

Verschlüsselt - Das Protokoll der Wiederherstellung

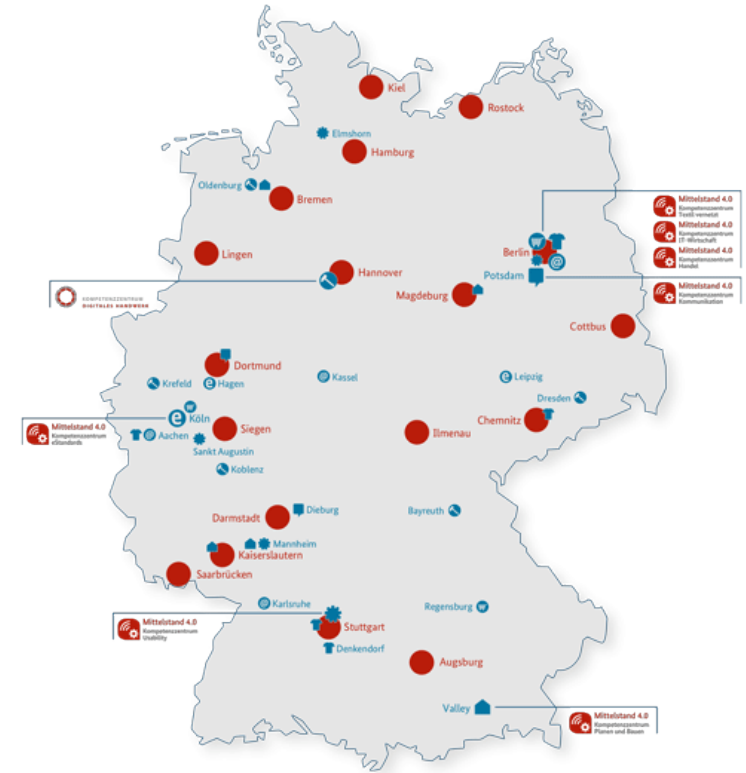
Roland Hallau

Mittelstand-Digital Zentrum Chemnitz

c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH

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



IT-Sicherheitsvorfall

Schilderung eines realen Vorfalls in einem klein- und mittelständischen Unternehmen

