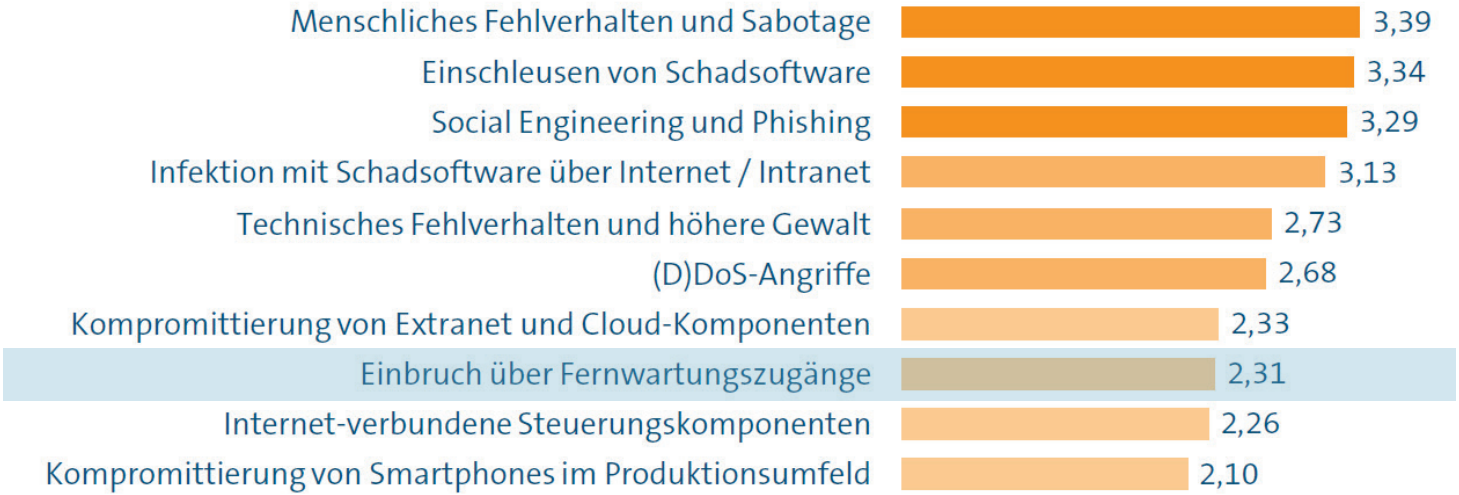
Remote Services

Digitaler Enabler und Bedrohung gleichzeitig

20. Mai 2021

TOP 10 Risiken im Maschinenbau

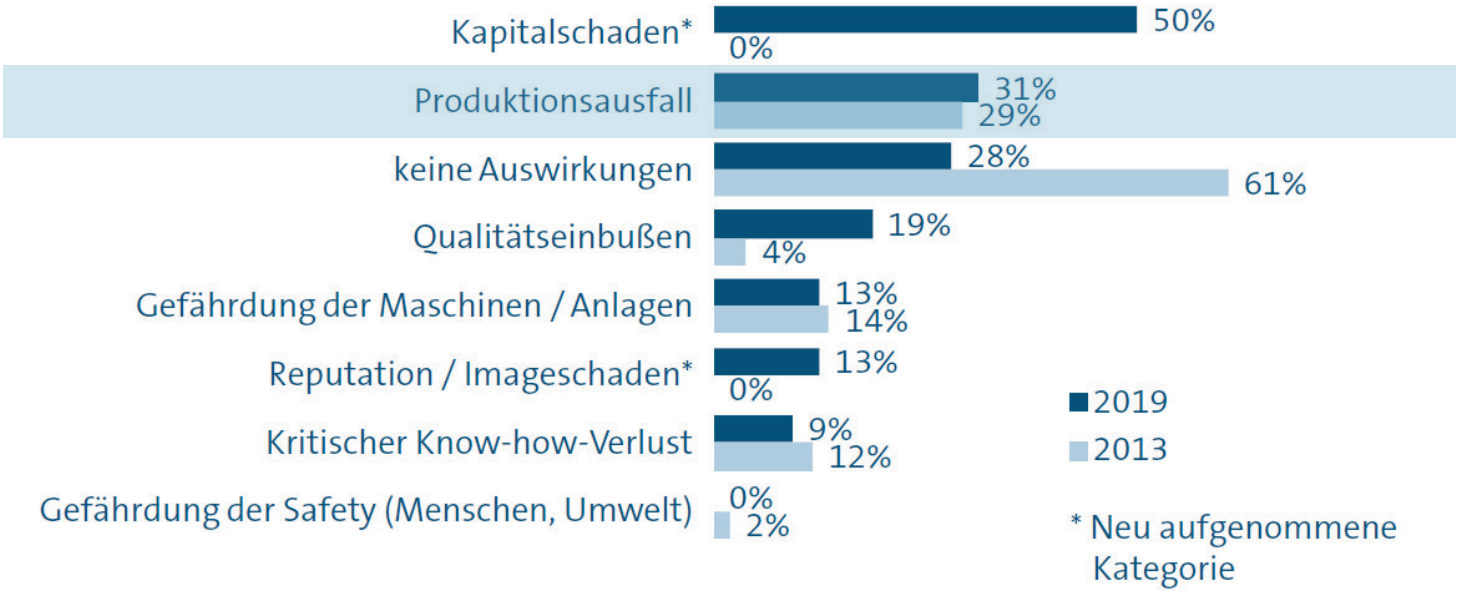
Wie schätzen Sie die Eintrittswahrscheinlichkeit für folgende Bedrohungen im Unternehmen ein?



