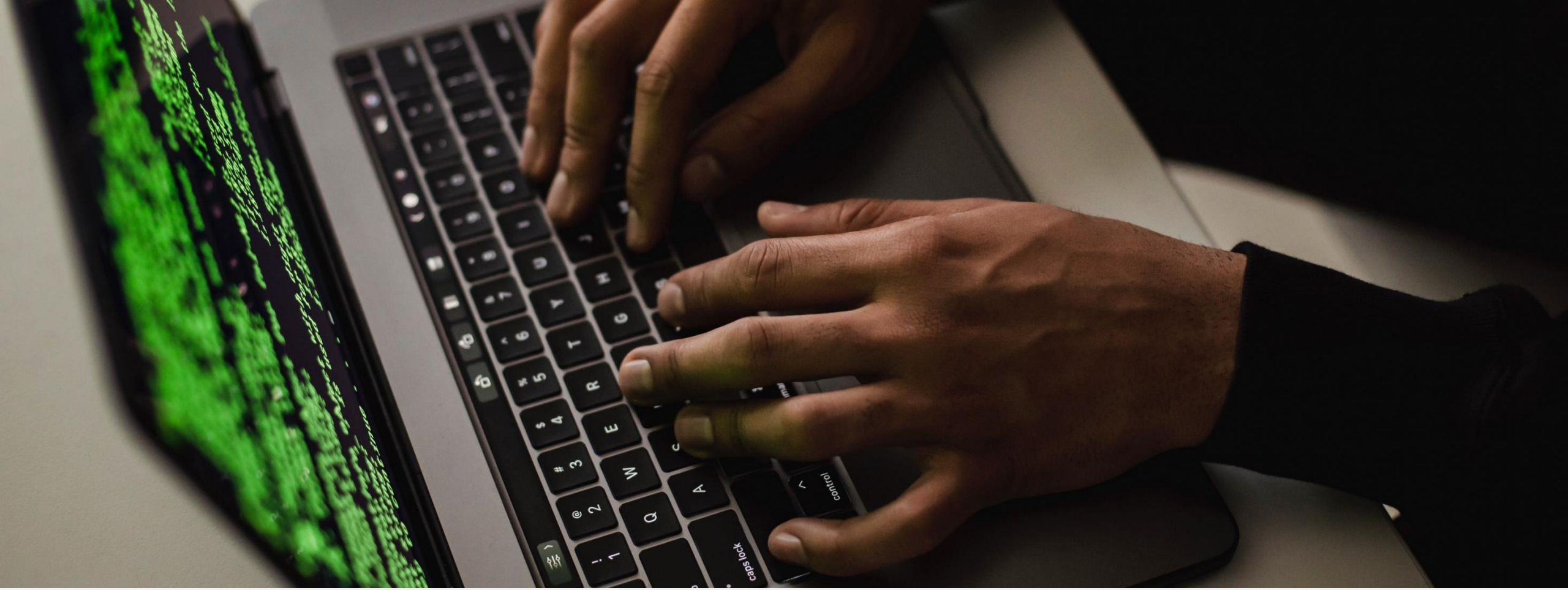


Wenn nichts mehr geht-
Professionelles Krisenmanagement und Lösegeldverhandlung mit Cyber-Erpressern

RiskWorkers
Your Life. Your Risk. Our Business.

Die Opfer

Continental

BISHER KEINE ERPRESSUNG

Deutschlandweite Cyberattacke auf die IHK

Nach einer Cyberattacke auf den IT-Dienstleister der IHK leiden die Kammern bundesweit unter Einschränkungen. Das Ziel des Angriffs scheint Spionage gewesen zu sein.

Home > Cyberangriffe

PRODUKTION STEHT STILL

Hipp gehackt

Der Babynahrungshersteller Hipp wurde gehackt. Ein Großteil der Mitarbeiter konnte vorerst nicht arbeiten, die Ermittlungen laufen.

Massiver Cyberangriff auf die Caritas München und Oberbayern

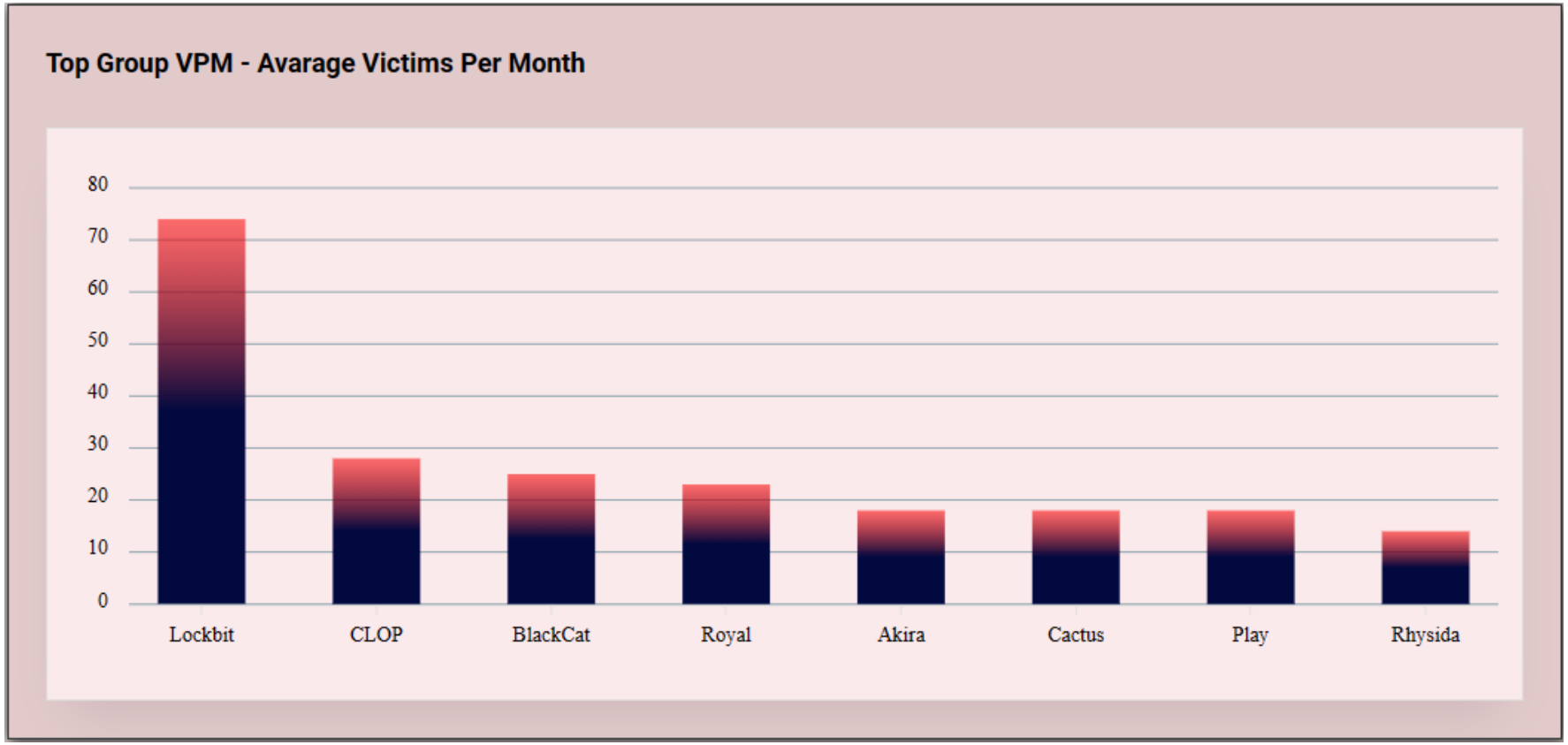
Gnadenlos: Der Cyberangriff auf die Caritas München und Oberbayern

