qSk!lls
innovation through education

Lautlos gehackt:

Ein Desaster in 5 Akten - und was Sie daraus lernen sollten

whoami - Björn Trappe

- Co-Gründer & Geschäftsführer von Laokoon Security GmbH
- Projektleitung Pentest / Red Teaming
- Kapitänleutnant a.D
  - Bundeswehr Zentrum Cyber Operationen
  - Weitere deutsche Sicherheitsbehörde

bjoern.trappe@laokoon-security.com

© qSkills GmbH & Co. KG, 2025

⚠️ Disclaimer ⚠️

- Die folgenden Inhalte basieren auf **realen Vorfällen aus dem letzten Jahr**.
- Es handelt sich um eine Auswahl der **häufigsten und eindrücklichsten Szenarien**, die wir in Unternehmen beobachtet haben.
- **Alle Namen, Details und Umgebungen sind anonymisiert** – Ziel ist nicht, einzelne Organisationen bloßzustellen, sondern die **Lernmomente und Muster** zu verdeutlichen.
- Die gezeigten Beispiele sollen **Awareness schaffen** und verdeutlichen, wie technische Schwächen, menschliche Routinen und organisatorische Lücken zusammenspielen.

👉 Kurz gesagt: **Echte Angriffe, echte Risiken**

© qSkills GmbH & Co. KG, 2025

Portfolio — Kraftwerk-Manufaktur.de

Kernfakten

- **Gegründet**: 1971
- **Mitarbeitende**: ~200 (Produktion, F&E, Service, Verwaltung)
- **Standorte**: HQ Bonn (Produktion & Verwaltung) + kleines Werk / Testcenter
- **Zielmärkte**: Maschinenbau-OEMs, Retrofit-Projekte, After-Sales Deutschland & EU

© qSkills GmbH & Co. KG, 2025

Portfolio — Kraftwerk-Manufaktur.de

Technologie & Digitalisierung

- **Hybrid-IT**: On-prem AD seit 2006, Entra ID / Azure AD (Hybrid, SSO) seit Corona
- **Device Management**: Intune für Office-Endpoints, Produktions-IT teilweise isoliert
- **Fertigung**: CNC-Zentren, Prüfstände, automatisierte Montageinseln
- **Monitoring**: Basis-SIEM / EDR in Verwaltung; SCADA/OT-Segmente separiert

© qSkills GmbH & Co. KG, 2025

Letzter „Pentest"

OpenVas Vulnerability Report — Kraftwerk-Manufaktur.local

Summary

This document reports on the results of an automatic security scan. The report first summarises the results found. Then, for each host, the report describes every issue found. Please consider the advice given in each description, in order to rectify the issue.

It only lists hosts that produced issues.

All dates are displayed using the timezone "Coordinated Universal Time", which is abbreviated "UTC".

Scan started: **Mon Dec 7 12:51:47 2015 UTC**
Scan ended:
Task: ad.kraftwerk-manufaktur.local

Vulnerability Summary

HIGH 2 | MEDIUM 8 | LOW 0

Any **HIGH** and **MEDIUM** risk vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be stepping stones to High risk attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log	False Positive
ad	Dec 7, 12:51:52	(not finished)	2	8	0	23	0
Total: 1			2	8	0	23	0

Results per Host

Host ad.kraftwerk-manufaktur.local

Scanning of this host started at: Mon Dec 7 12:51:52 2015 UTC
Number of results: 33