Quelle: VDMA Studie Industrial Security 2019

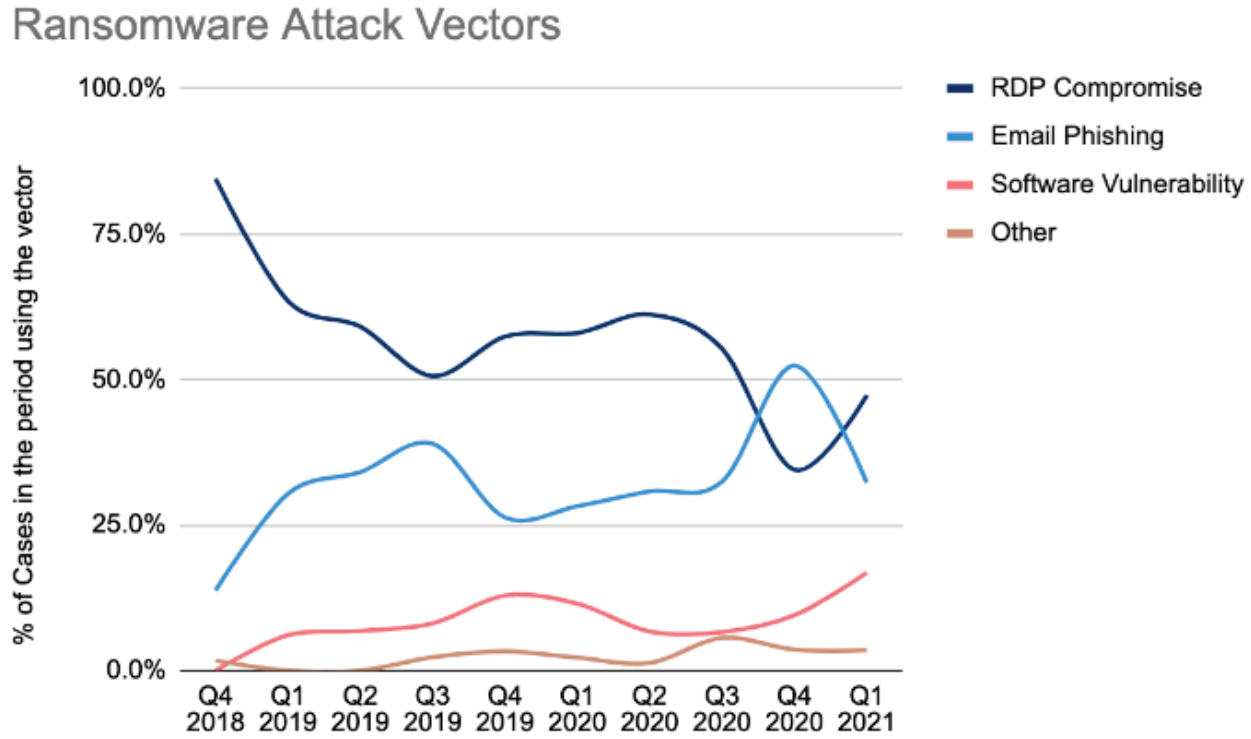
Status Quo im Maschinen- und Anlagenbau

Wie haben sich die Security-Vorfälle ausgewirkt?