17. September, 2022 08:36

Die Situation

Total Ransomware Incidents Analyzed

8478

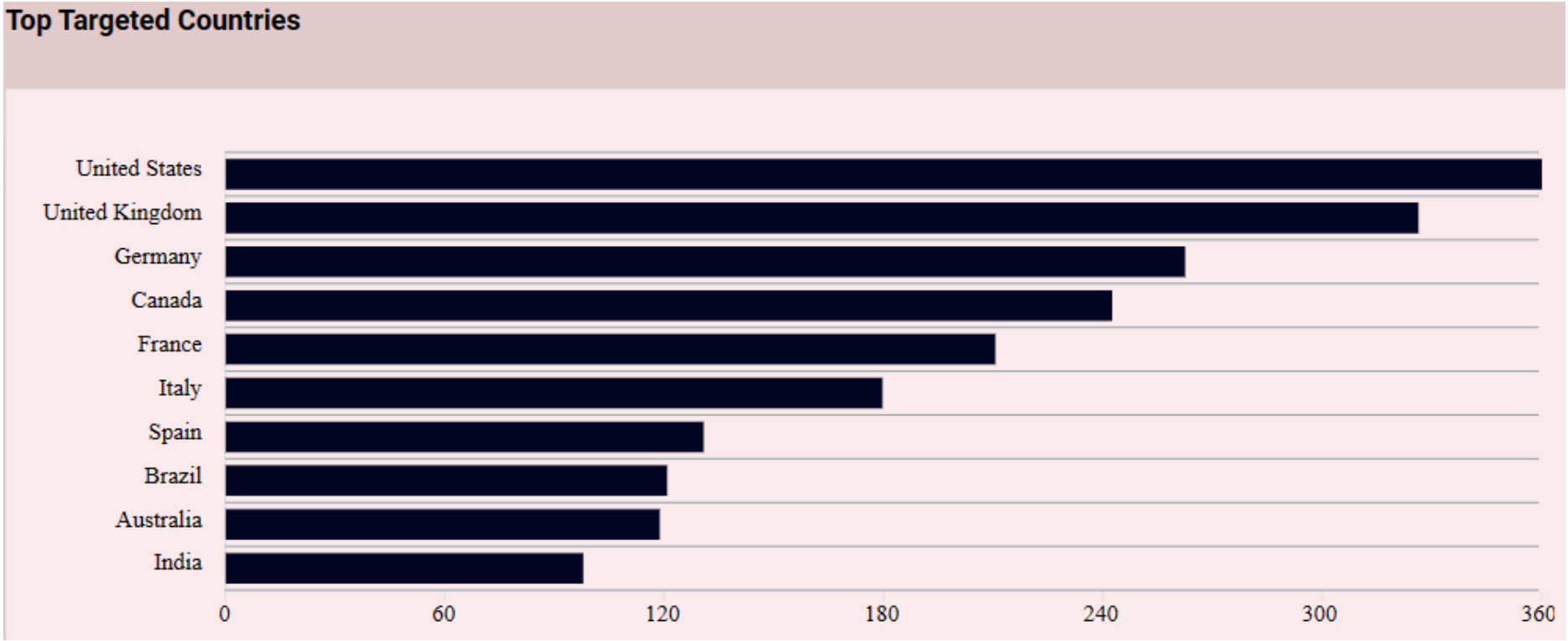


Die Situation

Total Ransomware Incidents Analyzed

8478

Top Targeted Countries

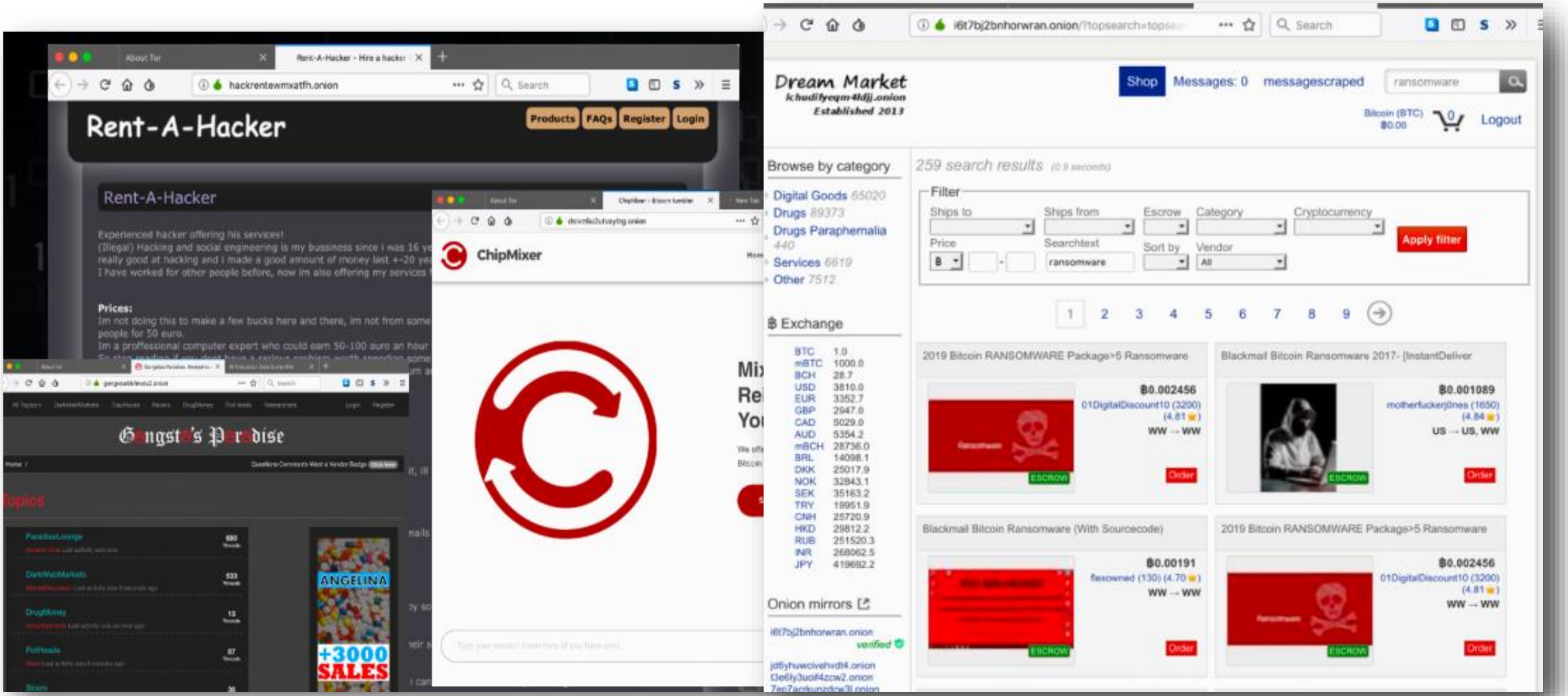


Der Schaden

Betriebsunterbrechung und Wiederherstellungs-kosten sind die Hauptursachen für Ransomware-Verluste

