Mittelstand-Digital Zentrum Chemnitz

IT-Sicherheit in 30 Minuten Sicherheitsvorfall: Das Protokoll der erfolgreichen 9 Stunden danach

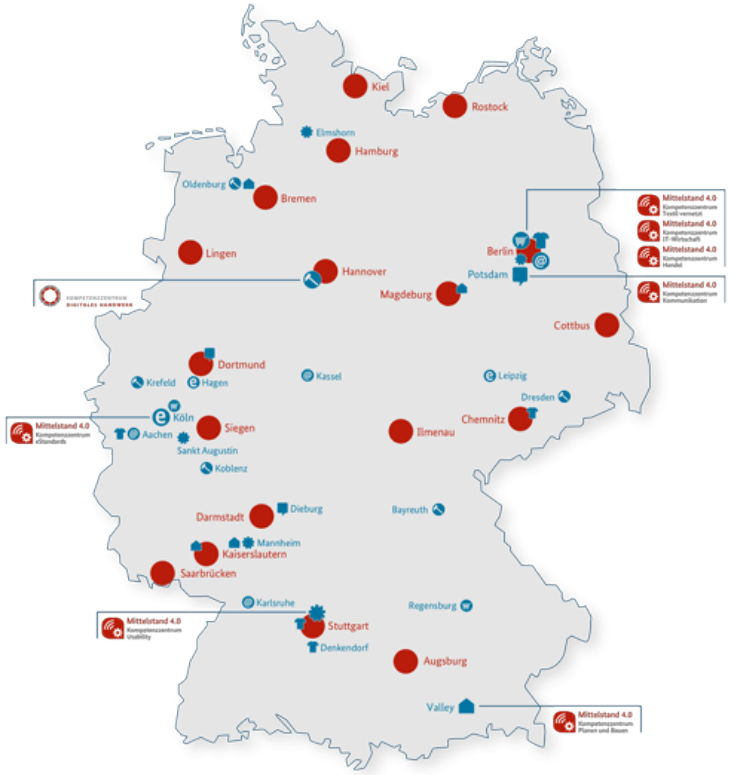
Mike Wäsche
Mittelstand-Digital Zentrum Chemnitz
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH

Mittelstand-Digital

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

Mittelstand-Digital Zentrum Chemnitz

- 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

IT-Sicherheitsvorfall

Schilderung eines realen Vorfalls in einem klein- und mittelständischen Unternehmen

- Unternehmen:
  - Gründung 1992
  - 15-20 Mitarbeiter
  - wirtschaftsfördernde Dienstleistungen
  - Verwaltung personenbezogener Kundendaten

