Mittelstand-Digital
Zentrum
Chemnitz

IT-Sicherheit in 30 Minuten
Schutzsoftware

Roland Hallau
Mittelstand-Digital Zentrum Chemnitz
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH

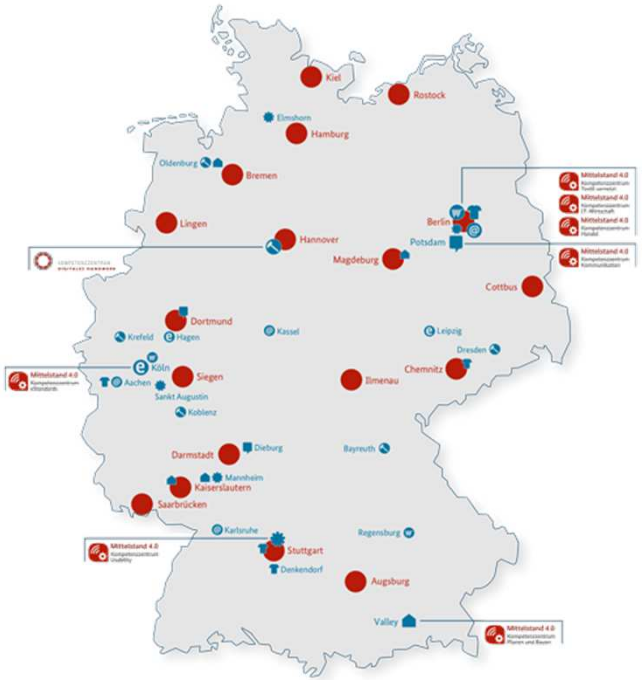
Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-Digital Zentrum Chemnitz

- als Teil von Mittelstand-Digital unterstützen wir KMU und Handwerk bei der Digitalisierung
- der Mensch im Mittelpunkt -
  als Befähiger digitaler Produktions- und Arbeitswelten
- Expertise u.a. in den Bereichen Geschäftsmodell-Entwicklung, Produktion und Logistik, IT-Sicherheit und Datenschutz, Recht und Produktgestaltung



Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Was ist Schutzsoftware?

Programme, die mögliche Auswirkungen von verschiedene Angriffsvektoren verhindern

fehlende Updates
- v.a. Sicherheitsupdates
- nicht geschlossene Sicherheitslücken

Ransomware
- Verschlüsselung von Daten
- Entschlüsselung nur gegen Zahlung

Hacker
- Ausnutzung von Sicherheitslücken
- verursacht verschiedene Schäden (z.B. Datendiebstahl, Fernsteuerung, Abschalten von Sicherheitsfunktionen)

fehlerhafte Konfiguration
- schlechte Absicherung
- unberechtigte Zugriffe

Malware/Viren
- verursacht verschiedene Schäden
- infiziert Software
- reproduzieren sich

Trojaner
- oft als nützliche Anwendung getarnt
- verursacht verschiedene Schäden

Quelle: The Tango! Desktop Project

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Voraussetzungen für eine effektive Schutzsoftware

Ein altes (Betriebs)-System bleibt trotz neuester Schutzsoftware ein altes (Betriebs)-System

- aktuelle Sicherheitsupdates
  - Betriebssystem
  - Standardsoftware
  - Spezialsoftware
  - Firmware
- funktionierende Datensicherungen
  - Daten
  - Systemeinstellungen
  - Benutzerrechte

Quellen: Visual Concepts, Mathias Rosenthal

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Schutzsoftware – Basisschutz

