AWARE7
full service awareness agency

Live Hacking

Wenn Daten auf Reisen gehen

Wer bin ich?

Chris Wojzechowski

Geschäftsführender Gesellschafter

- **Bachelor of Science**
  Westfälische Hochschule Bocholt
  Wirtschaftsinformatik

- **Master of Science**
  Westfälische Hochschule Gelsenkirchen
  Internet-Sicherheit

- **IT-Grundschutz Praktiker (TÜV)**
  Auf- und Ausbau von ISMS Systemen nach
  ISO 27001 auf Basis des IT-Grundschutzes

- **IT-Risk Manager (DGI)**
  IT-Risikoanalyse und Bewertung nach ISO 31000

  Veröffentlichungen:
  Kompass IT-Verschlüsselung
  Studie für das Bundesministerium für Wirtschaft und Energie (BMWi)
  Meine digitale Sicherheit - Tipps und Tricks für Dummies
  wiley Verlag, 06.10.2021

Unser Team – unsere Kompetenz

AWARE7
full service awareness agency

Kreativer & professioneller Dienstleister in der IT-Security Branche

- Penetrationstests & IT-Sicherheitsuntersuchungen
- Live Hacking Shows, Cyber Security Awareness Kampagnen & IT-Trainings
- IT-Sicherheitskonzeption - ISO 27001 (auf der Basis von IT-Grundschutz)

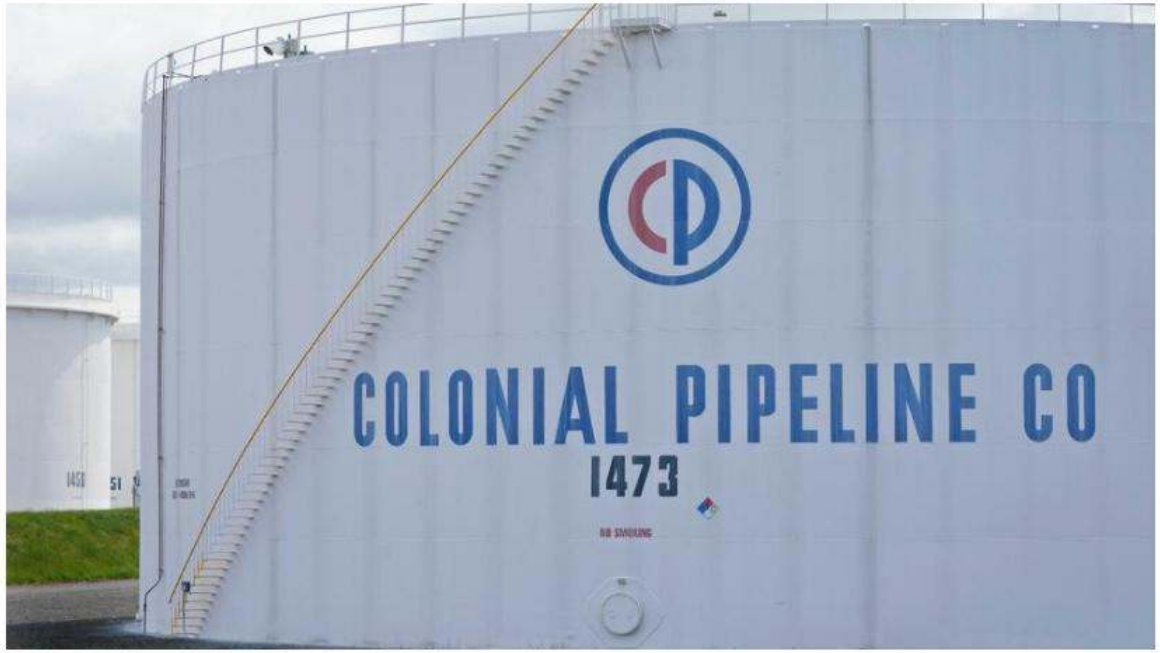
Beispiel 1: Colonial Pipeline

COLONIAL PIPELINE

Lösegeld nach Hackerangriff auf US-Pipeline sichergestellt

Colonial Pipeline hatte nach einem Hackerangriff 75 Bitcoin Lösegeld an Erpresser gezahlt. Das FBI hat nun einen Großteil davon sicherstellen können.

08.06.2021 - 00:22 Uhr • Kommentieren • 1 x geteilt



Die US-Regierung vermutet hinter der Tat Hacker der Gruppe DarkSide aus Russland. Sowohl US-Behörden als auch IT-Sicherheitsexperten raten Unternehmen dringend davon ab, Lösegeld zu zahlen, um Cyber-Kriminellen keine Anreize für Erpressungen zu bieten. Doch der Pipeline-Betreiber zahlte, wie Unternehmenschef Joseph Blount Ende Mai im „Wall Street Journal“ einräumte. Er habe eine Zahlung von 4,4 Millionen Dollar autorisiert. Die umstrittene Entscheidung erklärte Blount damit, dass sich das Unternehmen über das Ausmaß der verursachten Systemschäden unsicher gewesen sei.

Beispiel 1: Colonial Pipeline

USA

Tankstellen verklagen Colonial nach Ransomware-Angriff

Nach Ansicht hunderter Tankstellenbetreiber soll Pipeline-Eigentümer Colonial nach einem Ransomware-Angriff ihre Einnahmeausfälle erstatten.

in Pocket speichern merken

26. Juli 2021, 15:31 Uhr, Moritz Tremmel

(Bild: Succo/Pixabay)

Sicherheitsvorfälle und die Konsequenzen

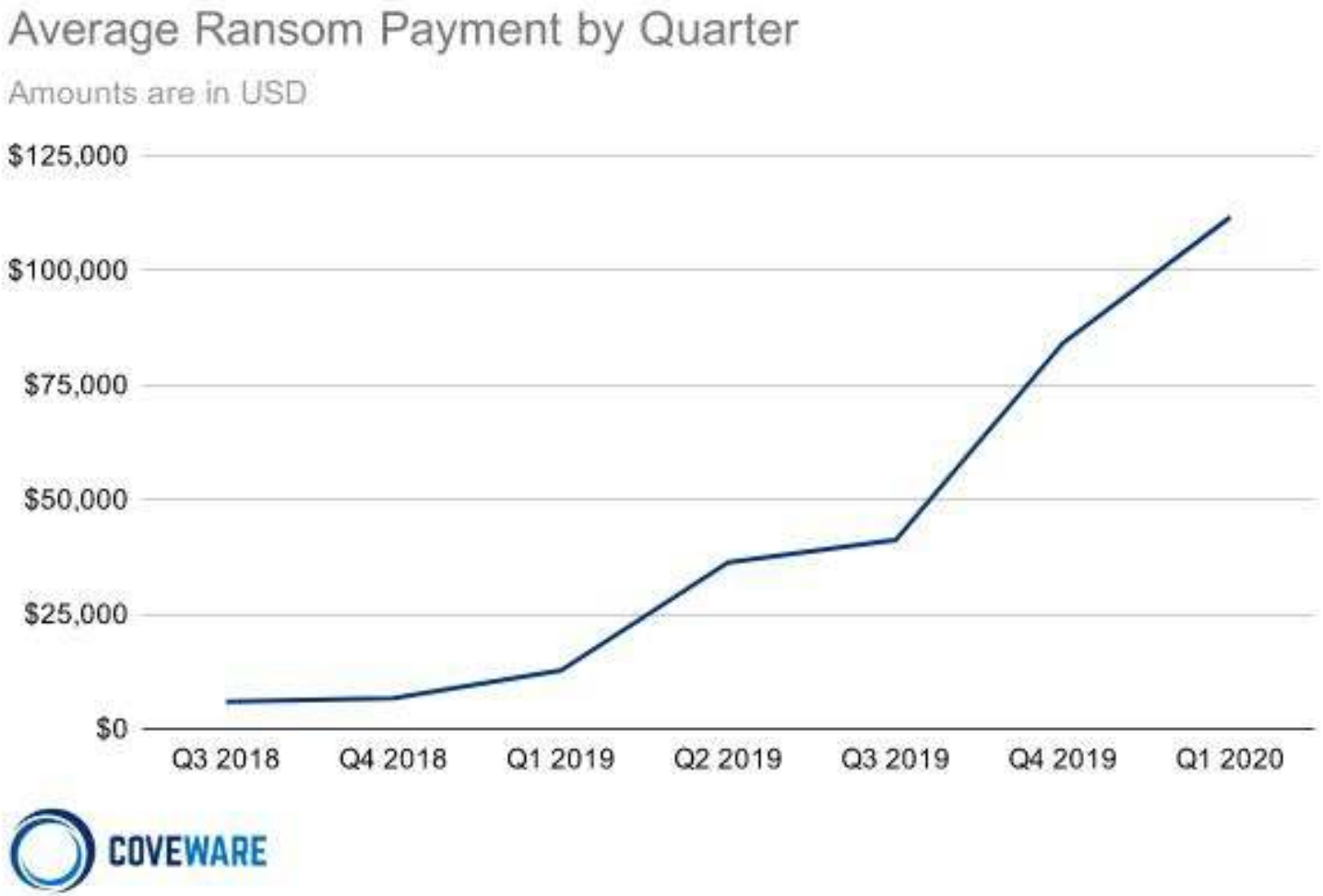
Ransomware wird teurer

Die Zeiten in denen Systeme für 5.000 USD entschlüsselt werden konnten sind vorbei.

In 99% der Zahlungen wurden Systeme erfolgreich entschlüsselt.

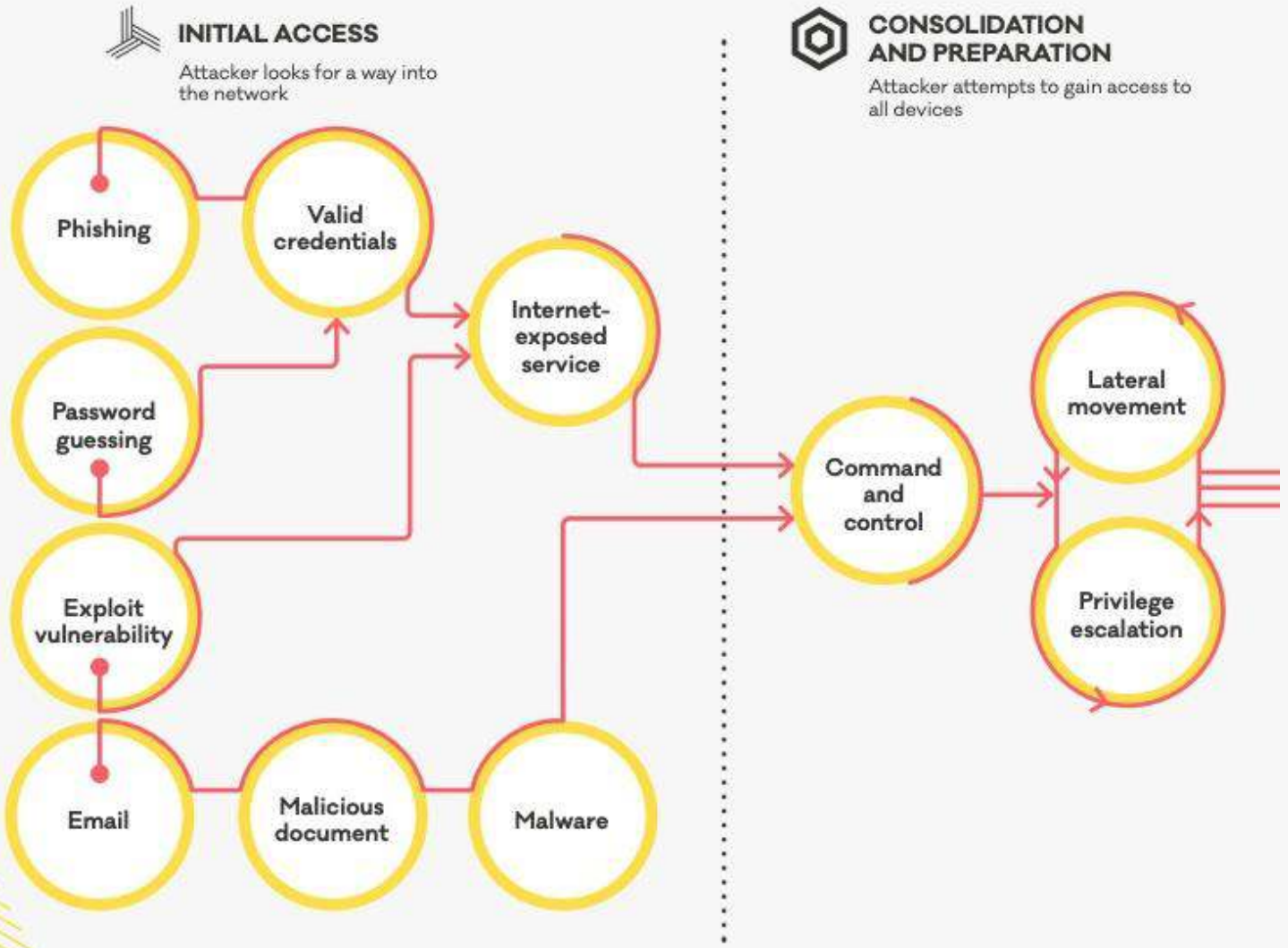
Ein Ransomware-Befall zieht durchschnittlich 15 Tage Ausfall mit sich.

99% der Lösegelder wurden über Bitcoin bezahlt.



LIFECYCLE OF A RANSOMWARE INCIDENT

The common attack paths of a human-operated ransomware incident based on examples CERT NZ has seen.



Berechenbare IT-Unsicherheit

Datenmissbrauch durch Cambridge Analytica

UPDATE 05.04.2018, 12:16 Uhr

Facebook-Skandal betrifft bis zu 310.000 Nutzer aus Deutschland

Hacker-Jackpot: Credit Bureau Equifax gehackt

08.09.2017 07:48 Uhr – Daniel AJ Sokolov

Passwörter im Klartext: 20.000 Euro Bußgeld nach DSGVO gegen Knuddels.de

380.000 Kreditkarten betroffen

Datenpanne bei British Airways

Stand: 07.09.2018 09:42 Uhr

Yahoo verliert bei weiterem Hack Daten von eine Milliarde Nutzerkonten

TOP 5 Passwörter in Deutschland

1. hallo
2. passwort
3. hallo123
4. schalke04
5. passwort1

TOP 5 Passwörter weltweit

1. 123456
2. 123456789
3. 1234
4. 12345
5. 12345678

Beispiel 2: Trinkwasser in Florida

tagesschau

Sendung verpasst?

Ausland ▸ Amerika ▸ US-Bundesstaat Florida: Hackerangriff auf Trinkwasseranlage

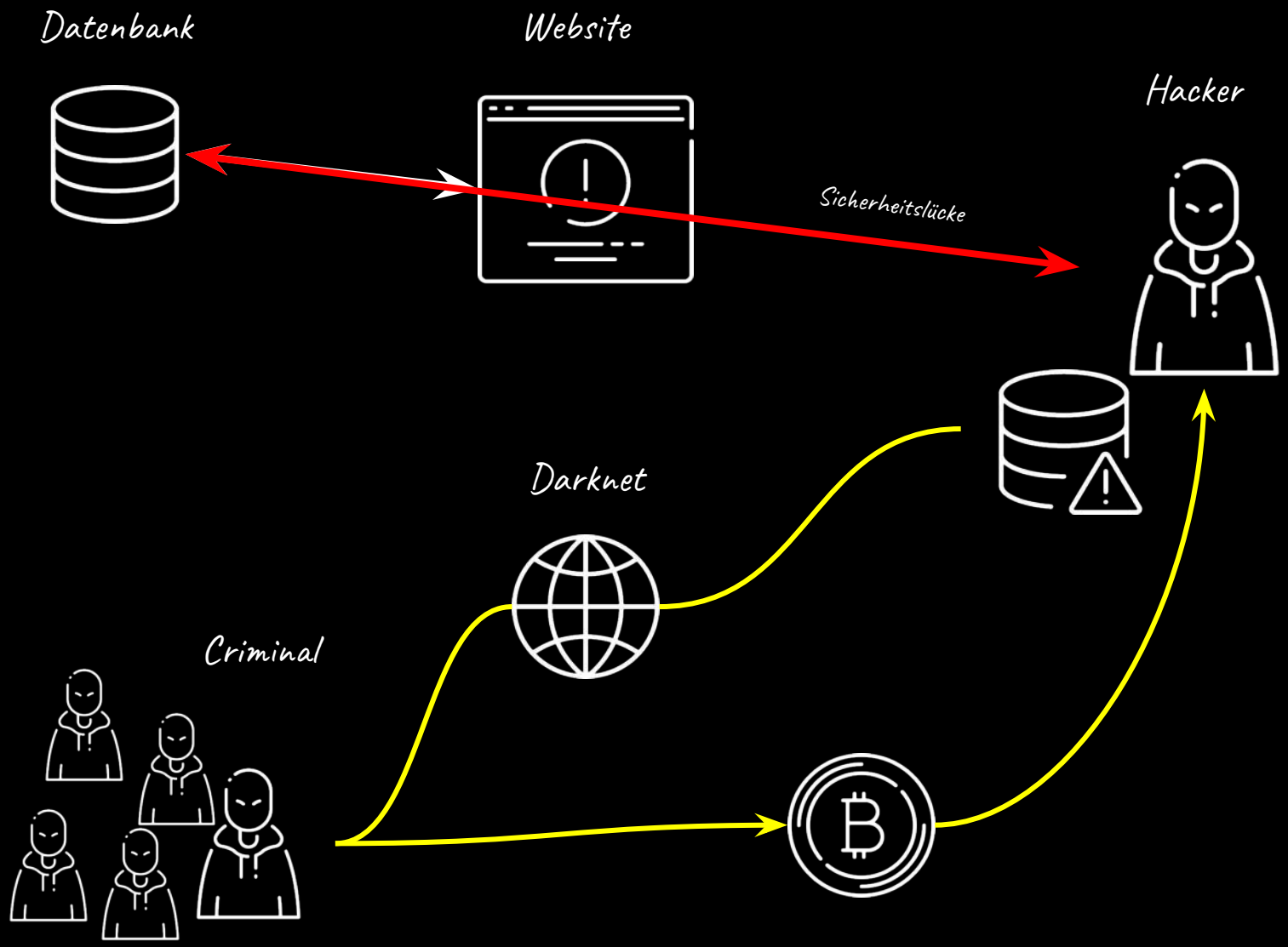
US-Bundesstaat Florida

Hackerangriff auf Trinkwasseranlage

Stand: 09.02.2021 08:25 Uhr

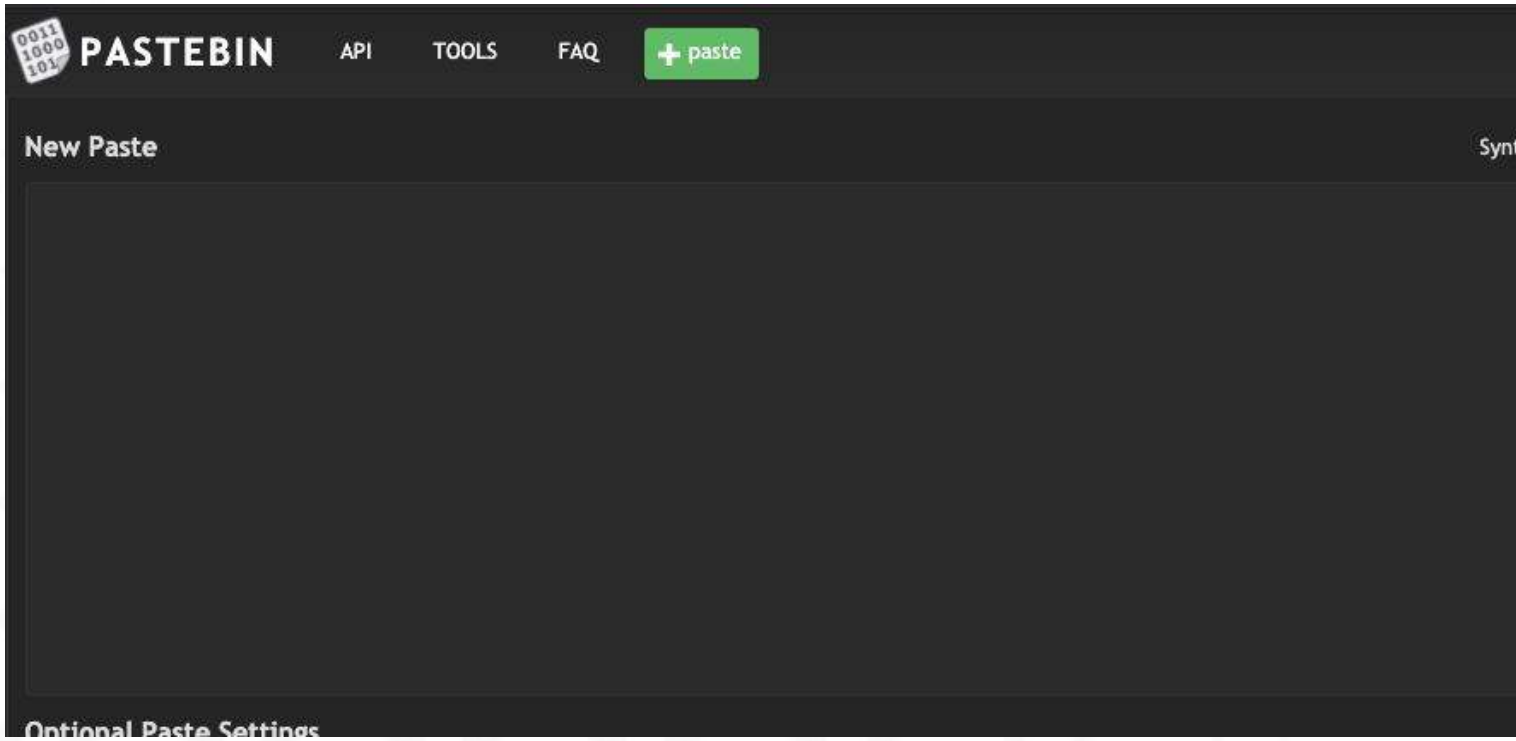
In Florida haben Hacker einen Angriff auf eine Aufbereitungsanlage für Trinkwasser verübt. Laut Behörden dabei wurde der Anteil von Natriumhydroxid im Wasser mehr als verhundertfacht - eine "potenziell gefährliche" Erhöhung.

Geschäftsmodell Darknet



Zielsuche

- Ohne Ziel kein Angriff!
- Suchmaschinen können gute Anlaufstellen für die Zielsuche sein
- Pastebin stellt anonyme Beiträge bereit



Die letzte Meile

LIVE DEMO
wie leicht lässt sich ein Telefonanruf manipulieren?

INFORMATIONEN ABFRAGEN?

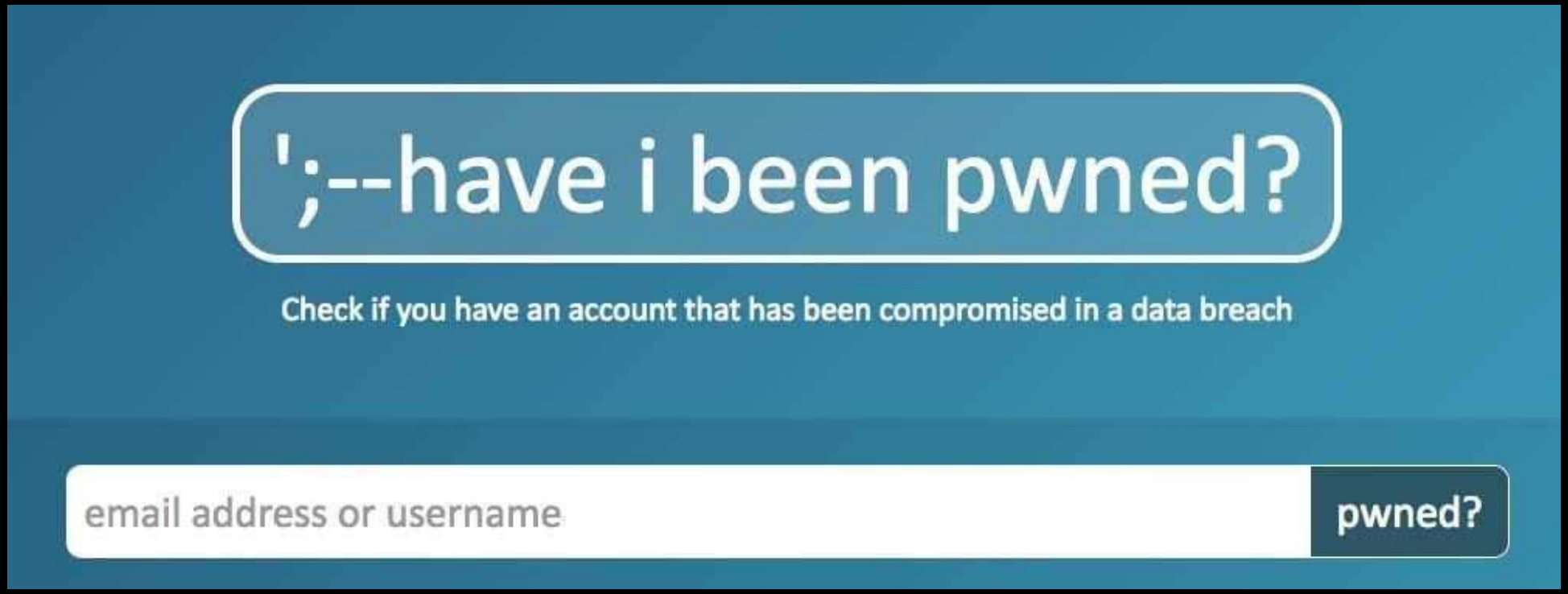
GEWONNEN?

NOTFALL?

ENKELTRICK/ POLIZEIMASCHE

ZURÜCKRUFEN!

Sind die eigenen Daten gestohlen worden?



Paretoprinzip

- Gilt auch in der IT-Sicherheit
- Hundertprozentige Sicherheit gibt es nicht
- Mit wenig Aufwand kann das eigene Schutzniveau stark erhöht werden

20% des Aufwands erzielen **80%** der Ergebnisse

Danke für Ihre Aufmerksamkeit!

Vorsicht bei E-Mail Anhängen und Links!

Software auf allen Geräten aktuell halten!

Backups anlegen!