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

IT-Sicherheitsvorfall

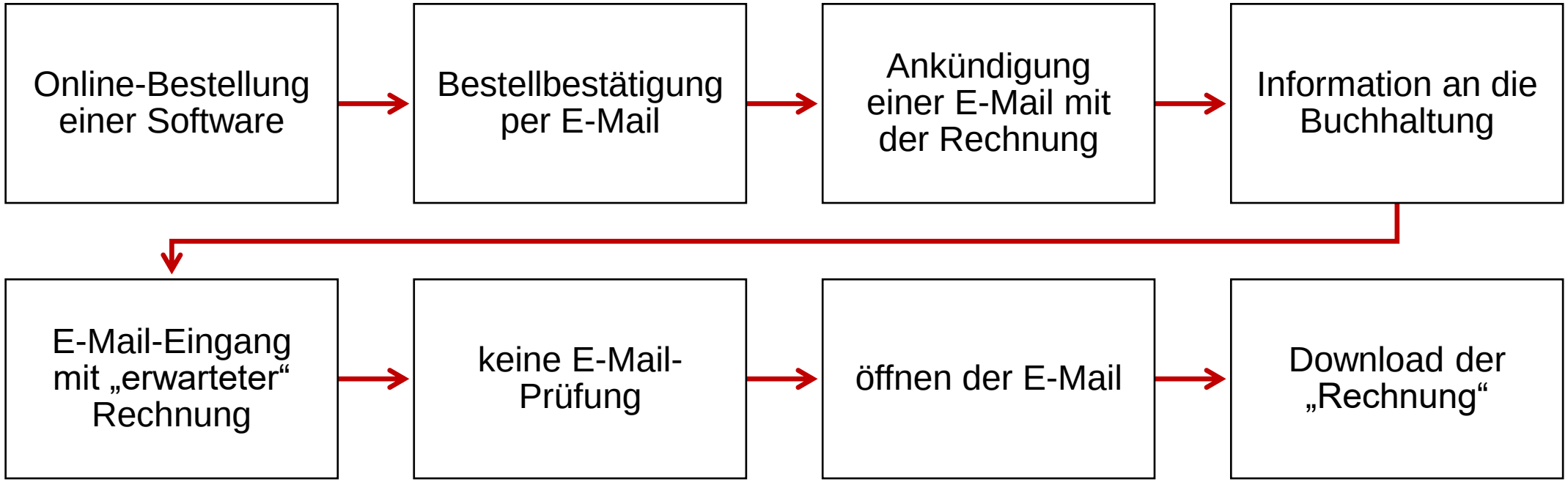
Anfang

- Meldung vom 14. März 2017 an den hauptverantwortlichen Mitarbeiter um 13:53 Uhr
  - Telefonat war nicht erfolgreich
  - SMS wurde gelesen und dann sofort reagiert

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

IT-Sicherheitsvorfall

Vorgeschichte am 14.03.2017



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

Wie wurde der Vorfall erkannt?