Antivirenprogramme

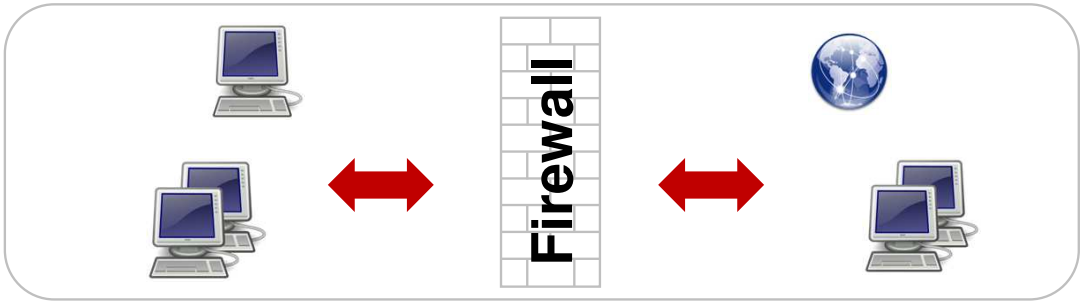
- freie und kommerzielle Systeme verschiedener Anbieter
  - oft Bestandteil mit anderen Schutzlösungen
  - Achtung: private vs. berufliche Nutzung
- regelmäßige Updates erforderlich
- diverse Bestenlisten im Internet
  - https://www.av-test.org
  - Fachzeitschriften

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Schutzsoftware – Basisschutz

Firewalls

- Unterscheidung Personal/Desktop-Firewall und Netzwerk-Firewall
- verhindert einen unautorisierten Zugriff durch Filterung des Datenverkehrs
  - PC / Unternehmensnetz – Internet
  - Unternehmensnetz Büro – Unternehmensnetz Produktion



Quelle: The Tango! Desktop Project

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Schutzsoftware – Basisschutz

Einrichtung und Betrieb einer Firewall

- nur richtig konfigurierte und geeignete Firewalls schützen durch
  - präzise Firewall-Richtlinien / Regeln
  - kompatible Hard- und Software
  - regelmäßige Updates
- falsche Einstellungen sind Fehlerquelle
  - zu restriktiv vs. zu offen
  - Fehlersuche langwierig durch fehlende Log-Files

→ Einstellungen durch IT-Experten!

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Schutzsoftware – Weitere Lösungen

Höheres IT-Sicherheitsniveau durch individuelle Schutzsoftware

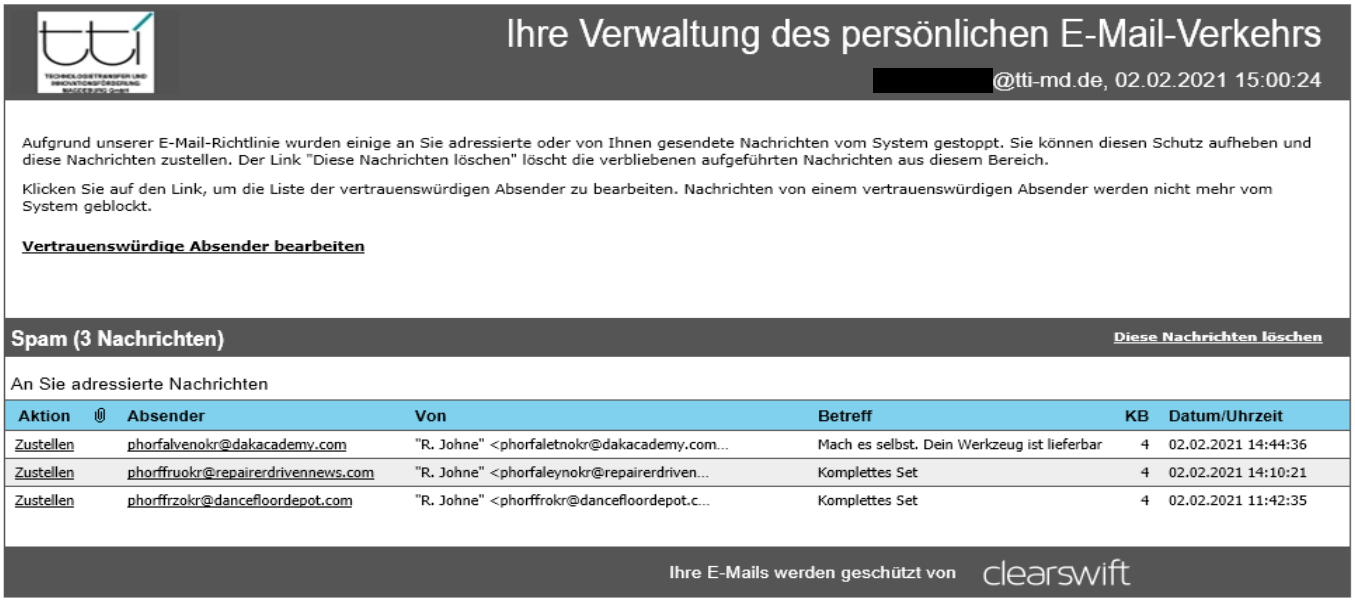
Mail-Proxy	erweiterter Web-Proxy	Monitoring-/ Update-System	Schwachstellen-Scanner
• Filterung von E-Mail-Anhängen (z.B. doc-Format) • Linkverfolgung und Verhinderung zusätzlicher Down-loads	• generelle Sperrung von Webseiten oder Inhalten • detaillierte Überprüfung der Daten / Dateien • sehr detaillierte Ein-stellmöglichkeiten und Auswertefunktionen	• prüft aktuelle Konfigurationen • verteilt neue Sicherheitsupdates innerhalb einer IT-Infrastruktur • hohe Automatisie-rungsmöglichkeit	• permanente Überwachung der IT-Infrastruktur • Abgleich mit Datenbanken zu veröffentlichten Schwachstellen • kombinierbar mit Update-Systemen

