Ausgangssituation| IoT Sicherheit

Praxisbeispiel| Speichersysteme

OPNsense Live-View

Fragerunde

THOMAS KRENN®
IT's people business

Thomas Niedermeier

39Jahre

- Senior Solution Engineer OPNsense bei Thomas-Krenn.AG
- B.Sc. Wirtschaftsinformatik

Branchenerfahrung:

- Seit 10 Jahren bei Thomas-Krenn
- Erfahrung im Bereich Firewalls, OPNsense, Monitoring Software, Open Source Software, Wissensmanagement, Produktmanagement, Marketing

THOMAS KRENN®
IT's people business

Uli Hurzlmeier

35 Jahre

- B. Eng Technologiemanagement
- Solution Sales Manager

Branchenerfahrung:

- Ausbildung zum Elektroniker für Geräte & Systeme
- Service-Techniker im globalen Einsatz
- Produkt-Manager, Director Product Management
- Industrie, Schwerpunkt: Maschinenbau für Lebensmittelindustrie
- 18 Jahre im industriellen Umfeld tätig

THOMAS KRENN®
IT's people business

Ricardo Kissinger

32 Jahre

- Head of IT Infrastructure & IT Security der ju:niz Energy GmbH
- Gelernter Fachinformatiker – Schwerpunkt Systemintegration

Branchenerfahrung:

- Entwicklung und Implementierung umfassender Netzwerkkonzepte.
- Koordination von IT-Systembereitstellungen für nahtlose Hardware- und Softwareintegration.
- Förderung robuster IT-Sicherheitsstrategien und Teamführung zum Schutz digitaler Vermögenswerte.
- Einführung neuester Technologien für kontinuierliche Verbesserungen in der IT-Infrastruktur.

THOMAS KRENN®
IT's people business

IoT Sicherheit mit OPNsense

ju:niz

THOMAS KRENN®

IT's people business

Sichere Anbindung von Windkraft-Speichersystemen

Vorfall 24.02.2022| Ausfall Satellitensystem

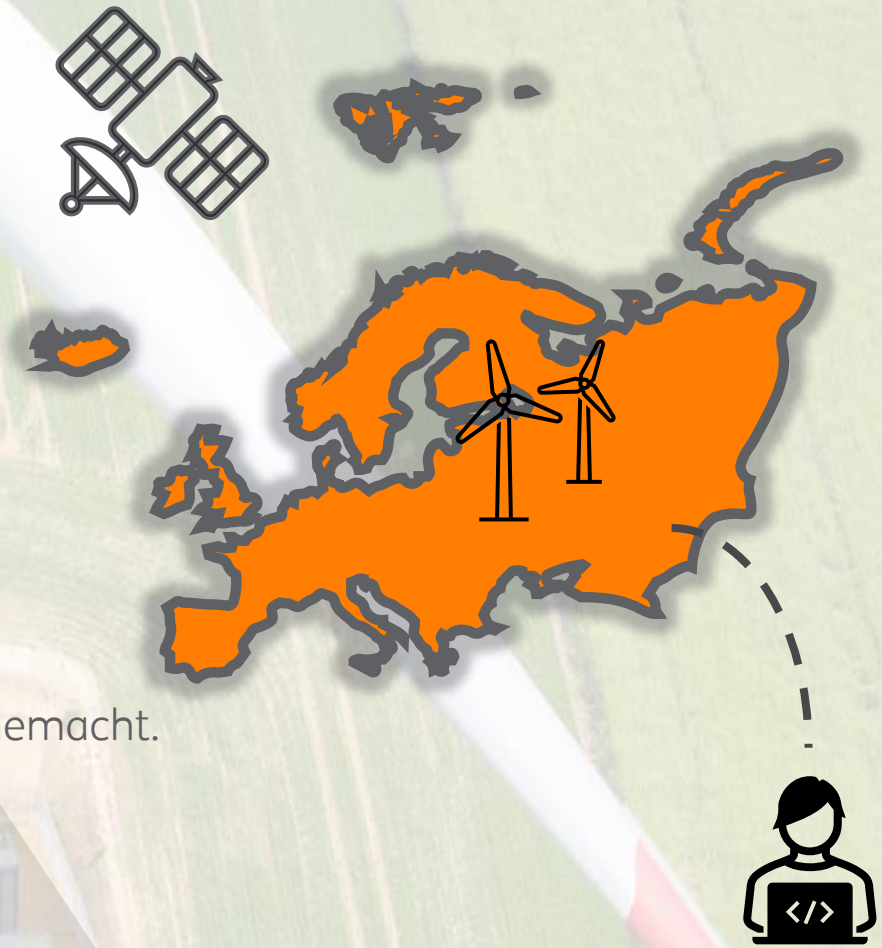
**Forensische Analyse:

Die forensische Analyse ergab, dass sich die **Angreifer** durch eine **fehlkonfigurierte VPN-Verbindung** **Zugang** zu einem Management-Netz verschafft hatten.

