



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



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

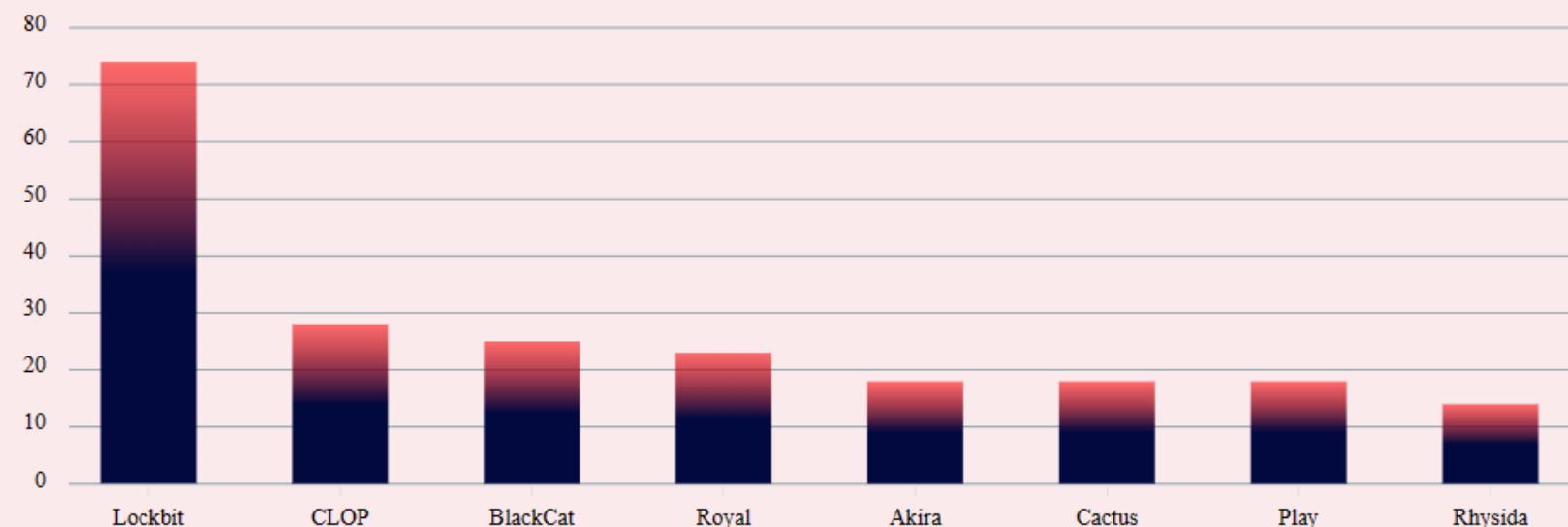
17. September, 2022 08:36

# Die Situation

**Total Ransomware Incidents Analyzed**

**8478**

**Top Group VPM - Average Victims Per Month**

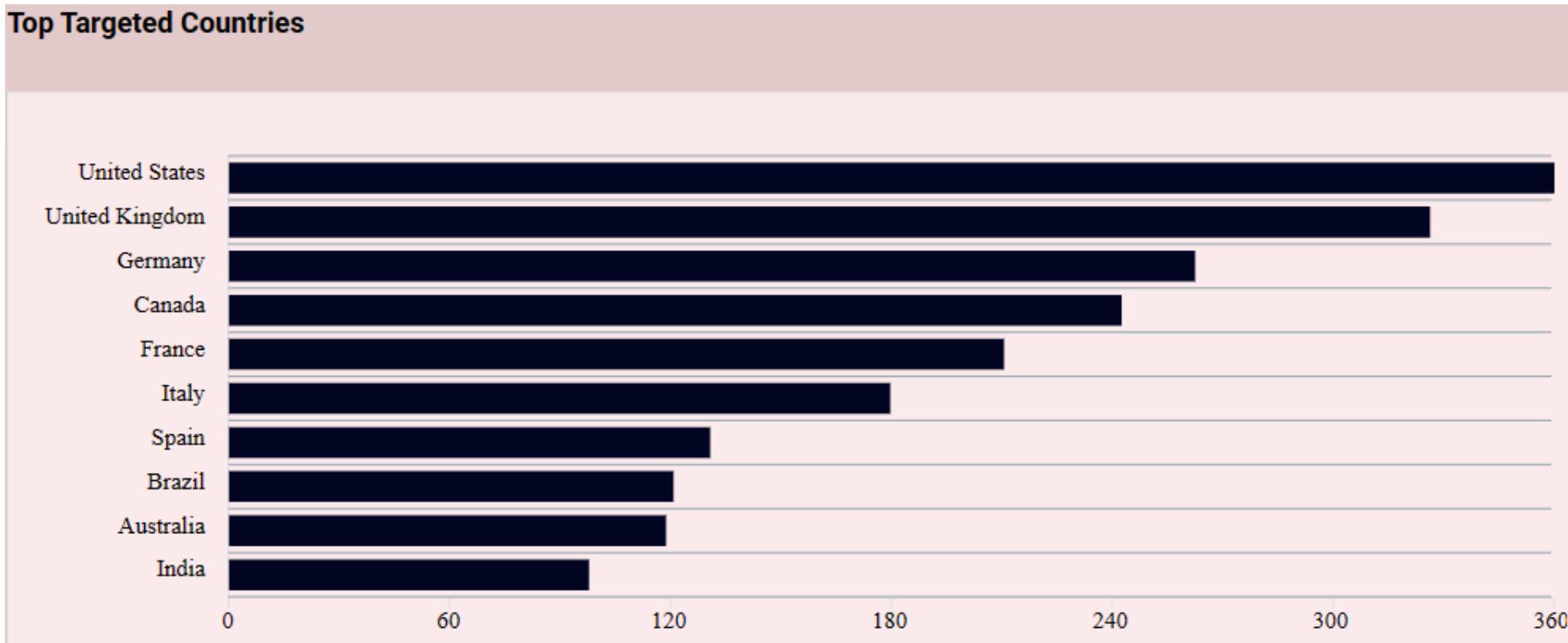


# Die Situation

Total Ransomware Incidents Analyzed

**8478**

## Top Targeted Countries



**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

The image is a collage of four screenshots from the Darknet, illustrating various cybercrime services:

- Rent-A-Hacker (Screenshot 1):** A service where an experienced hacker offers his services. The text on the page includes: "Experienced hacker offering his services! (Illegal) Hacking and social engineering is my business since I was 16 years old. I'm really good at hacking and I made a good amount of money last +20 years. I have worked for other people before, now I'm also offering my services! Prices: I'm not doing this to make a few bucks here and there, I'm not from some people for 50 euro. I'm a professional computer expert who could earn 50-100 euro an hour. So when you're reading this, if you don't know a certain number, just add some zeros to it. I'm not doing this to make a few bucks here and there, I'm not from some people for 50 euro. I'm a professional computer expert who could earn 50-100 euro an hour. So when you're reading this, if you don't know a certain number, just add some zeros to it."
- Dream Market (Screenshot 2):** A marketplace for various goods and services. The search results for "ransomware" are shown, with 259 results found. The top result is "2019 Bitcoin RANSOMWARE Package>5 Ransomware" for \$0.002456. Other results include "Blackmail Bitcoin Ransomware 2017- [InstantDelivery]" and "2019 Bitcoin RANSOMWARE Package>5 Ransomware".
- ChipMixer (Screenshot 3):** A service for mixing cryptocurrencies. It shows exchange rates for various currencies (e.g., BTC, mBTC, BCH, USD, EUR, GBP, CAD, AUD, mBCH, BRL, DKK, NOK, SEK, TRY, CNH, HKD, RUB, INR, JPY) and an "Onion mirrors" section with links to i6t7b2bnhorwan.onion and jd6yhucivehvd14.onion.
- Gangster's Paradise (Screenshot 4):** A marketplace for various items. It features a large red circular logo with a white arrow. The page shows categories like "ParadiseLounge", "DollWHORES", "DrugMoney", "Pornstars", and "Topics". A banner at the bottom says "+3000 SALES".

# 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.

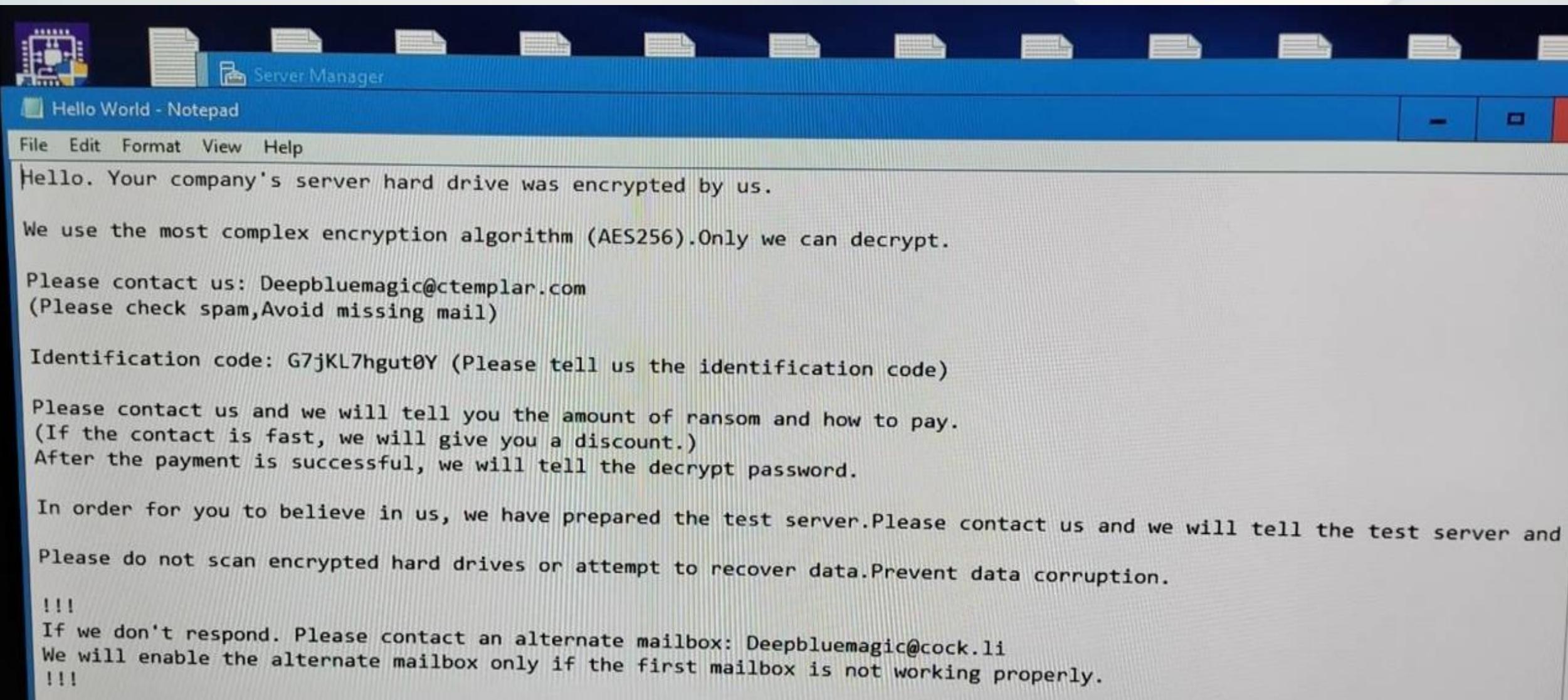
4

## **Daten werden zerstört, statt verschlüsselt**

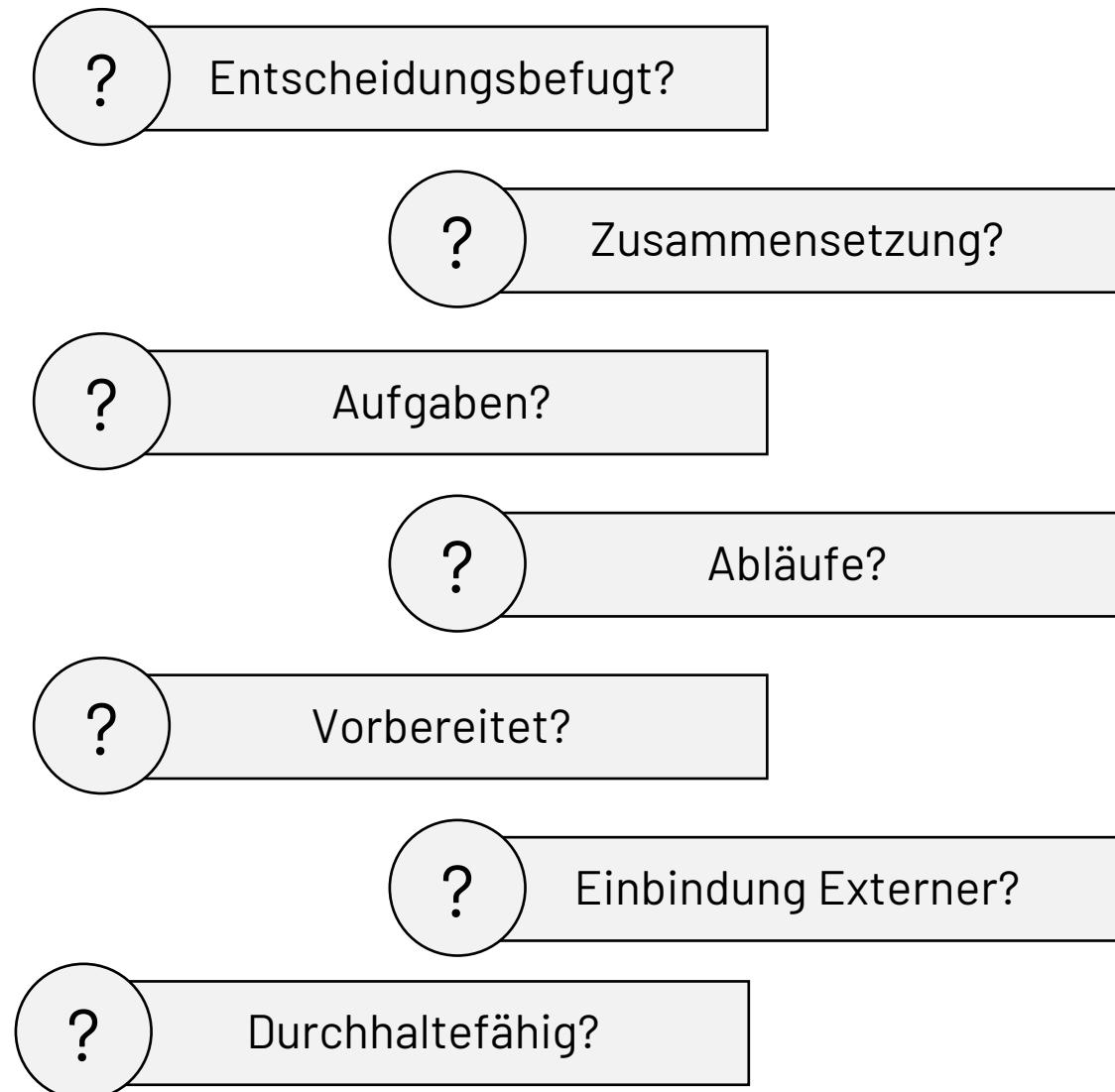
Dateien werden auf einen externen Server der Erpresser kopiert. Dateien auf den Servern des Unternehmens werden mit Daten aus anderen Files überschrieben und somit unbrauchbar gemacht.

Löschen statt Verschlüsselung als neueste Entwicklung.

# Das Ergebnis



# Cyber-Krisenstab



# 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!

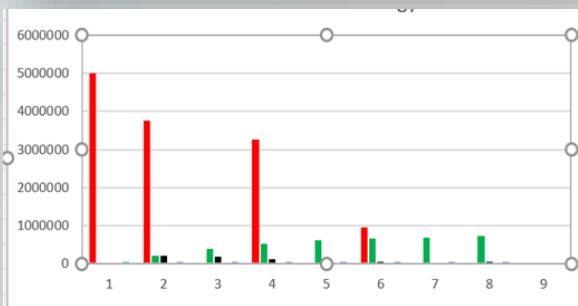
# Bestandteile der Verhandlungsstrategie



Signal unsrерeits: Bereitschaft zur Zahlung

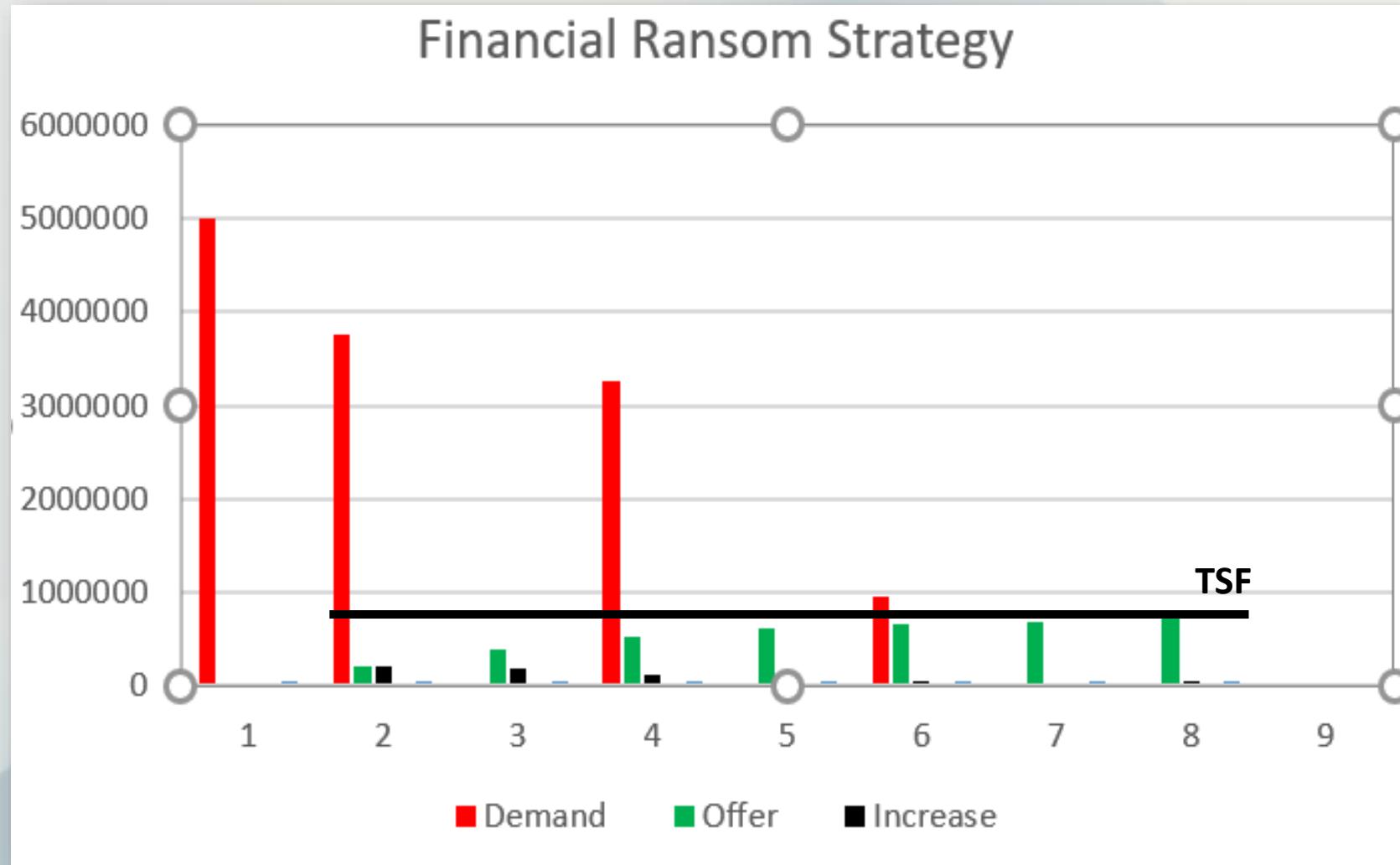


Erst kommt relativ viel, dann immer weniger



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

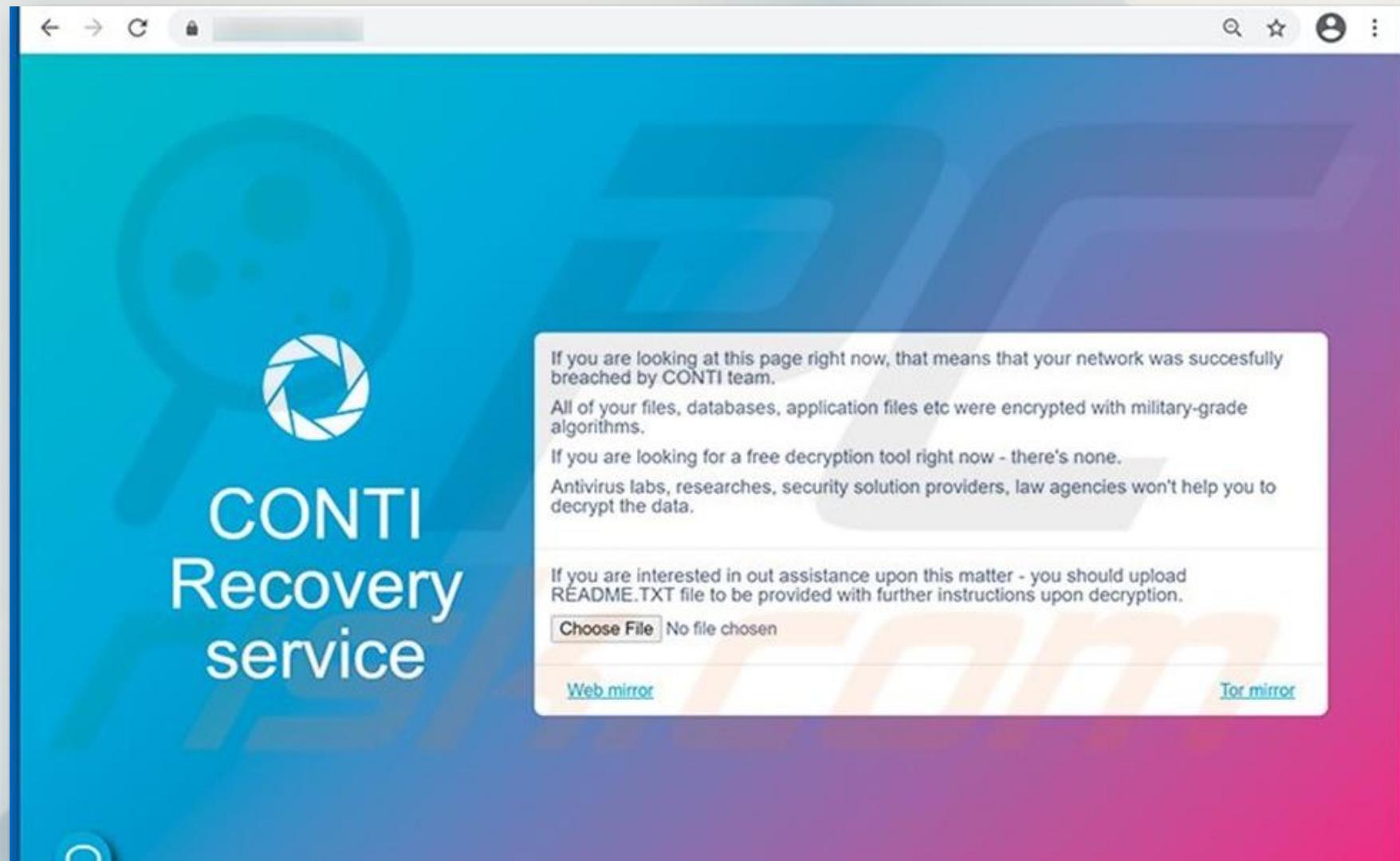
4

Erst Forderung der Erpresser, dann unser Gegenangebot

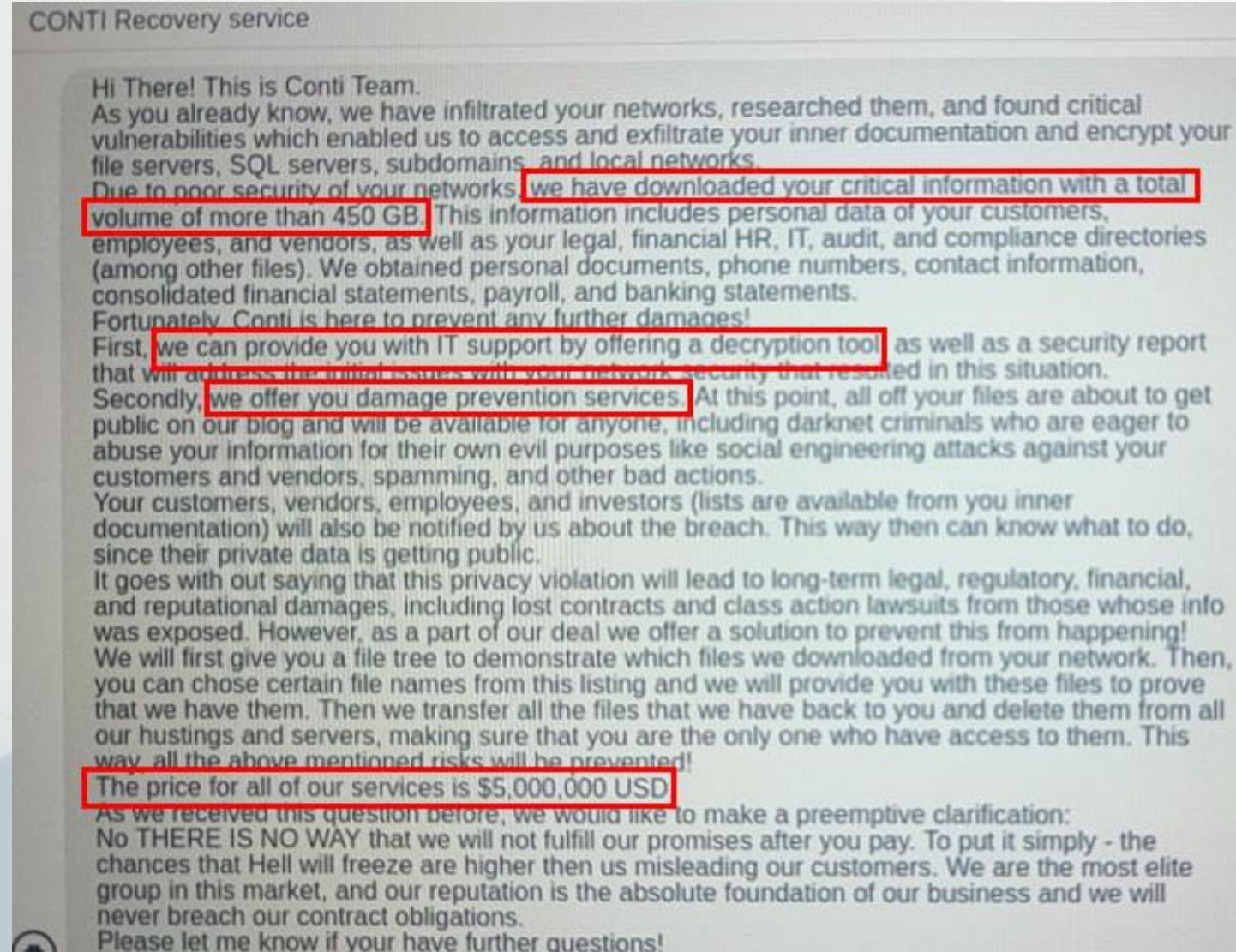
5

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

Hi CONTI team,  
As it is usual between business men we should finally write down a contract to what both parties have agreed on.  
Contract  
Between [REDACTED]  
And: Conti team (in the following: Conti)  
Terms and conditions  
Conti [REDACTED] agreed on 05.10.2021 on the following terms and conditions:  
1) Conti will provide a detailed written IT security report [REDACTED] contains when and how it was possible to breach the IT security systems of [REDACTED] servers were infiltrated and which data exactly was downloaded. The report will be forwarded by Conti directly after the payment was received.  
2) Conti confirms hereby that the complete data of the [REDACTED] has not been copied. The one and unique download will be handed over to [REDACTED] a cloud server that is only accessible by [REDACTED]. The Link to this cloud will be forwarded by Conti directly after the payment was received.  
3) Conti confirms hereby that [REDACTED] has not been sold in the past, the present or will be sold in the future to any [REDACTED] or Conti client.  
4) Conti confirms hereby that [REDACTED] has not been published in the past, the present or will be published in the future by [REDACTED] or any party that had access to [REDACTED] data.  
5) Conti [REDACTED] for the services and guarantees above on a payment of 725.000 USD. The payment will be transferred in BITCOIN.  
[REDACTED] 05.10.2021, Germany

On behalf of Conti Team.

1 hour ago



Operator Kay, speaking on behalf of Conti team, confirms all the abovementioned point of the agreement between the [REDACTED] and Conti Team.  
Also we want to add the time frames for the payment. 725.000 USD in BITCOIN must be transferred to address bc1lqcrqqt3gv4wwpvnrtgzw8en2ej3k3927nmw9zt in 48 hours from this statement.

39 minutes ago



Mr. Peter, you confirm?

# Die Verhandlung-Entschlüsselung und Security Report

Here is your data:  
mega.nz  
wzvebkxv@pokemail.net  
hysuiious65@45fGha!  
2 minutes ago

The decryptor is being prepared now.  
2 minutes ago

[0Y2bUdHGJV86rTP8Tu27AgfN91oYLnc2GES6JjNUJY6Wy4r1DlzS2E7P7QpX2VVe\\_decryptor.exe](#)  
[ 108kB ]  
1 minute ago

Decryptor:  
1) Launch the decryptor under Administrative rights  
2) Wait till the decryptor window is closed  
3) if any of the files haven't changed the extension back to the original - repeat 1 and 2  
1 minute ago

We have penetrated your network using email compromise. So, first of all - provide all your employees with strict instructions regarding security measures.  
Basic recommendations regarding network:  
1. Implement better email filtering policies  
2. Implement better password policies  
3. Consider blocking some particular attacks like pass-the-hash and pass-the-ticket  
4. Update all of your internal systems to the latest versions  
5. Review network segmentation and take care about buying hardware firewalls with filtering policies  
6. Block kerberoasting attacks  
7. Conduct full penetrations tests (both external and internal)  
8. Implement better AV/EDR systems  
9. Review group policies, remove domain and local admin rights for some users.  
10. Implement better DLP software system  
51 seconds ago



# 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](mailto:office@riskworkers.com)



**RiskWorkers**

Your Life. Your Risk. Our Business.