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Schutzsoftware – Mail-Proxy

Detaillierte Prüfung des Mailverkehrs inklusive Prüfung der Inhalte und Anhänge



Ihre Verwaltung des persönlichen E-Mail-Verkehrs

[redacted]@tti-md.de, 02.02.2021 15:00:24

Aufgrund unserer E-Mail-Richtlinie wurden einige an Sie adressierte oder von Ihnen gesendete Nachrichten vom System gestoppt. Sie können diesen Schutz aufheben und diese Nachrichten zustellen. Der Link "Diese Nachrichten löschen" löscht die verbliebenen aufgeführten Nachrichten aus diesem Bereich.

Klicken Sie auf den Link, um die Liste der vertrauenswürdigen Absender zu bearbeiten. Nachrichten von einem vertrauenswürdigen Absender werden nicht mehr vom System geblockt.

Vertrauenswürdige Absender bearbeiten

Spam (3 Nachrichten) — Diese Nachrichten löschen

An Sie adressierte Nachrichten

Aktion	Absender	Von	Betreff	KB	Datum/Uhrzeit
Zustellen	phorfalvenokr@dakacademy.com	"R. Johne" <phorfaletnokr@dakacademy.com...	Mach es selbst. Dein Werkzeug ist lieferbar	4	02.02.2021 14:44:36
Zustellen	phorffruokr@repairerdrivennews.com	"R. Johne" <phorfaleynokr@repairerdriven...	Komplettes Set	4	02.02.2021 14:10:21
Zustellen	phorffrzokr@dancefloordepot.com	"R. Johne" <phorffrokr@dancefloordepot.c...	Komplettes Set	4	02.02.2021 11:42:35

