VARONIS

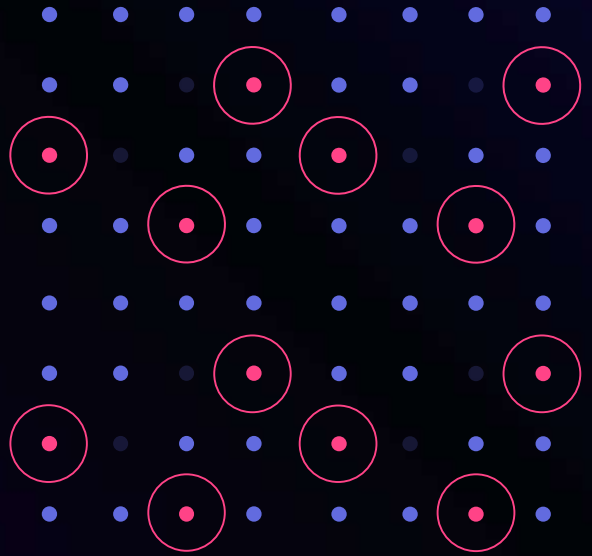
Achtung: CYBERANGRIFF!

Was Sie zum Schutz vor Ransomware jetzt wissen sollten!

ITSA 2022

Agenda

- Anstieg der Ransomware Attacken
- Alarmieren, untersuchen und in Echtzeit reagieren mit Varonis
- F&A



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

2022 Erneut starker Anstieg von Ransomware Attacken

Auch in 2022 registrieren Sicherheitsexperten einen starken Anstieg von Ransomware Attacken.

Abermals waren herstellende Unternehmen am stärksten im Fokus.
Den größten Anstieg sieht man derzeit im Gesundheitswesen mit über 600%!

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

Woran kann das liegen?

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

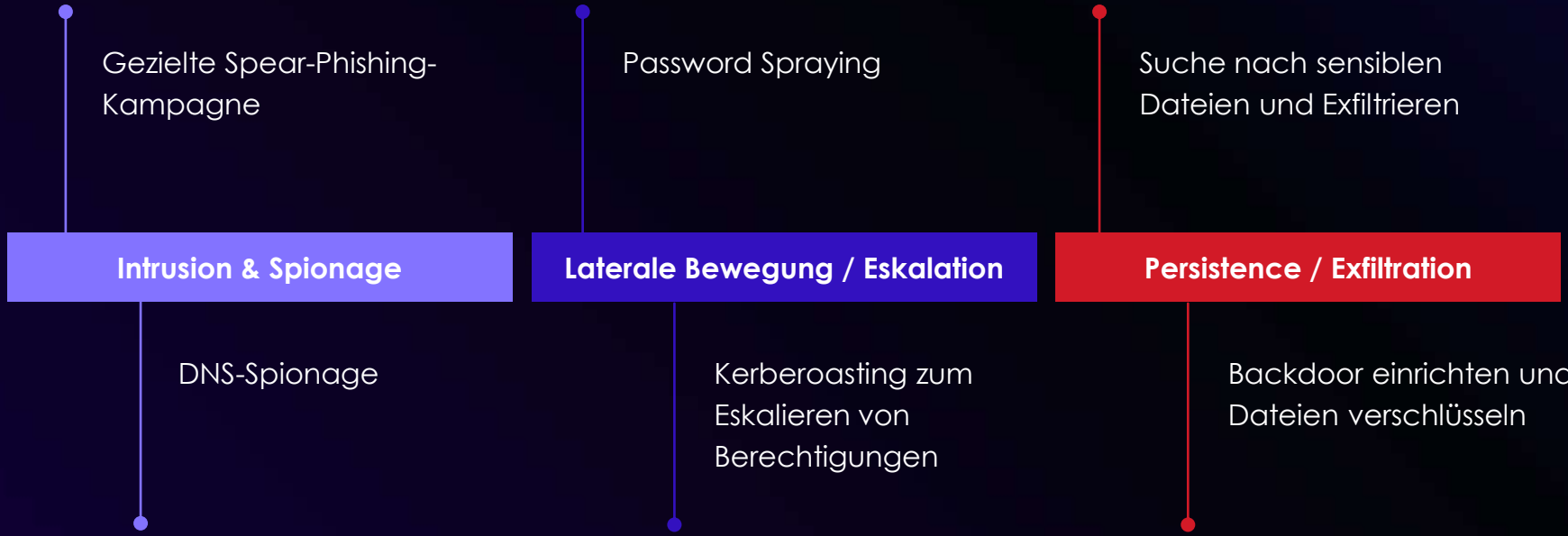
Von der digitalen Kleinkriminalität zu Angriffen in großem Maßstab

- **Damals:**
  - Script Kiddies
  - Angriffe im Gießkannenprinzip
  - Verschlüsselung ist das finale Ziel
  - Kann mit guten Backups wiederhergestellt werden
- **Heute:**
  - APT
  - Gezielt auf ein Opfer
  - Eigens entwickelte Malware
  - Exfiltrieren, verschlüsseln, **erpressen**
  - Gestohlene Daten können nicht aus Backups wiederhergestellt werden
  - Vorfall (und Daten) werden online veröffentlicht

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

Hier ist ein Beispiel für einen Angriffsablauf



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

ENDPOINTS
CLOUD DIRECTORY
GATEWAY
INTERNE SERVER
ACTIVE DIRECTORY
Es gibt viele VEKTOREN, um an Ihre Daten zu gelangen

Was kann ich tun?

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

1 0 0 1 0 1 0 1 0 1
0 1 0 1 1 0 1 0 1 0 0
1 0 1 0 0 1 0 1 0 1 1 1
0 1 0 1 1 0 1 0 1 0 0 1
HACKING DETECTED
RISK ALERT
85%

Prevention alleine reicht nicht....

- Reduktion des Risikos durch Umsetzung eines “Zero Trust” Berechtigungsmanagements
- Umfangreiche Preventive Maßnahmen zur Mitigation eines Angriffs
- Threat Hunting mit detectiven Maßnahmen
  - Auf Datenebene
  - Auf Kontoebene
  - Der unterstützenden Infrastruktur
  - Der Cloud und SaaS Anbieter

- Im Falle eines IOC`s Unterstützung durch ein Incident Response Team

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

Wie schützt Varonis Ihre Daten?

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

Varonis reduziert den möglichen Schaden

WENIGER ZUGRIFFE

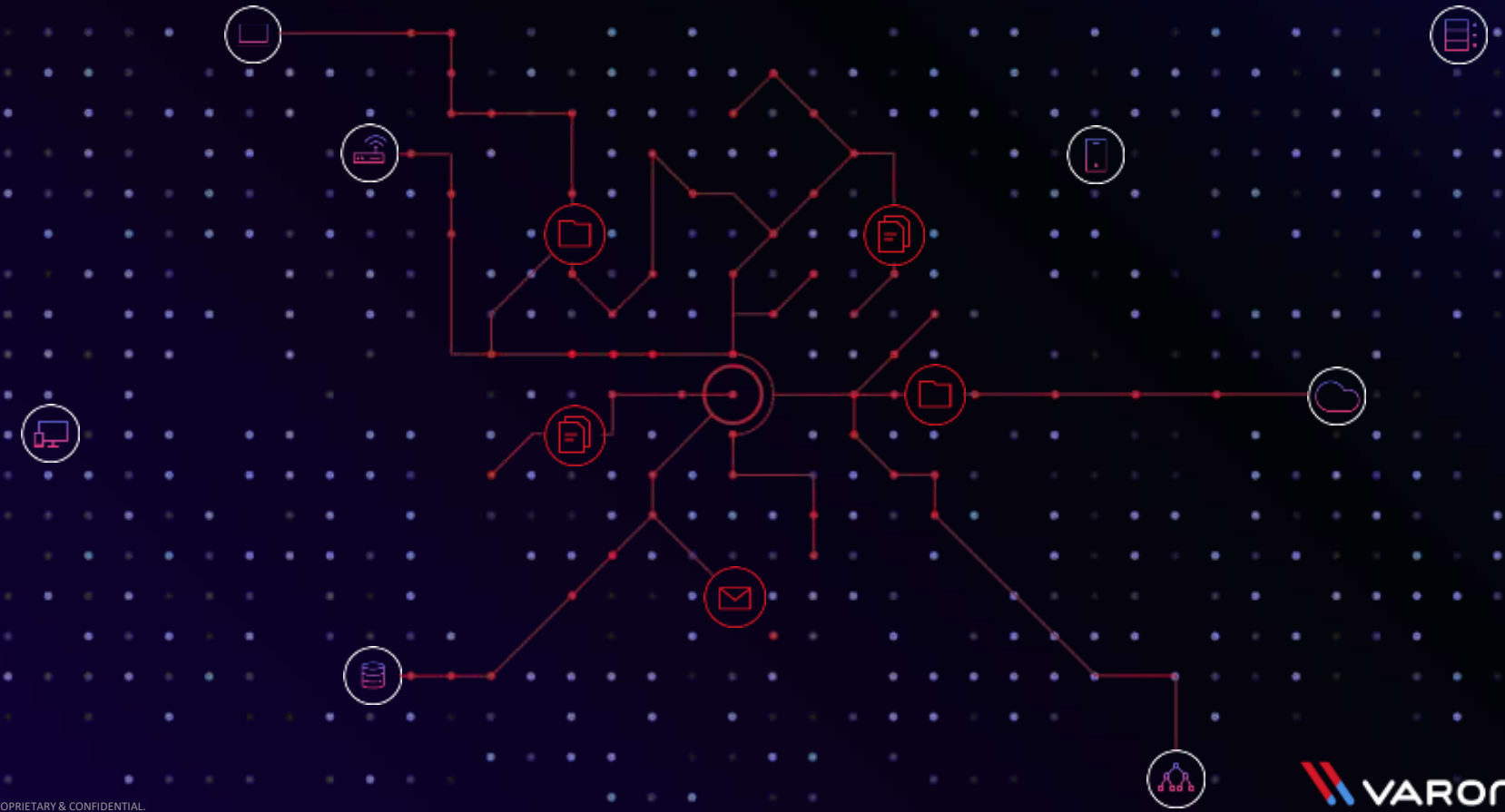
SCHÄDEN REDUZIEREN

VERLANGSAMTE ANGREIFER

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

Varonis überwacht die DATEN und Konten



VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

Wie Varonis funktioniert

Enterprise Data Stores,
Applikationen & Infrastruktur

Cloud

salesforce · aws · box · GitHub · okta · zoom · slack · Jira Software

On- Premise

VPN · DNS · PROXY

Analyse & Automatisierung

Use Cases

- **Datensicherheit**
- **Audit & Compliance**
- **Threat Detection & Response**

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.

VARONIS

Thank you

VARONIS SYSTEMS. PROPRIETARY & CONFIDENTIAL.