Das überraschendste ICS-Cybersecurity-Quiz der it-sa

Belden Industrial Network Solutions

Malte Marquardt

Solution Sales Cybersecurity Lead EMEA

Ein paar Infos über mich:

BELDEN

MALTE MARQUARDT

CYBERSECURITY LEAD EMEA

- **Erster PC** mit 10 Jahren
- **Erstes QBASIC Programm** mit 11 Jahren
- Studium der Luft- und Raumfahrt
  (weil ich mich nicht traute, Informatik zu studieren, was ich heute bereue)

- einige Jahre als **technischer Berater,** später als **Regionalmanager** für ein bekanntes Engineering Consulting Unternehmen tätig gewesen

- Schon immer interessiert an **Embedded Systems** und **Embedded Security**

- Suche nach iOS / LogicBoard / Baseband Schwachstellen **als Hobby** (“iPhone / Jailbreak Community”)

- vor etwa fünf Jahren während eines Beratungsprojekts auf **ICS Cybersecurity** gestoßen.

- Sie können mich einen **Enthusiasten** nennen, meine Familie nennt mich liebevoll: „**Unser technischer Support**“.


FRAGE
1
EINS

Snacksüchtig? Hier ist die Lösung!

Frage **EINS**

Der Cybersecurity Angestellte eines Unternehmens hat herausgefunden, dass **welche Art von Automat** gehackt werden kann, um durch Ausnutzung des Bezahlsystems kostenlose Waren auszugeben?

ANTWORT **A** **Getränke-Automat**

ANTWORT **B** **Süßigkeiten-Automat**

ANTWORT **C** **Kaffee-Automat**

ANTWORT **D** **Sandwich-Automat**

Snacksüchtig? Hier ist die Lösung!

Frage **EINS**

Der Cybersecurity Angestellte eines Unternehmens hat herausgefunden, dass **welche Art von Automat** gehackt werden kann, um durch Ausnutzung des Bezahlsystems kostenlose Waren auszugeben?

ANTWORT **A** **Getränke-Automat**

ANTWORT **B** **Süßigkeiten-Automat** ✓

ANTWORT **C** **Kaffee-Automat**

ANTWORT **D** **Sandwich-Automat**

Mehr Details zu Frage **EINS**

Was ist passiert?

- Ein Mann hat eine neue Stelle in einem Unternehmen angenommen, das NFC-Zugangskarten anbietet
- Die NFC-Karte wurde für Gebäudezugang, Zimmerbuchung, Geldkarte für Verkaufsautomaten benutzt
- Er beschloss, die Karte zu hacken, um die Möglichkeiten auszutesten
- Erste Scans ergaben, dass es sich um eine MIFARE™ Classic Card 1k handelte, die als alt und unsicher galt
- Er fand online Anleitungen um den privaten Schlüssel der Karte zu knacken
- Mit einem Tool namens mfoc gelang es ihm, die Schlüssel und Daten der Karte zu entschlüsseln
- Er entdeckte, dass das Guthaben des Automaten direkt auf der Karte und nicht etwa auf einem Server gespeichert war
- Dadurch konnte er die Werte der Karte ändern, um kostenlos Guthaben zu erhalten


FRAGE
2
ZWEI

Air-Gapping macht Sie nicht in jedem Fall sicher!

Frage **ZWEI**

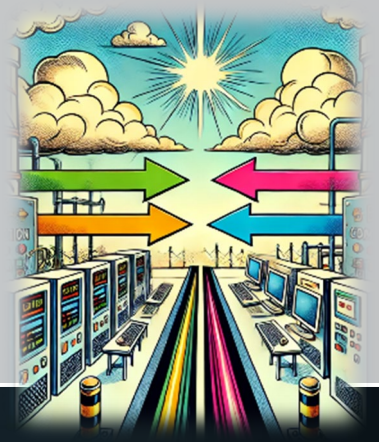
Welche **einzigartige Methode** haben Forscher im Jahr 2020 angewendet, um die **Anfälligkeit** von Industrieanlagen durch **Air-gapping** zu demonstrieren?