Glück, Zufall und Erfahrung

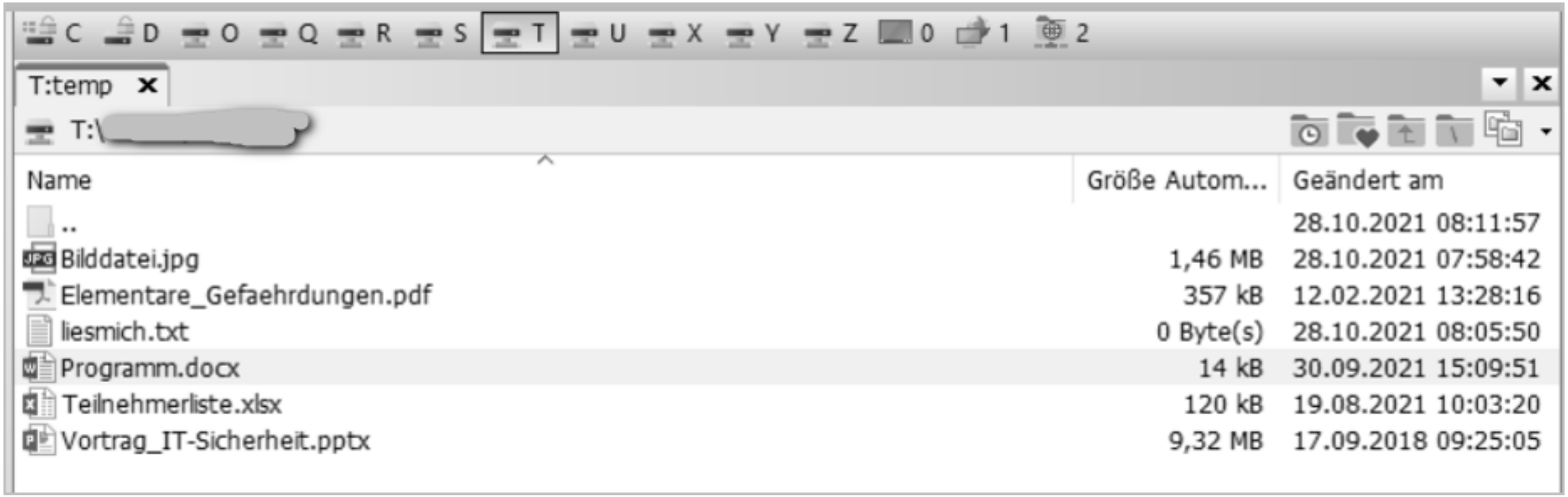
© Anna - stock.adobe.com

- IT-Schutzsysteme (Firewall, Antivirensoftware) haben nicht reagiert
  - Schutzmechanismen wurden ausgehebelt
  - manuelle Freigabe eines Downloads
- „Wo ist denn nun die Rechnung?“
  - Rechnung war nicht im Downloadordner
  - manuelle Suche initiiert
  - hohe Sensibilität einzelner Mitarbeiter führte zur Aufdeckung des Sicherheitsvorfalls

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

Feststellung der Verschlüsselung

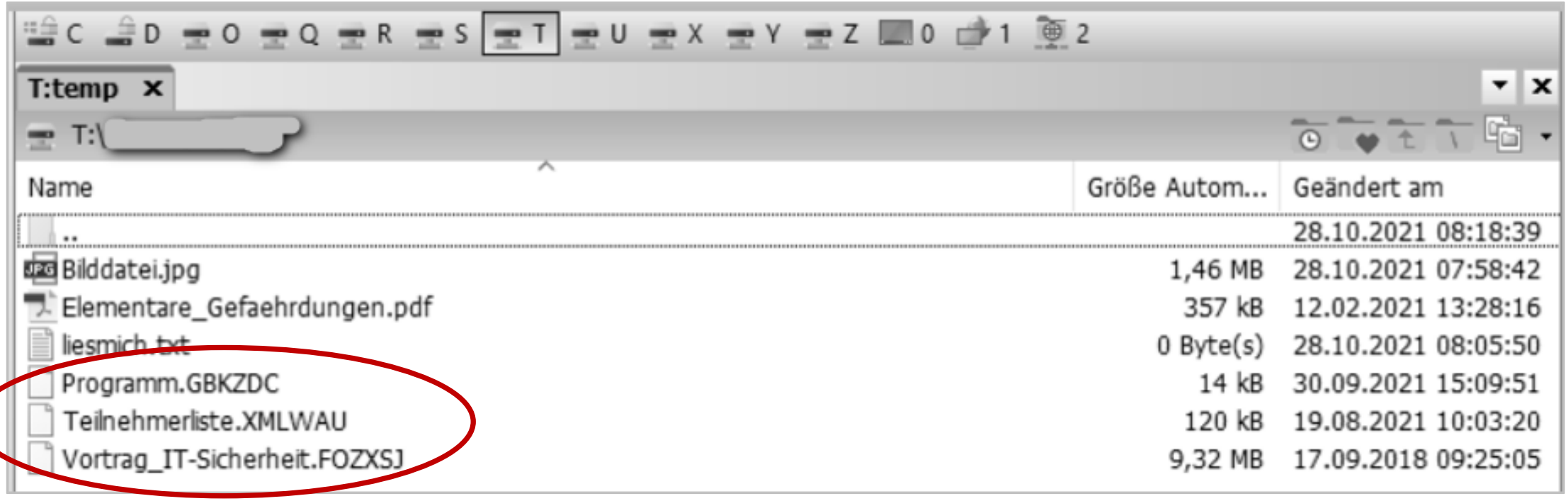
14.03.2017 – 12:41 Uhr – vor der Verschlüsselung



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

Feststellung der Verschlüsselung

14.03.2017 – 13:17 Uhr – nach der Verschlüsselung



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

Erstreaktion

14.03.2017 – 13:17 Uhr

- Information aller Mitarbeiter
  - mündlich
  - per Telefon
- IT-Systeme abschalten
  - Trennen der Netzwerkverbindungen
  - Trennen der Internetverbindung
  - Systeme herunterfahren
- Information an den IT-Dienstleister