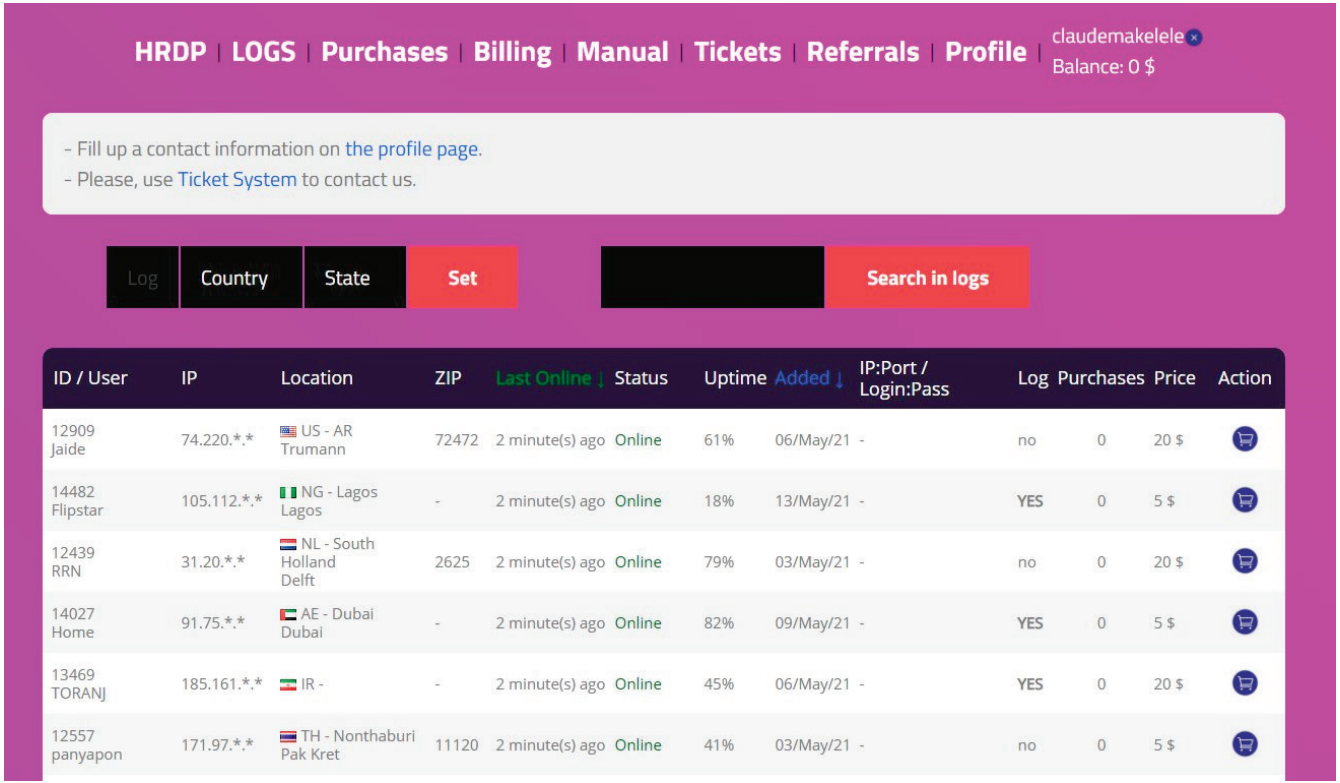
Quelle: VDMA Studie Industrial Security 2019 (Mehrfachnennungen möglich)

Ransomware – RDP ist #1 Angriffsvektor



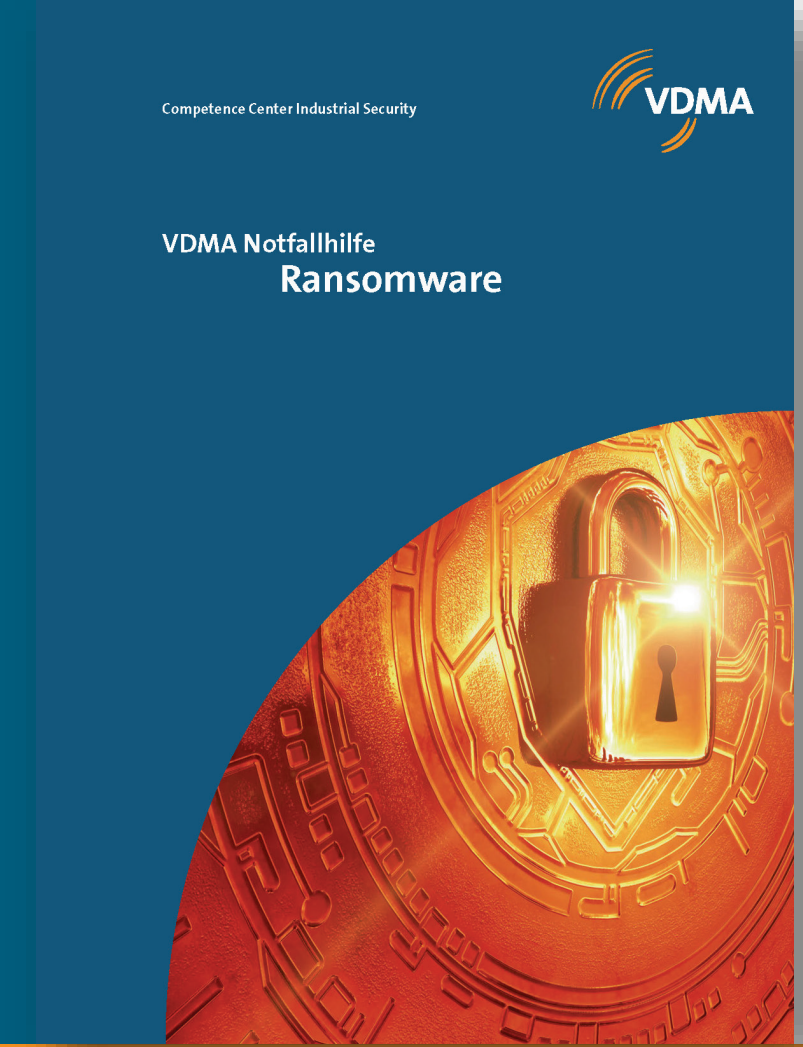
Quelle: Coveware Ransomware Report Q1/2021

