity Lead EMEA

Welcome to our it-sa **Belden Quizzy Session 2024**

What can you expect from this session?

This is our very first session of this kind & we hope you like it.
We also hope that you are enjoying this years it-sa as much as we do!

Let us guide you through some really interesting cybersecurity stories in a refreshing way.

We want to make sure that you can spend some quality time with us in contrast to your busy it-sa day and all the loaded talks & sessions!

But first, I would like to introduce myself …

A few words about me:

BELDEN

MALTE MARQUARDT

CYBERSECURITY LEAD EMEA

- **First PC** at the age of 10
- **First QBASIC program** at the age of 11
- Aerospace engineering degree
  (because I was not confident enough to study computer science, which I regret today)

- Worked as **engineering consultant** a couple of years, later acted as **regional manager** for a top-tier engineering consultancy

- Always interested in **embedded systems** and **embedded security**

- Researched iOS / LogicBoard / Baseband vulnerabilities **as a hobby** (“iPhone / Jailbreak Community”)

- Came across **ICS Cybersecurity** about five years ago during a consultancy project

- You can call me an **enthusiast**, my family calls me “**our dear tech support**”

Why do we call this „surprising“?

- Quizzes are uncommon for such sessions
- We won’t torture you with sales stuff
- You will leave our session with more than you came with

Before we get started…

Most importantly: **YOU CAN WIN PRIZES!**

But: We all need to follow some simple rules

1. If you know the answer: **Scream as loud as you can!**
2. Everyone is only allowed to **scream one time for each question**.
3. My lovely colleague Myroslava will be our tough judge, she will observe the audience to decide **who gave the correct answer first**.
4. You also **need to briefly explain your choice**!
5. Prizes will be **handed out to the WINNERS at the end** of this session.
6. Everyone can win **only ONE prize max**.

Question 1 ONE

Snack addicted? Here is the solution!

Question **ONE**

A cybersecurity researcher found that **which type of vending machine** could be hacked to dispense free snacks by exploiting its payment system?

ANSWER **A** **Soda machine**

ANSWER **B** **Candy machine**

ANSWER **C** **Coffee machine**

ANSWER **D** **Sandwich machine**

Snack addicted? Here is the solution!

Question **ONE**

A cybersecurity researcher found that **which type of vending machine** could be hacked to dispense free snacks by exploiting its payment system?

ANSWER **A** **Soda machine**

ANSWER **B** **Candy machine** ✓

ANSWER **C** **Coffee machine**

ANSWER **D** **Sandwich machine**


WINNER
PRIZE
1
TIME!

More details about Question **ONE**

What happened?

- A guy started a new job in a company that provided NFC access cards
- The NFC card was used for building access, room booking and as a wallet for vending machines
- He decided to hack the card to explore its capabilities
- Initial scans revealed it was an Infineon MIFARE™ Classic Card 1k, known for being old and insecure
- He found online guides for cracking the card’s private keys
- Using a tool called mfoc, he successfully dumped the keys and data from the card
- He discovered that the vending machine credit was stored directly on the card, rather than on a server
- This allowed him to easily modify the card’s values to obtain free credit for snacks

Question 2 TWO

Air-gapping won’t make you secure in every case!

Question **TWO**

What **unique method** did researchers use in 2020 to demonstrate the **vulnerability of air-gapped industrial systems**?

ANSWER **A** **Drones with Wi-Fi sniffers**

ANSWER **B** **Light commands via smart bulbs**

ANSWER **C** **Sound waves through power supplies**

ANSWER **D** **Magnetic fields from a distance**

Air-gapping won’t make you secure in every case!

Question **TWO**

What **unique method** did researchers use in 2020 to demonstrate the **vulnerability of air-gapped industrial systems**?

ANSWER **A** **Drones with Wi-Fi sniffers**

ANSWER **B** **Light commands via smart bulbs**

ANSWER **C** **Sound waves through power supplies** ✓

ANSWER **D** **Magnetic fields from a distance**


WINNER
PRIZE
2
TIME!

More details about Question **TWO**

What happened?