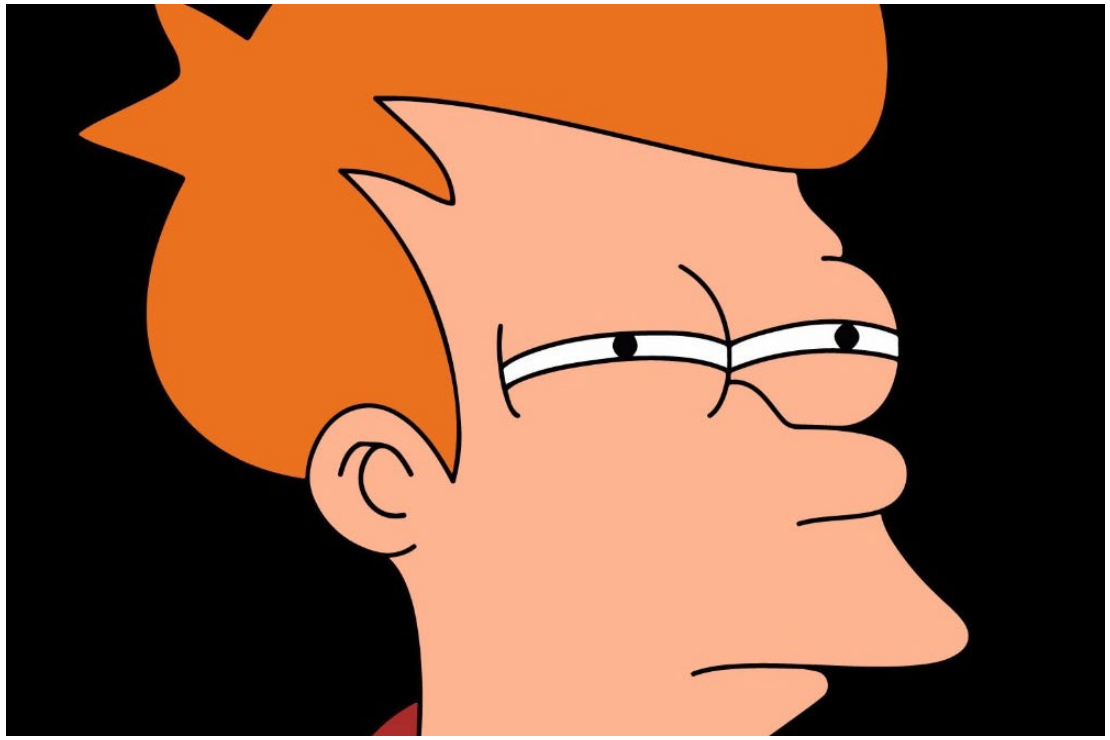
Port Summary for Host 87.230.29.167

Service (Port)	Threat Level
80/tcp	High
139/tcp	Log
3389/tcp	Medium
general/SMBClient	Log
135/tcp	Medium
general/icmp	Log
general/tcp	Log
8443/tcp	Medium

PAGE 3 of 871

3 of 871

Wem kommt das bekannt vor?



Vorlage für ein deutsches Familienunternehmen.

© qSkills GmbH & Co. KG, 2025

Akt I
Der stille Schlüssel

© qSkills GmbH & Co. KG, 2025

THEORIE

- Der häufigste Angriffsvektor ist nicht der Zero-Day, sondern der Missbrauch von *bekannten* Zugangsdaten.

- **Angriffsphase**: *Initial Access & Credential Access.*
- **Verteidigung:** Multi-Faktor-Authentifizierung, Credential-Monitoring, Erkennung ungewöhnlicher Logins, Passwort-Manager.

© qSkills GmbH & Co. KG, 2025

Gesicht zu den Passwörtern

Matches

email	username	fullname	password	source	image
j.schmidt@kraftwerk-manufaktur.de	j.schmidt	Julia Schmidt	`TokioHotelFan91`	public_paste/images	images/juliaschmidt.png
k.mueller@kraftwerk-manufaktur.de	k.mueller	Klaus Mueller	`Password123!`	public_paste/images	images/klausmueller.png
markus.weber@kraftwerk-manufaktur.de	m.weber	Markus Weber	`Qwertz!2022`	internal_leak_sim	images/markusweber.png
tobias.braun@kraftwerk-manufaktur.de	t.braun	Tobias Braun	`Kraftwerk!123`	phishing_dump	images/t_braun_01.jpg
anna.hoffmann@kraftwerk-manufaktur.de	a.hoffmann	Anna Hoffmann	`Welcome2024!`	vector_dump	images/a_hoffmann_01.jpg
support@kraftwerk-manufaktur.de	support	Support Team	`HelpDesk!2020`	leaked_helpdesk	images/support_01.jpg

Social Profiles

j.schmidt@kraftwerk-manufaktur.de

LinkedIn — j.schmidt71

© qSkills GmbH & Co. KG, 2025

Learnings

- Gestohlene Credentials sind einer der häufigsten Einstiegsvektoren.
- MFA und Passwort-Manager reduzieren die Angriffsfläche massiv.
- Credential Monitoring (Darknet, Paste-Sites) ist Pflicht für jedes Unternehmen.