Ransomware – RDP ist #1 Angriffsvektor



ID / User	IP	Location	ZIP	Last Online ↓	Status	Uptime	Added ↓	IP:Port / Login:Pass	Log	Purchases	Price	Action
12909 Jaide	74.220.*.*	US - AR Trumann	72472	2 minute(s) ago	Online	61%	06/May/21	-	no	0	20 $	
14482 Flipstar	105.112.*.*	NG - Lagos Lagos	-	2 minute(s) ago	Online	18%	13/May/21	-	YES	0	5 $	
12439 RRN	31.20.*.*	NL - South Holland Delft	2625	2 minute(s) ago	Online	79%	03/May/21	-	no	0	20 $	
14027 Home	91.75.*.*	AE - Dubai Dubai	-	2 minute(s) ago	Online	82%	09/May/21	-	YES	0	5 $	
13469 TORANJ	185.161.*.*	IR -	-	2 minute(s) ago	Online	45%	06/May/21	-	YES	0	20 $	
12557 panyapon	171.97.*.*	TH - Nonthaburi Pak Kret	11120	2 minute(s) ago	Online	41%	03/May/21	-	no	0	5 $	

Quelle: https://twitter.com/campuscodi



Ransomware Notfallhilfe

VDMA

Der VDMA Arbeitskreis rät Ihnen, folgende Maßnahmen grundlegend und unabhängig des Angriffsvektors zu beachten und umzusetzen:

- Vermeidung/Abschaltung direkter Remote-Administration-Zugänge auf interne IT-Systeme, insbesondere RDP, Citrix, SSH
- Zwei-Faktor Authentisierung bei Systemen, die aus dem Internet erreichbar sind
- Deaktivierung von SMBv1 auf allen Systemen
- Patchmanagement von Betriebssystemen und Applikationen (z. B. PDF-Reader, Office, Bildbearbeitung, etc.)

Stand der Technik für Fernwartungsarchitekturen

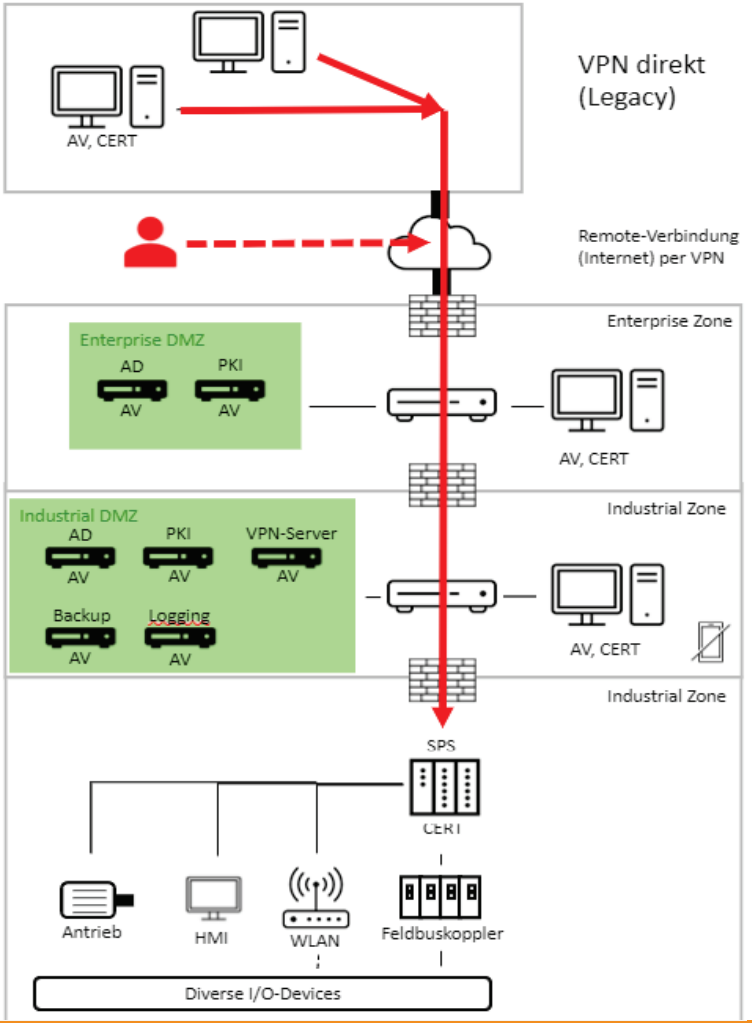
in Arbeit!

