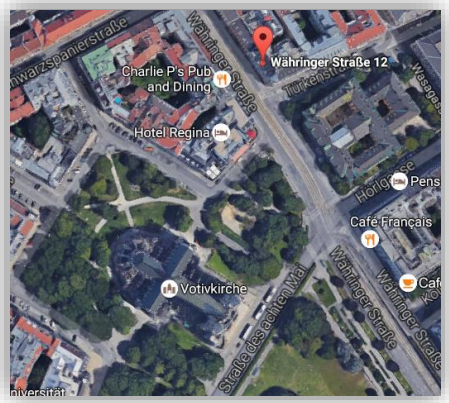
Ransomware ist allgegenwärtig

Restore als letzte Bastion

Andreas Pulker | Enablement | apu@quorum.at | +43 676 697 9561

Kurzvorstellung Quorum

- ✓ 2003 gegründet
- ✓ 100% Dienstleistung
- ✓ Fokussierung Datenverfügbarkeit
  - Backup | Restore
  - Archivierung
  - Storage
- ✓ Produktunabhängig vs. hoch spezialisiert
- ✓ breite Kundenbasis (indirekter Vertrieb)
- ✓ 15 Consultants mit jeweils mehr als 15 Jahren Erfahrung



Quorum Consulting GmbH
Währinger Straße 12/9
1090 Wien
www.quorum.at

Agenda

- ✓ Ransomware Kurzfassung
- ✓ Bedrohungen heute, morgen und übermorgen
- ✓ Backup steht im Rampenlicht
- ✓ Notwendige Maßnahmen
- ✓ Auf den Weg

Ransomware Kurzfassung

Verhinderung und Absicherung

- **Absicherung Eintrittspunkte** (Mail, interne Verteiler)
  - z.B.: Verteilung über RDP drive mapping
- **AD Berechtigungen:** Hack Domain Accounts = offenes Scheunentor
- **Kritische Applikationen** außerhalb eines zentralen Domainkonzepts

Maßnahmen zur Erkennung

- **Software** zur direkten Erkennung
- Analyse und Interpretation von **LOGs** (z.B.: splunk)

Aktionsplan bei verifizierter Infektion

- **Wiederherstellung** der Daten (Backup)

Bedrohung durch Ransomware …

… heute

- ✓ Überschaubarer Aufwand & maximale Wirkung
- ✓ Schaden & Aufmerksamkeit im Mittelpunkt
- ✓ „RW Anbieter“ verdienen noch wenig

Kernziele der Attacken

Masse

Client und dessen Daten

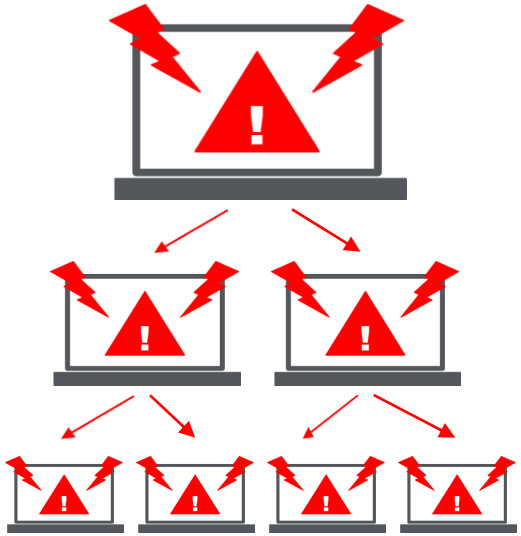
Windows Fileservices

VSS Services

Bedrohung durch Ransomware …

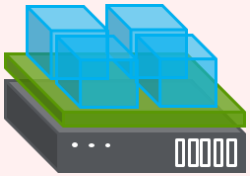
… morgen

- ✓ Optimierung des Profits der „RW Anbieter“
- ✓ Erhöhung Reichweite des Schadens



Kernziele der Attacken

Windows basierende Systeme



Virtuelle Systeme

Zentrale Filesysteme

Bedrohung durch Ransomware …

… übermorgen (ohne Gewähr)

- ✓ Gezielte Erpressung von Unternehmen
- ✓ Kombination von mehreren gleichzeitigen Attacken

Kernziele der Attacken

Zieldaten

Backup der Zieldaten

Backup steht im Rampenlicht …

… Restore als letzte Bastion

Anforderungen

- Richtiger Datenstand
- In der erforderlichen Zeit
- Regelmäßig im Vorfeld getestet

Backup steht im Rampenlicht …

… Backupumgebung unbewusst infiziert

Gefahrenquellen:

- ✓ Backup Server sind Teil einer Attacke
- ✓ Verteilung RW über Admin Account (RDP, direkt, …)
- ✓ Sicherungen liegen auf einem offenen Share
- ✓ VSS als Teil des Sicherungskonzepts

Backup steht im Rampenlicht …

… Backup Umgebung bewusst attackiert

Maßnahmen:

- ✓ Absicherung Backup-Server (Abschottung, Härtung, …)
- ✓ Absicherung Storage (Beispiel: SAN statt NAS)
- ✓ Kopien auf verschiedenen Medien (SAN, Appliances, Tape)
- ✓ Desaster Recovery Prozedur für Backup Service

Auf den Weg

- ✓ Ransomware kostet Unternehmen Geld → es gibt Budget für Backup
- ✓ Augenmerk auf Architektur und Absicherung der Backupumgebung
- ✓ Daten als Herz eines Unternehmens, achten Wir drauf

Quorum Consulting GmbH
Währingerstrasse 12/9
1090 Wien
www.quorum.at