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

Verschlüsselung

Feststellung

Analyse

Gegenmaßnahmen

Auswertung

IT-Sicherheitsvorfall

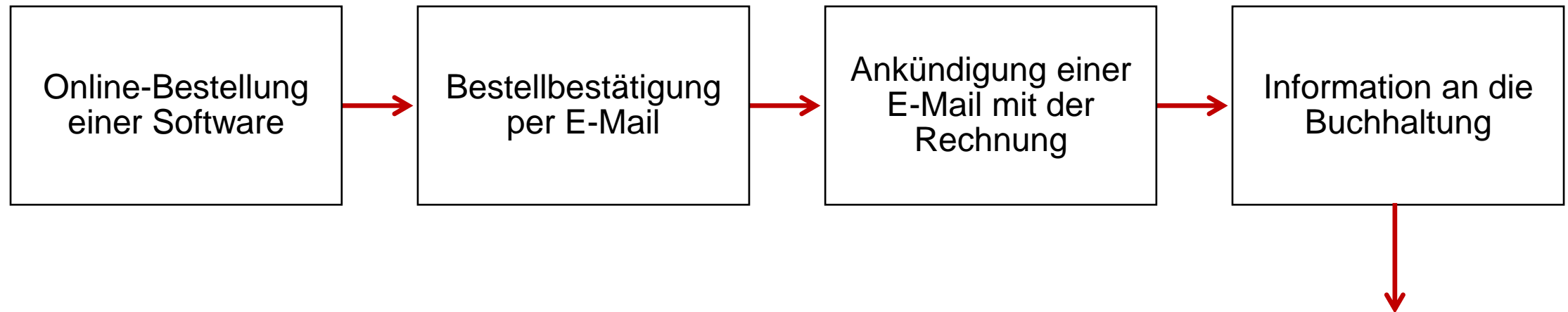
Anfang



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

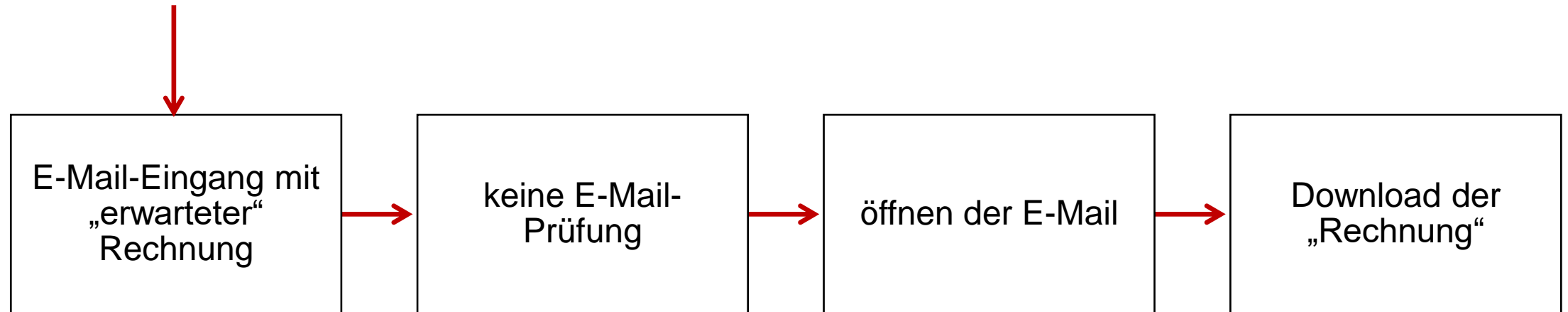
IT-Sicherheitsvorfall

Vorgeschichte am 14.03.2017 - vormittags



IT-Sicherheitsvorfall

Vorgeschichte am 14.03.2017 - nachmittags



Wie wurde der Vorfall erkannt?

Glück, Zufall und Erfahrung

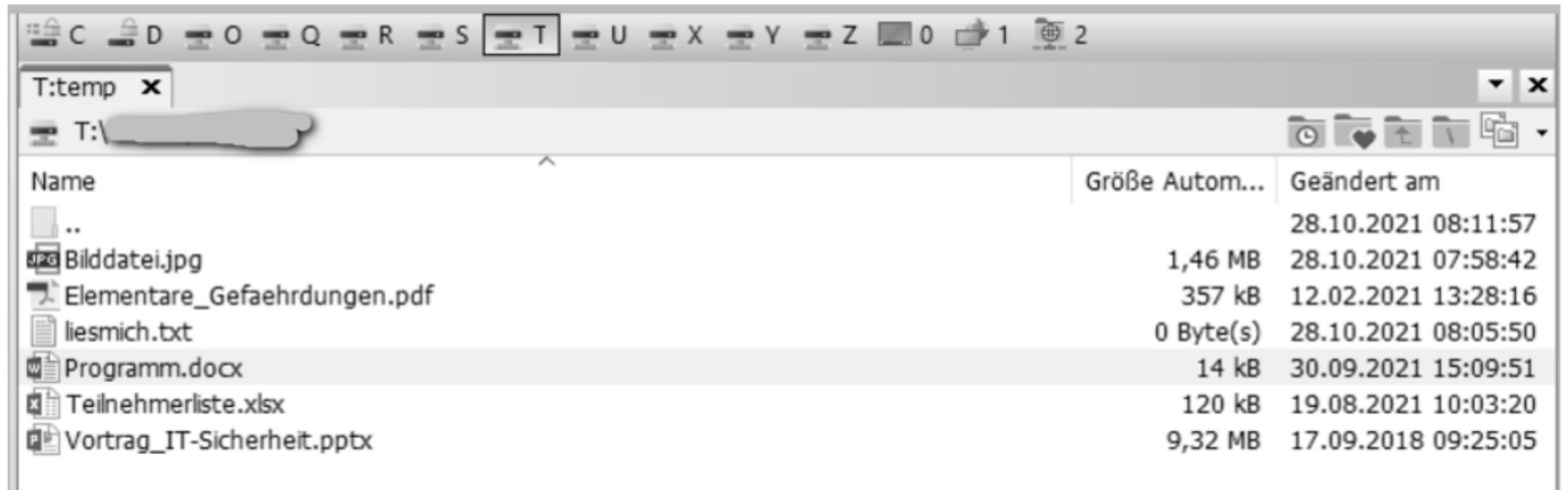


© Anna - stock.adobe.com

- 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

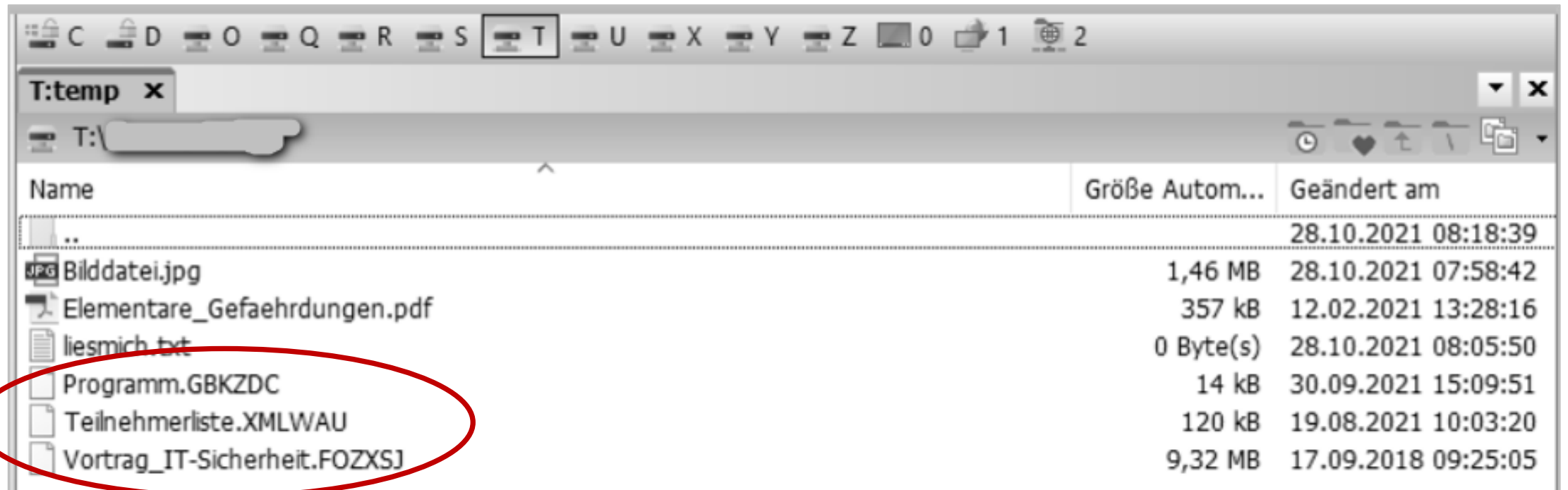
Feststellung der Verschlüsselung

14.03.2017 – 12:41 Uhr – vor der Verschlüsselung



Feststellung der Verschlüsselung

14.03.2017 – 13:17 Uhr – nach der Verschlüsselung



Name	Größe Autom...	Geändert am
..		28.10.2021 08:18:39
Bilddatei.jpg	1,46 MB	28.10.2021 07:58:42
Elementare_Gefahrenungen.pdf	357 kB	12.02.2021 13:28:16
liesmich.txt	0 Byte(s)	28.10.2021 08:05:50
Programm.GBKZDC	14 kB	30.09.2021 15:09:51
Teilnehmerliste.XMLWAU	120 kB	19.08.2021 10:03:20
Vortrag_IT-Sicherheit.FOZXSJ	9,32 MB	17.09.2018 09:25:05

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

Was tun?

Hat jemand einen (Notfall-) Plan?

ONLY IN CASE OF
CYBER EMERGENC

KUEMMERLING
WEISSWEIN
200ml/6.8oz

KUEMMERLING
WEISSWEIN
200ml/6.8oz

Slot 6 7 8 9 10 11 12 13 14 15 16

K1 K2 3.1 3.2 3.3 3.4 3.5 3.6 3.7 3.8 3.9

E11 E12 E13 E14 E15 E16 E17 E18 E19 1.1 1.2

1.19 1.20 1/21 1/22 13 14 15 16

Analyse

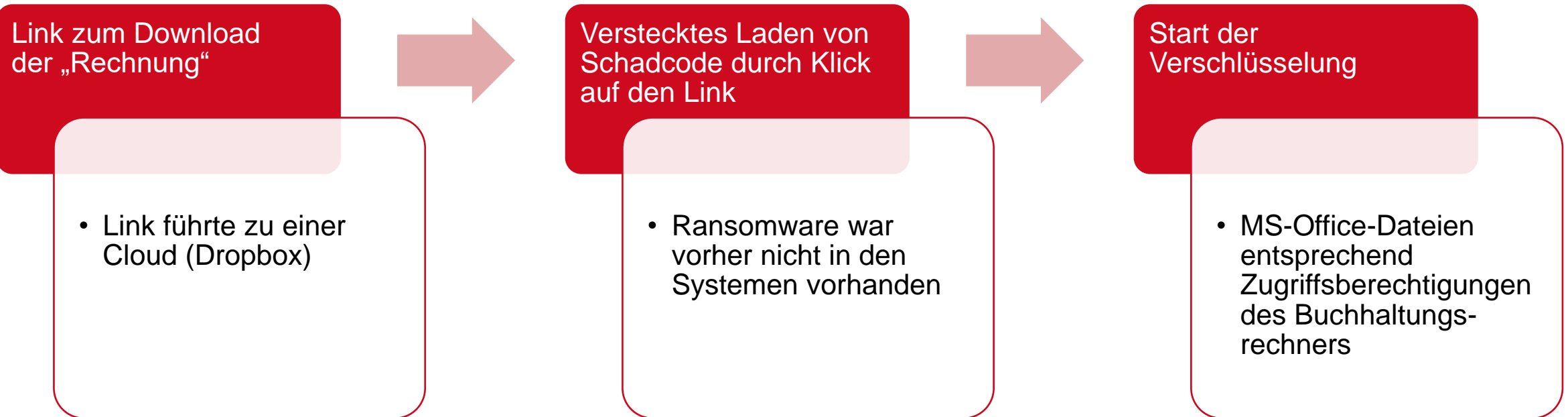
Was ist passiert?

- 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

The image shows three overlapping screenshots of software interfaces. The top-left screenshot is titled 'Held Messages' and shows a 'Message Filter' for 'Spam' applied to peers 'mdsv12'. It lists 148 messages with columns for checkboxes, status icons, and 'Sender' addresses. The top-right screenshot is titled 'Logs & Alarms' and shows a list of 'Available Logs' including Apache access/error logs, Audit, Backup Log, Console Authentication, Decryption Service, General System, and Hardware Event Log. The bottom-right screenshot is titled 'Ereignisanzeige' and shows a tree view of system logs, including 'Windows-Protokolle' with sub-items like 'Anwendung', 'Security', 'Installation', 'System', and 'Weitergeleitete Ereignisse'.

Ergebnis der Analyse

14.03.2017 – 14:45 Uhr



Festlegungen zur Vorgehensweise

14.03.2017 – 14:50 Uhr

Vollständige Neuinstallation des Arbeitsplatzrechners der Buchhaltung

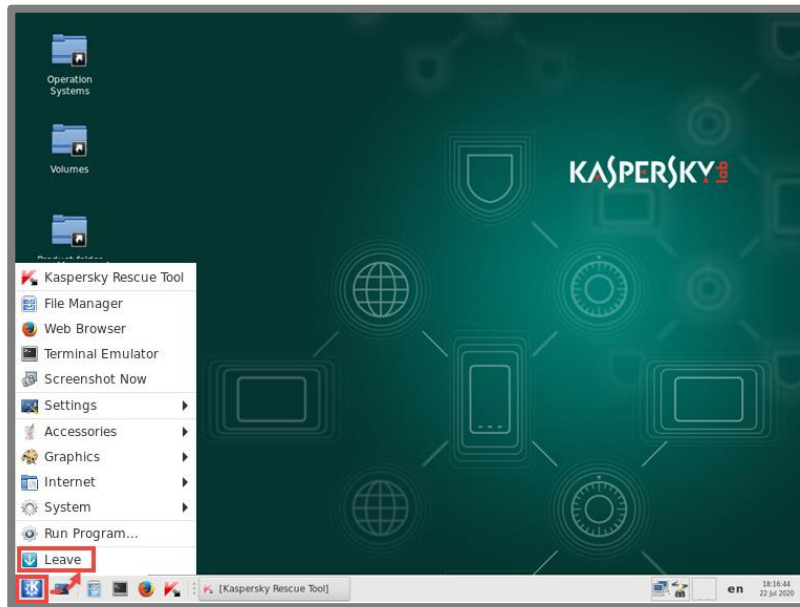
Check aller anderen Arbeitsplatzrechner (Kaspersky Rescue Disk)