Ihre E-Mails werden geschützt von clearswift

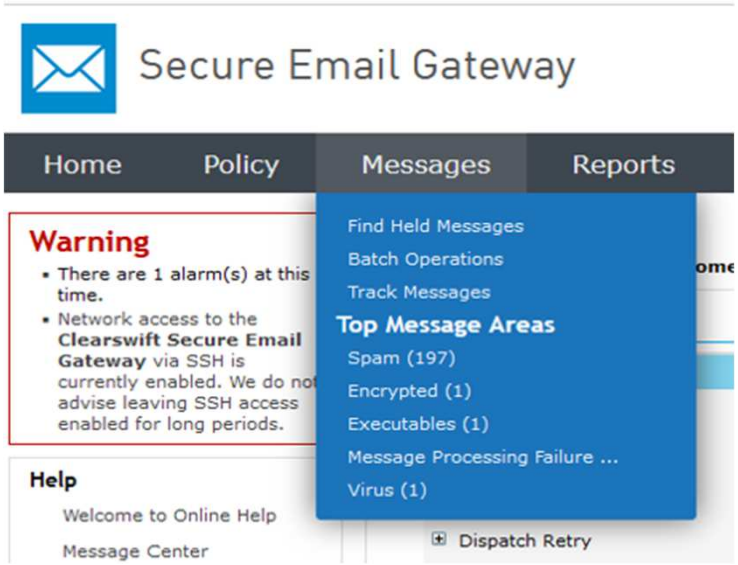
Quelle: Clearswift GmbH, tti

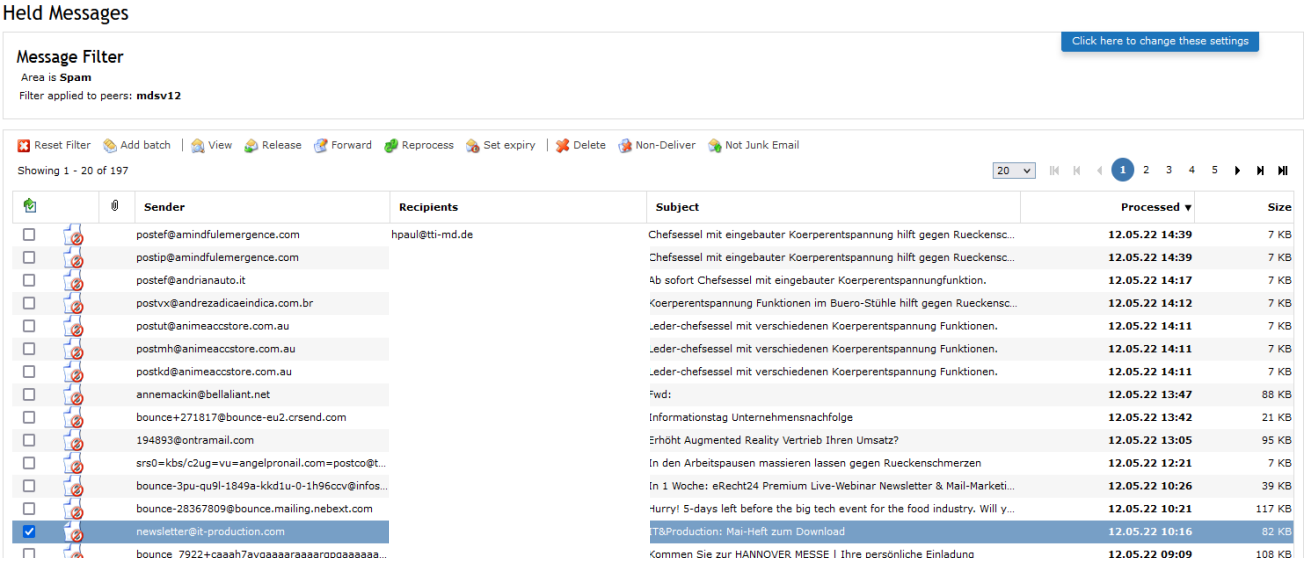
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Schutzsoftware – Mail-Proxy

Wichtige Hinweise in der Übersicht





Quelle: Clearswift GmbH, tti

Gefördert durch:

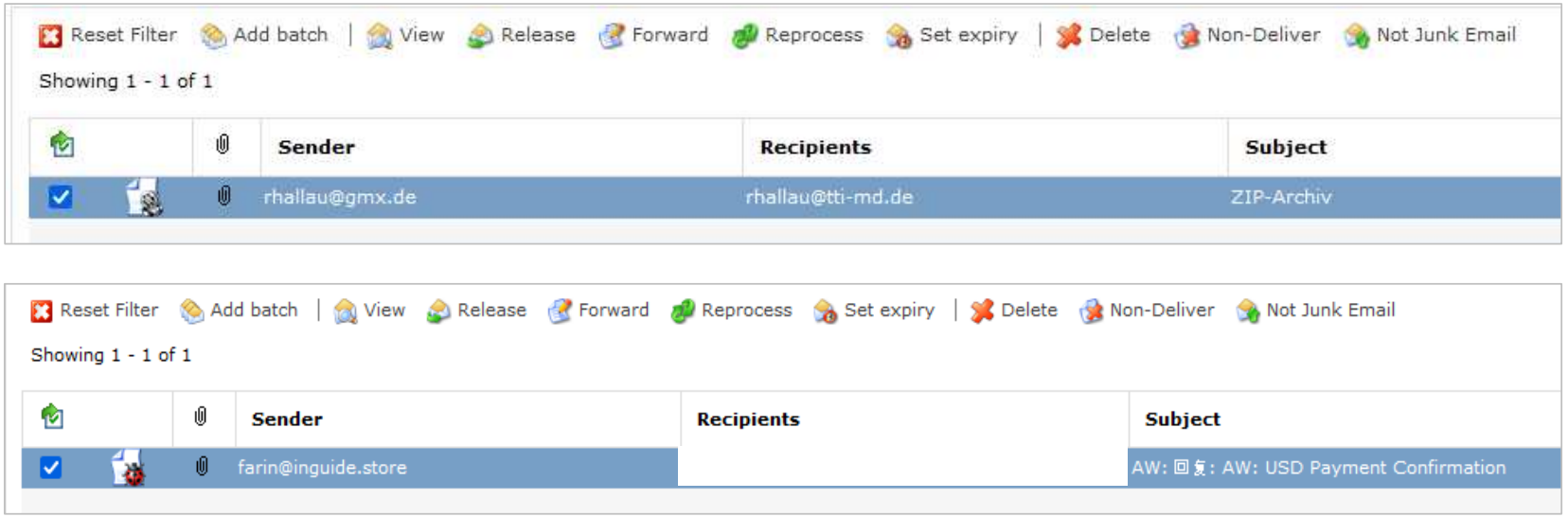
Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Schutzsoftware – Mail-Proxy

Detailinformationen und mögliche Maßnahmen



Quelle: Clearswift GmbH, tti

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

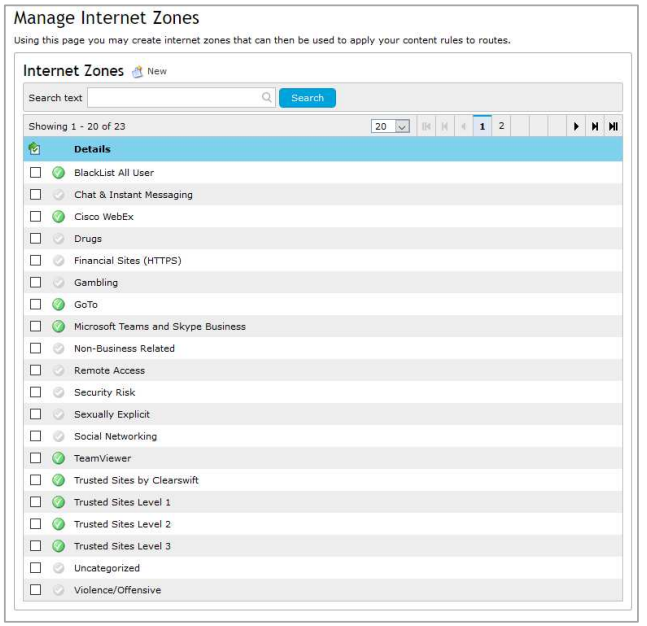
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Schutzsoftware – Erweiterter Web-Proxy

Filtern von aufgerufenen Webinhalten

- Prüfung von Website-Aufrufen
- Umfangreiche Einstellmöglichkeiten
  - Festlegung von Internetzonen mit individuellen Freigaben z.B. für Webkonferenztools
  - Ausschluss spezifischer Inhalte
  - (vollständige) Freigabe einzelner Seiten (nicht empfohlen)
- dient auch der Leistungsverbesserung durch Zwischenspeicherung der Inhalte



