
# Cybersecurity
# aus der Sicht eines Hackers

Prepared by:
**Bernd Koberwein**
**Head of Security Services**
**BearingPoint**

**14.12.2021**

BearingPoint®

# Agenda

1. Bedrohungslage
2. Motivation und Strategien
3. Werkzeuge
4. Vorgehen
5. Live-Demo: PenTest einer WordPress Umgebung
6. Empfehlungen

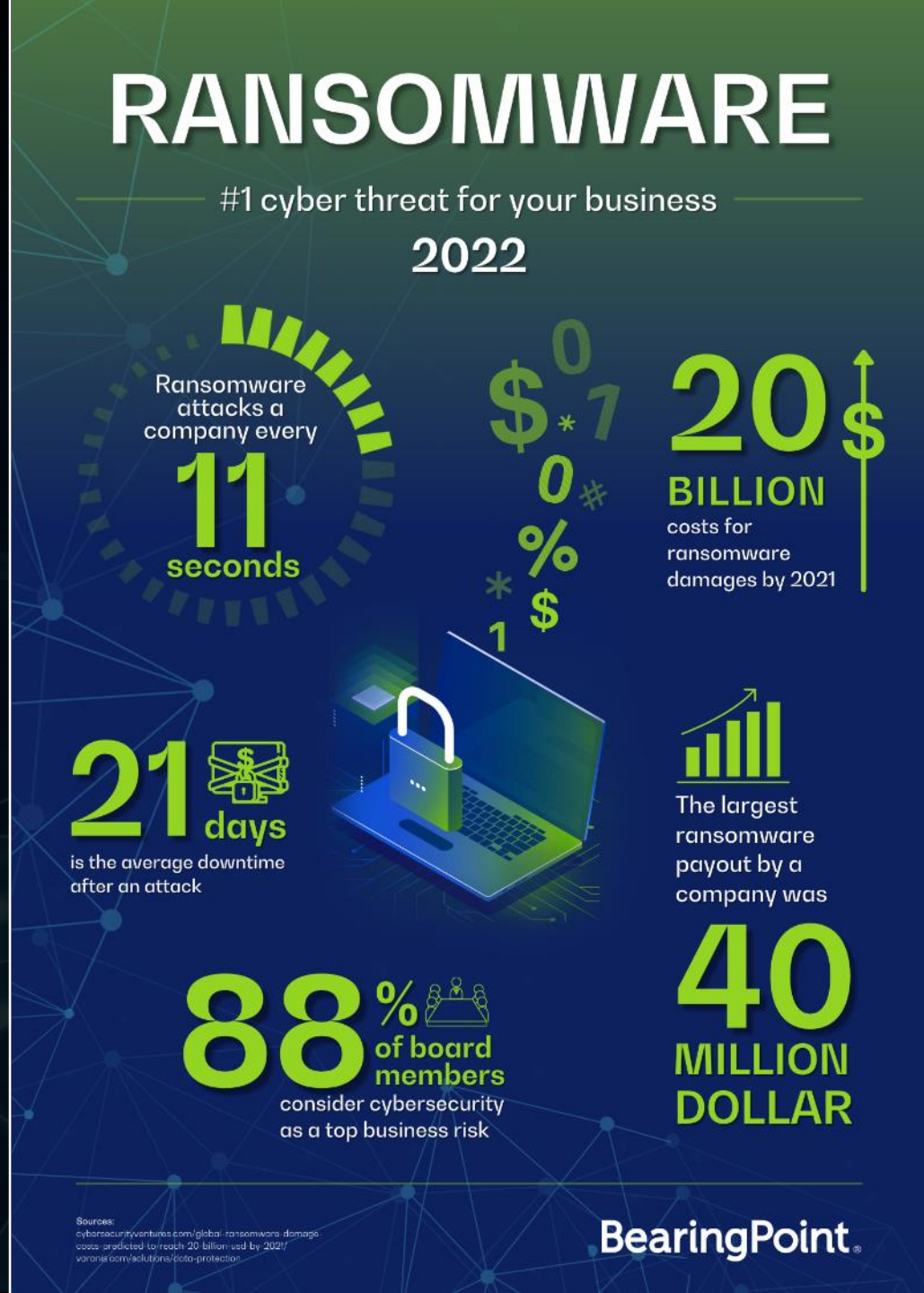
Deutsche Messe Technology Academy

BearingPoint®

# Bedrohungslage

**Das Risiko Opfer eines Cyberangriffs zu werden steigt seit Jahren kontinuierlich**

- Cyber Incidents befinden sich auf Platz 3 der global Geschäftsrisiken – und in Europa oft auf **Platz 1 oder 2**
- Im Schnitt wurden in 2021 ca. 400.000 neue Schadprogrammvarianten **pro Tag** veröffentlicht (+22% zu 2020)
- 36% aller erfolgreichen Einbrüche (breaches) nutzten Phishing
- Ransomware ist leider ein Erfolgsmodell
- Das Budget für Cybersecuritymaßnahmen wächst in den meisten Organisationen linear, oder bleibt statisch, während Angriffe exponentiell zunehmen



# Motivation und Strategien

**It's all about the money, mostly**

| | | | | |