- Der Angreifer bestimmt was er aus den Informationen macht
- Innentäter / Phishing / Erpressung sind valide Methode im Cyber Crime Umfeld

© qSkills GmbH & Co. KG, 2025

Akt II
Schatten im Netz

© qSkills GmbH & Co. KG, 2025

THEORIE

- Mit gültigen Zugangsdaten können Angreifer sich unauffällig einloggen und erste Befehle absetzen.
- Dafür wird meist ein Command & Control (C2)-Framework genutzt, wie Mythic, Cobalt Strike oder andere.

- **Angriffsphase**: *Execution, Persistence, Command & Control.*
- **Verteidigung:** Network-Detection, TLS-Inspection, EDR mit Beaconing-Erkennung, Zero-Trust-Zugänge.

© qSkills GmbH & Co. KG, 2025

Learnings

- Jeder initiale Zugang kann durch C2-Infrastruktur ausgebaut werden.
- Unauffälliger, verschlüsselter Traffic ist die Norm – reine Firewall reicht nicht.
- Network-Detection & EDR sind entscheidend, um Beaconing und Persistenz zu erkennen.

© qSkills GmbH & Co. KG, 2025

Akt III
Verborgene Wege

© qSkills GmbH & Co. KG, 2025

THEORIE

- Sobald der erste Host steht, beginnt die eigentliche „Reise“ durchs Netzwerk.
- Angreifer versuchen, Rechte auszuweiten (Privilege Escalation) und sich lateral zu bewegen: von einem kompromittierten Client zum File-Server, Domain-Controller oder Admin-Konto.

- **Angriffsphase**: *Discovery, Lateral Movement, Privilege Escalation.*
- **Verteidigung:** Netzwerksegmentierung, strikte Rechtevergabe, Just-in-Time-Privilegien, EDR-Regeln auf verdächtige interne Bewegungen.

© qSkills GmbH & Co. KG, 2025

Learnings

- Angreifer nutzen legitime Admin-Werkzeuge für laterale Bewegung.
- Sichtbarkeit im internen Netzwerk ist essenziell – nur so erkennt man Bewegungen.
- Zero-Trust, Segmentierung und strikte Privilegien sind starke Verteidigungsmaßnahmen.

© qSkills GmbH & Co. KG, 2025

Akt IV
Der Schatz im Dunkeln

© qSkills GmbH & Co. KG, 2025

THEORIE

- Angreifer suchen gezielt nach wertvollen Informationen: Kundendaten, Produktionspläne, Finanzdaten.
- *Zwei Motivationen:*
  - *Data Theft (klassische Spionage) – Daten werden an Dritte verkauft.*
  - *Double Extortion – Daten werden verschlüsselt und zusätzlich geleakt, um Druck zu erzeugen.*

- **Angriffsphase**: *Exfiltration.*
- **Verteidigung:** DLP-Systeme, Überwachung von Egress-Traffic, Monitoring ungewöhnlicher Dateioperationen, Verschlüsselung sensibler Daten „at rest“.

© qSkills GmbH & Co. KG, 2025

Learnings

- Daten sind das Ziel – ihre Klassifizierung und Schutz müssen Priorität haben.
- Exfiltration erzeugt fast immer Spuren, wenn man die richtigen Sensoren hat.
- DLP und Egress-Monitoring sind Schlüssel zur Früherkennung.

© qSkills GmbH & Co. KG, 2025

Akt V
Der letzte Vorhang

© qSkills GmbH & Co. KG, 2025

THEORIE

- Der finale Schlag: Ransomware oder Datenerpressung.
- Angreifer verschlüsseln produktive Daten und hinterlassen eine Ransom-Note mit Forderungen (oft in Kryptowährungen).

- **Angriffsphase**: *Impact*.
- **Verteidigung:** Backups (getestet & offline), Incident-Response-Playbooks, Krisenkommunikation, Cyberversicherung, Übung von Wiederanlauf-Szenarien.