VDMA

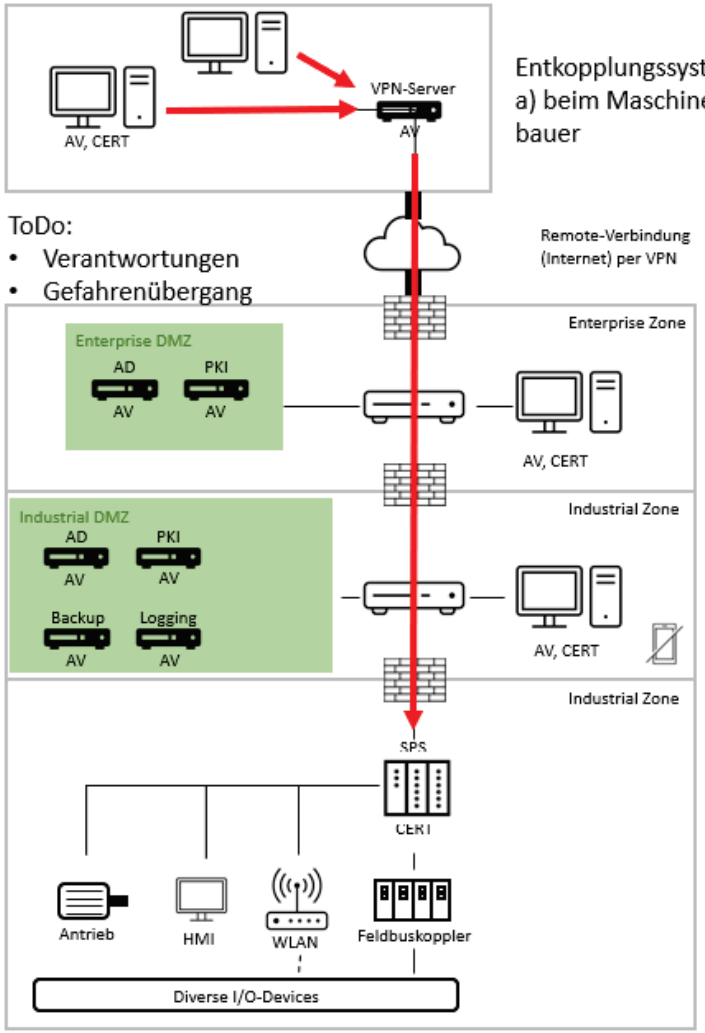
- **Aufgabe:**
  - Beschreibung generischer Architekturen für Fernwartung
  - Beurteilung der Risiken
  - Einschätzung: Stand der Technik?
  - Empfehlung des VDMA Arbeitskreises

pilz
symmedia
genua Ein Unternehmen der Bundesdruckerei
BEUMERGROUP
BOSCH
PHOENIX CONTACT
TRUMPF
KRONES
SIEMENS
Bundesamt für Sicherheit in der Informationstechnik
HAVER & BOECKER
Weidmüller
WINDMÖLLER & HÖLSCHER
PASSION FOR INNOVATION