ANTWORT **A** **Drohnen mit Wi-Fi-sniffer**

ANTWORT **B** **Lichtbefehle über intelligente Glühbirnen**

ANTWORT **C** **Schallwellen über die Stromversorgung**

ANTWORT **D** **Magnetfelder aus der Ferne**



Air-Gapping macht Sie nicht in jedem Fall sicher!

Frage **ZWEI**

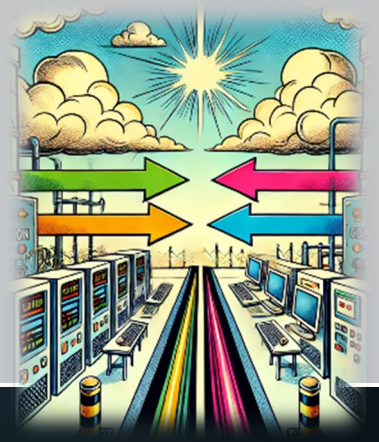
Welche **einzigartige Methode** haben Forscher im Jahr 2020 angewendet, um die **Anfälligkeit** von Industrieanlagen durch **Air-gapping** zu demonstrieren?

ANTWORT **A** **Drohnen mit Wi-Fi-sniffer**

ANTWORT **B** **Lichtbefehle über intelligente Glühbirnen**

ANTWORT **C** **Schallwellen über die Stromversorgung** ✓

ANTWORT **D** **Magnetfelder aus der Ferne**



Mehr Details zu Frage **ZWEI**

Was ist passiert?

- Angriff, um Daten aus abgekapselten Systemen zu exfiltrieren, indem Netzteile in Lautsprecher umgewandelt werden
- Eine Malware manipuliert die Schaltfrequenz des Netzteils eines Computers und veranlasst sie akustische Signale abzugeben
- Akustische Signale übertragen modulierte Daten (z.B. Dateien, Keylogs), die von einem infizierten Gerät in der Nähe, z.B. einem Smartphone, empfangen werden können
- Der Angriff funktioniert über eine Entfernung von bis zu 5 Metern mit einer Datenübertragungsrate von 50 bits/Sekunde
- Die Methode erfordert keine Lautsprecher oder besondere Privilegien, so dass sie sehrschwer zu entdecken ist
- Dieses Angriffsszenario zeigt, wie man selbst hochsichere, isolierte Systeme angreifen kann.


FRAGE
3
DREI

Wenn es smart ist, ist es auch angreifbar!

Frage **DREI**

Welches **gewöhnliche Büro-Gerät** wurde von Avast im Jahr 2020 ausgiebig untersucht, um **Ransomware darauf zu installieren**?

ANTWORT **A** **Drucker**

ANTWORT **B** **Smart Whiteboard**

ANTWORT **C** **IP-Desktop-Telefon**

ANTWORT **D** **Kaffeemaschine**

Wenn es smart ist, ist es auch angreifbar!

Frage **DREI**

Welches **gewöhnliche Büro-Gerät** wurde von Avast im Jahr 2020 ausgiebig untersucht, um **Ransomware darauf zu installieren**?

ANTWORT **A** **Drucker**

ANTWORT **B** **Smart Whiteboard**

ANTWORT **C** **IP-Desktop-Telefon**

ANTWORT **D** **Kaffeemaschine** ✓

Mehr Details zu Frage **DREI**

Was ist passiert?

- Es wurde festgestellt, dass die Firmware der Kaffeemaschinen grundlegende Sicherheitsmaßnahmen wie Verschlüsselung oder Authentifizierung vermissen ließ. Diese Schwachstelle machte sie anfällig für Fernangriffe, bei denen jeder, der Zugang zum Netzwerk hatte, das Gerät steuern konnte.
- Durch Reverse Engineering der Firmware war es möglich, sie zu modifizieren und einen schädlichen Code einzuschleusen, indem die Firmware analysiert wurde, um ihre Struktur zu verstehen und dann einen neuen Code einzuschleusen, der das Verhalten der Ransomware auslösen sollte.
- Indem die modifizierte Firmware den Prozess der Firmware-Aktualisierung manipulierte, verwandelte sie die Kaffeemaschine in eine Ransomware-Maschine, die sie unbrauchbar machte und eine Lösegeldnachricht anzeigte, bis das Gerät vom Stromnetz getrennt wurde.
- Es wurden verschiedene Angriffsvektoren erforscht, darunter Angriffe aus der Nähe, netzwerkbasierte Angriffe und Social Engineering
- Diese Arbeit verdeutlichte die allgemeinen Risiken im Zusammenhang mit IoT-Geräten und die Notwendigkeit besserer Sicherheitspraktiken bei der Entwicklung und Wartung von IoT-Firmware.


