BeyondTrust

# Die Remote Access Challenge – Hat VPN ausgedient?

25. Oktober 2022

**Christoph Pontau**
Solutions Engineer

# Was sind die heutigen Herausforderungen privilegierter Zugänge?

# Weitreichende Cyberattacken

## Cyber-Angriff auf Uniklinik Düsseldorf: #Shitrix schlug zu

Die Erpresser kamen über eine Sicherheitslücke im VPN-Gateway – wahrscheinlich schon vor Monaten.

Lesezeit: 3 Min. In Pocket speichern 207

## Hacker-Angriff auf Reiseveranstalter FTI: So groß ist der Schaden

Im Oktober hat das Touristikunternehmen FTI öffentlich gemacht, gehackt worden zu sein. Nun bekannte sich die Hacker-Gruppe Conti zu der Cyber-Attacke – und gibt einen Eindruck von dessen Ausmaß.

19.11.2021, 19:30 Uhr • 2 Min. Lesezeit

Zehntausende Kundendaten betroffen

## Hacker stoßen erneut auf Sicherheitslücken bei Corona-Testzentren

Knapp 174.000 Buchungsbestätigungen und Testergebnisse aus 34 Testzentren von Coronapoint ließen sich ohne großen Aufwand von Unbefugten abrufen. Sie enthielten Namen, Adressen und mitunter auch Ausweisnummern.

23.06.2021, 16.45 Uhr

## Hacker attackieren Media Markt Saturn

08.11.2021, 16:43 Uhr | t-online, jmm


## IT-Angriff legt Schwerin und Landkreis lahm

Der IT-Dienstleister für Schwerin und einen Landkreis musste nach einem Ransomware-Angriff offline gehen. Die Bürgerbüros sind vorerst geschlossen.

15. Oktober 2021, 13:00 Uhr, Sebastian Grüner/ dpa

## Erster Cyber-Katastrophenfall in Deutschland – Landkreis Anhalt-Bitterfeld lahmgelegt

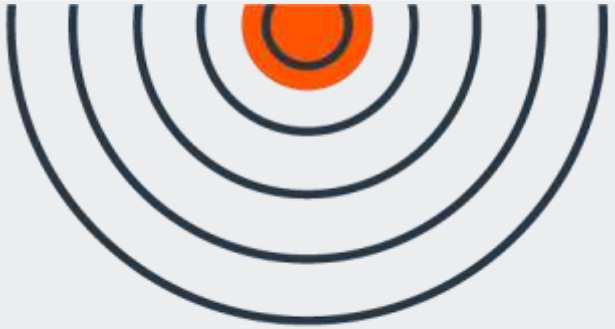
Veröffentlicht am 10.07.2021 | Lesedauer: 3 Minuten

# Digitaler Wandel mit Sicherheitsrisiken

**DIGITALE TRANSFORMATION UND CLOUD-NUTZUNG KÖNNEN HOHE SICHERHEITSRISIKEN SCHAFFEN**

- Verlagerung auf Remote-Work-Strukturen und beschleunigte Cloud-Nutzung
- Sicherheitsfragen werden zum Teil vernachlässigt
- Remote-Mitarbeiter sind durch Einsatz eigener Endgeräte (BYOD) anfälliger und verursachen Schatten-IT

*Wachstum der IT-Infrastruktur, Perimeter-Veränderungen, komplexeres Privilegien-Management.*



# ZERO TRUST

Eine sich entwickelnde Reihe von Cybersicherheitsmustern, welche die Verteidigung von statischen, netzwerkbasierten Perimetern auf Benutzer, Anlagen und Ressourcen ausrichten.

*NIST Special Publication 800-207, Zero Trust Architecture*

# Welche Nachteile können durch VPN Nutzung entstehen?

- Fehlende Möglichkeit der Auditierung
  - Wann war welcher User angemeldet
  - Auf welche Systeme hat der User zugegriffen
  - Wie hat der User auf Systeme zugegriffen

- Fehlende Möglichkeit der Einschränkung des Zugangs
  - User hat Zugriff auf gesamtes VLAN
  - Externe Dienstleister teilen sich Zugänge
  - Keine Nutzung unbekannter Geräte (BYOD)

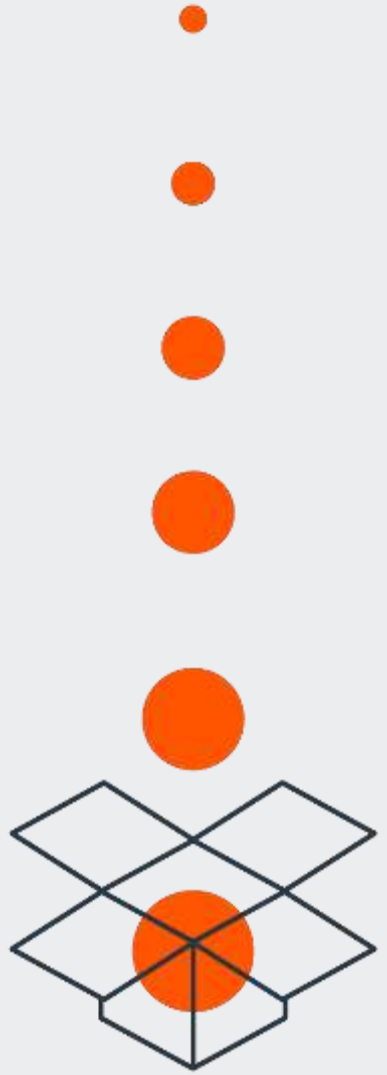
# Welche Nachteile können durch VPN Nutzung entstehen?

- Fehlende Limitierung der Benutzerberechtigung
  - User kann zu jeder Zeit auf Systeme springen
  - User kann auf alle Systeme im Netzwerksegment springen
  - Benutzer darf sich auf dem Zielsystem frei bewegen

- Fehlende Integrationsmöglichkeiten
  - Anbindung an Ticketsystem
  - Anbindung an MFA-System
  - Anbindung an SIEM-Tool

# Abhilfe schaffen

- Einschränkung der Zugriffe auf Zielsysteme
- Keine unüberwachten Zugänge
- Multi-Faktor-Authentifizierung
- Kein Direkt-Zugriff mit unbekannten Geräten
- Approval Workflows implementieren
- Überwachung der Lösung mit SIEM-Tool
- Verwaltung und Nutzung (Einspeisung) von Kennwörtern



# Vielen Dank

Bitte kontaktieren Sie uns, falls Sie weitere Fragen haben:
kontakt@beyondtrust.com

Besuchen Sie uns in

## Halle 7A
## Stand 317

beyondtrust.com