Quelle: Clearswift GmbH, tti

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

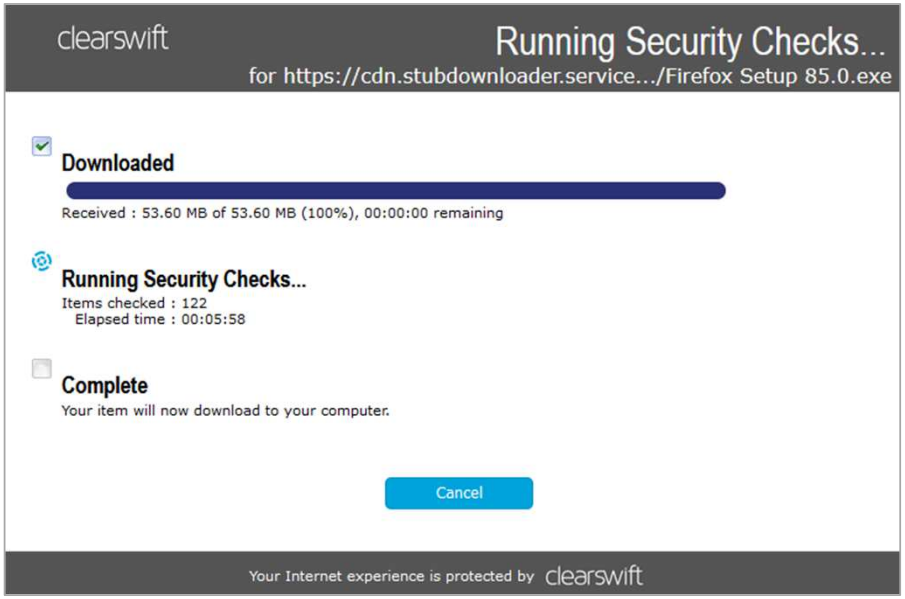
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Schutzsoftware – Erweiterter Web-Proxy

Filtern und Prüfung von herunterzuladenden Webinhalten

- Festlegung der zu prüfenden Inhalte
  - ausführbare Dateien
  - ältere Office-Formate
  - gepackte Dateien
  - Videodateien
  - …
- automatische Prüfung durch Web-Proxy
- komplette Sperrung von Inhalten möglich



Quelle: Clearswift GmbH, tti

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Schutzsoftware – Update-/Monitoring-System

Übersicht der gesamten Hardware-Infrastruktur

- verschiedene Ansichten
  - Hardware-Gruppen
  - Netzwerktopologien
  - laufende Dienste
  - verschiedene Auswertungen
- Initiierung von Updates
  - automatisch
  - teilautomatisch
  - manuell

00

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			Google	1	0	0	0	0
UP			Hosteurope	1	0	0	0	0

01

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			HBS, Router	15	0	0	0	0
UP			MD, Firewall	27	1	2	0	0

02

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, Switch	25	0	0	0	0

03

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, Telefonanlage	24	0	0	0	0

04

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, WLAN-AP EG	5	0	0	0	0
UP			MD, WLAN-AP 1.OG	5	0	0	0	0

05

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, HP-Server-MGMT	57	0	0	0	0

06

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, HP-Server	36	0	0	0	0

07

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, Monitoring	27	0	0	0	0

08

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, DC 1	73	0	0	0	0
UP			MD, DC 2	73	0	0	0	0
UP			MD, File, Print, WSUS, CA, NPS	75	0	0	0	0
UP			MD, Exchange	159	0	0	0	0
UP			MD, McAfee	69	0	0	0	0
UP			MD, Veeam Backup	76	0	0	0	0

09

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, Web-Proxy	10	0	0	0	0
UP			MD, Firmen-DB & Intranet	26	0	0	0	0
UP			MD, Benutzer- & Hosteurope-Backup	28	0	0	0	0
UP			MD, ownCloud & Exchange-Reverse-Proxy	24	0	0	0	0
UP			MD, Mail-Proxy	10	0	0	0	0
UP			MD, WLAN-Ticket	24	0	0	0	0
UP			MD, USV-Shutdown	10	0	0	0	0

