Resilienz kritischer Infrastrukturen
Herausforderungen und Lösungsansätze der Digitalisierung

Fachtagung Katastrophenvorsorge

DKKV

Fachtagung virtuell – 25. / 26.10.2021
Katastrophenvorsorge

Manuel Atug

Ich habe #KRITIS im Endstadium

Über mich

Manuel Atug

Head of Business Development der HiSolutions AG

> 23 Jahre in der Informationssicherheit tätig

- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- langjährige Erfahrung im Bereich technische IT-Sicherheit und Auditierungen
- Themen: KRITIS, Hackback, Ethik, Cyberresilienz, Bevölkerungsschutz

- Vorstand im Cyber Security Cluster Bonn

CYBER SECURITY CLUSTER BONN

- Leitung der AG KRITIS: https://ag.kritis.info

AG KRITIS

@HonkHase

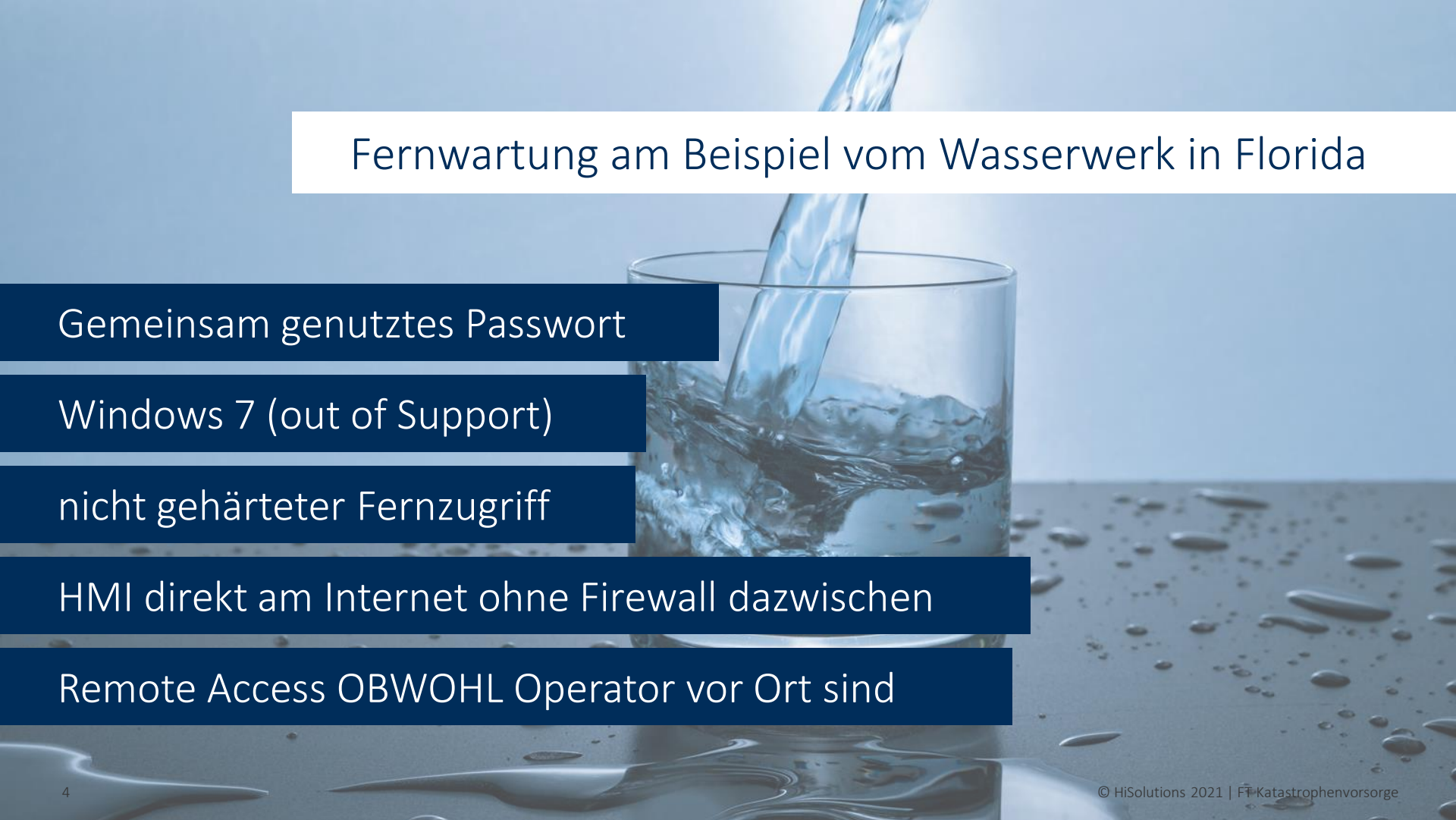
© HiSolutions 2021 | FT Katastrophenvorsorge

Fernwartung der Wasseraufbereitung in Oldsmar, Florida…

…eine Ausnahme?

© HiSolutions 2021 | FT Katastrophenvorsorge

Fernwartung am Beispiel vom Wasserwerk in Florida



- Gemeinsam genutztes Passwort
- Windows 7 (out of Support)
- nicht gehärteter Fernzugriff
- HMI direkt am Internet ohne Firewall dazwischen
- Remote Access OBWOHL Operator vor Ort sind

© HiSolutions 2021 | FT Katastrophenvorsorge

Beim Wort „Fernwartung“ leide ich innerlich immer ein bisschen!

© HiSolutions 2021 | FT Katastrophenvorsorge

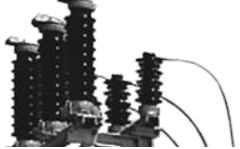
Fernwartung

Fernwartung bzw. Fernadministration

Unzureichend gesicherte Remote Zugänge

Yet another Citrix #Shitrix…

© HiSolutions [illegible] | FT Katastrophenvorsorge



Ferne Fernwartung

Unbekannte ferne Fernzugänge

z. B. auf Außenstationen oder Trafostationen

Unbekannt, aber vorhanden

© HiSolutions 2021 | FT Katastrophenvorsorge

Ganz nahe ferne Fernwartung

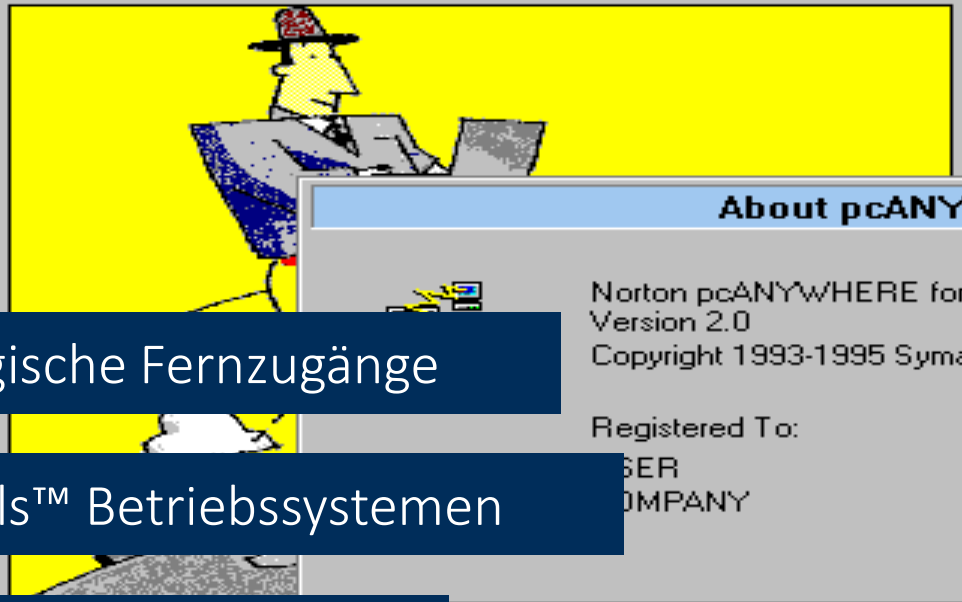
Unbekannte ganz nahe Fernzugänge

z. B. Leitstand

Dienstleister hatte da mal eine Idee…

© HiSolutions 2021 | FT Katastrophenvorsorge

Fernwartungsarchäologie



- Archäologische Fernzugänge
- Auf damals™ Betriebssystemen
- Install once, use forever

© HiSolutions 2021 | FT Katastrophenvorsorge

https://winworldpc.com/screenshot/c2b0c38c-6705-c2a9-c2b4-11c3a6e28094/6a723a36-c38d-c5be-11c3-a6c2bb2a5254

Maßnahmen und Lösungen…

…gibt es schon länger!

© HiSolutions 2021 | FT Katastrophenvorsorge

Allianz für Cyber-Sicherheit

Fernwartung im industriellen Umfeld

1. Architektur
2. Sichere Kommunikation
3. Authentisierungsmechanismen
4. Organisatorische Anforderungen
5. Sonstiges

Bundesamt für Sicherheit in der Informationstechnik

EMPFEHLUNG: IN DER PRODUKTION

Fernwartung im industriellen Umfeld

BSI-Veröffentlichungen zur Cyber-Sicherheit

Systeme zur Prozesssteuerung, Fertigung und Automatisierung – subsumiert unter dem Begriff Industrial Control Systems (ICS) – sind inzwischen ähnlichen Bedrohungen ausgesetzt wie konventionelle IT-Systeme. Aufgrund von betrieblichen oder wirtschaftlichen Gründen besteht häufig die Anforderung, eine Fernwartung der Systeme über öffentliche Netze vornehmen zu können. Derart angelegte Fernwartungszugänge führen dazu, dass industrielle Anlagen sehr viel stärker exponiert werden und somit zugleich einer gestiegenen Bedrohungslage ausgesetzt sind. Industrielle Fernwartungskomponenten müssen daher heute ein hinreichendes Sicherheitsniveau erfüllen.

Das Spektrum der am Markt verfügbaren Lösungen für Fernwartung im industriellen Umfeld ist sehr groß. Die Angebote reichen von VPN-Lösungen über Cloud-basierte Ansätze bis hin zu Provider-Lösungen im Bereich Machine-to-Machine (M2M). Die Produkteigenschaften einzelner Lösungen unterscheiden sich dabei teilweise signifikant. Die vorliegende Empfehlung gibt einen Überblick über die generischen Anforderungen für industrielle Fernwartung gemäß dem Stand der Technik. Es sei explizit darauf hingewiesen, dass Bestandslösungen auf Basis von analogen oder ISDN-Modems sowie die direkte Internetanbindung von Komponenten wie Speicher-programmierbaren Steuerungen (SPS) nicht dem aktuellen Stand der Technik genügen.

1 Architektur

Die folgenden Anforderungen sollten bereits bei der Planung und Integration einer Fernwartungslösung beachtet werden:

- Einheitliche Lösung: Besonders in größeren Infrastrukturen sollte möglichst eine einheitliche Lösung zum Einsatz kommen. Dies verringert sowohl die Anzahl der Angriffsvektoren als auch die Komplexität (kein „Wildwuchs").
- DMZ: Die Fernwartungskomponente sollte sich möglichst in einer vorgelagerten Zone (DMZ) befinden und nicht direkt im Produktionsnetz lokalisiert sein. Fernwartungszugänge dürfen nicht dazu führen, dass vorhandene umgangen werden. Vielmehr sind Firewalls geeignet, um beispielsweise erlaubte IP-Adressbereiche für eine Fernwartung festzulegen.
- Granularität der Kommunikationsverbindungen: Der Fernwartungszugriff sollte möglichst nicht pauschal pro (Sub)Netz erfolgen, sondern vielmehr feingranular pro IP und Port geregelt werden können. Dies minimiert die „Reichweite" von Fernwartungszugängen und beschränkt somit auch die Folgen einer Kompromittierung. Ein möglicher Ansatz ist beispielsweise der Aufbau von 1:1-Verbindungen mittels SSH statt der Kopplung ganzer Netze durch IPsec.

BSI-CS 108 | Version 2.0 vom 11.07.2018 Seite 1 von 4

https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_108.html

© HiSolutions 2021 | FT Katastrophenvorsorge

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com

© HiSolutions 2021 | FT Katastrophenvorsorge