Variante VPN direkt

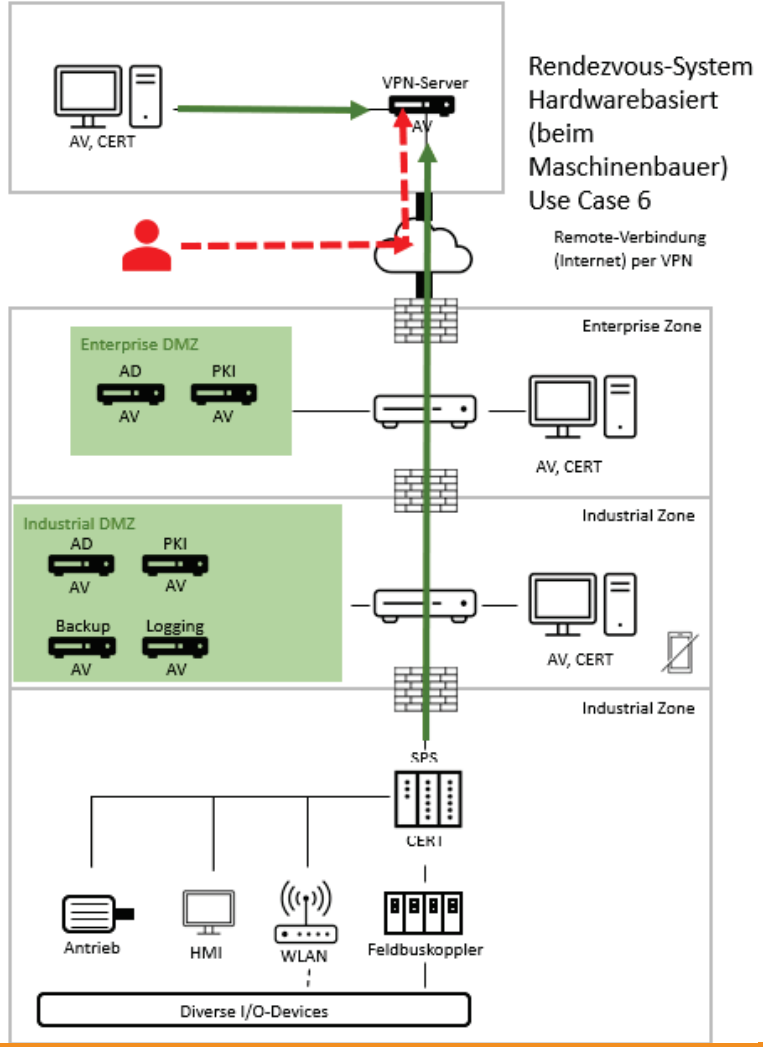


- **Risiken?**
- **Stand der Technik?**
- **Empfehlungen?**



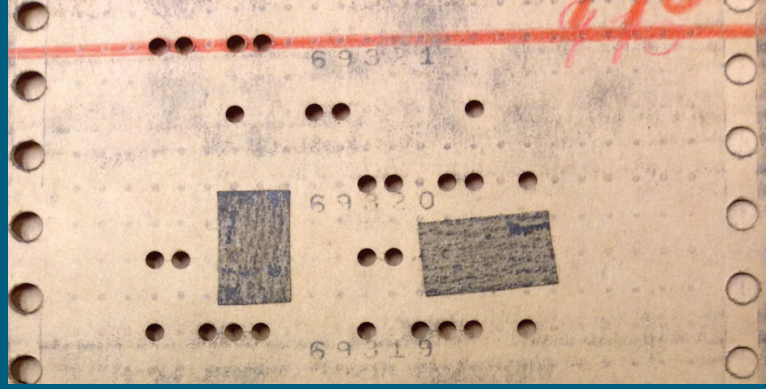
Jump Host Hersteller

- **Risiken?**
- **Stand der Technik?**
- **Empfehlungen?**

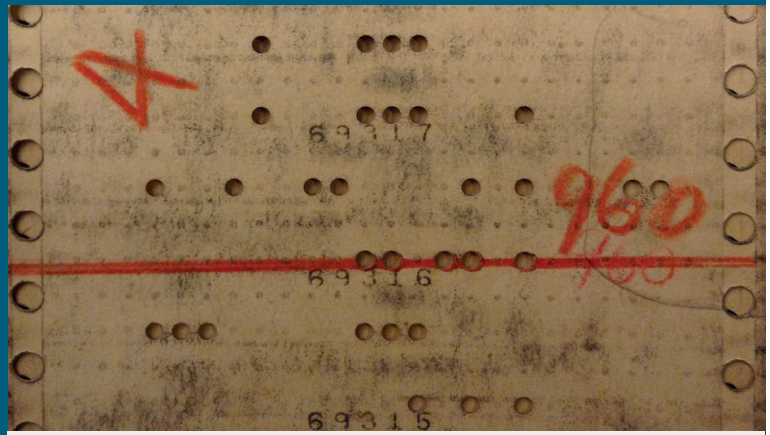


Rendezvous-System

- **Risiken?**
- **Stand der Technik?**
- **Empfehlungen?**



Was müssen wir tun?



"The Patch" – Small corrections to the programmed sequence could be done by patching over portions of the paper tape and re-punching the holes in that section.

http://sites.harvard.edu/~chsi/markone/language.html

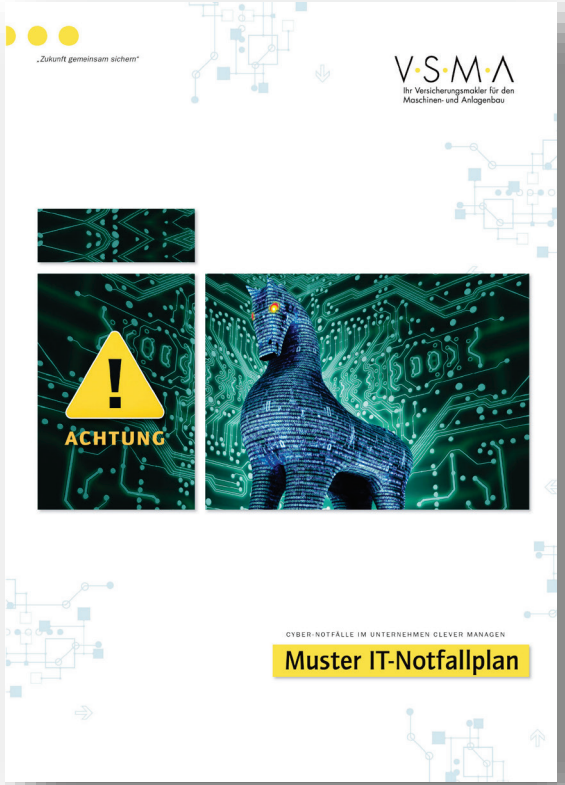
Jeder muss seinen Beitrag leisten!

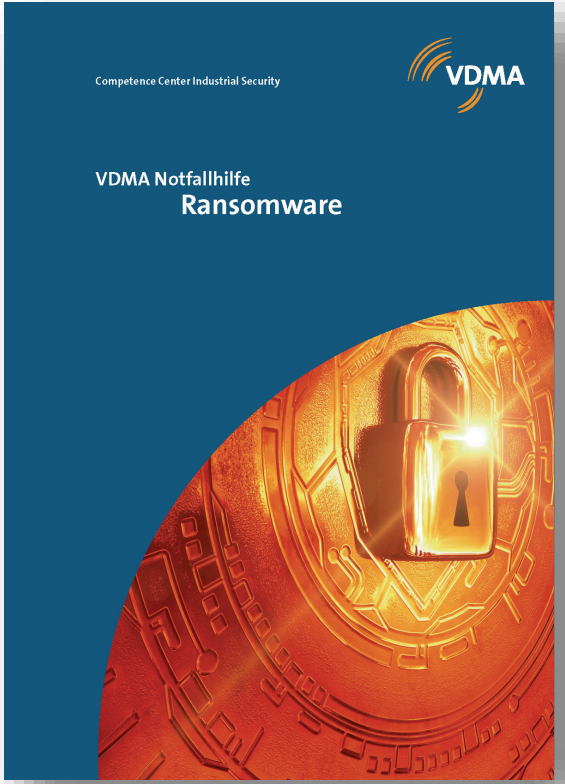
Keiner ist allein unterwegs!

Nichts hält ewig!

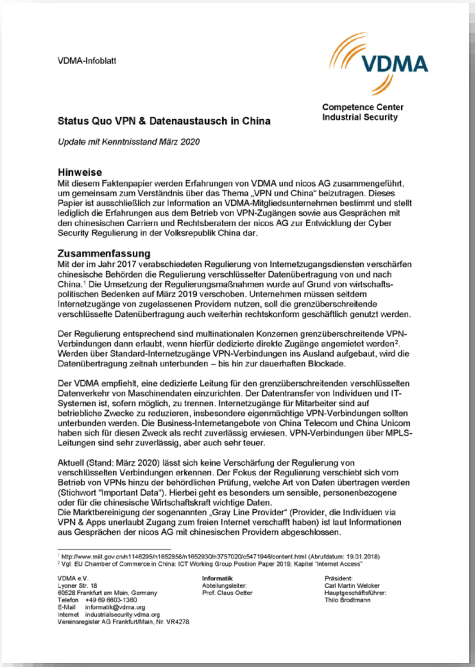
Irgendwann knallts!

Hilfe im Schadenfall





Unterstützung für die Praxis #2



VDMA-Infoblatt

Competence Center Industrial Security

Status Quo VPN & Datenaustausch in China

Update mit Kenntnisstand März 2020

Hinweise

Mit diesem Faktenpapier werden Erfahrungen von VDMA und nicos AG zusammengeführt, um gemeinsam zum Verständnis über das Thema „VPN und China" beizutragen. Dieses Papier ist ausschließlich zur Information an VDMA-Mitgliedsunternehmen bestimmt und stellt lediglich die Erfahrungen aus dem Betrieb von VPN-Zugängen sowie aus Gesprächen mit den chinesischen Carriern und Rechtsberatern der nicos AG zur Entwicklung der Cyber Security Regulierung in der Volksrepublik China dar.

Zusammenfassung

Mit der im Jahr 2017 verabschiedeten Regulierung von Internetzugangsdiensten verschärfen chinesische Behörden die Regulierung verschlüsselter Datenübertragung von und nach China.[1] Die Umsetzung der Regulierungsmaßnahmen wurde auf Grund von wirtschafts-politischen Bedenken auf März 2019 verschoben. Unternehmen müssen seitdem Internetzugänge von zugelassenen Providern nutzen, soll die grenzüberschreitende verschlüsselte Datenübertragung auch weiterhin rechtskonform geschäftlich genutzt werden.

Der Regulierung entsprechend sind multinationalen Konzernen grenzüberschreitende VPN-Verbindungen dann erlaubt, wenn hierfür dedizierte direkte Zugänge angemietet werden[2]. Werden über Standard-Internetzugänge VPN-Verbindungen ins Ausland aufgebaut, wird die Datenübertragung zeitnah unterbunden – bis hin zur dauerhaften Blockade.

Der VDMA empfiehlt, eine dedizierte Leitung für den grenzüberschreitenden verschlüsselten Datenverkehr von Maschinendaten einzurichten. Der Datentransfer von Individuen und IT-Systemen ist, sofern möglich, zu trennen. Internetzugänge für Mitarbeiter sind auf betriebliche Zwecke zu reduzieren, insbesondere eigenmächtige VPN-Verbindungen sollten unterbunden werden. Die Business-Internetangebote von China Telecom und China Unicom haben sich für diesen Zweck als recht zuverlässig erwiesen. VPN-Verbindungen über MPLS-Leitungen sind sehr zuverlässig, aber auch sehr teuer.

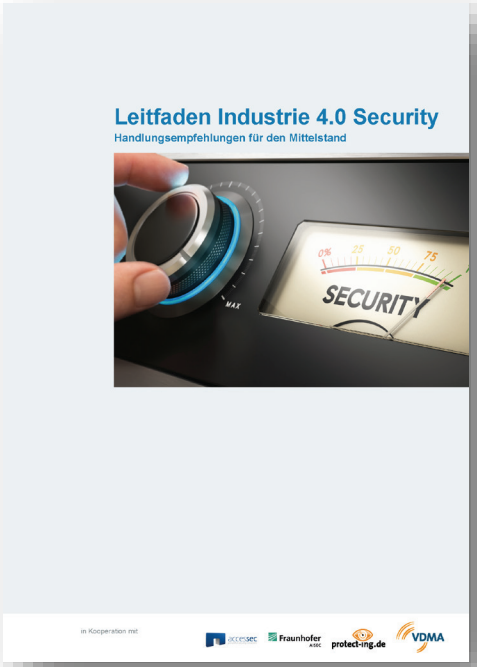
Aktuell (Stand: März 2020) lässt sich keine Verschärfung der Regulierung von verschlüsselten Verbindungen erkennen. Der Fokus der Regulierung verschiebt sich vom Betrieb von VPNs hinzu der behördlichen Prüfung, welche Art von Daten übertragen werden (Stichwort "Important Data"). Hierbei geht es besonders um sensible, personenbezogene oder für die chinesische Wirtschaftskraft wichtige Daten.
Die Marktbereinigung der sogenannten „Gray Line Provider" (Provider, die Individuen via VPN & Apps unerlaubt Zugang zum freien Internet verschafft haben) ist laut Informationen aus Gesprächen der nicos AG mit chinesischen Providern abgeschlossen.