*https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/agcs-ransomware-trends-risks-and-resilience-de.pdf

Im Darknet: Cybercrime as a Service



Die 3 gängigsten Einfallstore für Cyber-Kriminelle

1. Infizierte Software eines Providers
2. Social Engineering & Phishing E-Mails
3. Fehlerhafte oder nicht installierte Sicherheitsupdates

Ransomware – Modi Operandi

1

Daten inkl. BackUps wurden verschlüsselt

Entschlüsselungssoftware ist nicht bekannt. Täter fordern Lösegeld und stellen Entschlüsselung in Aussicht.

2

Daten inkl. BackUps wurden verschlüsselt und von den Servern gestohlen

Täter drohen mit Veröffentlichung und fordern Lösegeld, stellen Entschlüsselung in Aussicht. Dieses Vorgehen wird Double Extortion genannt und avanciert zum Standard-Modus-Operandi.

Ransomware – Modi Operandi

3

Mitarbeiter werden unter Druck gesetzt (Triple Extortion)

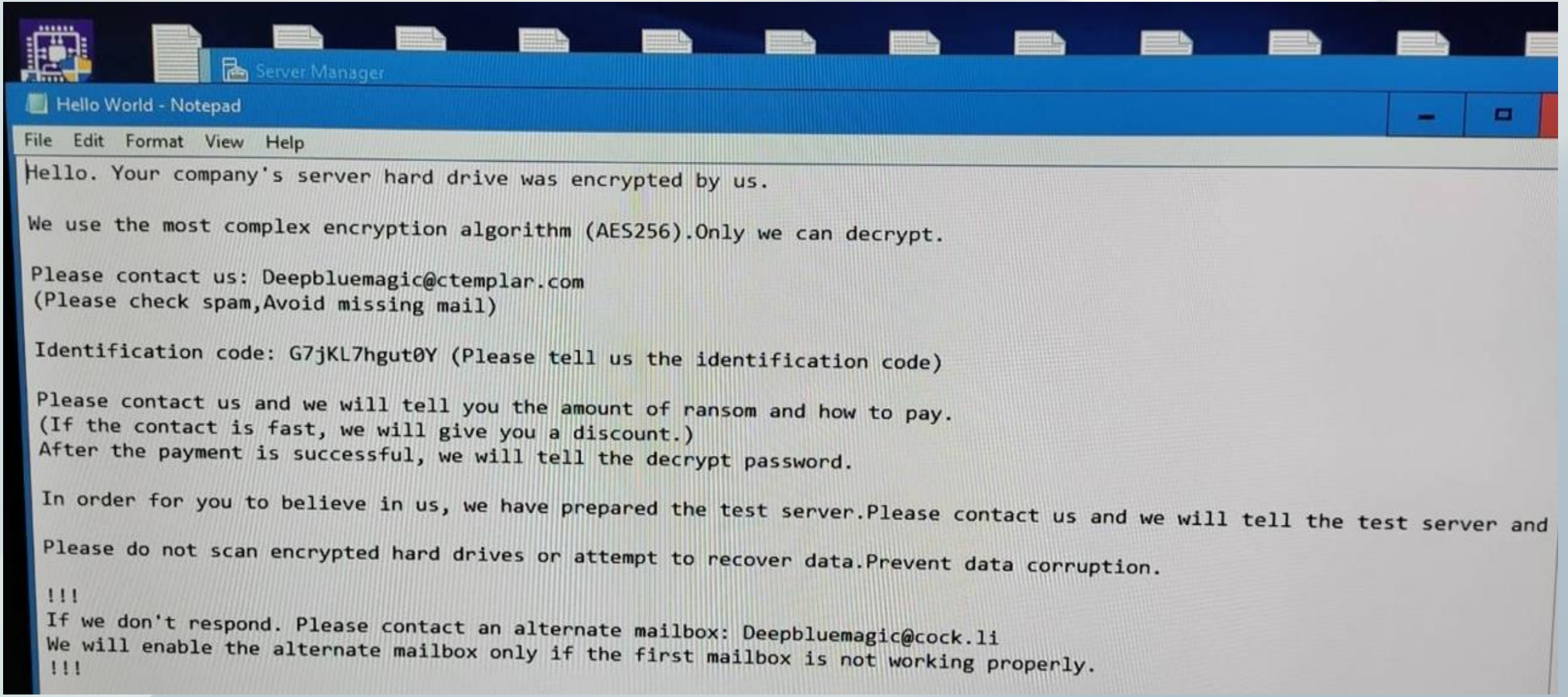
Die Erpresser nehmen per Email oder Messenger Verbindung mit Mitarbeitern des erpressten Unternehmens auf und konfrontieren sie mit persönlichen Daten wie z.B. Abmahnungen, Arbeitsverträgen o.ä.