Photo by www_slon_pics on pixabay.com

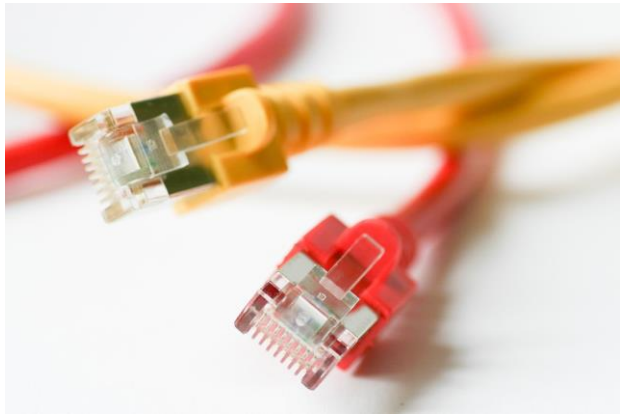


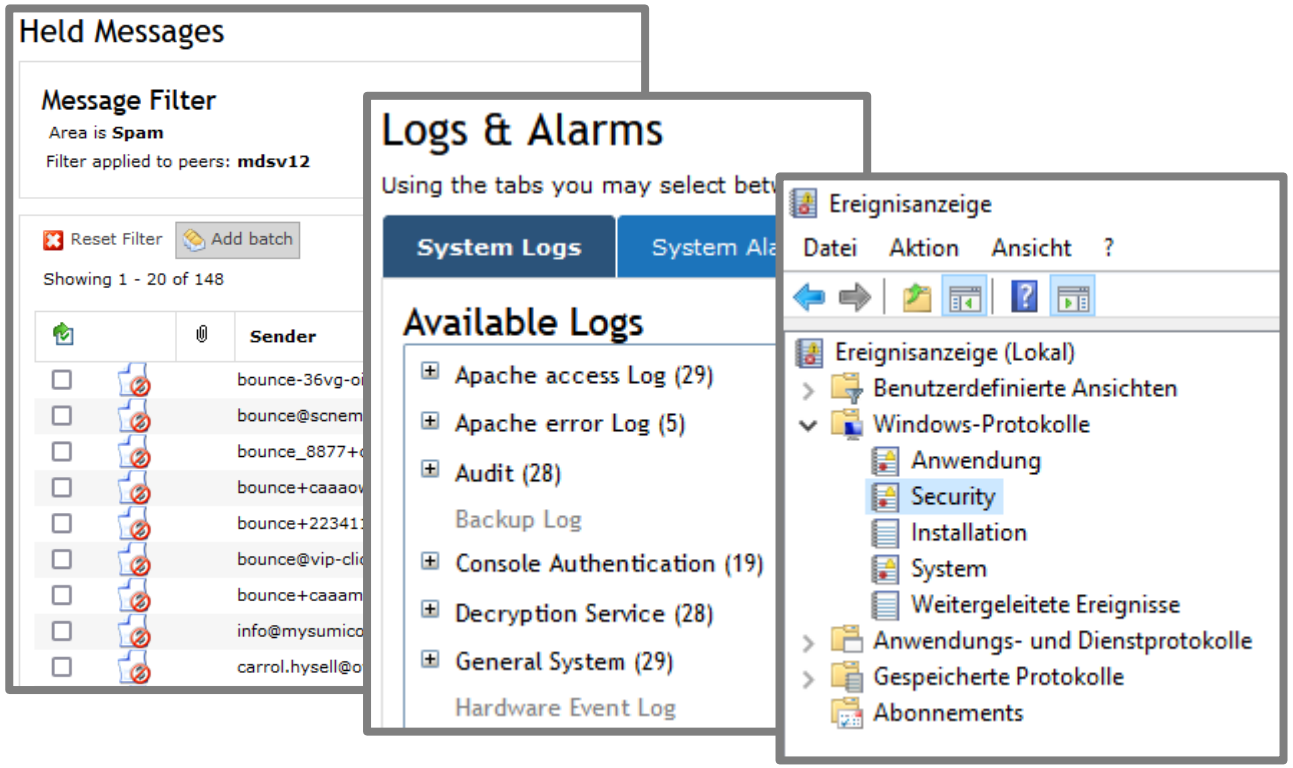
Photo by fotofixautomat on pixabay.com

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

Analyse

Was ist passiert?

- Prüfung von separat abgelegten Log-Files
  - Internetverkehr
  - E-Mails
  - Systemmeldungen
- Eingrenzung entsprechend der Prozesse
  - Einzelinterviews: Wer hat was gerade bearbeitet?
  - Prüfung auf Querverweise in den Logfiles



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

Ergebnis der Analyse

14.03.2017 – 14:45 Uhr

Link zum Download der „Rechnung“

- Link führte zu einer Cloud (Dropbox)

Verstecktes Laden von Schadcode durch Klick auf den Link

- Ransomware war vorher nicht in den Systemen vorhanden

Start der Verschlüsselung

- MS-Office-Dateien entsprechend Zugriffsberechtigungen des Buchhaltungs-rechners

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

Festlegungen zur Vorgehensweise

14.03.2017 – 14:50 Uhr

- Vollständige Neuinstallation des Arbeitsplatzrechners der Buchhaltung
- Check aller anderen Arbeitsplatzrechner (Kaspersky Rescue Disk)
- Rücksicherung aller 13 Server aus dem letzten Backup
- Abschließende Systemprüfung

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

IT-Sicherheitsvorfall - Wiederherstellung I

14.03.2017 – 14:50-21:00 Uhr

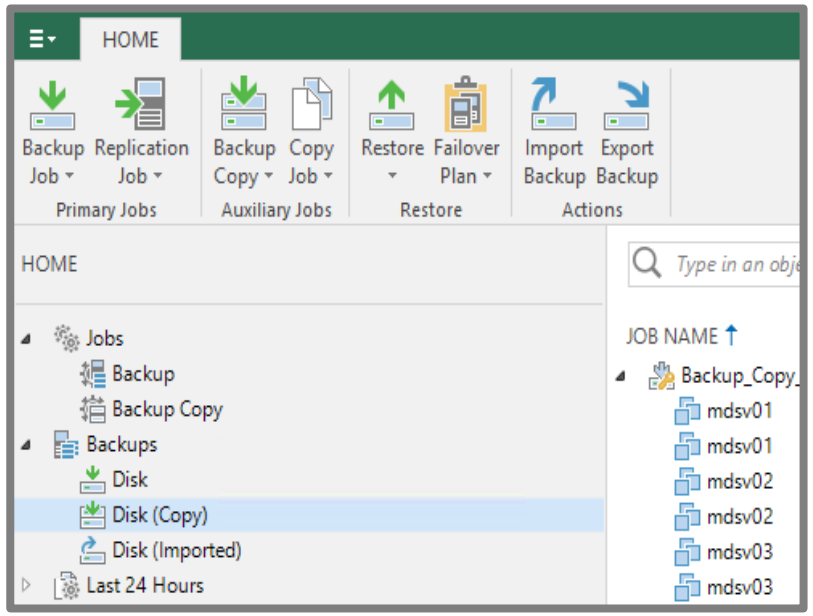
- Download der aktuellen Kaspersky Rescue Disk, Erstellen mehrerer Kopien (Admins des KMU)
- Check von Arbeitsplatzrechnern mit der Kaspersky Rescue Disk (Admins des KMU)
- Rücksicherung der ersten (notwendigen/wichtigen) Server (IT-Dienstleister)

- 21:00 Uhr Feierabend (alle)

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

IT-Sicherheitsvorfall - Wiederherstellung II

15.03.2017 – 07:00-10:30 Uhr



- Check der restlichen Arbeitsplatzrechner mit der Kaspersky Rescue Disk (Admins des KMU)
- Neuinstallation des Arbeitsplatzrechners in der Buchhaltung und Rücksicherung der Daten aus dem letzten Backup (Admins des KMU)
- Rücksicherung der anderen Server (IT-Dienstleister)
- 10:30 Uhr - Abschluss aller notwendigen Arbeiten

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

Auswertung

Kosten

Wer	Kosten	Bemerkungen
IT-Dienstleister	910 Euro	8 Stunden * 110 €/h und 2 * Anfahrtspauschale 15 € (EVB-IT Instandhaltungsvertrag vorhanden, vereinbarte Reaktionszeit 3 Stunden nach Meldung)
KMU, 2 interne Admins	2.000 Euro	je Mitarbeiter 10 Stunden * 100 €/h
KMU, 14 Mitarbeiter	7.000 Euro	Annahme: 50% tatsächlicher Ausfall - Erledigung tlw. (aufgeschobene) unproduktive Arbeiten - Fokussierung auf Kundenkontakte (Akquise, lfd. Projekte)
gesamt:	9.910 Euro	

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

Auswertung

Lessons Learned

Fragestellung	Bemerkungen
Wo lag der Fehler?	- Vorhandene Schutzsoftware/Technik war korrekt konfiguriert. - Menschliches Versagen trotz regelmäßiger Schulungen
Wurde richtig reagiert?	- Herunterfahren der Rechner - Anzeige des Vorfalls Polizei/LKA
War das KMU gut vorbereitet?	- sensibilisierte und geschulte Mitarbeiter - Vertrag mit IT-Dienstleister (Reaktionszeit) - Dokumentation der IT-Infrastruktur

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

Auswertung

Abgeleitete Maßnahmen

Technische Maßnahmen	Organisatorische Maßnahmen
Überprüfung der Konfiguration des E-Mail-Proxys	- Fortsetzung und Intensivierung der Sensibilisierung und Schulung der Mitarbeiter
Installation eines Web-Proxys	- Zeitnahe Auswertung auch von kleinen Vorfällen unter Einbeziehung aller Mitarbeiter

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

Basis einer erfolgreichen Systemwiederherstellung

Datensicherung

- Aktuelles Datensicherungskonzept
- Ausreichende periodische Datensicherung inkl. Kontrolle
- etablierte Prozesse zur Wiederherstellung
- IT-Dienstleister (bzw. eigene Ressourcen und Know-how)

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

Basis einer erfolgreichen Systemwiederherstellung

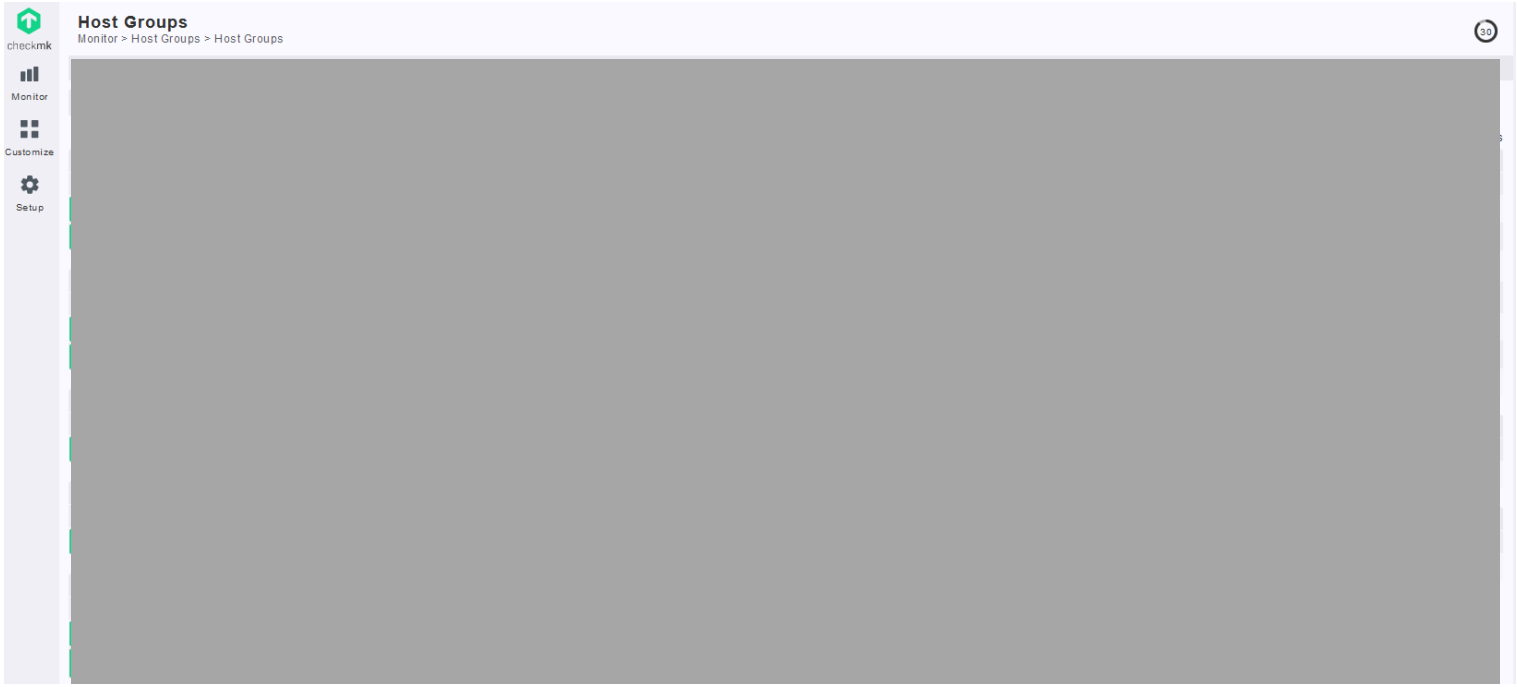
Dokumentation

- Aktuelles Datensicherungskonzept
- Ausreichende periodische Datensicherung inkl. Kontrolle
- Dokumentation der IT-Systeme
- IT-Dienstleister (bzw. eigene Ressourcen und Know-how)
- Monitoring

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

Basis einer erfolgreichen Systemwiederherstellung

Grundüberwachung der vorhandenen Systeme



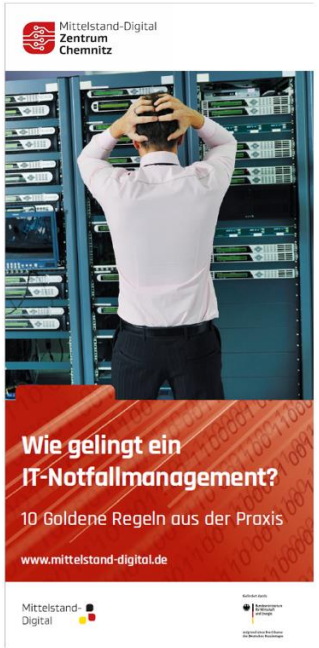
Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

Basis einer erfolgreichen Systemwiederherstellung

Prozesse verbessern und Mitarbeiter schulen

Quelle: https://betrieb-machen.de/download/9767

- Feedback von Mitarbeitern zu Maßnahmen und Richtlinien einholen
- Schadensvorfälle analysieren und Lehren daraus ziehen
- Notfallmanagement aufbauen
- Wissens- und Bewusstseinsaufbau kontinuierlich erweitern sowie aktuell halten



Quelle: http://betrieb-machen.de/download/15019

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