10

STATE	HOST	ICONS	ALIAS	OK	WA	UN	CR	PD
UP			MD, NAS Synology Flur 1.OG	24	0	0	0	0

Quelle: tribe29 GmbH, tti

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

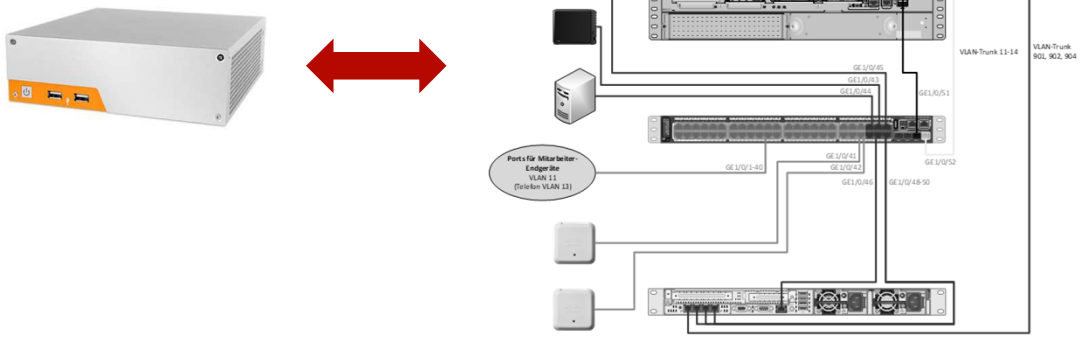
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital Zentrum Chemnitz

Schutzsoftware – Schwachstellenscanner

Am Beispiel eines Demonstrator des Mittelstand-Digital Zentrums Chemnitz

- Überprüfung von Netzwerkstrukturen
  - Einbindung in eigene Umgebungen
  - Einrichtung über Weboberfläche
- Identifikation möglicher Schwachstellen
  - Prüfung auf Angriffsmöglichkeiten
  - Abgleich mit CVE-Datenbanken
- Management der Schwachstellen
  - Anpassung der Netzwerkstrukturen
  - Updates und Überwachung



Quelle: tti

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Schutzsoftware – Was tun bei einem Sicherheitsvorfall?

Es kann immer was passieren – es gibt keinen absoluten Schutz

- bei Virus- oder Malware-Befall
  - Live-CDs / USB-Sticks als Notfallbetriebssystem mit aktuellen Virendaten
  - https://www.security-insider.de - Vergleich von verschiedenen Anbietern
- Prüfung von Mails mit Anhängen und Spyware- und Trojaner-Check
  - reine Online-Lösungen
  - Freeware (Vorsicht: Zusatzsoftware!)
  - kommerzielle Lösungen

Virustotal https://www.virustotal.com
AdwCleaner https://toolslib.net/downloads
Spybot https://www.safer-networking.org

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Schutzsoftware

Weitere Informationen

- Schutzsoftware – Basisschutzlösungen
  - www.av-test.org
  - www.virustotal.com
- Aktuelle Bedrohungen
  - https://portal.av-atlas.org
  - https://cybermap.kaspersky.com/de
  - https://www.sicherheitstacho.eu/start/main
  - https://ics-radar.shodan.io/

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

VIELEN DANK

für Ihre Aufmerksamkeit!

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Klimaschutz
aufgrund eines Beschlusses
des Deutschen Bundestages

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-Digital Zentrum Chemnitz

- c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
  Bruno-Wille-Straße 9
  39108 Magdeburg

Roland Hallau
0391 74435-24
rhallau@tti-md.de

Andreas Neuenfels
0391 74435-23
aneuenfels@tti-md.de

David Wagner
0391 74435-28
dwagner@tti-md.de

Mike Wäsche
0391 74435-34
mwaesche@tti-md.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages