Cyber Security Erfahrungsbericht

April 2023

KONVERTO

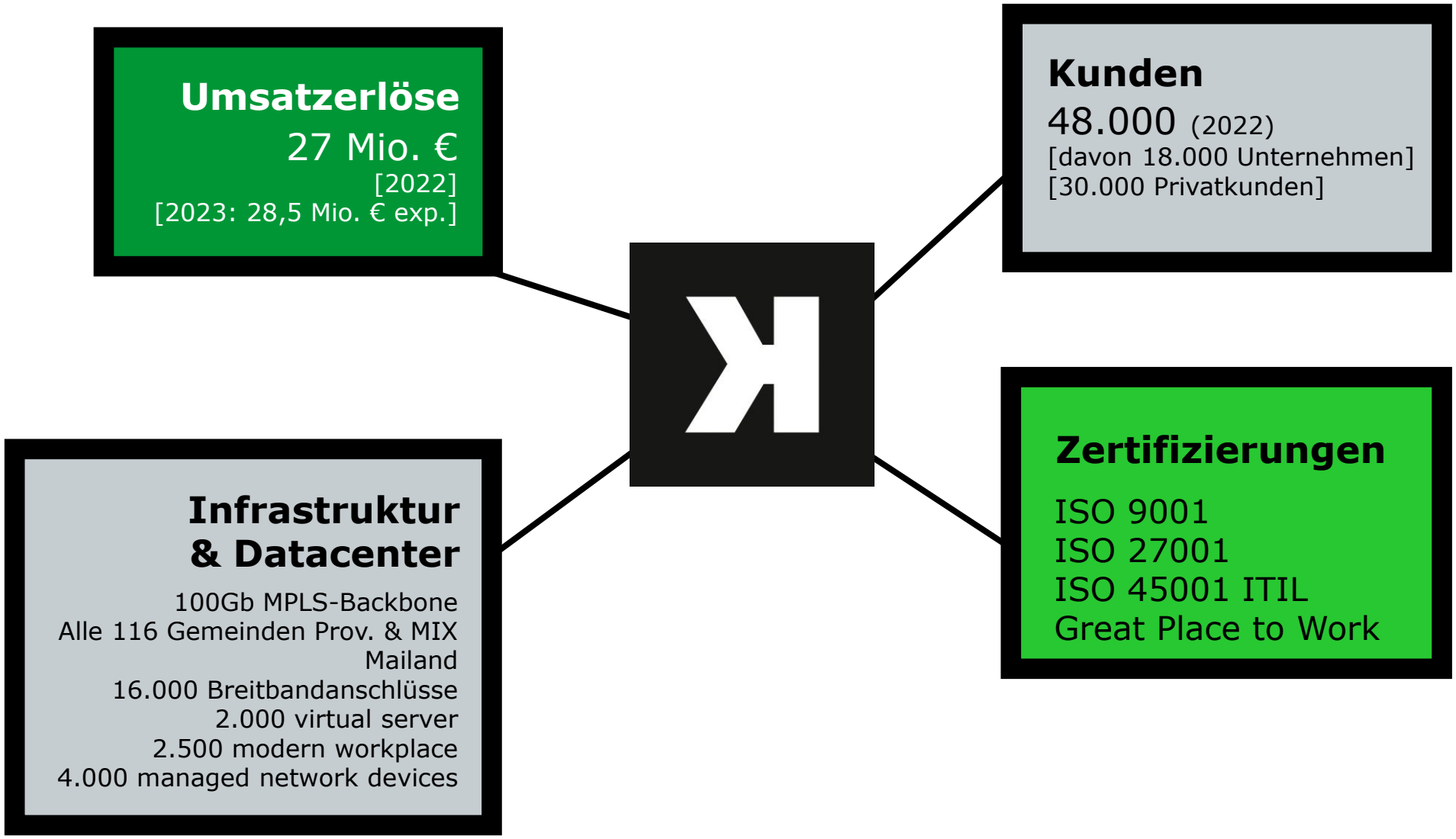
Martin Galler

Information Security & Privacy

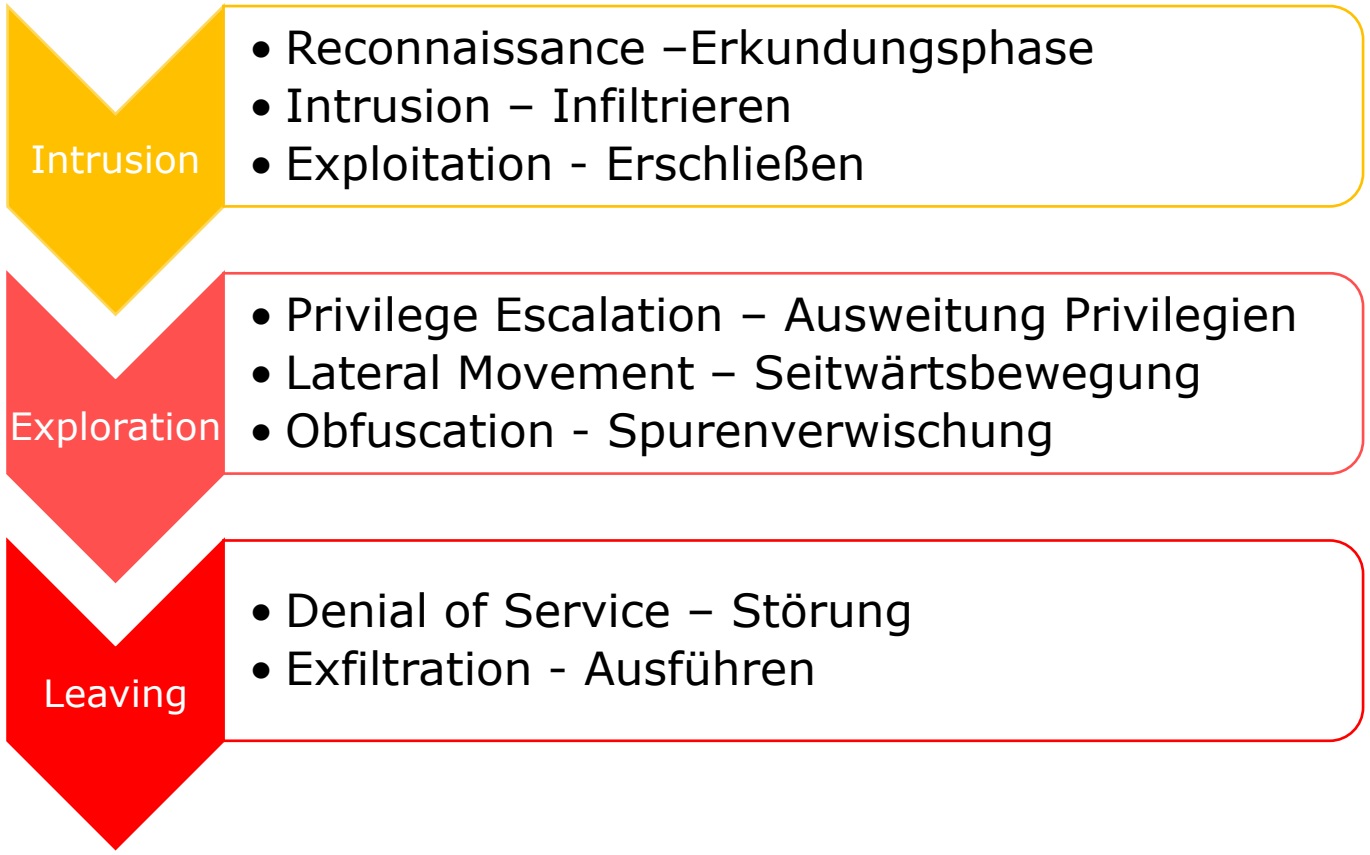
martin.galler@konverto.eu

KONVERTO

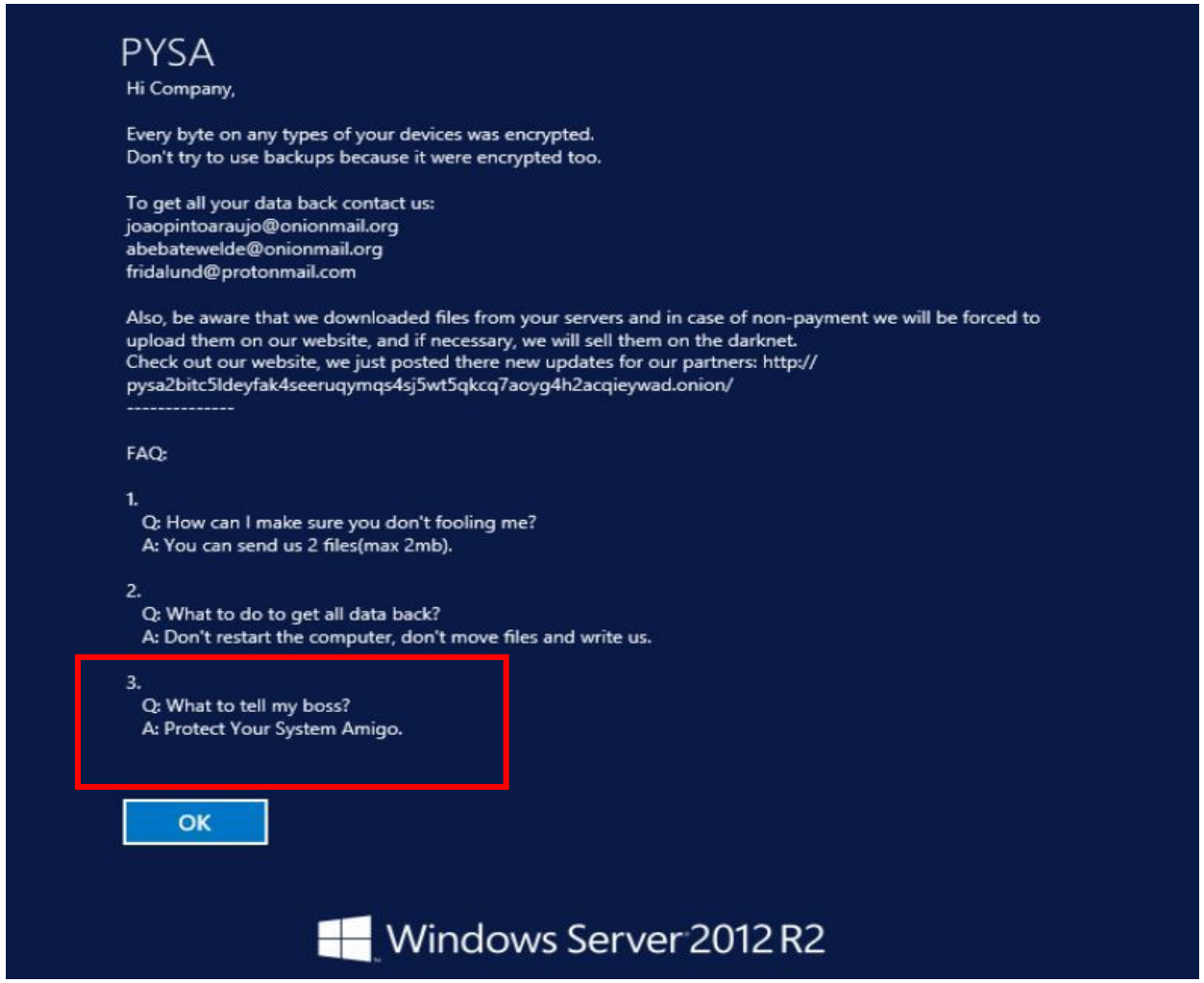
KONVERTO . FAKTEN



Theorie – die Cyber Kill Chain



Mittwoch um 10:00

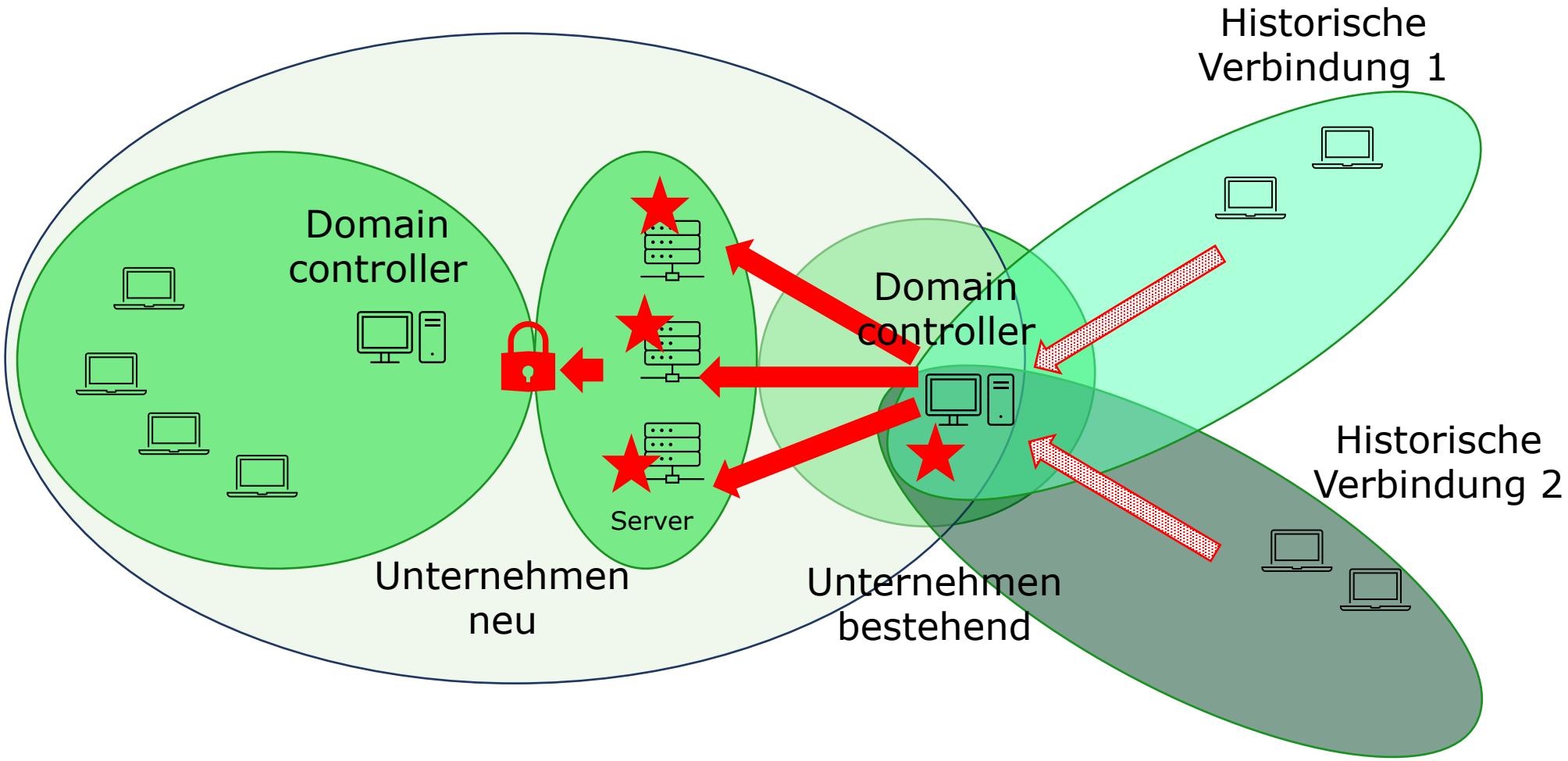


KONVERTO

Zeitleiste des Angriffs

Sonntag	11:00	Zugriff mit kompromittiertem User-Account
	18:30	Administrator Account kompromittiert
Montag		Keine Auffälligkeiten
Dienstag	01:40	UPLOAD Files
	04:00	Weiteres Ausbreiten
	23:30	Weiteres Ausbreiten
Mittwoch	01:50	**Zerstörung !!!!!!!!!!!**
Mittwoch	08:00	**Systeme außer Betrieb**

Ausbreitung



Sofortmaßnahmen

- Vom Internet abtrennen (Firewallregel)
- Sicherung der aktuellen Situation
  - Als Spurensicherung
  - Als Rettung aktueller Daten
- Analyse des Ausmaßes (was ist noch OK?)
- Überprüfung der Datensicherungen
- Einsetzung Krisenstab
- Kommunikationssperre

KONVERTO

Welche Datensicherung?

Mittwoch	02:00	Sicherung OK
Donnerstag	02:00	Sicherung OK
Freitag	02:00	Sicherung OK
Samstag	02:00	Sicherung OK
Montag	02:00	**Sicherung OK** ???
Dienstag	02:00	Sicherung mit verschlüsselten File aber **Datenbanksicherung OK**
Mittwoch	02:00	Sicherung mit verschlüsselten Files

KONVERTO

Wiederherstellung

- KEINE Kontaktaufnahme mit Erpressern
- Wiederherstellung
  - Neue saubere Grundstruktur
  - System Stand Montag 02:00
  - Datenbank Stand Dienstag 02:00
- 1 Tag Datenverlust in Kauf nehmen
- 15 Terabyte Daten Wiederherstellung
  - Zwischensicherungen und Kontrollen
  - Donnerstag: Systemwiederherstellung
  - Freitag: Überprüfung und Datenbankwiederherstellung
  - Samstag: Überprüfung Gesamtsystem und Freigabe

KONVERTO

Kommunikation

- Allgemeine Krisenеröffnung
- Nächster Tag: genauere Angaben, Aussichten
- Diskussion über Pressemitteilung
- Krisenbeendigung: Angabe der Maßnahmen

- Kommunikation an oberster Stelle angesiedelt
- Eindeutige klare Botschaften
- Single Point of Contact

KONVERTO

Koordinierung

- Notwendig, da oft unterschiedliche Interessen vorliegen (Lösegeld zahlen?)
- Nicht immer klar, was zu tun ist und wer was macht.
  - Systembetreuung
  - Anwendungsbetreuung
  - Betroffener Kunde
- Teams als Kommunikationsinstrument hervorragend
- Meldung an Postpolizei

KONVERTO

Lesson Learned: Vorbeugung

- Standardmittel reichen allgemein aus:
  - Backup (welches Backup ist sauber?)
  - Segmentierung
  - Antimalware
  - Berechtigungen
  - Zugriffsregeln ins Internet
  - Aktualisierung
  - Sensibilisierung
  - „alte Systeme sind zu löschen“ und **nicht** „für alle Fälle aufbewahren“
- Erschwerte Umstände durch unkontrollierten Upload
  - Wann wurden Daten gestohlen?

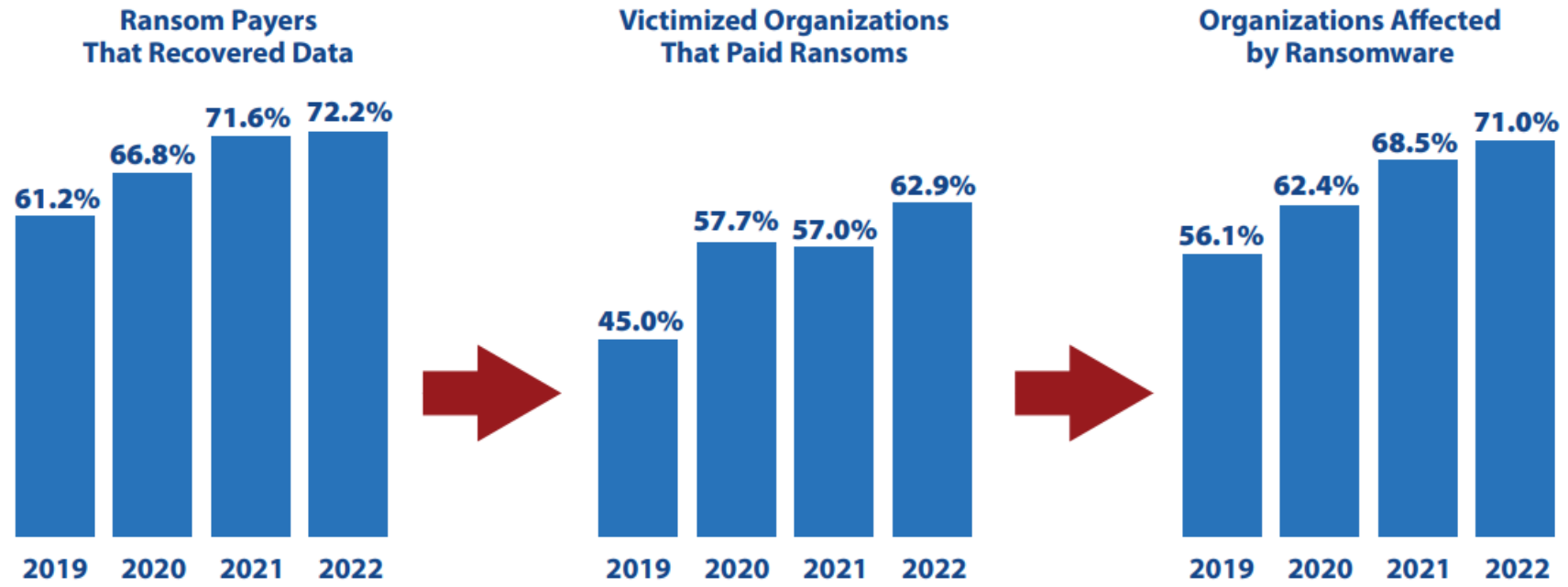
KONVERTO

Besondere Zutaten

- Löschen der **Datensicherungen**
- Auch **ausgeschaltete** Maschinen werden infiziert (durch vorheriges Einschalten)
- Analyseinstrumente sind für die vollständige Aufklärung unzureichend (nur teilweise rückverfolgbar)
- Üblicherweise 4-6 Wochen (Monate?) Zeit für Nachbearbeitung

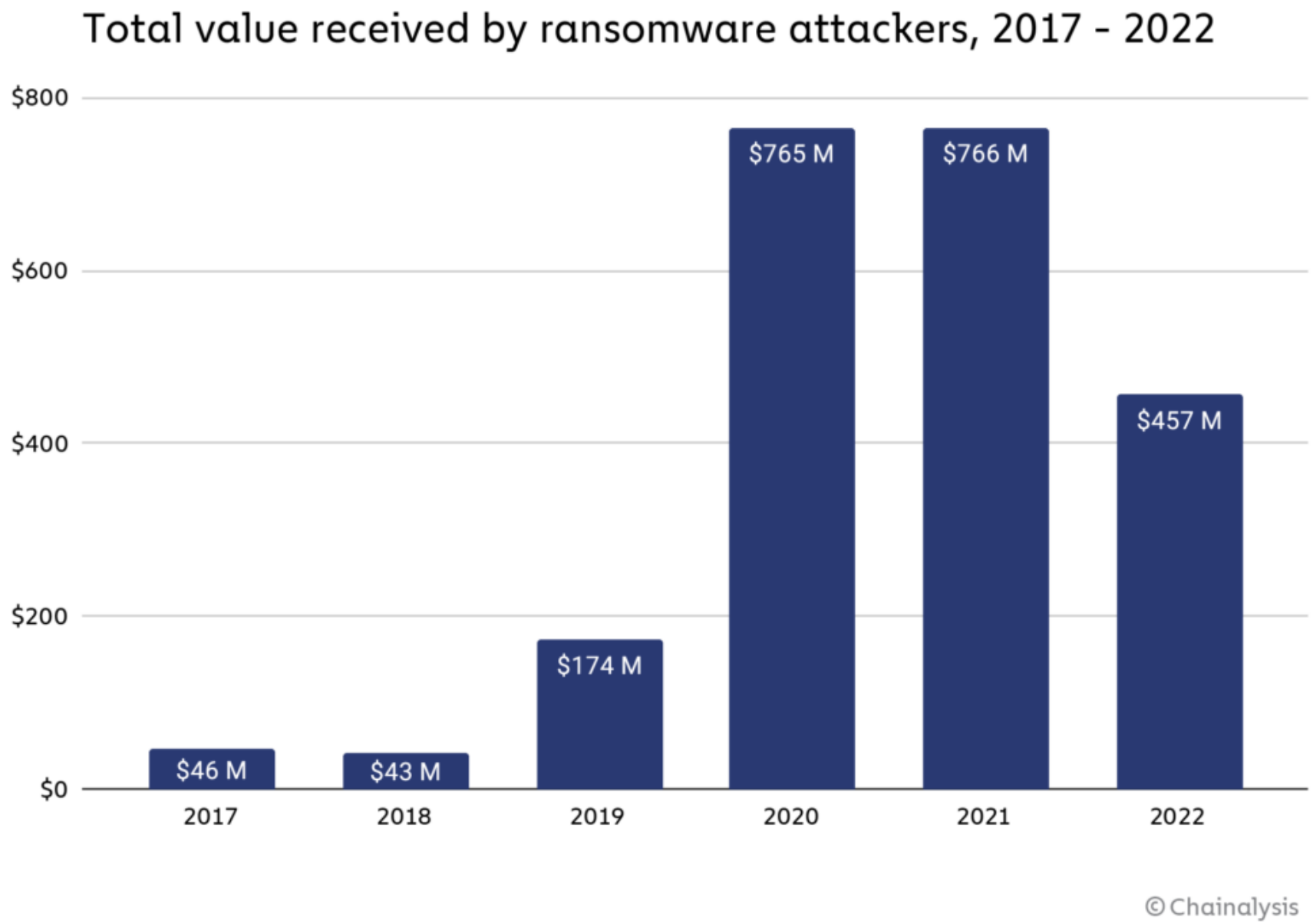
KONVERTO

Teufelskreis Ransomware



Bessere Rückgewinnung -> Mehr Opfer zahlen -> mehr Angriffe

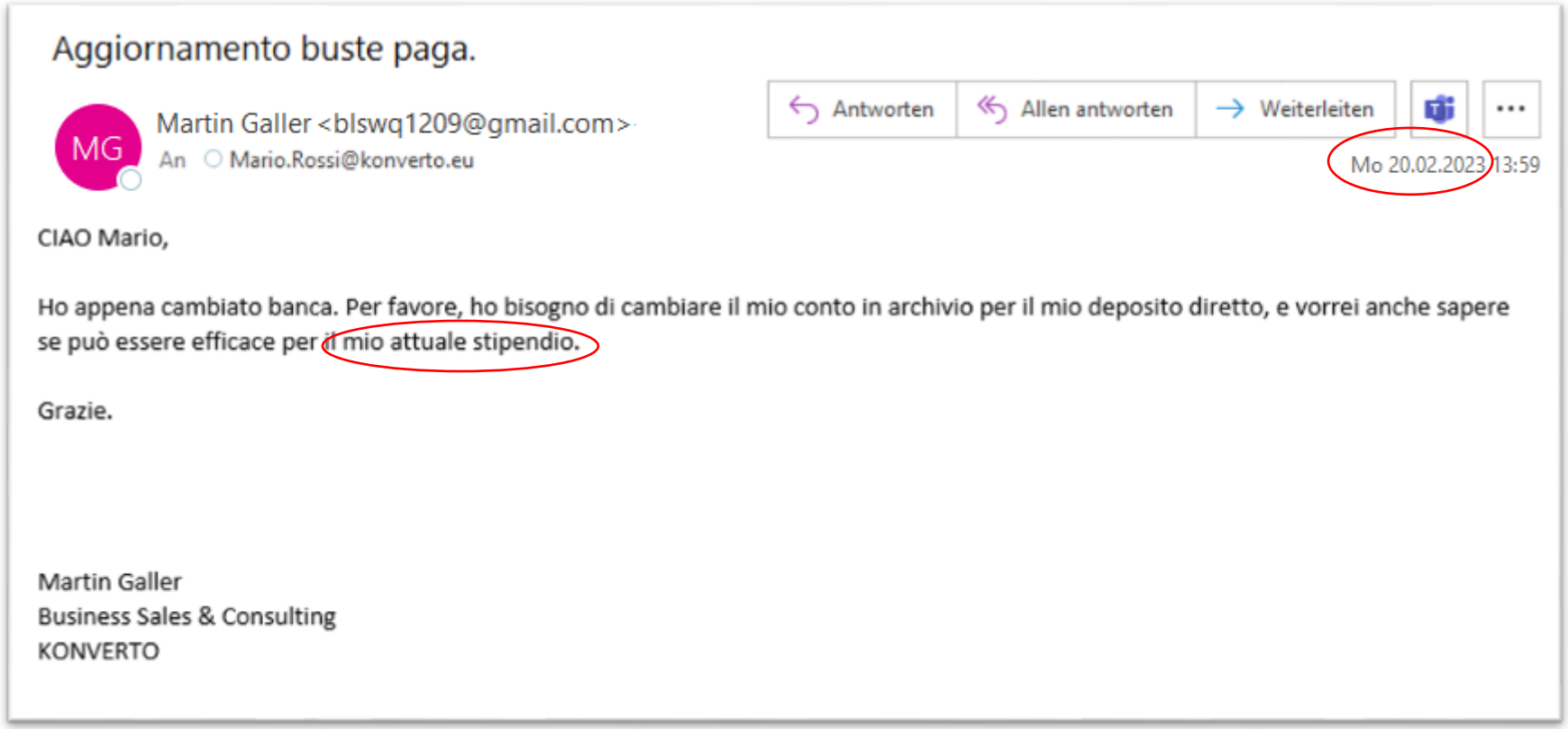
Quelle: 2022 Cyberthreat Defense Report – Cyberedge Group



Quelle: Chainalysis The 2023 Crypto Crime Report

KONVERTO

Payroll Diversion Scam



Aggiornamento buste paga.

MG

Martin Galler <blswq1209@gmail.com>

An Mario.Rossi@konverto.eu

Antworten | Allen antworten | Weiterleiten | ...

Mo 20.02.2023 13:59

CIAO Mario,

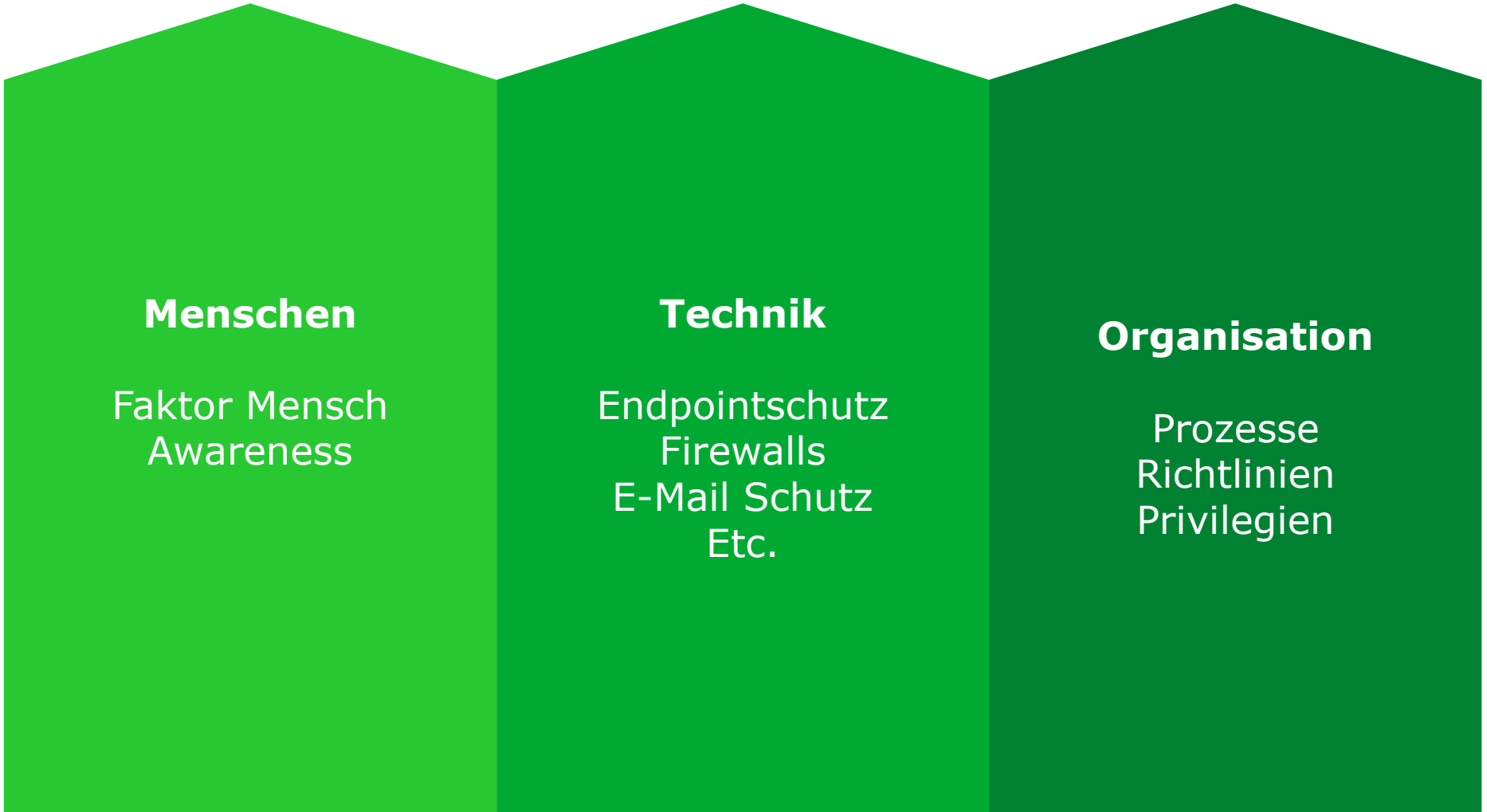
Ho appena cambiato banca. Per favore, ho bisogno di cambiare il mio conto in archivio per il mio deposito diretto, e vorrei anche sapere se può essere efficace per il mio attuale stipendio.

Grazie.

Martin Galler
Business Sales & Consulting
KONVERTO

KONVERTO

Das 1x1 der Cybersicherheit



KONVERTO

passion for technology

Vielen Dank für die Aufmerksamkeit

KONVERTO

KONVERTO AG Bruno-Buozzi-Str. 8, Bozen
info@konverto.eu konverto.eu