4

Daten werden zerstört, statt verschlüsselt

Dateien werden auf einen externen Server der Erpresser kopiert. Dateien auf den Servern des Unternehmens werden mit Daten aus anderen Files überschrieben und somit unbrauchbar gemacht.
Löschen statt Verschlüsselung als neueste Entwicklung.

Das Ergebnis



Cyber-Krisenstab

- ? Entscheidungsbefugt?
- ? Zusammensetzung?
- ? Aufgaben?
- ? Abläufe?
- ? Vorbereitet?
- ? Einbindung Externer?
- ? Durchhaltefähig?

Entscheidungsfindung im Krisenstab

1. „Die drei Optionen“
2. Was kostet mich der Ausfall meiner Systeme pro Tag?
3. Was kostet mich der Verlust der Reputation gegenüber meinen Stake Holdern?
4. Was kostet mich die Wiederherstellung der Daten bei Nicht-Zahlung?
5. Was kostet mich die Zahlung von Lösegeld inkl. Berater u. Ausfall der Systeme?

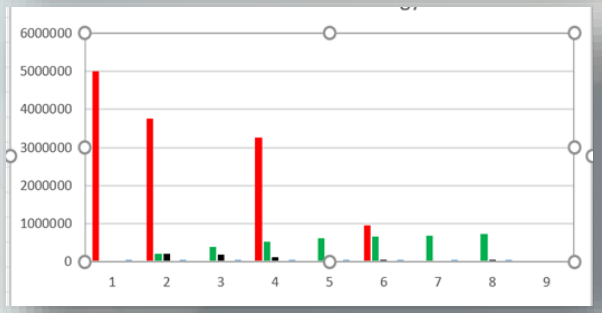
Die Rolle der Polizei

1. Anzeige möglich, aber nicht verpflichtend
2. LKA: Zahlen Sie kein Lösegeld!
3. Ermittlung der Täter vs. Abwendung des wirtschaftlichen Schadens
4. Lösegeldzahlung ist per se nicht verboten!

Bestandteile der Verhandlungsstrategie

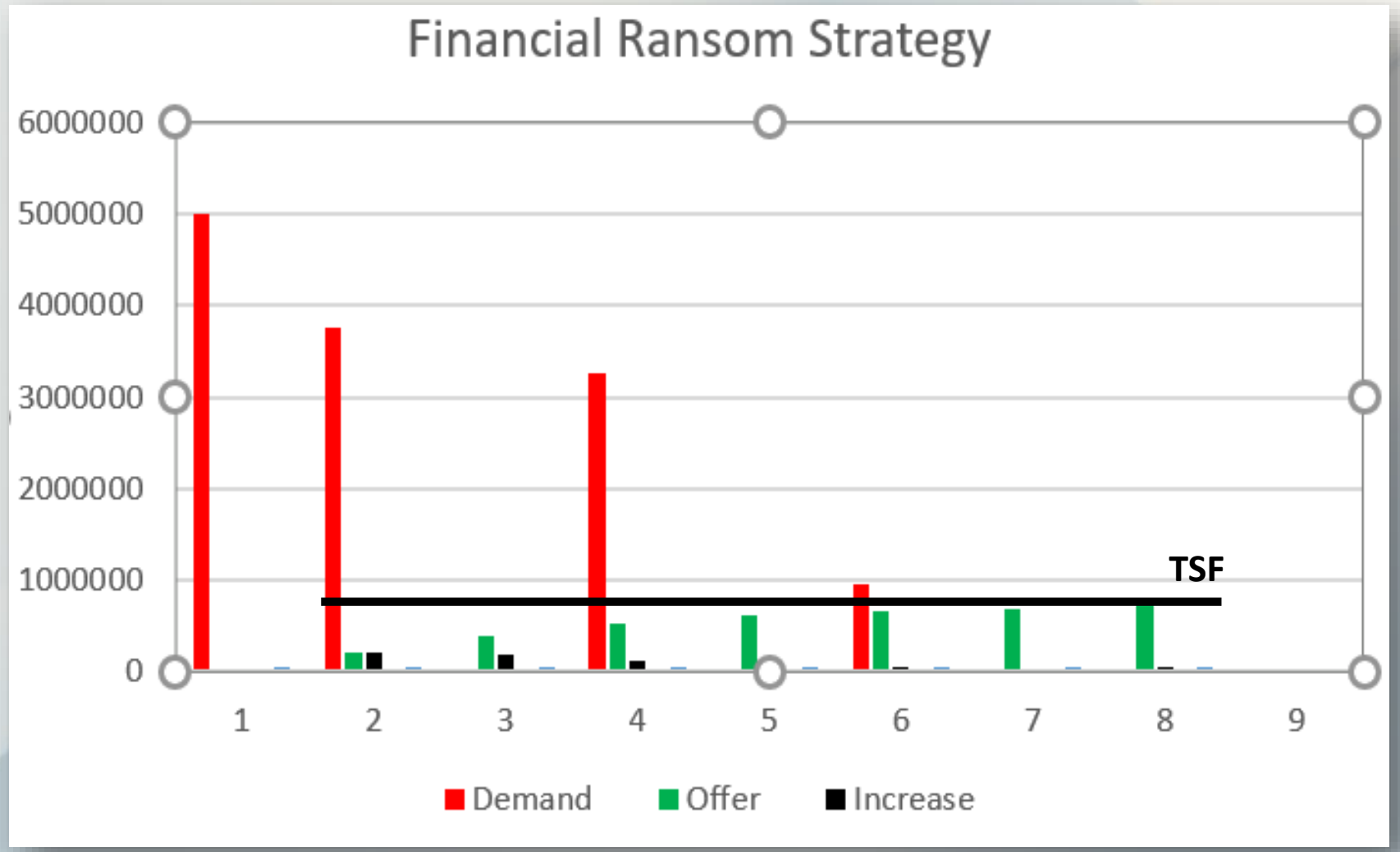
Signal unsrerseits: Bereitschaft zur Zahlung

