IT-Sicherheit im Home-Office

@cmitasch
Christoph Mitasch, Thomas-Krenn.AG

Webinar, 16. Juli 2020

THOMAS KRENN®

Über mich

- Christoph Mitasch
- seit 2005 bei der Thomas-Krenn.AG
  Niederlassung Österreich
- Diplomstudium
  Computer- und Mediensicherheit
- Erfahrung in Web Operations,
  Linux und HA
- Cyber-Security-Practitioner (v1)

Thomas-Krenn.AG

- 2002 gegründet
- Standort Freyung, Bayern
- Server- und Storage-Systeme
- Flexibilität bei Kundenanfragen

32 belieferte EU und EFTA-Länder

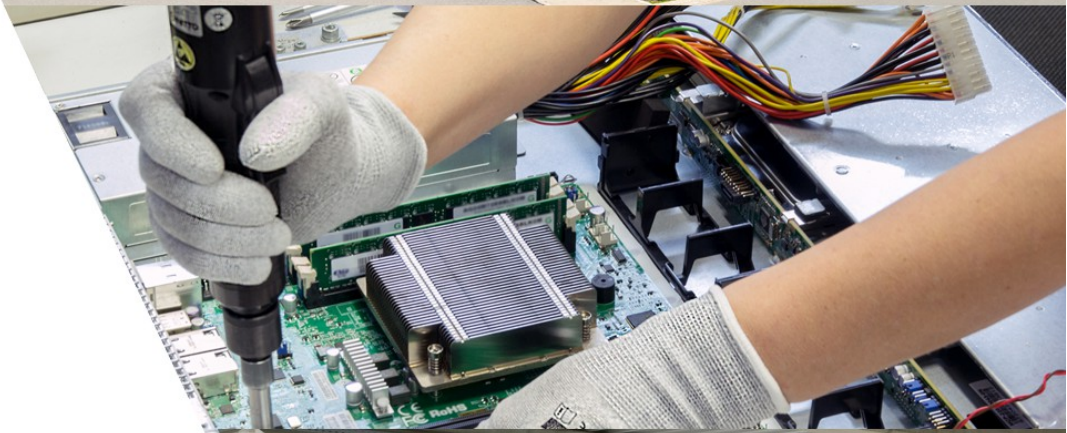
15.120 gebaute Server

ca. 100 getestete Systeme und Einzelkomponenten

6,4 Millionen Domain-Visits

41 Millionen Euro Gesamtumsatz

aktiver Kundenstamm: 18.000 Kunden mit 1550 Neukunden im Jahr 2019



Agenda

- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

Agenda

- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

Home Office bei der Thomas-Krenn.AG

- Großteil der Mitarbeiter von März bis Juni im Home-Office
- Virtueller Desktop (VDI) schon seit 2013 durchgängig im Einsatz
- Internet-Bandbreite hat ausgereicht, symmetrisch wichtig
  - zeitweise über 100 Desktop Sitzungen parallel von extern
  - Bandbreite/Latenz beim Mitarbeiter auch relevant
- Grundsatz für externen Zugriff:
  - MFA/2FA, Passwort alleine reicht nicht
  - keinerlei unverschlüsselte Verbindungen

Home Office bei der Thomas-Krenn.AG

- Telefonie mit gewohnter Nebenstelle via App am Handy oder VDI-Desktop möglich
- Kommunikations-Tool für Instant Messaging und Video-Konferenzen → Headset sehr wichtig
- Richtlinien von HR und DSB für Home-Office
  - z.B. keine Dokumente zu Hause ausdrucken
  - „Gesunde Distanz zur Kaffeemaschine. (ca. 12 Schritte)“ ;-)
- E-Mail Spoofing-Schutz verbessert
- zusätzliche Sensibilisierung der Mitarbeiter für IT-Sicherheit
  - „Cyber-Kriminelle nutzen Corona-Krise vermehrt aus“

Agenda

- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

Quelle: https://www.flickr.com/photos/apes_abroad/5416445001

Der häusliche Arbeitsplatz

Bundesamt
für Sicherheit in der
Informationstechnik

Klar geregelt:
Kommunizieren Sie klare und verbindliche IT-Sicherheitsregelungen.

Hier gibt es nichts zu sehen:
Stellen Sie sicher, dass Unbefugte keinen Einblick in Ihre Daten haben.

Eindeutige Verifizierung:
Kommunizieren Sie nur über Kanäle, die vertrauenswürdig sind.

Vorsicht Phishing:
Durch COVID-19 können vermehrt Phishing-Mails im Umlauf sein.

VPN

VPN:
Kommunikation per VPN ist der Standard.
Informieren Sie sich über sichere Lösungen.

Der häusliche Arbeitsplatz

- IT-Grundschutz Bausteine
  - INF.8 Häuslicher Arbeitsplatz
    - plus Umsetzungshinweise zum Baustein INF.9 (von 02/2020)
  - OPS.1.2.4 Telearbeit
  - https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/bausteine_node.html
- Tipps vom BSI
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf?__blob=publicationFile&v=9
  - Fenster und Türen abschließen
  - Verschlüsselung der Datenträger
  - Vertrauliche Dokumente entsorgen (Media Disposal)
  - Clean Desk Policy

INF.8 Häuslicher Arbeitsplatz

Schnell zum Abschnitt

OPS.1.2.4 Telearbeit

Schnell zum Abschnitt

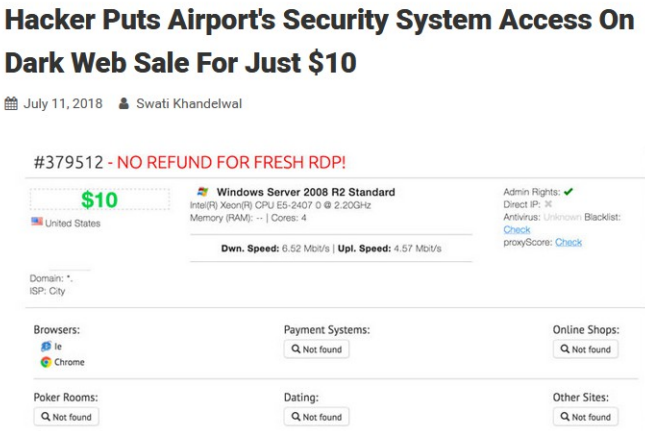
Agenda

- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

Remote Zugang Desktop

- Wo läuft Desktop?
  - Firmen-Netz
  - am PC/Notebook zu Hause
  - Cloud
- Zugriff auf Desktop in Firma/Cloud
  - RDP, VPN, Teamviewer
  - VDI Client
- Anbindung von lokalem Desktop ans Firmen-Netzwerk
  - unverschlüsselt → NEIN
  - SSH Tunneling → als temporäre Lösung
  - VPN (Layer 2/3) → optimal

Remote Zugang Desktop

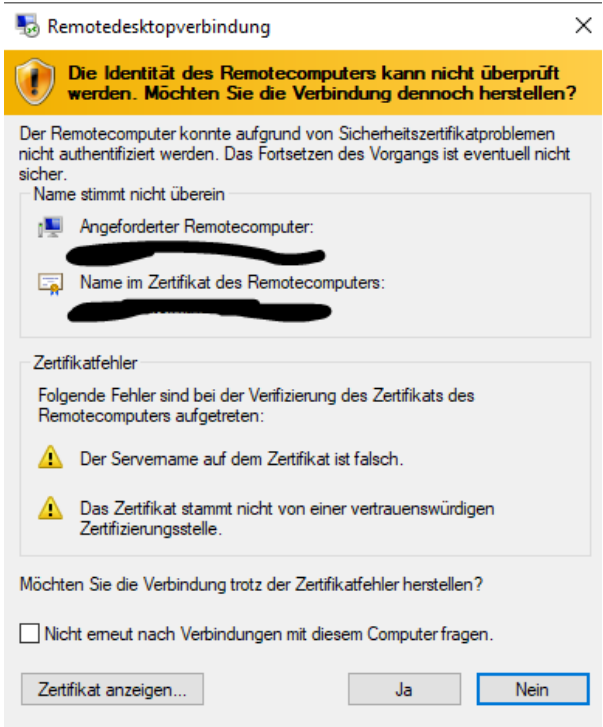


Quelle: https://thehackernews.com/2018/07/rdp-shop-dark-web.html

- RDP (Remote Desktop Protocol)
  - v10 mit Windows 10 (Update 1511) und Server 2016 TP 4
  - TCP-Port 3389, seit v8 auch UDP 3389 (schneller)
  - seit v5.2(Vista) TLS 1.0 Support
  - Desktop soll nie offen im Internet sein (ohne Firewall und VPN)
    offene RDP Zugänge werden weiterverkauft
  - laut FBI wird RDP für 70-80% aller Ransomware Angriffe verwendet
    sobald ein Angreifer einen Rechner innerhalb des Firmennetzes kontrolliert, kann er mit Man-in-the-Middle potentiell weitere RDP-Zugangsdaten abgreifen
  - via Downgrade-Attacke kann man Zugangsdaten erbeuten
  - viele Windows-Systeme akzeptieren die unzureichende Verschlüsselung "Standard RDP Security“

Remote Zugang Desktop

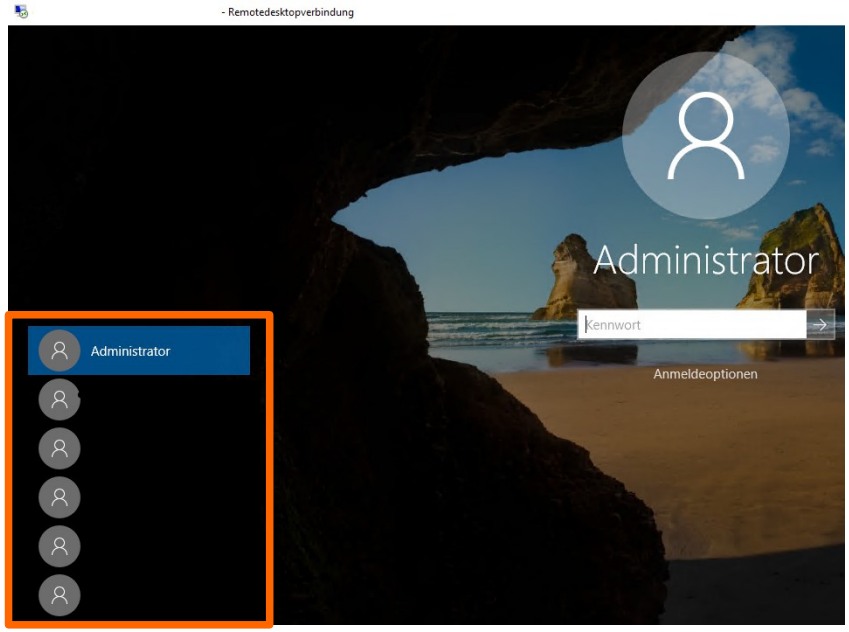
- RDP (Remote Desktop Protocol)
  - selbstsignierte Zertifikate problematisch
    „In einer ordentlich konfigurierten IT-Landschaft sollten derartige Warnungen eine Ausnahme darstellen, die einen Anruf bei der IT-Abteilung rechtfertigt.“
  - Enhanced RDP Security = Standard RDP in TLS-Tunnel
  - Optimal ist: Enhanced RDP Security mit NLA (Network Level Authentication) und CredSSP-Protokoll (Credential Security Support Provider)
  - RDP-Authentifizierung ohne NLA offenbart Benutzernamen des Systems und erleichtert Brute-Force-Angriffe
  - Nachteile NLA
    - rdesktop nicht out-of-the-box, freerdp schon
    - Passwortänderung beim Login nicht möglich, falls es abgelaufen ist



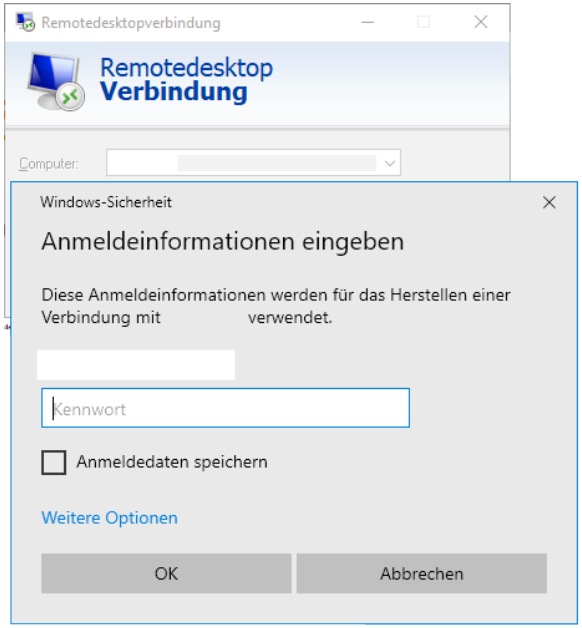
Quelle: https://www.syss.de/fileadmin/dokumente/Publikationen/2017/2017_11_07_Vollmer_Angriffe_auf_RDP.pdf

Remote Zugang Desktop

- RDP (Remote Desktop Protocol)
  - ohne NLA (Network Level Authentication)



mit NLA



Remote Zugang Desktop

- RDP (Remote Desktop Protocol)
  - Wie kann man RDP Modus testen:

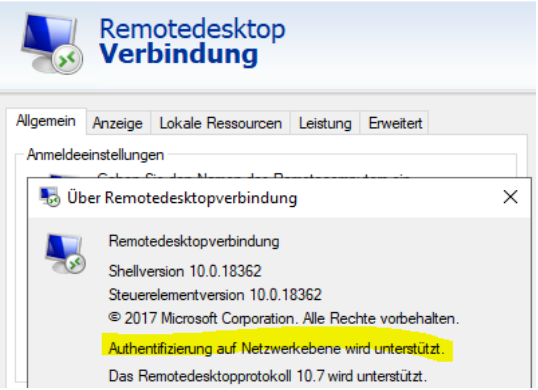
```
~# nmap -P0 -p 3389 --script rdp-enum-encryption 192.168.x.x

Starting Nmap x.xx (  ) at 2020-05-06 15:00 CEST Nmap scan report for 192.168.x.x
Host is up (0.00046s latency).
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-enum-encryption:
|   Security layer
|_    CredSSP: SUCCESS
```

  - zum Testen ob RDP Standard Security erlaubt wird:

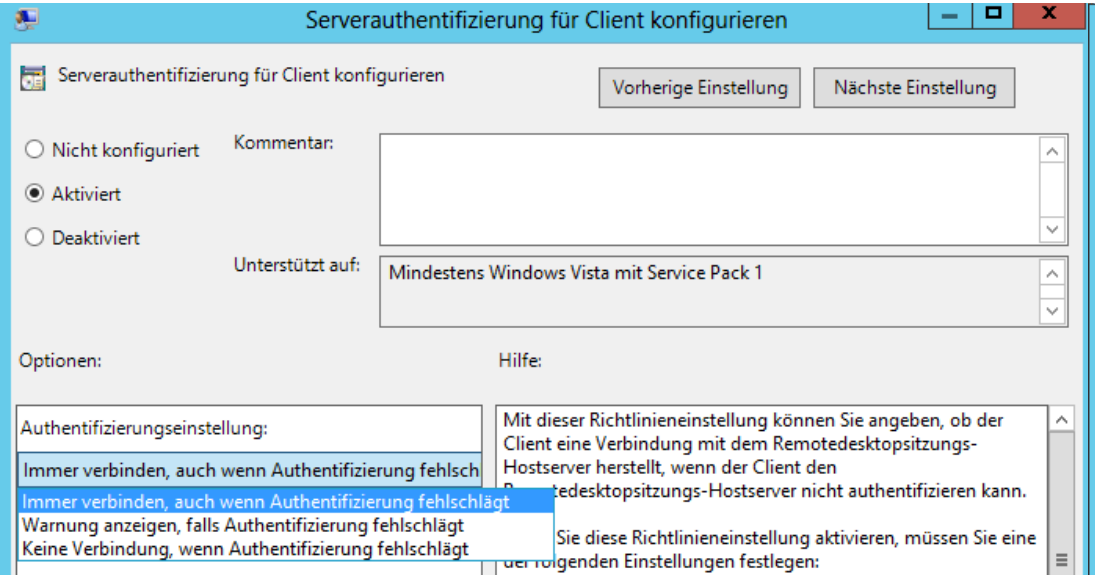
    xfreerdp /sec:rdp /v:<IP> /u:
    /sec … force protocol security. proto can be one of rdp, tls or nla.

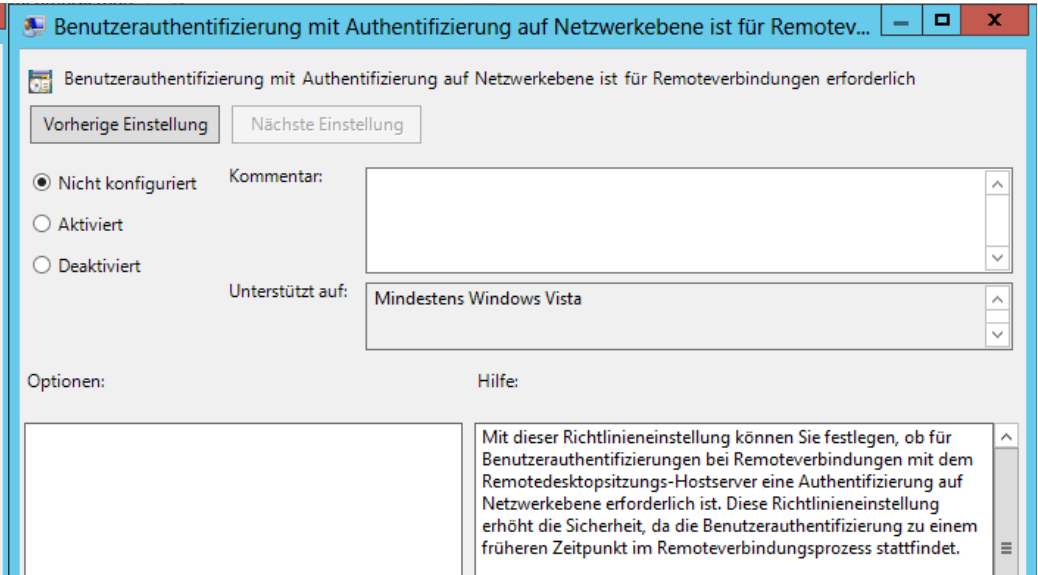
    mstsc.exe
    „enablecredsspsupport:i:0“ in ../Documents/Default.rdp setzten (**Zurücksetzen nach Test!**)



Remote Zugang Desktop

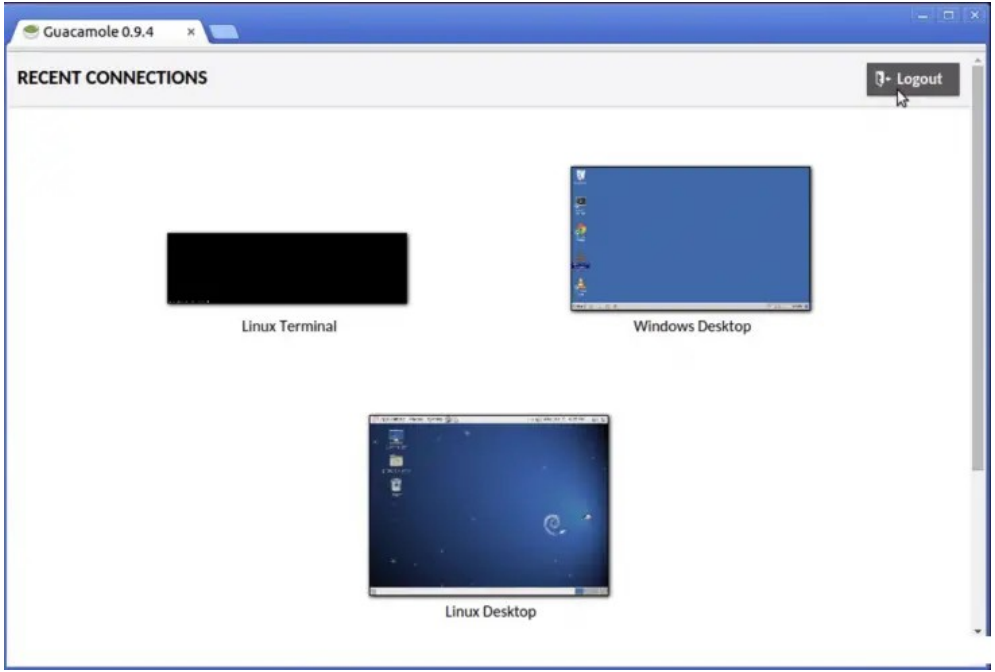
- RDP (Remote Desktop Protocol)
  - Gruppenrichtlinie für RDP Client und Server
    - Client: Computer Configuration\Policies\Administrative Templates\Windows Components\Terminal Services\Remote Desktop Connection Client\Configure server authentication for client
    - Server: Computer\Policies\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security





Remote Zugang Desktop

- RDP (Remote Desktop Protocol)
  - Zugriff über zentralen Gateway
    - Alternative zu direkten Zugriff
    - MS RDS oder VMware UAG
    - OSS Apache Guacamole
      - RDP, VNC, SSH
  - Mehr RDP Infos bei Heise
    - Artikelserie
    - plus Webinar
    - https://heise.de/-4700048



Quelle: https://www.heise.de/hintergrund/Remote-Desktop-via-RDP-Best-Practices-4-4-4711807.html

Agenda

- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

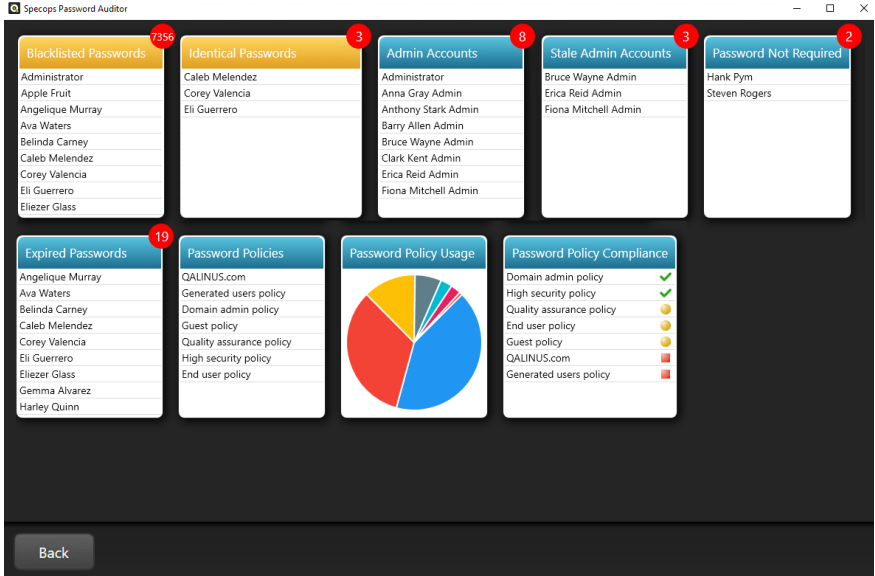
Passwörter und 2FA

- Passwort-Richtlinien
  - BSI IT-Grundschutz ORP.4.A23
    - „IT-Systeme oder Anwendungen SOLLTEN NUR mit einem validen Grund zum Wechsel des Passworts auffordern. Reine zeitgesteuerte Wechsel SOLLTEN vermieden werden. Es MÜSSEN Maßnahmen ergriffen werden, um die Kompromittierung von Passwörtern zu erkennen.“
  - NIST.SP.800-63b
  - Microsoft Password Guidance, 2016
  - Specops Password Auditor
    - Freeware

Advice to IT Administrators

Azure Active Directory and Active Directory allow you to support the recommendations in this paper:

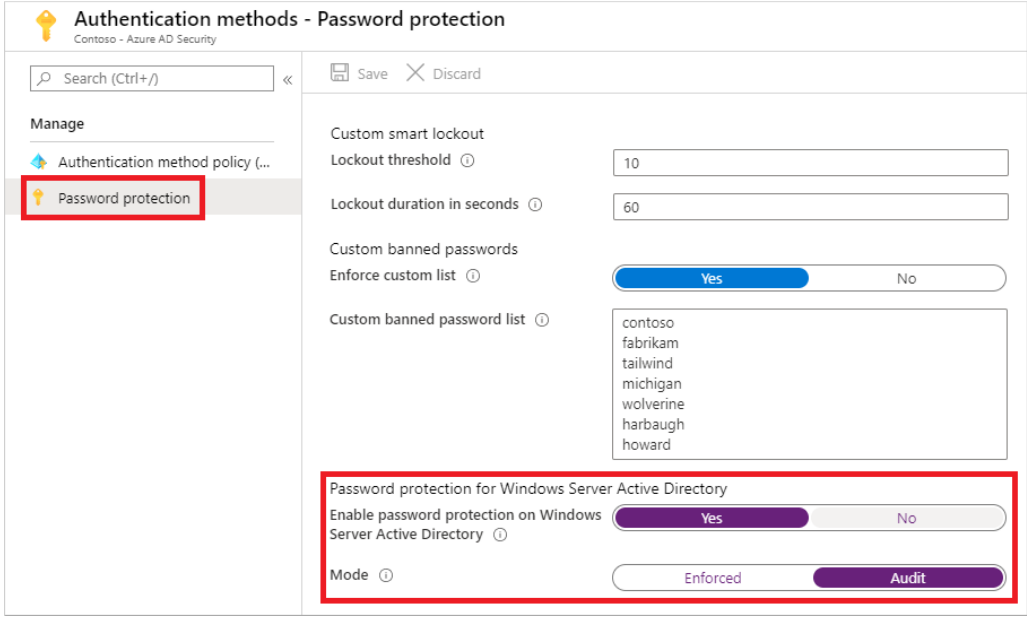
1. Maintain an 8-character minimum length requirement (and longer is not necessarily better).
2. Eliminate character-composition requirements.
3. Eliminate mandatory periodic password resets for user accounts.
4. Ban common passwords, to keep the most vulnerable passwords out of your system.
5. Educate your users not to re-use their password for non-work-related purposes.
6. Enforce registration for multi-factor authentication.
7. Enable risk based multi-factor authentication challenges.

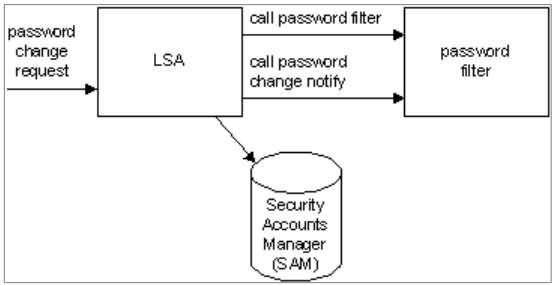


Quelle: https://specopssoft.com/support-docs/specops-password-auditor/overview/
Quelle: https://www.microsoft.com/en-us/research/wp-content/uploads/2016/06/Microsoft_Password_Guidance-1.pdf

Passwörter und 2FA

- Passwort-Richtlinien
  - Technische Umsetzung
    - AD Domain Policy
    - verschiedenen Richtlinien im AD mit: Fine-Grained Password Policy (FGPP)
    - Password-Filter DLL
      - Azure AD Password Protection
      - Specops Password Policy via GPO (kostenpflichtig)
      - Lithnet Password Protection for Active Directory (LPP)





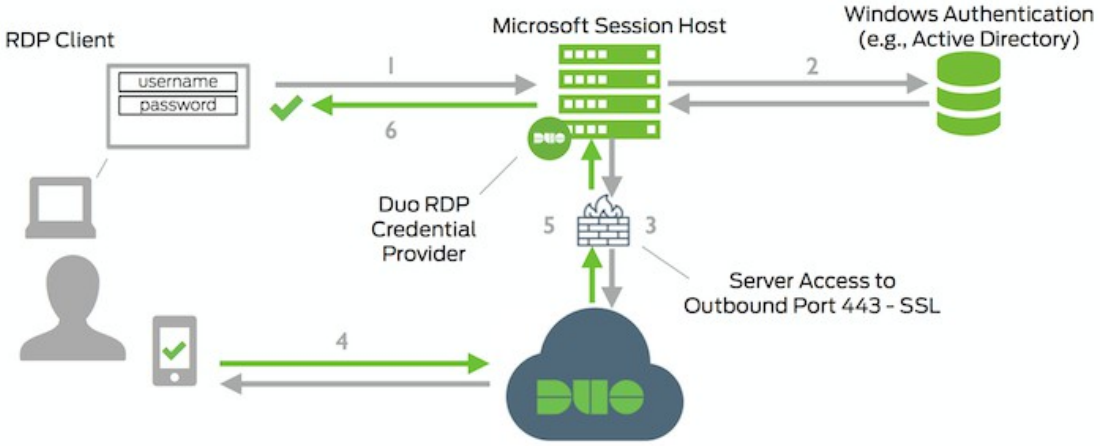
Quelle: https://docs.microsoft.com/en-us/windows/win32/secmgmt/installing-and-registering-a-password-filter-dll
Quelle: https://docs.microsoft.com/de-de/azure/active-directory/authentication/howto-password-ban-bad-on-premises-operations

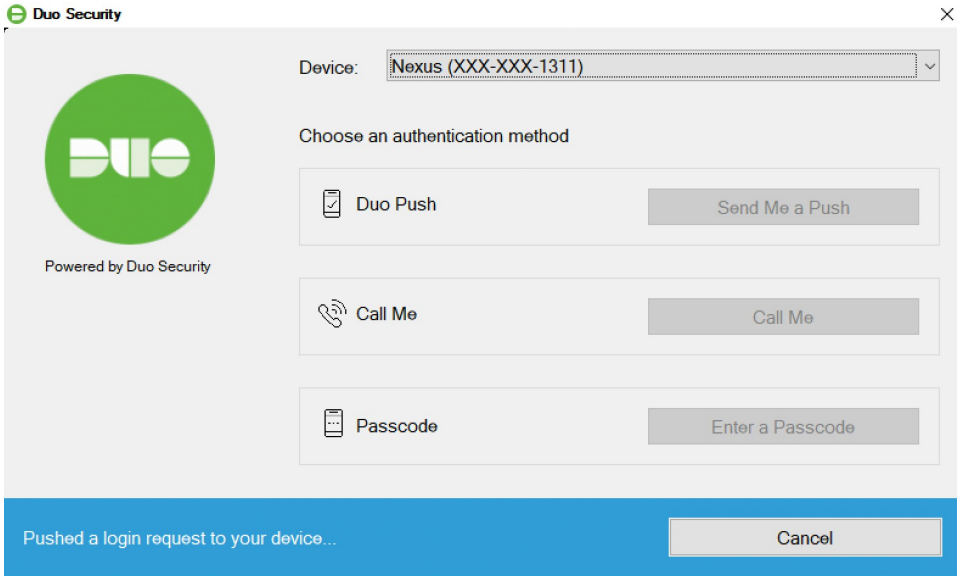
Passwörter und 2FA

- 2FA für Home-Office Zugang umso wichtiger
- für RDP, VDI, Web, VPN sinnvoll
  - Smartcard für RDP in Windows integriert
  - klassiches 2FA mit TOTP, HOTP nicht in Windows integriert
- Azure MFA von Microsoft
  - für Terminal-Services seit Server 2012 R2 nur mehr via Remote Desktop Gateway (RDG)
  - kann auch an internen RADIUS-Server angebunden werden
  - lokaler MFA-Server per 1.7.2019 nicht mehr für Neuinstallationen verfügbar
  - viele Features von verwendeter Lizenz abhängig
  - SSO mit sehr vielen Third-Party-Apps

Passwörter und 2FA

- Duo MFA von Cisco
  - Duo Free: bis 10 User kostenlos
  - Abo-Modelle mit Preis pro User/Monat
  - Duo Authentication for Windows Logon
    - auch für RDP-Login





Quelle: https://www.duo.com

Passwörter und 2FA

- PrivacyIDEA
  - Webinterface für Token-Verwaltung
  - OpenSource
  - flexible Anbindung via RADIUS, SAML und LDAP-Proxy
  - kostenpflichtiger Windows Credential Provider
  - eigene App für Software-Token (SHA1/SHA256/SHA512)
  - Vielzahl an Token wird unterstützt
  - mit Authentication Policy „otppin=userstore“ können nahezu beliebige Apps MFA-fähig gemacht werden („Passwort + OTP“)

`otppin=tokenpin`

This is the default behaviour. The user needs to pass the OTP PIN concatenated with the OTP value.

`otppin=userstore`

The user needs to pass the user store password concatenated with the OTP value. It does not matter if the OTP PIN is set or not. If the user is located in an Active Directory the user needs to pass his domain password together with the OTP value.

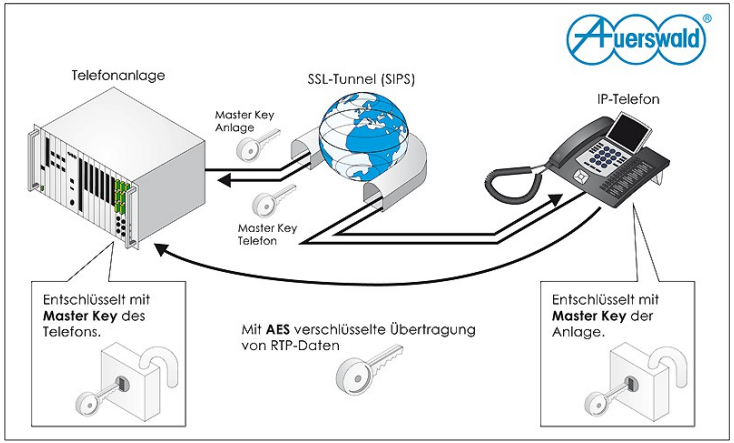
Quelle: https://netknights.it/produkte/privacyidea-credential-provider/

Agenda

- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

Telefonie/VOIP und Kommunikations-Tools

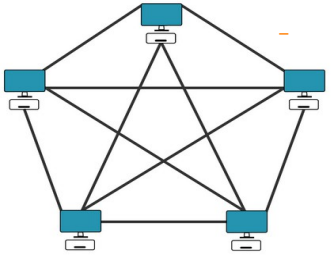
- Klassische Telefonanlage im Home-Office
  - oft nur Weiterleitung der DW an Handy/Festnetz als Option?
- VOIP
  - Zugriff auch im Home-Office möglich
  - VOIP-Server sollte nicht offen im Internet stehen
  - Verschlüsselung soweit möglich verwenden
  - Limitierung auf fixe IP-Adressen oder via VPN (vorallem ohne Verschlüsselung)
  - Session Initiation Protocol (SIP): TCP/UDP Port 5060, 5061(TLS)
  - Real-time Transport Protocol (RTP) und Secure RTP (SRTP), UDP, Port>1024
  - Schlüsselaustauch von SRTP erfolgt via SDP/SIP
    - Alternative dazu ist DTLS (TLS over UDP)



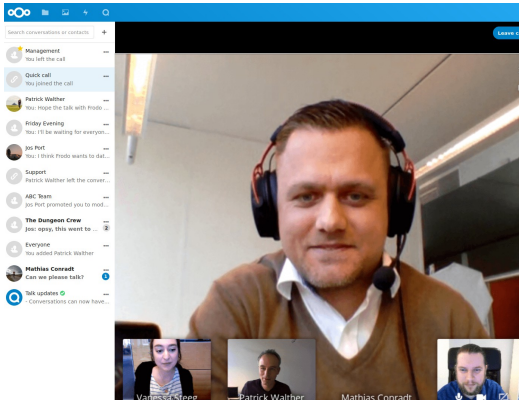
Quelle: https://blog.auerswald.de/wp-content/uploads/2013/01/Grafik_Verschl%C3%BCsselung_VoIP_Gespr%C3%A4che_13_02.png

Telefonie/VOIP und Kommunikations-Tools

- Kommunikations-Tools
  - On Premise und Open Source:
    - Openfire Server: XMPP-Server für Instant Messaging
      - z.b. Spark oder Pidgin als Client
      - TLS möglich, Chat-Verlauf und IM-Account Passwort unverschlüsselt
    - Nextcloud Talk
      - WebRTC mit Peer-to-Peer (4-6 TN), High Performance Backend kostenpflichtig
      - End-to-end encryption (E2EE) ohne High-performance Backend (HPB)
      - HPB kann selbst gehostet werden
      - Video Verification für Dokumente
    - Jitsi Meeting
      - 1:1 Meetings mit DTLS-SRTP für Audio, Video verschlüsselt
      - größere Meetings auf Jitsi Videobridge zentral entschlüsselt
      - E2EE in Arbeit mit neuem insertable stream API von Chrome



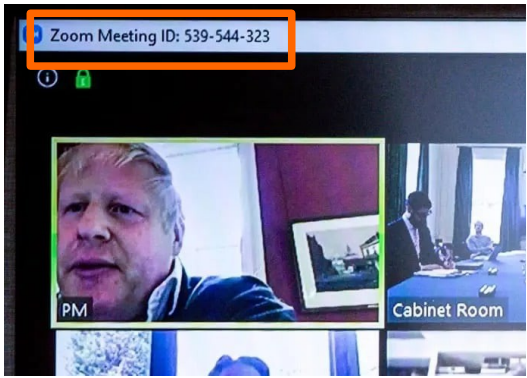
OnSIP uses a full mesh network for end-to-end encryption in video calls.



Quelle: https://onsip.com

Quelle: https://github.com/nextcloud/spreed/#scalability

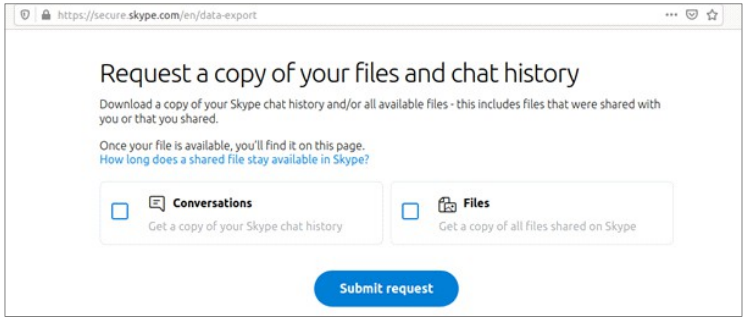
Telefonie/VOIP und Kommunikations-Tools



- Gehostete Lösungen für Unternehmenseinsatz
  - BSI Kompendium Videokonferenzsysteme (vom 14.4.2020)
  - Microsoft Teams
    - Skype for Business wurde integriert, keine On-Premise Option
    - seit Ende März ist auch ein Chat/Anruf von Teams an Skype-User möglich
    - Video-Konferenz (max. 300 Teilnehmer, dzt 9 Videos gleichzeitig)
      → wird noch 2020 auf 49 gleichzeitige Videos erhöht
    - viele Unternehmensfeatures, Telefonanlage auch integrierbar, kein E2EE
  - Zoom
    - für Video-Konferenzen, bis zu 49 Videos gleichzeitig
      rasant gewachsen, einige Sicherheitsprobleme, z.B. Zoom-Bombing
    - E2EE seit Juni optional möglich
  - Google Meet
    - kein E2EE, 16 gleichzeitige Videos

Quelle: https://hotforsecurity.bitdefender.com/blog/zoom-takes-action-after-meeting-ids-leak-in-careless-screenshots-22923.html

Telefonie/VOIP und Kommunikations-Tools



- Nicht speziell für Unternehmenseinsatz
  - Skype
    - für Unternehmenseinsatz nur bedingt zu empfehlen siehe https://heise.de/-3082090
    - Desktop-Sharing, Video-Konferenz (max. 50 Teilnehmer, 9 Videos gleichzeitig)
    - alle übertragenen Daten verschlüsselt, private Schlüssel liegen bei Microsoft, kein E2EE
  - WhatsApp
    - Video-Konferenz mit max. 4 Teilnehmern, in aktuellster Version 8 Teilnehmer
    - Video nur via Smartphone-App, nicht in Web-Whatsapp
    - E2EE, Nachrichten auch am Smartphone verschlüsselt gespeichert Backups in GDrive/iCloud unverschlüsselt
  - Telegram, Signal
    - freie Alternative zu WhatsApp, E2EE-Option

Quelle: https://www.igniterealtime.org und https://blog.whatsapp.com/group-video-and-voice-calls-now-support-8-participants

Agenda

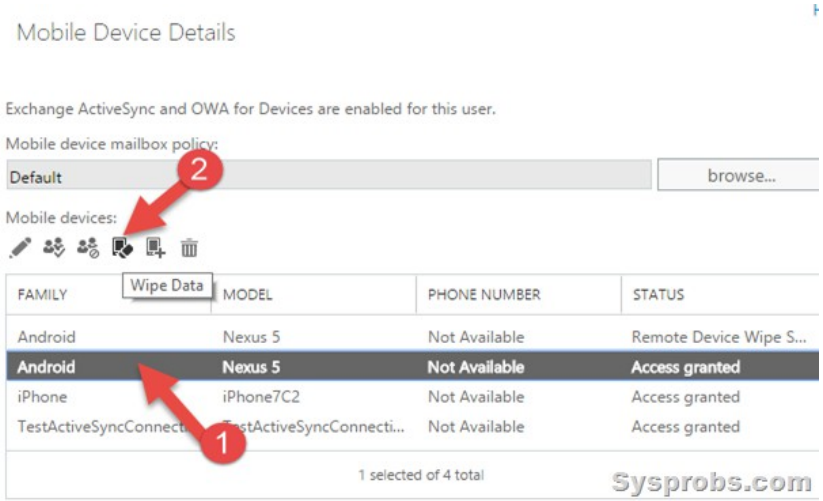
- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

Tragbare IT-Systeme (Notebook, Smartphone)

- BSI IT-Grundschutz Bausteine/Maßnahmen:
  - INF.9.M5 Zeitnahe Verlustmeldung
  - INF.9.M6 Entsorgung von vertraulichen Informationen
  - INF.9.M9 Verschlüsselung tragbarer IT-Systeme und Datenträger
  - INF.9.M10 Einsatz von Diebstahlsicherungen
  - INF.9.M11 Verbot der Nutzung unsicherer Umgebungen
  - OPS.1.2.7 Verkauf/Aussonderung von IT
  - SYS.3.2.2 Mobile Device Management

Tragbare IT-Systeme (Notebook, Smartphone)

- Bring your own device (BYOD) oder firmeneigene Hardware
- seit MS Exchange 2010 gibt es ActiveSync Quarantäne mit Remote Wipe
- MS Intune
  - sehr umfassende cloudbasierte Lösung
  - Lizenzierung nur über Abo-Modell möglich
- VMware Workspace ONE
  - Unified Endpoint Management (UEM)
  - Airwatch wurde integriert
  - OPSWAT end-point compliance check
  - Lizenzierung pro User/Gerät



Quelle: https://www.sysprobs.com/how-to-disable-or-enable-activesync-particular-user-on-exchange-2013-2016

Agenda

- Home-Office bei der Thomas-Krenn.AG
- der häusliche Arbeitsplatz
- Remote Zugang Desktop
- Passwörter und 2FA
- Telefonie/VOIP und Kommunikations-Tools
- Tragbare IT-Systeme (Notebook, Smartphone)
- Sensibilisierung der Mitarbeiter

Sensibilisierung der Mitarbeiter

- IT-Notfallkarte
  - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/IT-Notfallkarte/IT-Notfallkarte/it-notfallkarte_node.html
- Checkliste Home-Office mit 7 Fragen
  - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Angebote/Checkliste-Home-Office/Seite01/checkhoffice_frage1_node.html
- Awareness gerade im Home-Office umso wichtiger

VERHALTEN BEI IT-NOTFÄLLEN

Ruhe bewahren & IT-Notfall melden
Lieber einmal mehr als einmal zu wenig anrufen!

IT-Notfallrufnummer:

Wer meldet?

Welches IT-System ist betroffen?

Wie haben Sie mit dem IT-System gearbeitet?
Was haben Sie beobachtet?

Wann ist das Ereignis eingetreten?

Wo befindet sich das betroffene IT-System?
(Gebäude, Raum, Arbeitsplatz)

Verhaltenshinweise

Weitere Arbeit am IT-System einstellen | Beobachtungen dokumentieren | Maßnahmen nur nach Anweisung einleiten

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik

„If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.“ *Bruce Schneier, 2000*

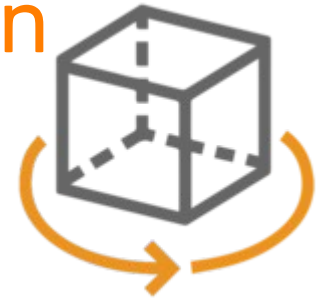
GUT GERÜSTET

Aufmerksames Personal ist für Cyber-Sicherheit so wichtig wie Firewall und Co.

Allianz für Cyber-Sicherheit

© Bundesamt für Sicherheit in der Informationstechnik (BSI)

Produkte und Lösungen von Thomas Krenn



- Produkte und Lösungen
  - https://www.thomas-krenn.com/de/produkte/einsatzzweck/vdi.html
  - https://www.thomas-krenn.com/de/produkte/einsatzzweck/opnsense-firewalls.html
  - https://www.thomas-krenn.com/de/produkte/pcs-thinclients/zero-thin-clients.html
- Webinare zu dem Thema:
  - https://www.thomas-krenn.com/de/tkmag/webinare/home-office-die-moeglichkeit-fuer-business-continuity/
  - https://www.thomas-krenn.com/de/tkmag/webinare/mit-vdi-und-rds-zur-flexiblen-home-office-loesung-fuer-unternehmen/
  - https://www.thomas-krenn.com/de/tkmag/webinare/virtuelle-desktop-infrastruktur-vdi-ein-paradigmenwechsel-der-server-client-infrastruktur
- #buylocal #buymittelstand
  - https://www.thomas-krenn.com/de/tkmag/allgemein/corona-hausaufgaben-fuer-den-deutschen-mittelstand/

Vielen Dank für Ihre Aufmerksamkeit!

THOMAS KRENN®