- Attack to exfiltrate data from air-gapped, audio-gapped systems by turning power supplies into speakers
- Malware manipulates switching frequency of a computer's power supply, causing it to emit acoustic signals
- Acoustic signals carry modulated data (e.g. files, keylogs) which can be received by a nearby infected device like a smartphone
- The attack works over a distance of up to 5 meters, with data transfer rates of 50 bits/sec
- The method doesn’t require speakers or special privileges, making it hard to detect
- This attack scenario demonstrates how to breach even highly secure, isolated systems


Question 3 THREE

When it’s smart, it’s also vulnerable!

Question **THREE**

Which **ordinary type of office machine** was extensively examined by Avast in 2020 to **deploy ransomware to it**?

ANSWER **A** **Printer**

ANSWER **B** **Smart whiteboard**

ANSWER **C** **IP desktop phone**

ANSWER **D** **Coffee machine**

When it’s smart, it’s also vulnerable!

Question **THREE**

Which **ordinary type of office machine** was extensively examined by Avast in 2020 to **deploy ransomware to it**?

ANSWER **A** **Printer**

ANSWER **B** **Smart whiteboard**

ANSWER **C** **IP desktop phone**

ANSWER **D** **Coffee machine** ✓


WINNER
PRIZE
3
TIME!

More details about Question **THREE**

What happened?

- It was identified that the coffee machines firmware lacked basic security measures such as encryption or authentication. This weakness made it vulnerable to remote attacks where anyone with access to the network could control the device.
- By reverse engineering the firmware, it was possible to modify it to introduce malicious code. This involved dissecting the firmware to understand its structure and then injecting new code that would trigger the ransomware behavior.
- By hijacking the firmware update process the modified firmware turned the coffee maker into a ransomware machine, making it unusable and displaying a ransom message until the device was unplugged.
- Various attack vectors were explored, including physical proximity attacks, network-based attacks and social engineering.
- This work highlighted the broader risks associated with IoT devices and the need for better security practices in the development and maintenance of IoT firmware.

How it was done

Question 4 FOUR

Two-factor authentication isn’t secure in every case

Question **FOUR**

In a cyberattack on a **semiconductor company**, hackers used a **very sneaky method** to bypass **two-factor authentication** (2FA). What was their trick?

ANSWER **A** **Provision of fake 2FA codes via phishing emails to employees**

ANSWER **B** **Interception of calls via spoofed phone numbers to bypass 2FA**

ANSWER **C** **Broken into the company to steal hardware-based 2FA tokens**

ANSWER **D** **Placed malware on company printers to log 2FA tokens**

Two-factor authentication isn’t secure in every case

Question **FOUR**

In a cyberattack on a **semiconductor company**, hackers used a **very sneaky method** to bypass **two-factor authentication** (2FA). What was their trick?

ANSWER **A** **Provision of fake 2FA codes via phishing emails to employees**

ANSWER **B** **Interception of calls via spoofed phone numbers to bypass 2FA** ✓

ANSWER **C** **Broken into the company to steal hardware-based 2FA tokens**

ANSWER **D** **Placed malware on company printers to log 2FA tokens**


WINNER
PRIZE
4
TIME!

More details about Question **FOUR**

What happened?

- The attack lasted from 2017 to 2020 and targeted Dutch semiconductor giant NXP™.
- Hackers used spoofed phone numbers to bypass two-factor authentication (2FA), allowing them to access employee accounts.
- They exploited social media data (like LinkedIn leaks) to gather critical information on employees (“OSINT”).
- The group expanded their access within the network and exfiltrated sensitive data via cloud services like Google™ Drive and Dropbox™.
- The attack was only discovered during the investigation of a separate airline hack in 2019.

Let’s wrap-up!

- Always check for the weakest link in your cyber-chain.
  → *exploitation of candy machine*
- Consider that attackers use uncommon attack vectors more and more.
  → *power supply frequency attack*
- New devices and extended connectivity also generate risks, not just opportunities.
  → *coffee machine ransomware*
- Always combine technologies and procedures to build comprehensive defenses
  → *2FA phone spoofing*

All stories to dive deeper

Take a photo and tap on the QR codes later!

1. *exploitation of candy machine*
2. *power supply frequency attack*
3. *coffee machine ransomware*
4. *2FA phone spoofing*

Meet our Security Experts here at the it-sa:

HALL 9 | BOOTH 135