# Cyber-Security

**Dirk Nehring, MarcanT AG**

Prävention statt Frustration

18.08.2021

# Wir über uns
# MarcanT-Team

# Wir über uns
## Überblick

- Die MARCANT® AG ist als M2M Solution Provider, Internet Systemhaus und ISP (RIPE-Mitglied) spezialisiert auf
  - Sicherheit im Internet
  - Vernetzung von Standorten, Maschinen und mobilen Mitarbeitern
  - Mobile Lösungen mit LTE/ UMTS/ GPRS für Business- und M2M-Anwendungen
  - Monitoring Services
  - Netzwerkinfrastruktur
  - Cloud Backup inkl. Desaster Recovery

# IT-Herausforderungen 2021

- Globalisierung des Marktes
- Fortschreitende Digitalisierung
- Covid19-Pandemie, weltweite Rezession, Lieferkettenausfälle
- Innovation, geistiges Eigentum, Schutz des Eigentums
- Angriffe von Außen (oder Innen?), Datendiebstahl, Manipulation

Ransomware-Attacke

# Erpresser verlangen Lösegeld von Landkreis Anhalt-Bitterfeld

Seit Tagen herrscht amtlicher Notstand in Anhalt-Bitterfeld, weil Daten des Landkreises verschlüsselt wurden. Die Kriminellen verschafften sich den Zugang wohl durch eine Windows-Sicherheitslücke.

Fleischkonzern JBS

## US-Präsident Biden e… Hackerangriff Vergelt…

Der Ransomware-Angriff auf den weltgrößte… Plan. Der US-Präsident denkt über einen Ge…

03.06.2021, 11.02 Uhr

RANSOMWARE

## Selbst die Drucker sprangen nicht mehr an

VON STEPHAN FINSTERBUSCH - AKTUALISIERT AM 06.07.2021 - 15:25

## Microsoft meldet … mutmaßlich russis…

Die Hackergruppe Nobelium s… diplomatische Spannungen z… Angaben von Microsoft erneu…

28.05.2021, 19.36 Uhr

…narktkette Coop und

…ter Kaseya wurden Opfer von … bei Kaseya hatten es die Angreifer offenbar …

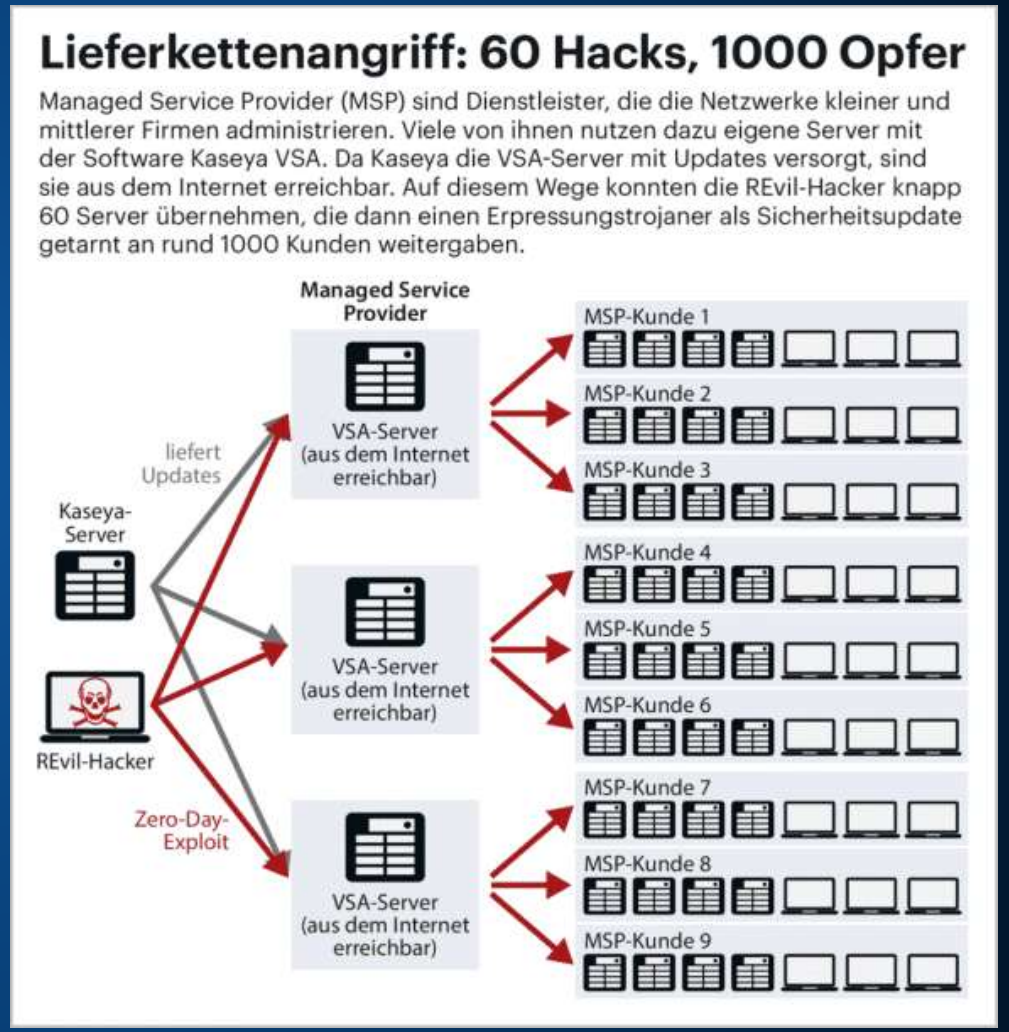
Cyberkriminalität

## Industrie warnt vor zunehmenden Hackerangriffen auf deutsche Unternehmen

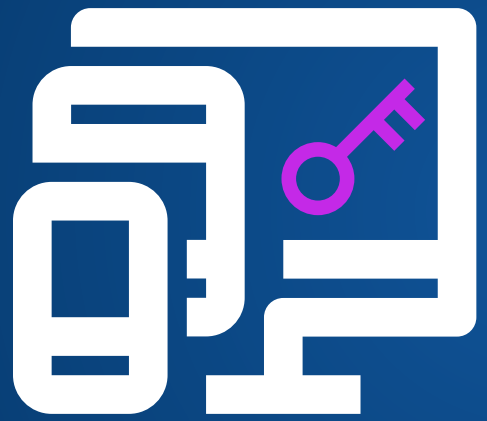
Computersysteme werden blockiert und erst freigeschaltet, wenn das Unternehmen Lösegeld zahlt: Noch nie war die Zahl der Hackerangriffe so hoch wie jetzt. Die Pandemie verschärft die Situation.

04.07.2021, 14.27 Uhr

# Beispiel Kaseya: Lieferkettenangriff


Quelle: ct



WannaCry
RYUK
REVIL

BitPaymer
MegaCortex
Dharma

# So sieht die Realität aus

- die meisten Opfer sind außerstande, alle Backdoors in der eigenen Umgebung zu entdecken, die von den Hackern zurückgelassen wurden.
- Einmal drüber nachdenken: 80% der Organisationen, die die Lösegeldforderungen für Ransomware gezahlt haben, werden erneut angegriffen, ca. 50% von derselben Gruppe!
- Das ist auch der Hauptgrund, warum einige Unternehmen ihre IT-Infrastruktur „from scratch“ inkl. neuem AD aufbauen, anstelle alle Sicherheitslücken des Altsystems zu schließen.

Quelle: VentureBeat

# Gründe

- IT-Basics fehlen:
  - überalterte Monokultur aus Windows-Systemen
  - kein ordentliches Patchmanagement, Fokus liegt auf Betriebsfähigkeit
- Labile Sicherheitslage
  - ein gestohlenes Passwort
  - ein erfolgreicher Scan auf bekannte Sicherheitslöcher
- wenige, grundlegende Sicherheitsregeln werden nicht befolgt
  - Sicherheits-Updates zügig einspielen
  - konsequent mit minimalen Rechten arbeiten
  - MFA nutzen bei Remote-Zugängen
  - funktionierende Backup-Strategie

# IT-Challenges 2021

- Agieren statt Reagieren
  - Veränderte Marktsituation
  - Neue, innovative Konzepte mit Mehrwert
- Digitalisierung, Optimierung
  - Wettbewerbsfähig bleiben
  - Arbeitsprozesse intern, Arbeitsprozesse flexibilisieren
- Sicherheit erhöhen
  - Schutz vor Angriffen
  - Daten müssen geschützt sein
  - Falls Angriffe statt finden, müssen die Pläne und Maßnahmen vorher feststehen
- Produktivität verbessern
  - Alte Prozesse durch Infrastruktur optimieren
  - Weniger manuelle Schritte (Anomalien)
  - Veraltete Ressourcen durch neue moderne und leistungsfähigere Komponenten austauschen

# Der Weg zur ganzheitlichen IT-Sicherheit I

- Optimierung der bestehenden Infrastruktur
  - Netzwerk (Redundanz, Performance)
  - Virtualisierung
  - Archivierung von Langzeitdaten

# Der Weg zur ganzheitlichen IT-Sicherheit II

- Cloud wo es Sinn macht
  - Mail Online, kein lokaler Betrieb des Servers mehr notwendig
  - Collaboration-Tools (Chats, Dokumente, Projektmanagement)
  - Effizientes Arbeiten für Mitarbeiter, unabhängig vom Standort (z.B. Home-Office)

# Der Weg zur ganzheitlichen IT-Sicherheit III

- Höhere Security
  - Next Generation Firewall für maximalen Schutz
  - Integrierte Endpoint-Lösung, abgestimmt auf die Firewall
  - Sicherheit auch auf den Smartphones
  - Regelmäßige Awareness-Tests der Mitarbeiter

# Was haben diese 3 Unternehmen gemeinsam?



## Die 3 am häufigsten gefälschten Marken bei Phishing-Attacken

[Support Account] [Added Daily Update] We ensure the security of your account is not secure - unknown devices has added on Ontario,Canada 06/09/2019.

A

Amazon.co.uk <anj4ysamaz0nsrvcs-8512506@himilowescompaniesiwi.org>
Fri 06/09/2019 10:35
customer@live.com

amazon

Customer Support

Hello Dear Customer,

We have faced some problems with your account, So Please update your account details. If you do not update your account within 24 hours (from opening this email) will be officially permanently disabled.

Update Now

We hope to see you again soon.

Amazon.com

[Support Account] [Added Daily Update] We ensure the security of your account is not secure - unknown devices has added on Ontario,Canada 06/09/2019.

A

Amazon.co.uk <anj4ysamaz0nsrvcs-8512506@himilowescompaniesiwi.org>

Fri 06/09/2019 10:35

customer@live.com

amazon

Customer Support

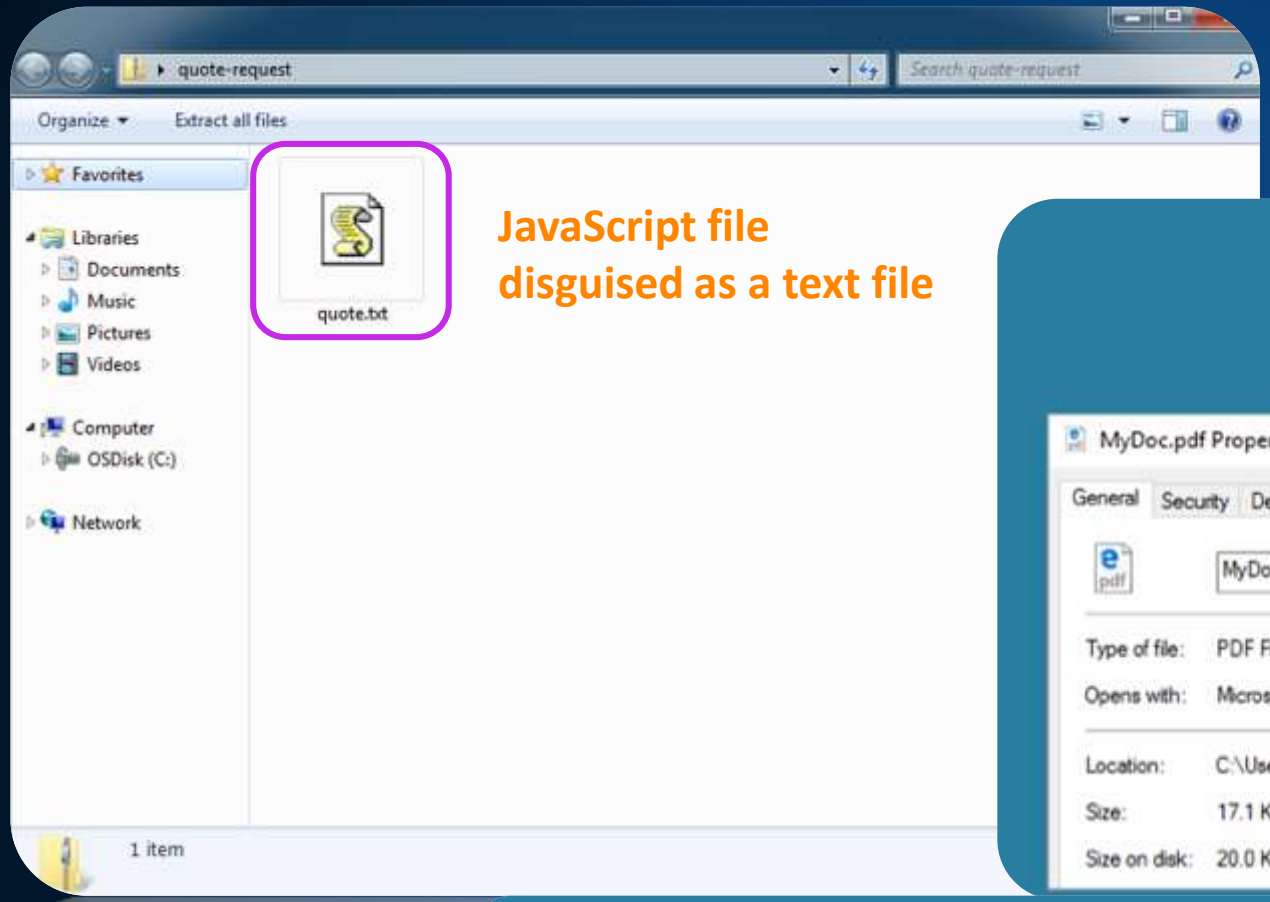
Hello Dear Customer,

We have faced some problems with your account, So Please update your account details. If you do not update your account within 24 hours (from opening this email) will be officially permanently disabled.

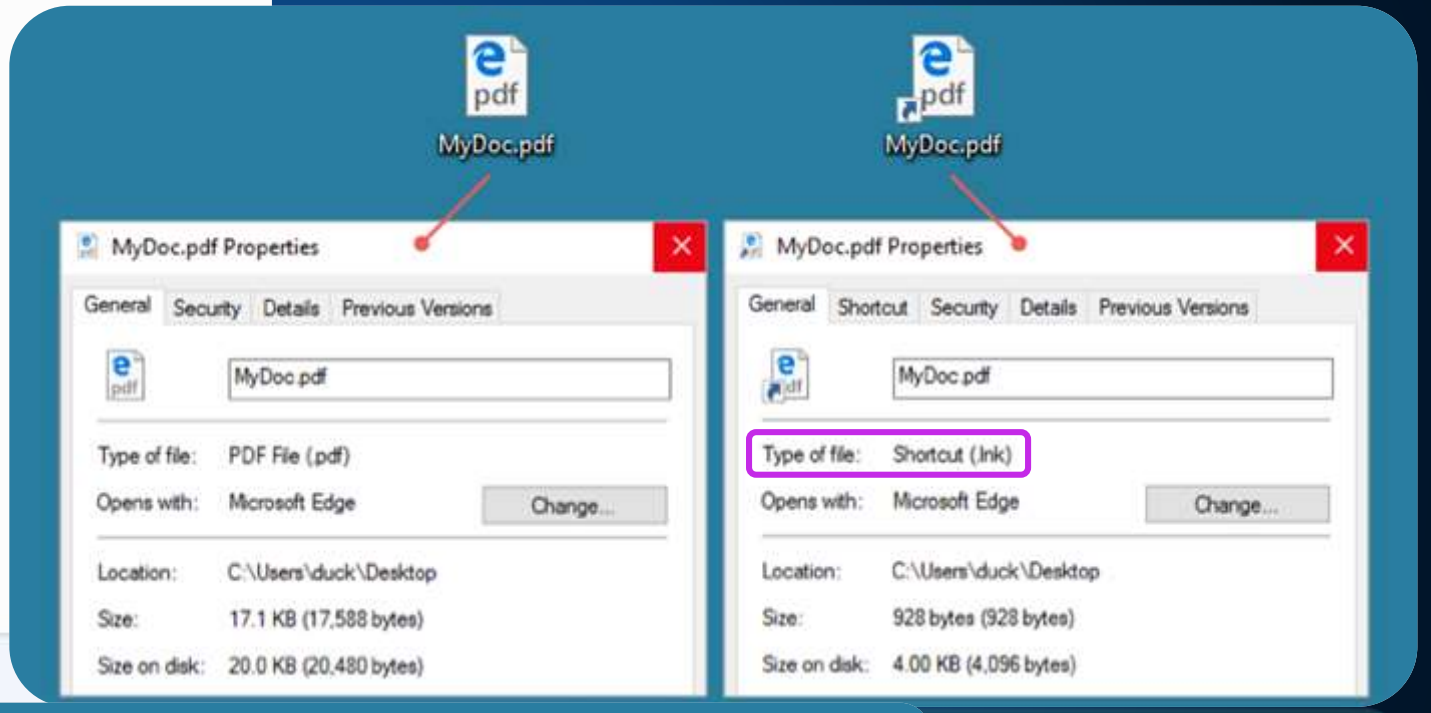
Update Now

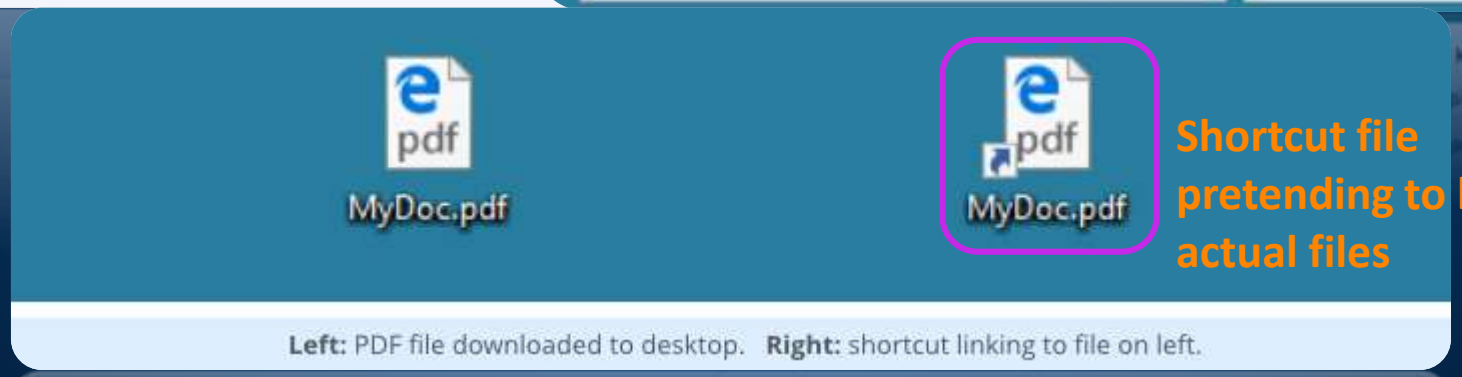
We hope to see you again soon.

Amazon.com



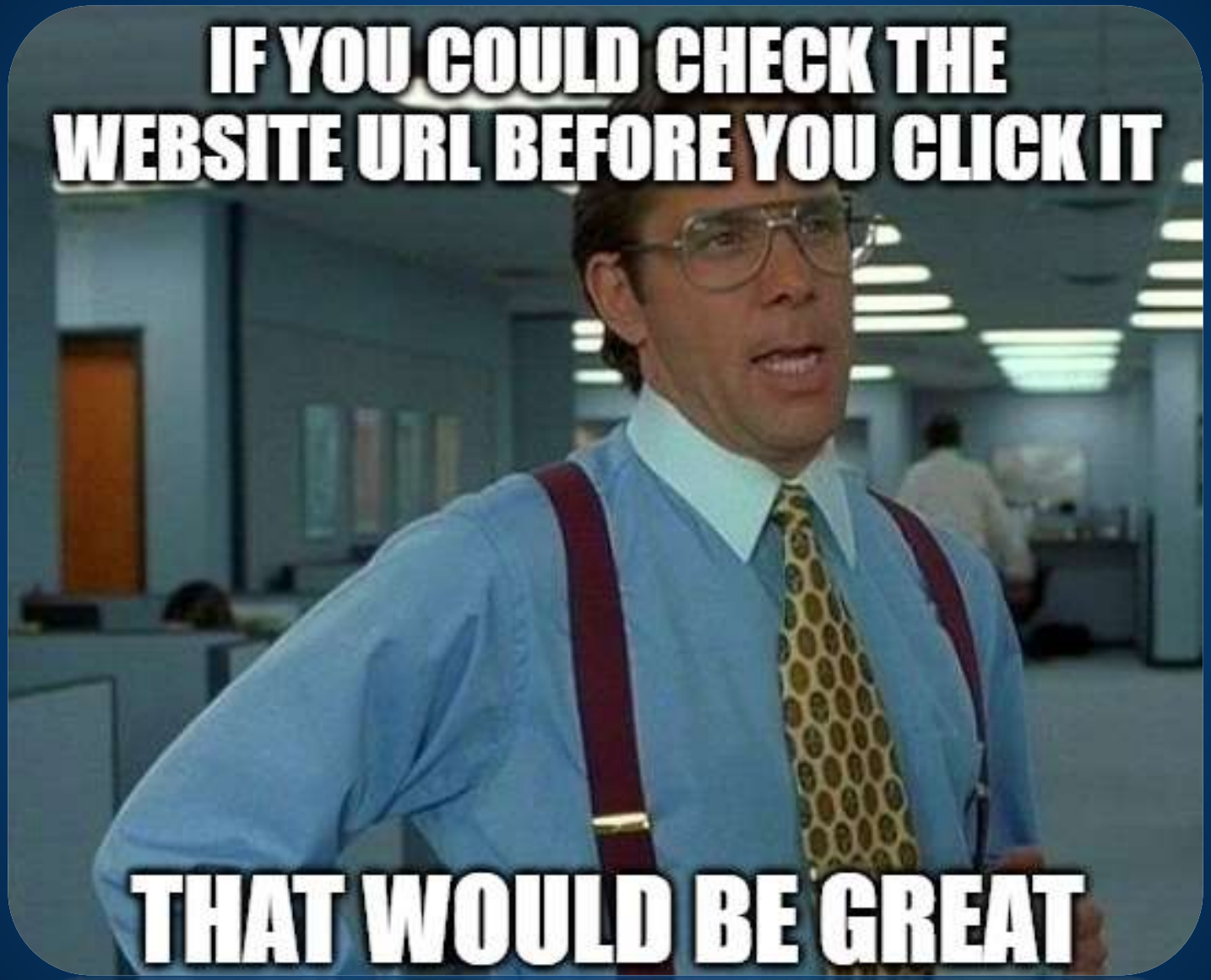

**JavaScript file disguised as a text file**



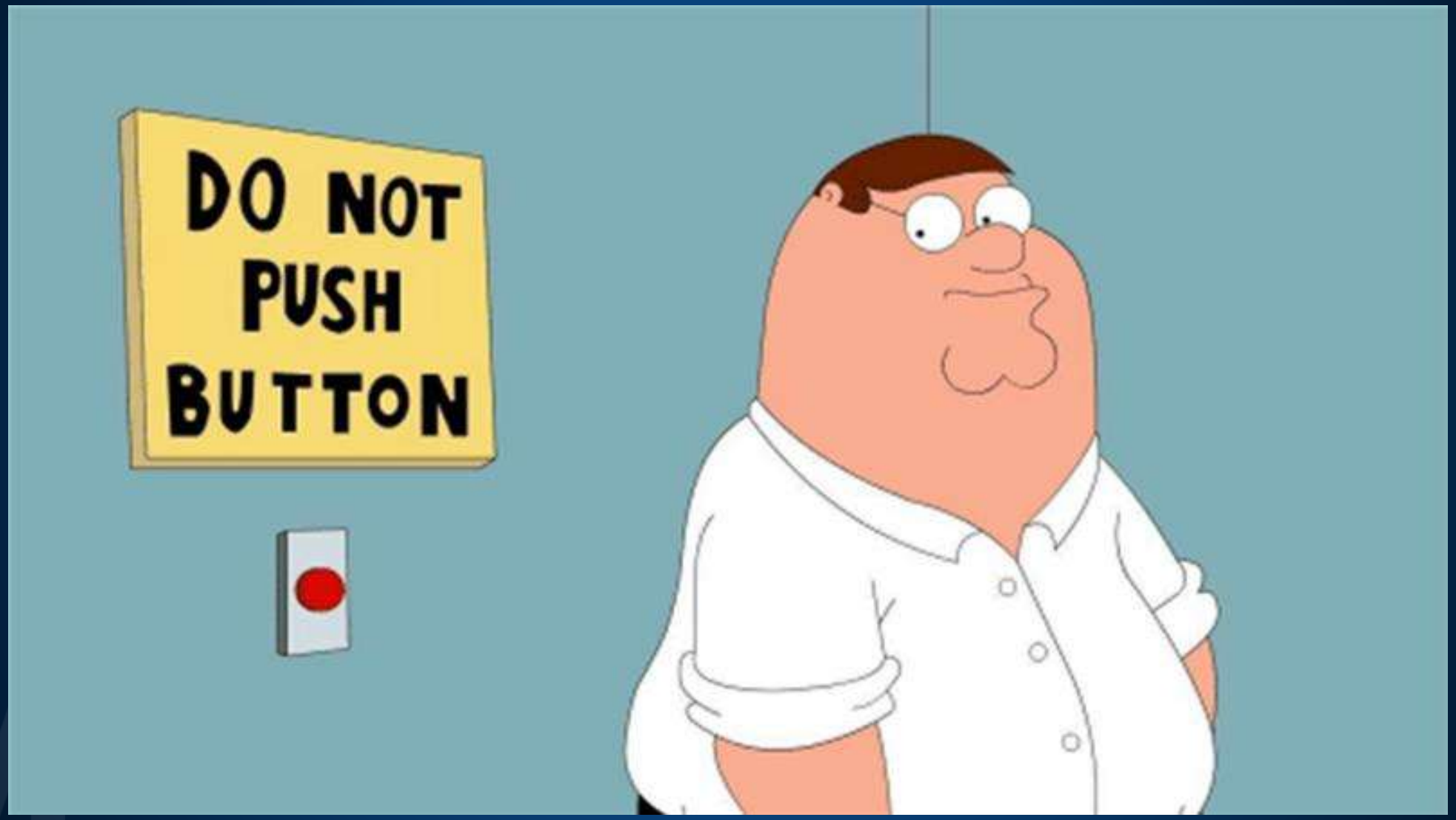

**Shortcut file pretending to be the actual files**


WWW


IF YOU COULD CHECK THE
WEBSITE URL BEFORE YOU CLICK IT
THAT WOULD BE GREAT

|  |  |
| --- | --- |
| www.google.com | www.g00gle.com |
| www.twitter.com | www.twotter.com |
| www.facebook.com | www.facebok.com |

# Mitarbeiter-Awareness



# Awareness
# Sind meine Mitarbeiter eine Gefahr für mein Unternehmen?

- Regelmäßige IT-Schulungen
- Prozesse sauber dokumentieren
- Zugriffsrechte minimal verteilen
- Authentisierung (kein Password-Sharing), MFA
- Admin-Rechte gering halten
- Überprüfen der Mitarbeiterfähigkeiten im Umgang mit Spam E-Mails

# Backup

# Backup-Strategie

- Backup Strategie mit Fallback-Lösungen (3-2-1 Prinzip)
  - Hoch Performantes und einfach zu bedienendes Backup-System
  - Mehrfache Sicherung
  - Gegen Ransomware: entweder Tape oder immutable Backups
- Infrastruktur für den „Worst-Case“ in der Cloud nachgebaut

# Fazit
# Prävention statt Frustration

- Egal wie viel Aufwand wir investieren, es wird erfolgreiche Angriffe geben
- Infrastruktur nach dem KISS-Prinzip aufbauen
- Redundanzen dort aufbauen, wo der Aufwand gering, der Vorteil hoch ist
- Zugriff auf geschultes IT-Personal
- Kosten- Nutzen Analyse für Infrastrukturentscheidungen
- Netzwerk filtern und Überwachen der Aktivitäten
- Cyber-Security für das Netzwerk
- Cyber-Security für die Enduser
- Backup-Lösung nach dem 3-2-1 Prinzip

MarcanT AG
Dirk Nehring
dnehring@marcant.net

+49 (521) 95945-0