Frage 4 VIER

Eine Zwei-Faktor-Authentifizierung ist nicht in jedem Fall sicher!

Frage **VIER**

Bei einem Cyberangriff auf ein **Halbleiterunternehmen** verwendeten Hacker eine **raffinierte Methode**, um die **Zwei-Faktor-Authentifizierung** (2FA) zu umgehen. Was war ihr Trick?

ANTWORT **A** **Weitergabe von gefälschten 2FA-Codes über Phishing E-Mails an Mitarbeiter**

ANTWORT **B** **Abfangen von Anrufen über gefälschte Telefonnummern zur Umgehung der 2FA**

ANTWORT **C** **Einbruch in das Unternehmen, um hardwarebasierte 2FA-Tokens zu stehlen**

ANTWORT **D** **Malware auf Unternehmensdruckern platziert, um 2FA-Tokens zu protokollieren**

Eine Zwei-Faktor-Authentifizierung ist nicht in jedem Fall sicher!

Frage **VIER**

Bei einem Cyberangriff auf ein **Halbleiterunternehmen** verwendeten Hacker eine **raffinierte Methode**, um die **Zwei-Faktor-Authentifizierung** (2FA) zu umgehen. Was war ihr Trick?

ANTWORT **A** **Weitergabe von gefälschten 2FA-Codes über Phishing E-Mails an Mitarbeiter**

ANTWORT **B** **Abfangen von Anrufen über gefälschte Telefonnummern zur Umgehung der 2FA** ✓

ANTWORT **C** **Einbruch in das Unternehmen, um hardwarebasierte 2FA-Tokens zu stehlen**

ANTWORT **D** **Malware auf Unternehmensdruckern platziert, um 2FA-Tokens zu protokollieren**

Mehr Details zu Frage **VIER**

Was ist passiert?

- Der Angriff dauerte von 2017-2020 und richtete sich Gegen den niederländischen Halbleiterriesen NXP™
- Die Hacker nutzten gefälschte Telefonnummern, um die Zwei-Faktor-Authentifizierung (2FA) zu umgehen, und konnten so auf Mitarbeiterkonten zugreifen
- Sie nutzten Social-Media-Daten (wie LinkedIn-Leaks), um wichtige Informationen über Mitarbeiter zu sammeln (“OSINT”).
- Die Gruppe erweiterte ihren Zugang innerhalb des Netzwerks und exfiltrierte sensible Daten über Cloud-Dienste wie Google™ Drive und Dropbox™.
- Der Angriff wurde erst während einer Untersuchung eines seperaten Airline-Hacks im Jahr 2019 entdeckt.

Wrap-Up!

- Suchen Sie immer nach dem schwächsten Glied in Ihrer Cyber Kette!
  → *Ausbeutung des Süßigkeiten-Automats*
- Bedenken Sie, dass Angreifer immer häufiger auch ungewöhnliche Angriffsvektoren verwenden
  → *Angriff auf die Netzfrequenz*
- Neue Geräte und erweiterte Konnektivität bieten nicht nur Chancen, sondern auch Risiken.
  → *Kaffeemaschinen-Ransomware*
- Kombinieren Sie stets Technologien und Verfahren, um einen umfassenden Schutz aufzubauen
  → *2FA Telefon-Spoofing*

Alle vier Cybersecurity-Fälle zum Nachlesen:

Machen Sie ein Foto und tippen Sie später auf die **QR-Codes!**

1. *Ausbeutung des Süßigkeiten-Automats*
2. *Angriff auf die Netzfrequenz*
3. *Kaffee-maschinen Ransomware*
4. *2FA Telefon-Spoofing*

Treffen Sie unsere Security-Experten hier auf der it-sa:

HALLE 9 | STAND 135