Rücksicherung aller 13 Server aus dem letzten Backup

Abschließende Systemprüfung

IT-Sicherheitsvorfall - Wiederherstellung I

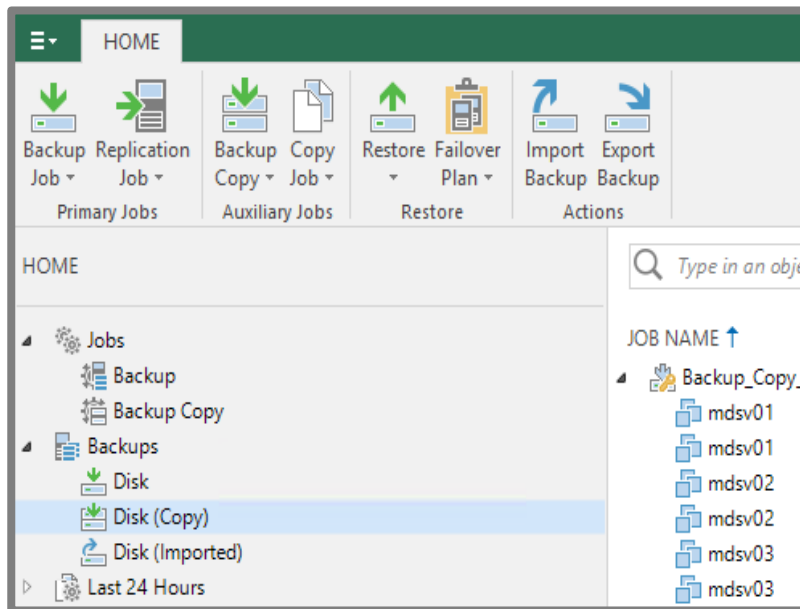
14.03.2017 - 14:50-19:00 Uhr



- 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)
- 19:00 Uhr Feierabend (alle)

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

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	

Auswertung

Lessons Learned

Fragestellung	Bemerkungen
Wo lag der Fehler?	<ul style="list-style-type: none">- Vorhandene Schutzsoftware/Technik war korrekt konfiguriert.- Menschliches Versagen trotz regelmäßiger Schulungen
Wurde richtig reagiert?	<ul style="list-style-type: none">- Herunterfahren der Rechner- Anzeige des Vorfalls Polizei/LKA
War das KMU gut vorbereitet?	<ul style="list-style-type: none">- sensibilisierte und geschulte Mitarbeiter- Vertrag mit IT-Dienstleister (Reaktionszeit)- Dokumentation der IT-Infrastruktur

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

Basis einer erfolgreichen Systemwiederherstellung

Datensicherung

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

The screenshot displays a backup management interface. At the top, a notification for a backup job is shown: "Backup job: Backup_Job_to_USB" created on 07.11.2016 at 17:06. Below this, a summary table shows 13 successful backups, 1 warning, and 0 errors. A detailed table follows, listing individual backup jobs (mdsv01 to mdsv12) with their start/end times and sizes. A large email notification is overlaid on the interface, titled "mdns01 Synology <synology@...> mdns01 Synology: Monatlicher Festplattenintegritätsbericht". The email text reads: "Sehr geehrter Benutzer, nachfolgend erhalten Sie den monatlichen Integritätsbericht zu den Festplatten auf mdns01. Den Zustand einzelner Laufwerke können Sie auch unter Speicher-Manager > HDD/SSD > Integritätsstatus überprüfen. Bei den Laufwerken in DSM wurden keine Probleme erkannt. Mit freundlichen Grüßen Synology DiskStation". A smaller window in the bottom right corner shows a list of disk statuses, all marked as "OK".

Success	Warning	Error	Total size	Data read	Transferred
13	1	0			

Name	Status	Start time	End time	Size
mdsv01	Success	19:00:35	19:04:21	32,0 GB
mdsv02	Success	19:00:35	19:05:10	32,0 GB
mdsv03	Success	19:00:35	19:14:46	384,0 GB
mdsv04	Success	19:03:05	19:18:21	192,0 GB
mdsv05	Success	19:13:14	19:21:18	96,0 GB
mdsv06	Success	19:32:53	19:39:09	64,0 GB
mdsv09	Success	19:13:32	19:16:36	8,0 GB
mdsv10	Success	19:15:42	19:23:20	8,0 GB
mdsv11	Success	19:13:57	19:18:00	32,0 GB
mdsv13	Success	19:17:08	19:21:28	8,0 GB
mdsv14	Success	19:19:53	19:23:15	10,0 GB
mdsv01	Success	19:16:33	19:31:21	96,0 GB
mdsv07	Success	19:21:19	19:30:24	256,0 GB
mdsv12	Warning	19:21:29	19:32:46	256,0 GB

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

Schutzschild Mensch

Prozesse zur Verbesserung



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>

Vorfall

Weitere Informationen

→ BSI – Digitaler Ersthelfer

→ https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Cyber-Sicherheitsnetzwerk/Onlinekurs/Onlinekurs_node.html

→ IHKn

→ <https://www.ihk.de/themen/innovation/daten-und-informationssicherheit>

Vielen Dank
für Ihre Aufmerksamkeit!

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

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