TEMET
end-to-end IT security

Cyber-Angriffe - Ein Blick hinter die Schlagzeilen

03.05.2023

Ein Blick zurück

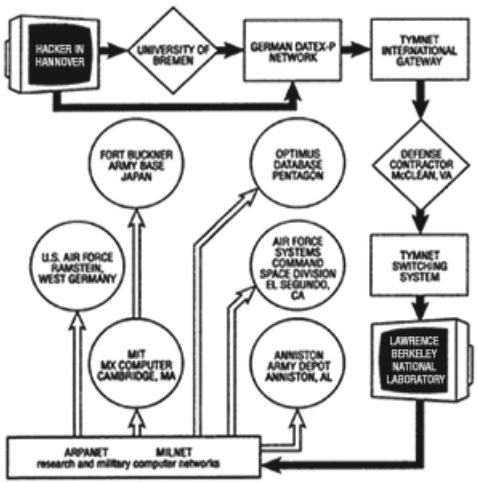
1989 - Eine erste Schlagzeile

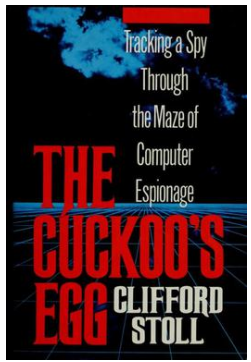
Die Polizei stürmt eine Wohnung im Norden Deutschlands. Es ist der Moment, in dem die Öffentlichkeit das erste Mal von den Ereignissen erfährt, welche bekannt werden sollten als — *der KGB Hack.*

In der ARD Tagesschau vom 02.03.1989

https://www.youtube.com/embed/gRr2zVVFkQw

Der KGB Hack





Die Merkmale des Hacks

Die Angreifer

- Keine einmalige Aktion, sondern eine langandauernde Operation.
- Das eigentliche Ziel wurde nicht direkt angegriffen.
- Ein staatlich geförderter Angriff mit zivilen und staatlichen Zielen.
- Die Angreifer waren keine Staatsangestellten, sondern Söldner.

Die Verteidiger

- Zufall und Neugier brachten die Verteidiger auf die Spur.
- Logs, Alerts und Attrappen waren wichtige Mittel.
- Die Täter agieren international und die Behörden aber national.

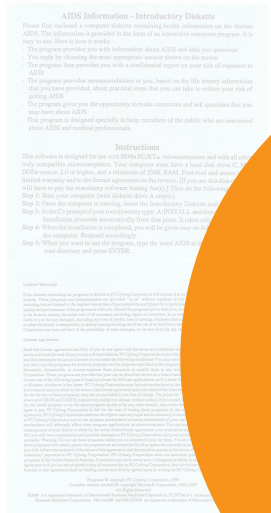
Zurück in die Gegenwart

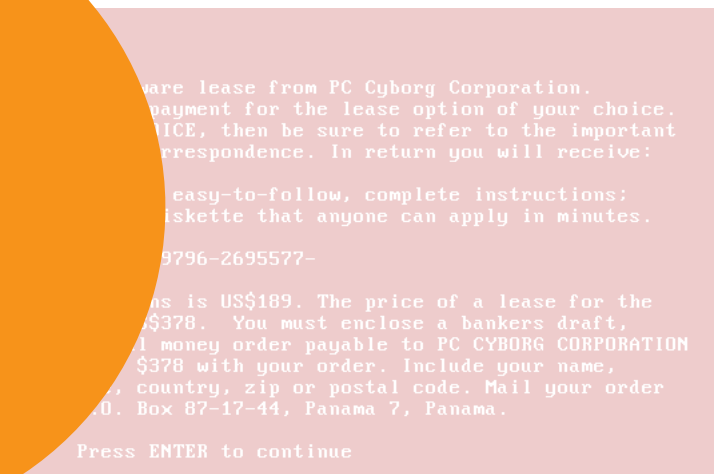
Ransomware - Die andere Pandemie

- Dominante Form der Cyberkriminalität
- Erpressung durch Verschlüsselung
- Ransomware kann ein Unternehmen runinieren
- IT-Abhängigkeit wird sichtbar
- Jeder kann zum Opfer werden

TEMET
end-to-end IT security

Wie wurde Ransomware zur Pandemie?

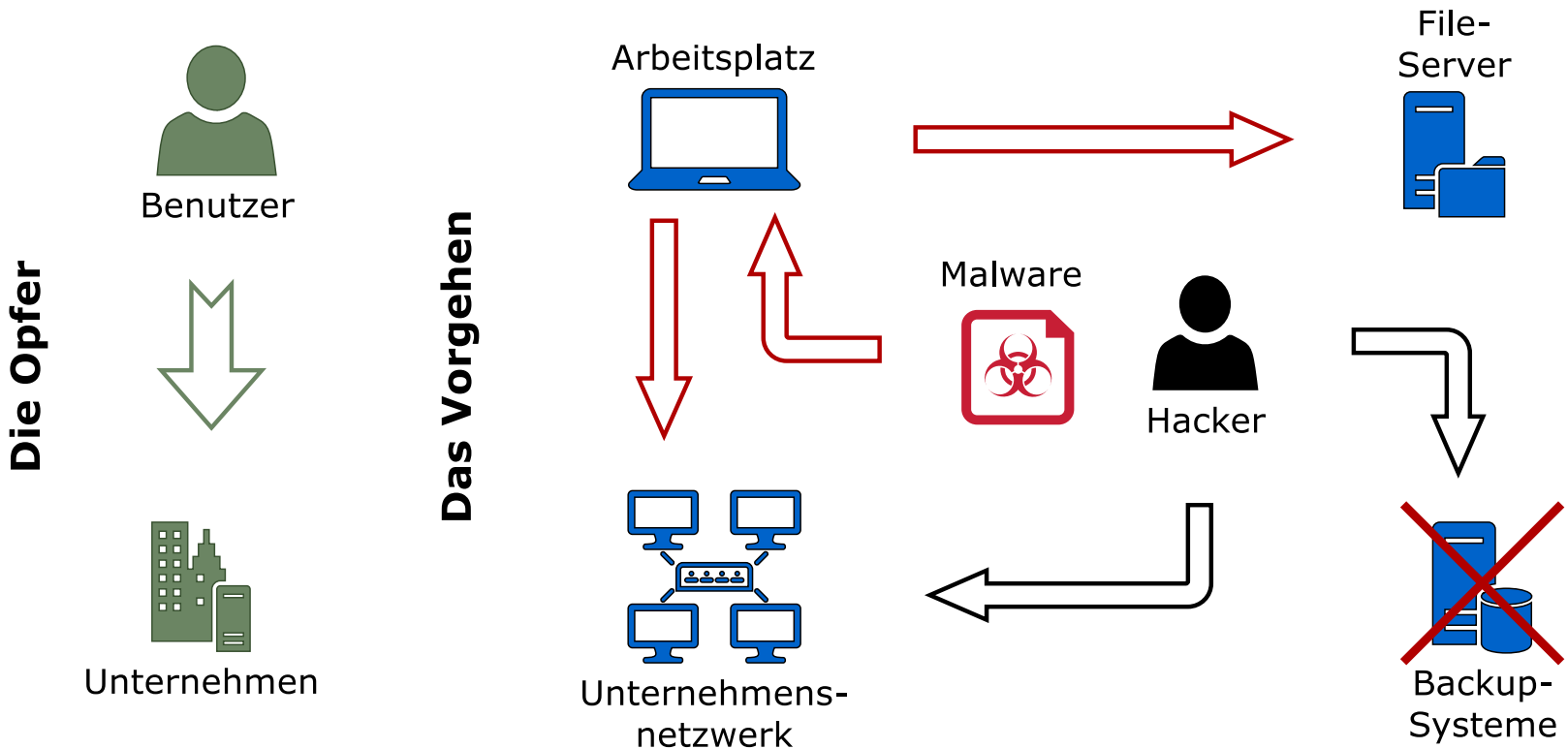




AIDS oder PC Cyborg Trojan, die erste Ransomware von 1989.

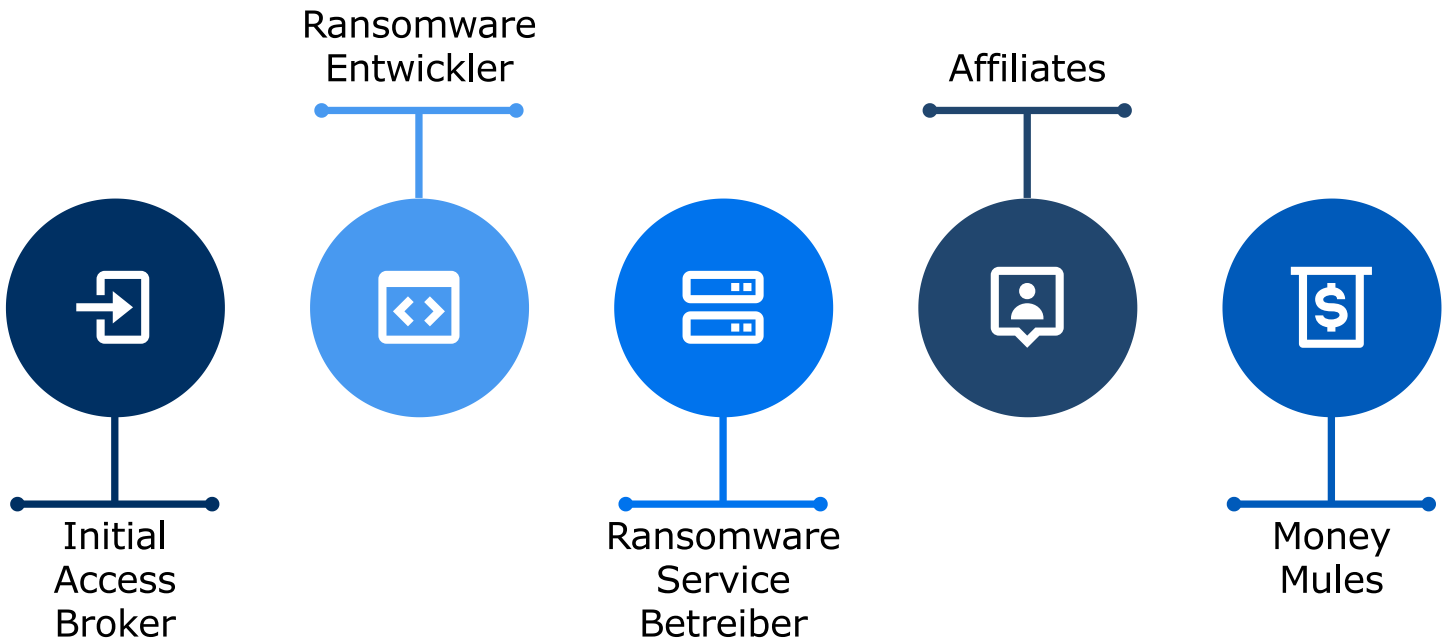
TEMET
end-to-end IT security

Die Evolution der Ransomware-Angriffe



TEMET
end-to-end IT security

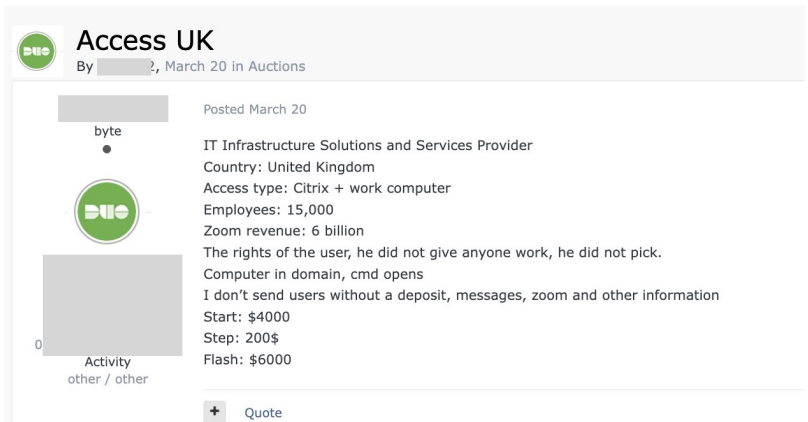
Das Ransomware-Ökosystem



Inital Access Broker

Stehlen von Zugangs-daten z.B. mittels Phishing

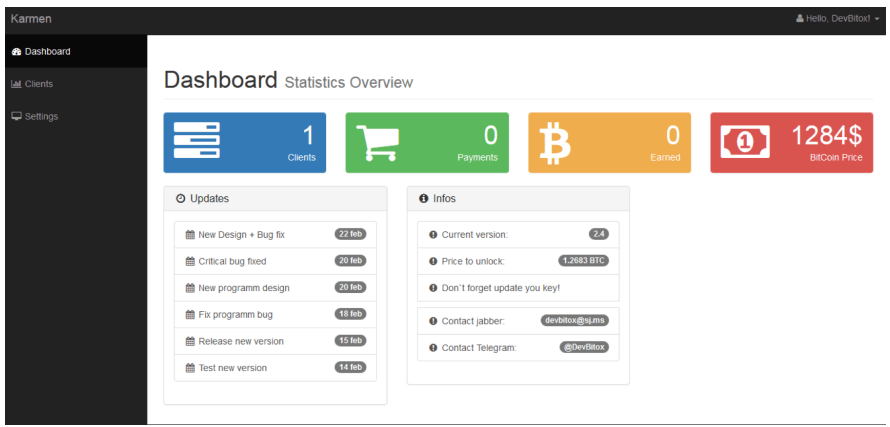
Verkauf der Zugangsdaten im Darkweb



Ransomware Entwickler

Entwicklung der Ransomware-Software

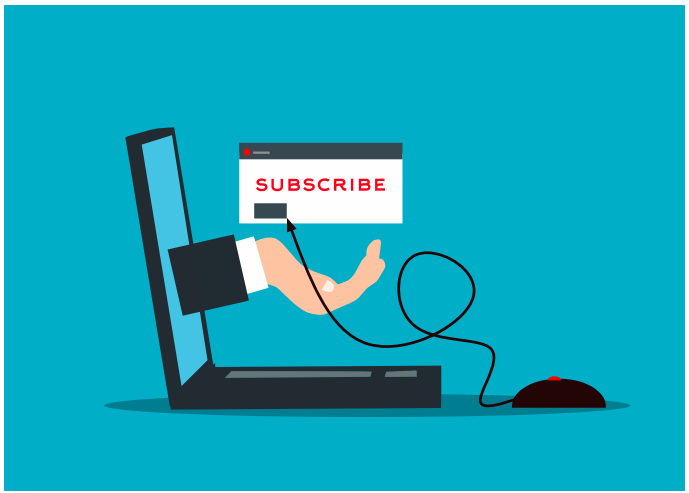
Inklusive der notwendigen Serverkomponenten



Ransomware Service Betreiber

Betrieb der Server-Infrastruktur

Bereitstellen der Software als Service



Affiliates

Verteilen und Ausführen der Ransomware

Bezahlung via Service Provider mittels Cryptocurrency

Money Mules

Umtauschen der Cryptowährung in traditionelle Währungen

Überweisen der Geldes mittels Geldtransfer-Service

Vielen Dank für ihre Aufmerksamkeit.

TEMET
end-to-end IT security