|---|---|---|---|---|
| **Akteure** | Organisierte Kriminalität | Staatliche Akteure | Hacktivists | Script Kiddies |
| **Motivation** | Datendiebstahl<br>Erpressung<br>Lösegeld | Spionage<br>Sabotage<br>Diebstahl | Imageschaden<br>Leaks<br>wirtsch. Schaden | Just 4 fun |
| **Strategien** | Drive-by malware<br>Gezielte Angriffe | Supply-Chain Angriffe<br>APT<br>Advanced Persistent Threats | Gezielte Angriffe<br>Denial of Service | Hacking toolsets |

**Ziele**

| | | | | | | |
|---|---|---|---|---|---|---|
| Webseiten & APIs | Webshop | Server | VPN | Mobile Apps | Mitarbeiter-accounts | WLAN |
| Cloud-Infrastruktur | Remote Access | SW-Dev Umgebung | Business-applikationen | SCADA | IoT Devices | ... |

# Werkzeuge

**Angreifern steht eine gut gefüllte Werkzeugkiste zur Verfügung**

## Zielauswahl/Information Gathering

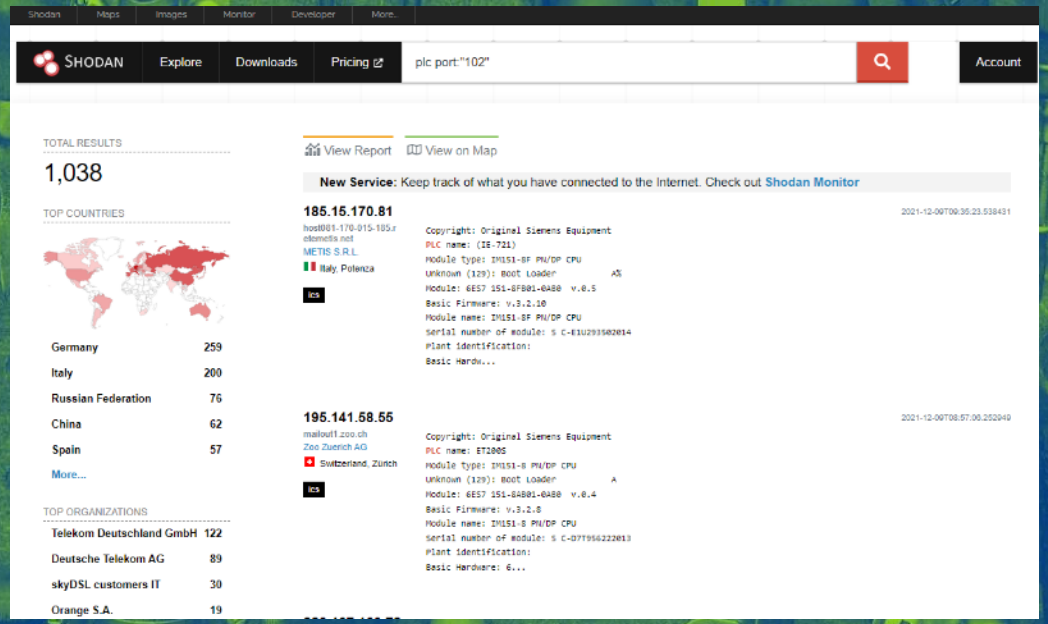
- Google (z.B. Google Hacking Database)
- Social Networks (LinkedIn, etc.)
- Spezielle Suchmaschinen (Shodan und Censys)

## Zugriff erhalten

- Darkweb
  - Advanced Phishing Kits
  - Zugänge – aktiver Backdoorzugriff (z.B. ADFS)
  - Credentials – Abgegriffen zum Zeitpunkt x
- Vulnerability databases

## Angriff

- Kali Linux/Exploit-DB/Metasploit Framework
- Mimikatz – Windows post exploitation tool
- Zero-Day Exploits - $$$
- Ransomware (as a Service)

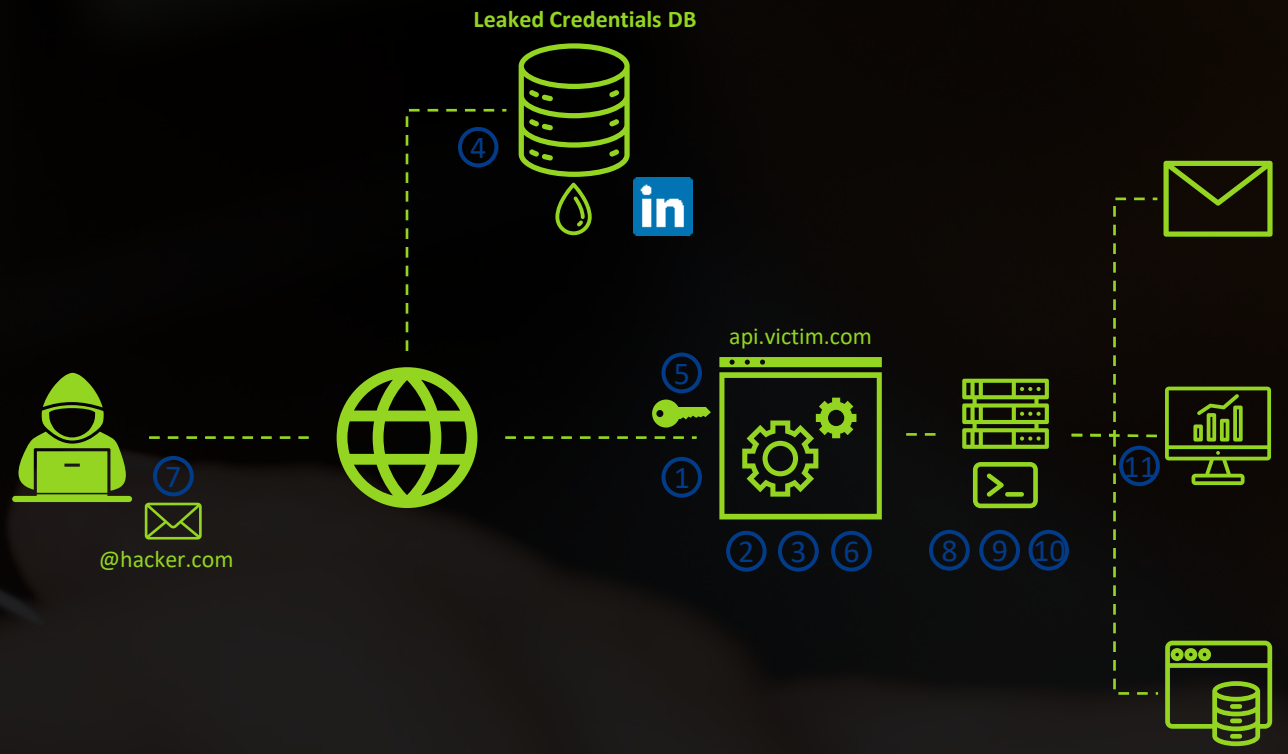

Deutsche Messe Technology Academy

BearingPoint®

# Vorgehen

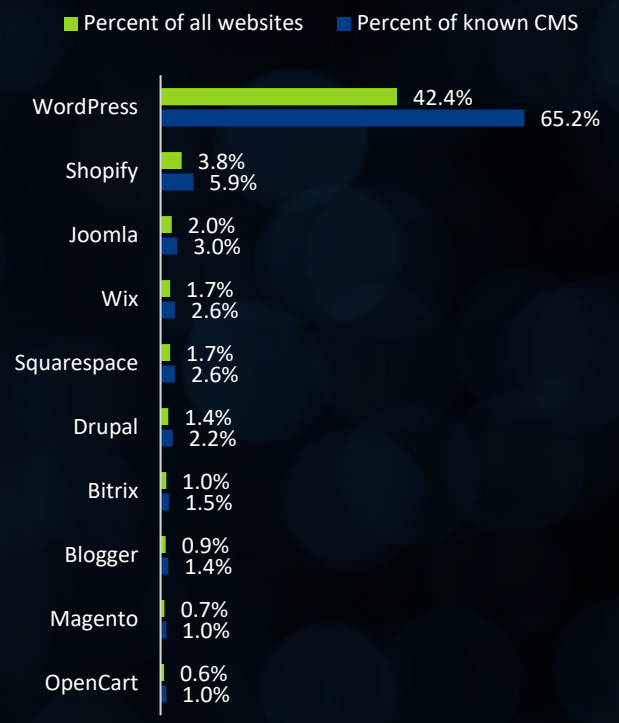
**Anatomie eines echten Angriffs**

1. Unautenticated API Zugriff möglich (!)
2. API Request liefert Usernames, Email Addressen und User IDs (!)
3. Drei @victim.com Email Adressen identifiziert
4. Leaked Passwords für @victim.com Adressen – shared passwords (!)
5. Anmeldung mit @victim.com User und leaked Passwort möglich
6. API call mit valider User ID erlaubt Email-Adressen zu ändern, für beliebige User (!) – Update auf @hacker.com
