



Erfahrungsbericht – Ransomware-Angriff

LEIDENSCHAFT FÜR LÖSUNGEN



Hi friends,

Whatever who you are and what your title is is fully or partially dead, all your backups removed. Moreover, we have taken a great amount of your data.

Well, for now let's keep all the tears and remember to be aware of what damage we caused by locking your files.

1. Dealing with us you will save A LOT due to your finance, bank & income statements, your tax returns, etc. If you have an active cyber insurance, let us know. The negotiation process will lead to failing of a deal.
2. Paying us you save your TIME, MONEY, EFFORT. We will restore properly on any files or systems, so you will not lose anything of our conversation. If you decide to refuse our offer, we will delete the files or accidentally corrupt them – in this case we will not be responsible.
3. The security report or the exclusive first-hand information has a great value, since NO full audit of your network is possible in order to get into, identify backup solutions, etc.
4. As for your data, if we fail to agree, we will delete it. – generally speaking, everything that has a value will be published in our blog – <https://akira.com>
5. We're more than negotiable and will definitely find a way to satisfy both of us.

If you're indeed interested in our assistance, please contact us via info@reichhart-logistik.com or <https://akira.com>

Instructions:

1. Install TOR Browser to get access to our website
2. Paste this link – <https://akira.com>
3. Use this code – XXXX-XX-XXXX-XXXX – to login

Keep in mind that the faster you will get in touch with us, the better it will be for you.



Agenda

- » Ransomware-Angriff: Krisenmanagement und Sofortmaßnahmen
- » Strategien zur Überbrückung und Wiederaufbau
- » Stakeholder-Management und Reaktionen beim Angriff
- » Exkurs: Idealtypischer Fall einer Cyber-Attacke
- » Empfehlungen für Unternehmen für mehr Cybersicherheit

Ransomware-Angriff: Krisenmanagement und Sofortmaßnahmen



Erste Bestandsaufnahme

- » Kein Zugriff auf bestimmte Systeme
- » Ransomware mit Verschlüsselung und Lösegeldforderung
- » Vielzahl von Systemen & Bereichen betroffen
- » Back-up war ebenso verschlüsselt



Akute Reaktion

- » Einrichtung des Krisenstabes
- » Definition Sofort-Maßnahmen
- » Erst-Analyse der Auswirkungen
- » Definition relevanter Stakeholder
- » Aufbau Erpresserkommunikation

Strategien zur Überbrückung und Wiederaufbau

- » Aufbau einer neuen **Interims-Kommunikationsplattform**
- » **Datenrekonstruktion** über geteilte Inhalte in der Cloud
- » Aufbau der **IT-Infrastruktur auf der grünen Wiese**

Strategie auf zwei Ebenen

1. Netzwerkzugang

2. Datenzugriff

Lösungsansätze

Cloud-Lösungen, Neueste Technologien, Systemüberprüfung und
– Monitoring, Mitarbeiter-Aufklärung, etc.



Stakeholder-Management und Reaktionen beim Angriff



Versicherung

Aufbau IT-Hardware-
Interimsinfrastruktur &
Unterstützung beim
Wiederaufbau



Kunde

Professionelle sowie
pragmatische Reaktionen
ohne hohe Bürokratie



Mitarbeiter

Belastbares und
leistungsfähiges Team mit
hoher Expertise



Behörden

Teils bemüht, aber
fehlende Tools,
Kompetenzen &
Zuständigkeiten



Banken

Teils Finanzierung bis zur
Wiedererlangung des
normalen Cash-Flows

Exkurs: Idealtypischer Fall einer Cyber-Attacke

- 1 Vorbereitung durch Eindringen in das Unternehmensnetzwerk
- 2 Kontaktaufnahme des Täters mit dem Opfer
- 3 Prüfung auf tatsächlichen Täter
- 4 Verhandlungen über Lösegeld mit den Erpressern
- 5 Vertragsabschluss über bspw. Analyseprotokoll



Empfehlungen für Unternehmen für mehr Cybersicherheit



1

Investition in IT-Sicherheit

2

Abschluss einer Cyberversicherung und Prüfen der Leistungsfähigkeit

3

Pflegen einer offenen Fehlerkultur im Unternehmen



LOGISTIK

LEIDENSCHAFT FÜR LÖSUNGEN