[1] http://www.mit.gov.cn/zh114/295/n1652558/n1652930/n3757020/c5471946/content.html (Abrufdatum: 19.01.2018)
[2] Vgl. EU Chamber of Commerce in China: ICT Working Group Position Paper 2018, Kapitel "Internet Access"

VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main, Germany
Telefon +49 69 6603-1360
E-Mail informatik@vdma.org
Internet industrialsecurity.vdma.org
Vereinsregister AG Frankfurt/Main, Nr. VR4278

Informatik
Abteilungsleiter:
Prof. Claus Oetter

Präsident:
Carl Martin Welcker
Hauptgeschäftsführer:
Thilo Brodtmann

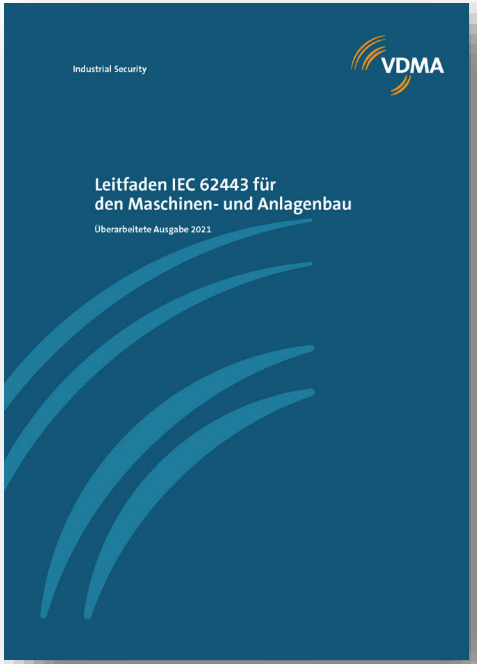


Leitfaden Industrie 4.0 Security

Handlungsempfehlungen für den Mittelstand

in Kooperation mit

accessec · Fraunhofer IOSB · protect-ing.de · VDMA



Industrial Security

VDMA

Leitfaden IEC 62443 für den Maschinen- und Anlagenbau

Überarbeitete Ausgabe 2021

Digitales Lernportal für Industrial Security

Industry 4.0 Security for Manufacturers and Integrators (17)

Industrial Security

Monitoring und Angriffserkennung

Warum braucht man Monitoring und Angriffserkennung?
Monitoring von Komponentenzu...

14 minutes

Industrial Security

Wiederherstellungsplan

Wie kann ein Wiederherstellungsplan helfen?
Was passiert ohne guten Wiederherst...

15 minutes

Industrial Security

Sicherer Produkt-Lebenszyklus

Was ist ein sicherer Produkt-Lebenszyklus?
Warum braucht Industrie 4.0 einen sic...

17 minutes

www.u4i.io/vdma

Quelle: www.u4i.io/vdma

Security By Design – Cybersichere Maschinen

Kooperationspartner

Fraunhofer IEM

Fraunhofer IOSB

UNIVERSITY 4 INDUSTRY

Seminar

Maschinen sicher entwickeln (virtuell)

Security by Design nach IEC 62443

© putilov_denis/ Adobe Stock

Mit der **zunehmenden Vernetzung von Maschinen und Anlagen** nimmt auch die Abhängigkeit von Embedded Software stetig zu. **Sicherheit wird häufig erst am Ende integriert** obwohl klar ist, dass Sicherheitsvorfälle und Cyberangriffe bereits heute enormen Einfluss auf die Produktion und das Image eines Unternehmens haben können. Das **neue virtuelle Seminar „Security by Design“** wurde auf **Basis der IEC 62443** entwickelt und verfolgt das Ziel, Produktentwickler im Maschinenbau zu befähigen, **Bedrohungen frühzeitig zu erkennen**, **Schutzbedarfe zu ermitteln** und **geeignete Sicherheitsmaßnahmen zu ergreifen**.

Veranstaltungsdetails

29.06. – 01.07.2021
Dauer: 1,5 Tage

Online

Gebühren (zzgl. MwSt.)
VDMA-Mitglieder € 790
Nichtmitglieder € 960

Jetzt anmelden

Präsenz-Seminar

Security by Design

Jetzt informieren

https://www.maschinenbau-institut.de/security/

Competence Center Industrial Security
VDMA e.V.
Lyoner Str. 18
60528 Frankfurt am Main - Germany

Steffen Zimmermann
+49 69 6603 - 1978
Steffen.Zimmermann@vdma.org

Biljana Gabric
+49 69 6603 - 1360
Biljana.Gabric@vdma.org

Kai Kalusa
+49 30 3069 – 4624
Kai.Kalusa@vdma.org

https://IndustrialSecurity.vdma.org