Über dieses sollen die Angreifer **Befehle auf zehntausenden Modems** **zeitgleich** ausgeführt haben.

Hohes Volumen an Datenverkehr

Dabei wurde der Flashspeicher überschrieben und die Modems unbrauchbar gemacht.



5.800

THOMAS KRENN®
IT's people business

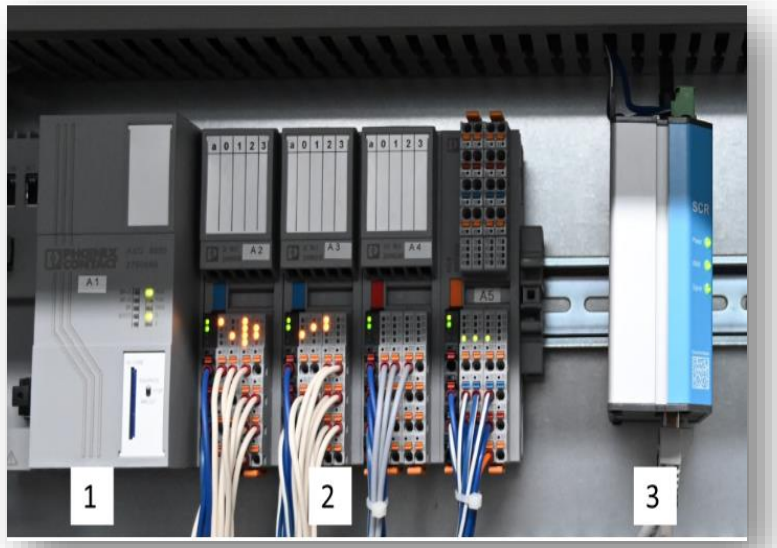
**Quelle: Die Lage der IT-Sicherheit in Deutschland, Lagebericht 2022: 21.11.2023

Status Quo

THOMAS KRENN®
IT's people business

Status Quo

Standardausstattung der Anlagen – seit 2016



- Setups mit einfachen LTE-Routern
- „Managed“ VPN-Services des Betreibers
- Rudimentäre Funktionen der VPN-Router
- Inkl. Automatischer Hintergrund-Updates zum Zertifikat-Austausch des Herstellers
- Keine Nennenswerten Sicherheitsfunktionen
- Erlaubt „absurde“ Konfigurationen (Netzwerk-Start-Adressen als Gateway u.a.)
- Eingeschränkte Nachvollziehbarkeit von Konfigurationsänderungen

Status Quo

„Managed“ VPN-Services

Quelle: Dall-E

- Abhängigkeit von OpenVPN Versionen des Herstellers
- Unklarer Sicherheitsstandard
- Keine Multi-Faktor-Login für die OpenVPN Verbindungen
- Veraltete Sicherheitsstandards aufgrund von „Rückwärtskompatiblität“

Praxisbeispiel

THOMAS KRENN®
IT's people business

Hardware-Bindung moderner Firewalls

Typische BESS Deployments (Battery Energy Storage System)

<40MWh Speicher

- Erfüllt nicht die Notwendigkeit von KRITIS
- Meist Speicher zwischen 5-20MWh nur mit Schaltschränken, keine separaten Serverschränke
- Anbindung per LTE oder Starlink

>40MWh Speicher

- Zählt zu kritischer Infrastruktur
- Aufgrund der anfallenden Daten in der Regel inkl. Serverschrank
- Genug Platz für Standard 1HE Firewall-Systeme
- Anbindung via DSL/LWL und zusätzlich Failover per LTE/Starlink

THOMAS KRENN®
IT's people business

Hardware-Bindung moderner Firewalls

Photovoltaik/Windenergie-Erzeuger <-> BESS

Photovoltaik/Windturbinen

- Viel weniger Komponenten, von denen im 1s/5s Takt Daten erfasst werden müssen
- Die meisten Komponenten sind viel weniger sensibel und haben generell weniger Messpunkte
- Geringerer Monitoring Aufwand

=> Notwendigkeit in umfassendere Firewall-Lösungen zu investieren, wird als gering eingeschätzt