© qSkills GmbH & Co. KG, 2025

Learnings

- Der Schaden tritt erst am Ende sichtbar auf – die Vorbereitung lief lange unbemerkt.
- Backups sind nur wertvoll, wenn sie getestet und isoliert sind.
- Incident Response, Krisenkommunikation und rechtliche Pflichten (NIS2/DORA) müssen vorbereitet sein.

© qSkills GmbH & Co. KG, 2025

Zusammenfassung

© qSkills GmbH & Co. KG, 2025

Zusammenfassung

Akt I – Der stille Schlüssel

- Leaked Credentials öffnen die erste Tür.
- Vertrauen ist der schwächste Punkt.

Akt II – Schatten im Netz

- Unbemerkte Bewegungen im Active Directory und Entra.
- Sichtbarkeit entscheidet.

Akt III – Verborgene Wege

- C2-Infrastruktur (Mythic) etabliert.
- Tools allein stoppen keine Angreifer.

Akt IV – Der Schatz im Dunkeln

- Datenabfluss & interne Routinen.
- Business as usual = Risiko.

Akt V – Der letzte Vorhang

- Ransomware & Erpressung
- Konsequenzen treffen alle.

© qSkills GmbH & Co. KG, 2025

Woran hat es gelegen? Man fragt sich immer woran et jelegen hat!

© qSkills GmbH & Co. KG, 2025

Alles war da. Aber niemand hat es gesehen.

Der Angriff war da

- Leaked Credentials im Umlauf
- Auffällige Logins aus fremden Regionen
- Ungewöhnliche interne Scans
- Wiederkehrende Muster im Mailverkehr

Die Technik hat gesehen…

- Zahlen, Events, Datenpunkte
- Aber: kein „High Alert“

Der Mensch hätte verstanden

- Muster und Zusammenhänge erkannt
- Risiko bewertet statt nur gezählt
- Eskaliert, bevor Verschlüsselung startet

© qSkills GmbH & Co. KG, 2025

Von Admins zu Analysten - die nächste Stufe

Unsere Realität

- 3 Admins, seit 15 Jahren im Unternehmen
- Tiefes Systemwissen, stabiler Betrieb
- Infrastruktur läuft – Business as usual

Nur weil ein EDR ausgerollt wurde bzw. betrieben wird, heißt es nicht das es verstanden wird.

© qSkills GmbH & Co. KG, 2025

Von Admins zu Analysten – die nächste Stufe

Die Herausforderung

- Angriffe sind leise & mehrstufig
- Routine wird zum Risiko
- Tools sehen nur das Offensichtliche

© qSkills GmbH & Co. KG, 2025

Von Admins zu Analysten – die nächste Stufe

Der Missing Link

- Jemand, der Logfiles liest statt nur speichert
- Muster erkennt, bevor sie gefährlich werden
- Risiken bewertet & **Handlungsempfehlungen gibt**

© qSkills GmbH & Co. KG, 2025

Cybersecurity Operations Analyst

Die menschliche Sensorik gegen das Unsichtbare.

- Ergänzt das Admin-Team, statt es zu ersetzen.
- Macht Unternehmen reaktionsfähig – NIS2 & DORA ready.
- Kostengünstig für KMUs – wächst mit.
- Ansprechpartner für:
  - Externe Sicherheitsdienstleister (SOC / SIEM / Pentester / Red Teamer / IR Teams)
  - Admins – als Sparringspartner
  - Entscheider

© qSkills GmbH & Co. KG, 2025

qSk!lls
innovation through education

29
OKTOBER
Nürnberg

HERZLICHEN DANK
für Ihre Teilnahme

Björn Trappe

Lautlos gehackt
Ein Desaster in 5 Akten – und was Sie daraus lernen sollten

qSk!lls
innovation through education

Wir setzen auf Qualität.
Setzen Sie sich zu uns.

Exkl. Rabatt 350€
qs350BIHK

SC250

ISACA™ Certified Cybersecurity Operations Analyst (CCOA) Vorbereitung

SC415

EC-Council™ Certified Ethical Hacker (CEH Elite)

SC425

EC-Council™ Certified Penetration Testing Professional (CPENT AI)