Erst kommt relativ viel, dann immer weniger



Wir orientieren uns nicht an der Forderung,
sondern an dem, was wir bereit sind zu zahlen

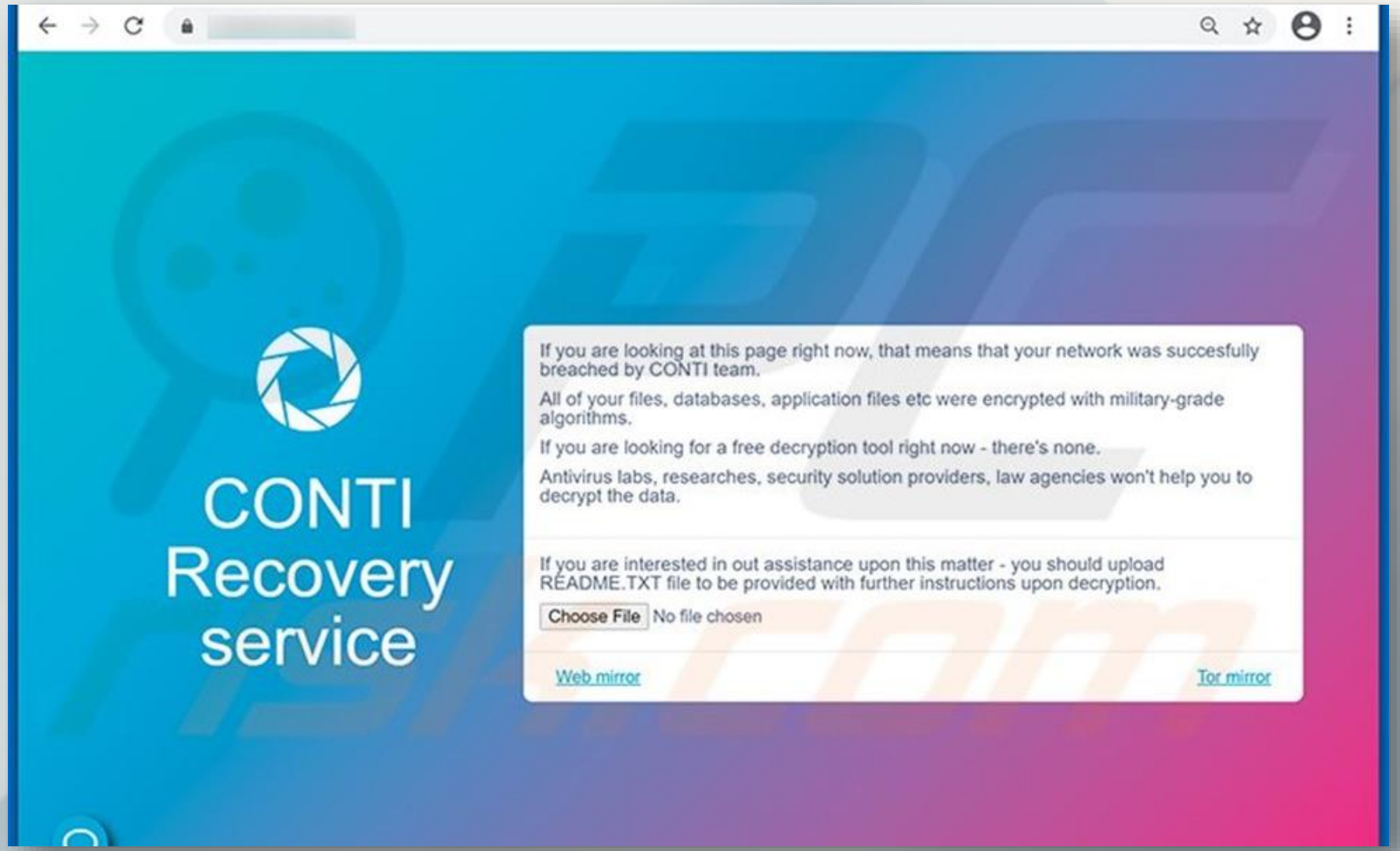
Bestimmen der Höhe des Lösegelds



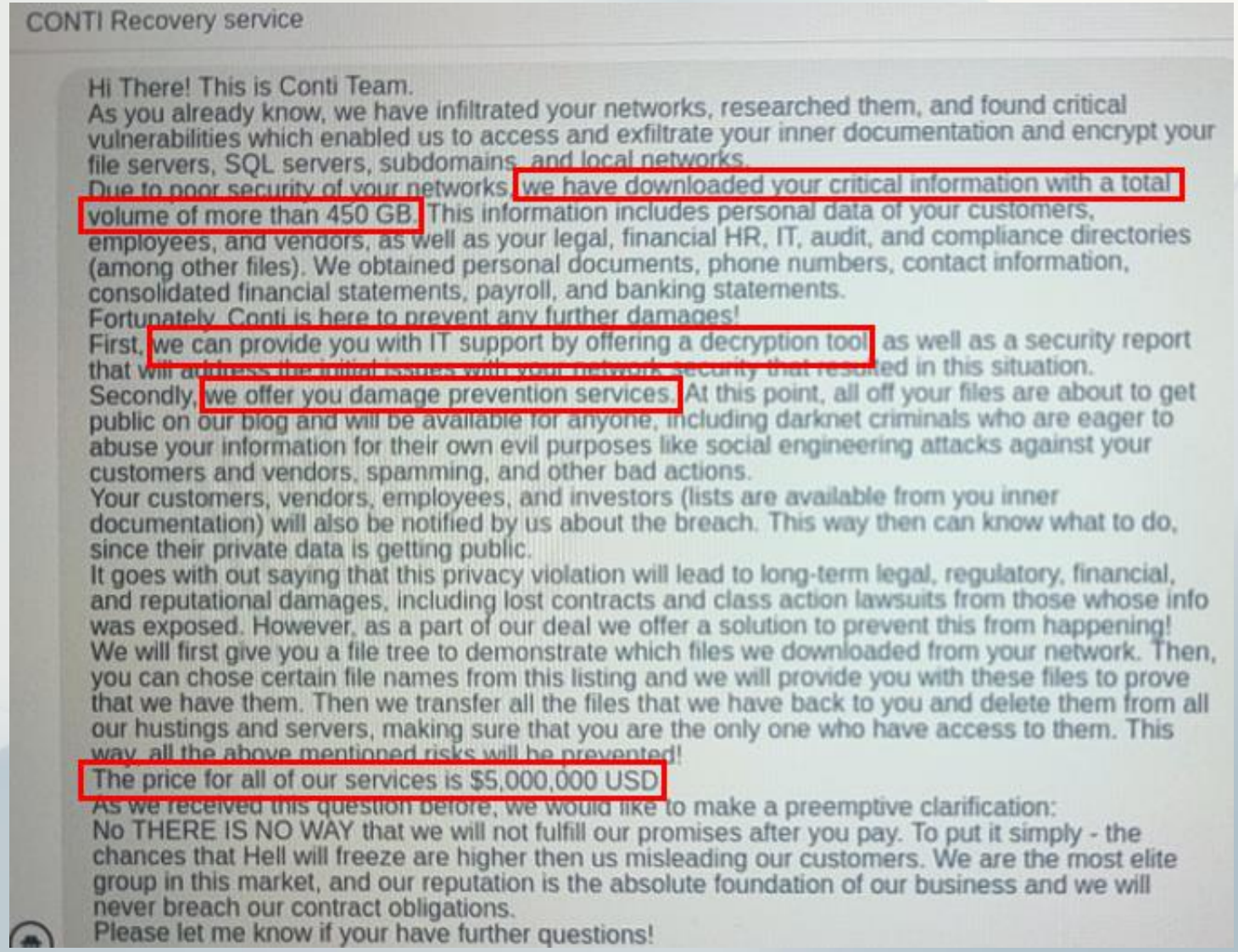
Inhalte der Verhandlung

1. Über was genau werden wir verhandeln? (Schlüssel, Security Report, Währung, keine weitere Veröffentlichung)
2. Keine Verhandlung ohne , Proof of Documents‘
3. Keine Verhandlung ohne Script
4. Erst Forderung der Erpresser, dann unser Gegenangebot
5. Unser erstes Angebot kauft uns Zeit und zeigt der Gegenseite, dass etwas zu holen ist, Faktor Zeit wird zu „unserem Freund“

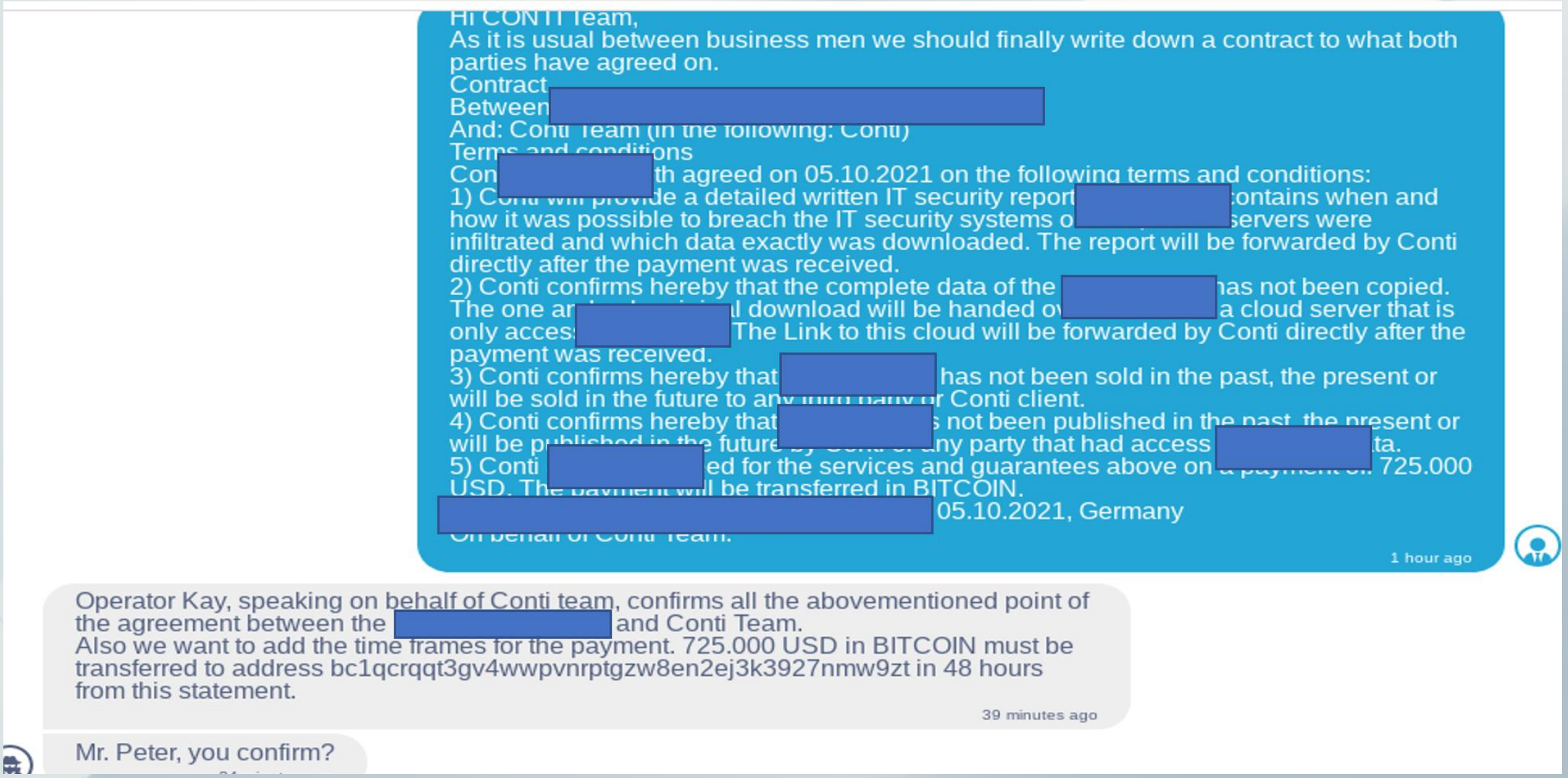
Die Verhandlung – Der Chat beginnt



Die Verhandlung – Der Chat beginnt



Die Verhandlung – Der Vertrag



Die Verhandlung–Entschlüsselung und Security Report

Tip of the Day

Krisenmanagement-Handout für alle Mitglieder des Krisenstabs – Roles and Responsibilities

Cyber-Krisenübungen lassen Sie in der Krise schneller, besonnener und effektiver entscheiden

Social Engineering Awareness Schulungen sind unverzichtbarer Bestandteil einer ganzheitlichen IT-Security

Darknet Intelligence as a Service als wirksames Frühwarnsystem zum Schutz des Unternehmens. Abgeflossene Credentials, Waren, Informationen, etc. werden so beobachtet; unternehmensbezogene Schadsoftware wird frühzeitig identifiziert

Red Teamings/ Pen-Tests (Partner)

Cyberversicherung inkl. Lösegelddeckung

Kontakt

RiskWorkers GmbH

Konrad-Zuse-Platz 8
81829 München

Telefon: +49 89/20 70 42- 630
Fax: +49 89/20 70 42- 631
Email: office@riskworkers.com

RiskWorkers
Your Life. Your Risk. Our Business.