7. Passwort Reset für @victim.com Account – Email geht an @hacker.com; Admin Zugriff auf Webapplikation erlangt
8. Erstellung einer PHP-Reverse Shell um Shell Zugriff auf Server zu erlangen
9. Lokale Privilege Escalation am Linux Server (via LinPeas Script) – I AM ROOT
10. Einrichtung einer Portweiterleitung, um weitere Port-Scans durchführen zu können
11. Lateral Movement und Versuch, weitere Systeme unter Kontrolle zu bringen



# PenTest einer Wordpressumgebung

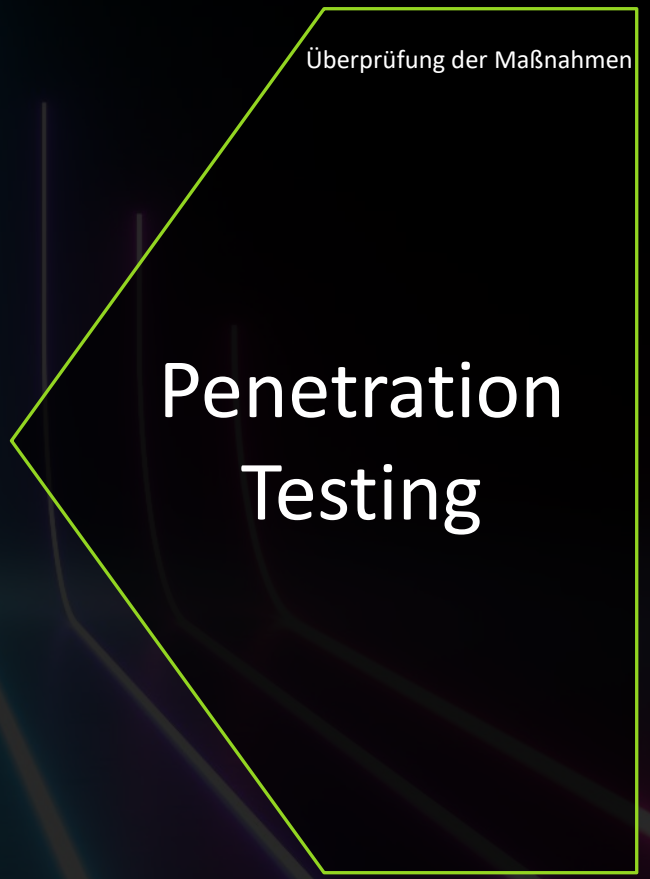
Wordpress wird auf 42% aller Webseiten im Internet verwendet

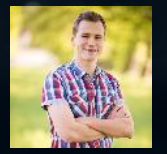

https://w3techs.com/technologies/overview/content_management

# Empfehlungen

- Aktives Asset- und Vulnerability Management
- Mitarbeiterawareness und Schulungen
  z.B. Phishing
- Threat Intelligence
- Fortgeschrittene Schutztechnologien
  (Email, