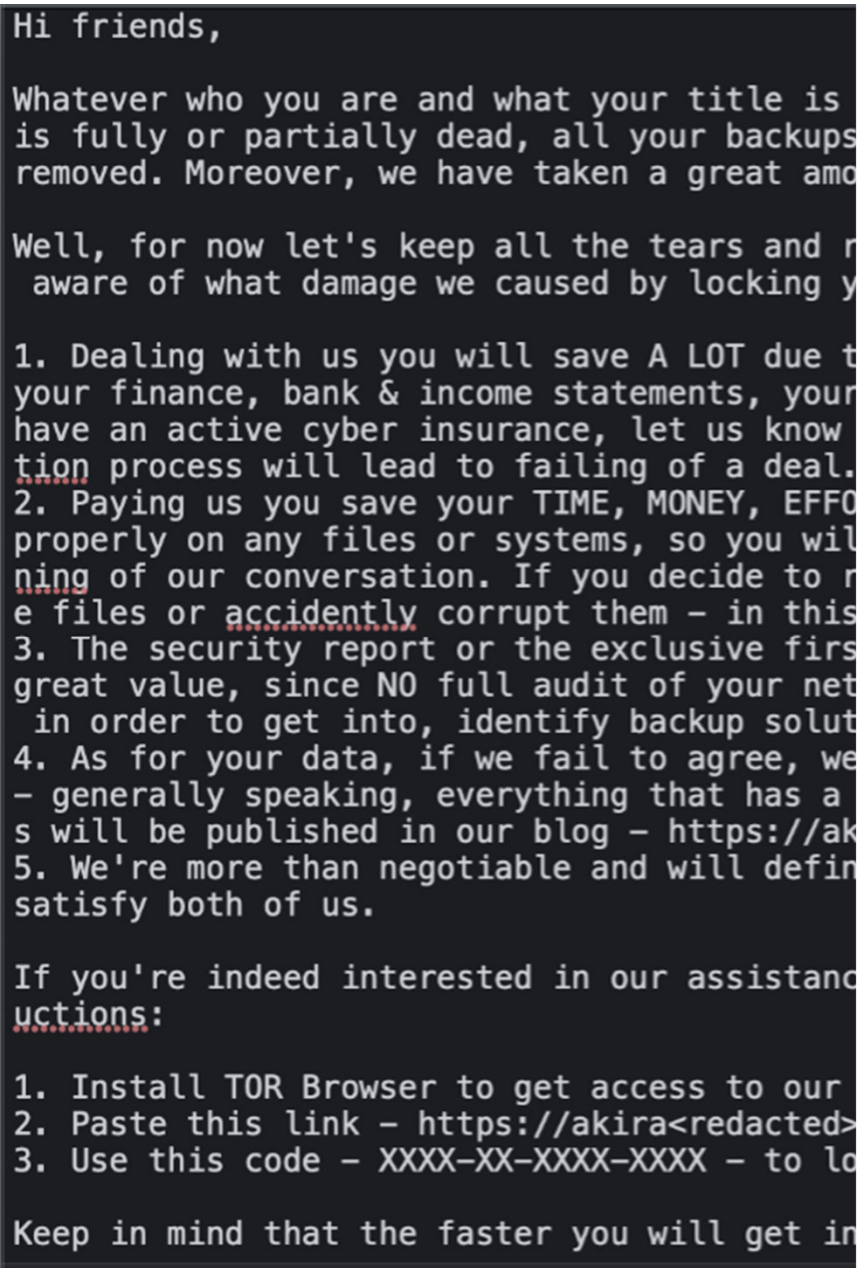
REICHHART

LOGISTIK

Erfahrungsbericht – Ransomware-Angriff

LEIDENSCHAFT FÜR LÖSUNGEN


RECHENZE



REICHHART LOGISTIK

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