BESS

- Komplexeres Energie-Management notwendig
- Temperatur- und Ladezyklen-Überwachung von jeder Zelle notwendig
- Netzintegration und -stabilisierung spielt eine wichtigere Rolle
- Beispiel: Einer unserer 12MWh Speicher verbraucht seitdem er am Netz hängt, 40GB täglich Traffic zusätzlich nur für Kommunikation der Vermarkter/Netzbetreiber

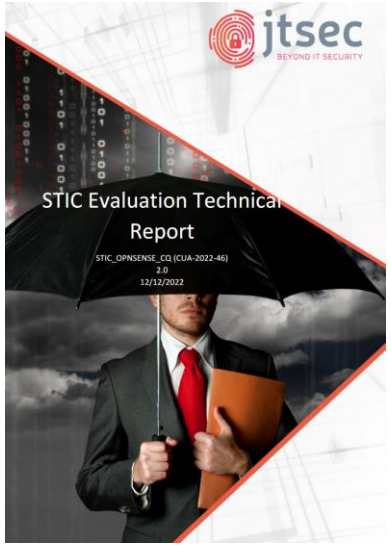
THOMAS KRENN®
IT's people business

OPNsense Firewalls

THOMAS KRENN®
IT's people business

OPNsense Firewall Sicherheit

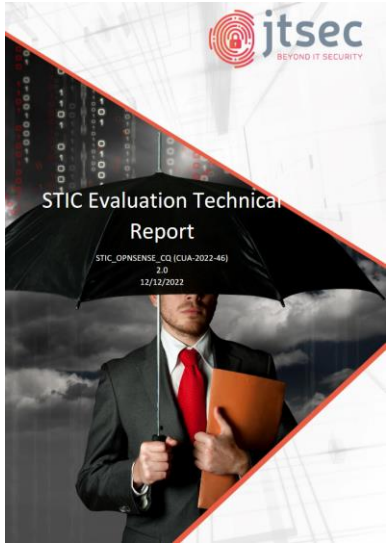
- **Schnelle Reaktion auf Sicherheitslücken**
- **Mitarbeit am FreeBSD Kernel** durch OPNsense Entwickler
- **Kein Vendor Lock-In** (Standardhardware und Software ohne Lizenzen)
- **Möglichkeit zur Beteiligung** per Github (Issues, Pull Requests) und Foreneinträge
- **Keine Lizenzen die ablaufen könnten** (Business Edition ist eine Subscription)
- **jtsec STIC Zertifizierung** der OPNsense Business Edition



THOMAS KRENN®
IT's people business

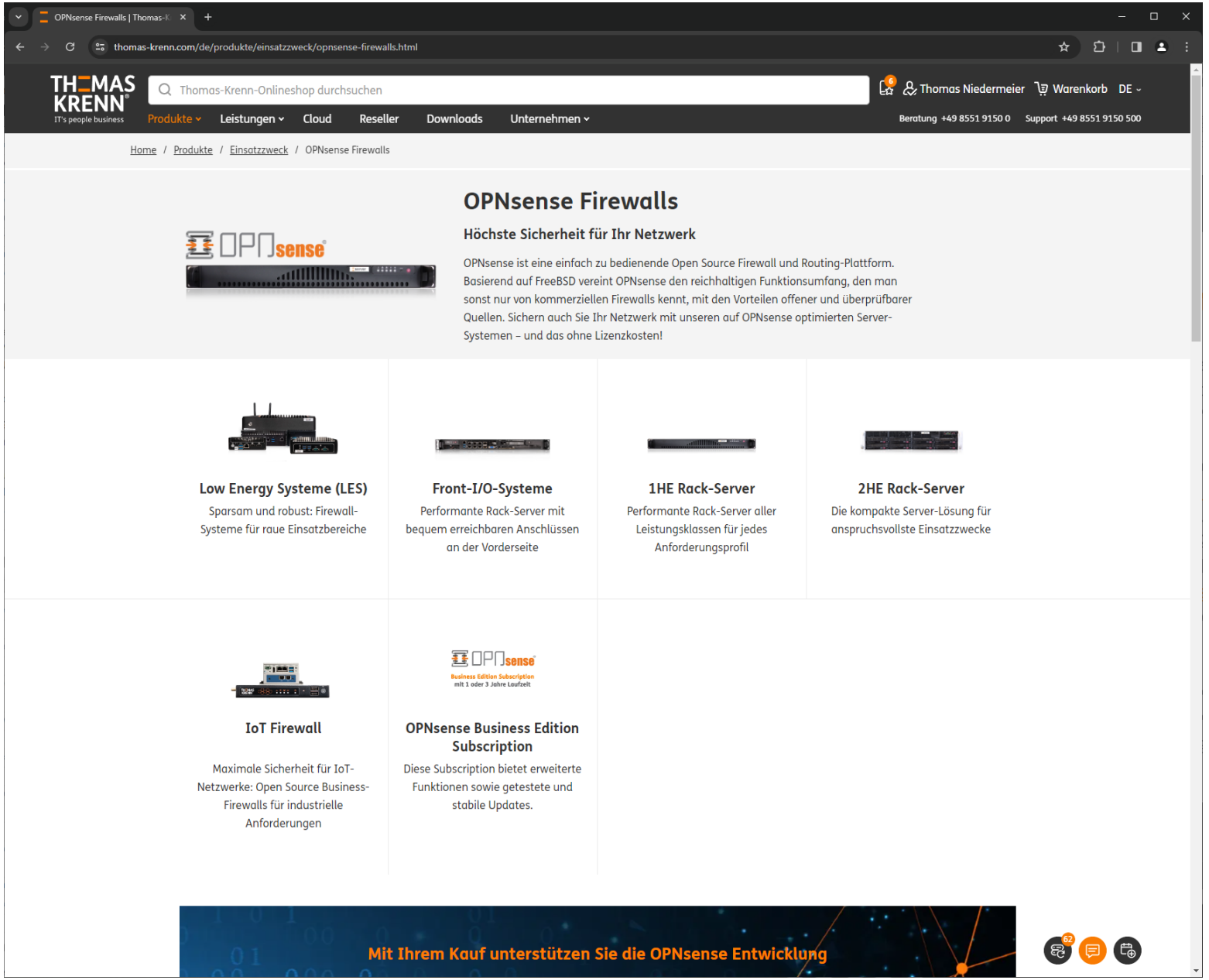
OPNsense Firewall Sicherheit

- Integrierter Security Check:
  System → Firmware → Tab Status →Button: Run an Audit
- OPNsense Docs Security
- Security Vulnerabilities Übersicht zu OPNsense
- Anleitung von Zenarmor: OPNsense Security and Hardening Best Practice Guide
- Aktuelles Kernel Patch-Level: FreeBSD 13.2-RELEASE-p9 (vom 19.12.2023):
- **Webinar Tipp auf Abruf:** Praxisbericht - Migration auf OPNsense HA-Cluster
- Server mit Remote Management: Die Absicherung des BMCs nicht vergessen
- BIOS und BMC Firmware Updates einspielen



THOMAS KRENN®
IT's people business

Fragen


OPNsense Firewalls | Thomas-K
thomas-krenn.com/de/produkte/einsatzzweck/opnsense-firewalls.html
THOMAS KRENN
IT's people business
Thomas-Krenn-Onlineshop durchsuchen
Thomas Niedermeier
Warenkorb
DE
Produkte
Leistungen
Cloud
Reseller
Downloads
Unternehmen
Beratung +49 8551 9150 0
Support +49 8551 9150 500
Home / Produkte / Einsatzzweck / OPNsense Firewalls
OPNsense Firewalls
Höchste Sicherheit für Ihr Netzwerk
OPNsense ist eine einfach zu bedienende Open Source Firewall und Routing-Plattform. Basierend auf FreeBSD vereint OPNsense den reichhaltigen Funktionsumfang, den man sonst nur von kommerziellen Firewalls kennt, mit den Vorteilen offener und überprüfbarer Quellen. Sichern auch Sie Ihr Netzwerk mit unseren auf OPNsense optimierten Server-Systemen – und das ohne Lizenzkosten!
Low Energy Systeme (LES)
Sparsam und robust: Firewall-Systeme für raue Einsatzbereiche
Front-I/O-Systeme
Performante Rack-Server mit bequem erreichbaren Anschlüssen an der Vorderseite
1HE Rack-Server
Performante Rack-Server aller Leistungsklassen für jedes Anforderungsprofil
2HE Rack-Server
Die kompakte Server-Lösung für anspruchsvollste Einsatzzwecke
IoT Firewall
Maximale Sicherheit für IoT-Netzwerke: Open Source Business-Firewalls für industrielle Anforderungen
OPNsense Business Edition Subscription
Diese Subscription bietet erweiterte Funktionen sowie getestete und stabile Updates.
Mit Ihrem Kauf unterstützen Sie die OPNsense Entwicklung

Kontakt

Uli Hurzlmeier

Solution Sales Manager,
Thomas-Krenn.AG

Thomas Niedermeier

Senior Solution Engineer OPNsense,
Thomas-Krenn.AG

THOMAS KRENN®
IT's people business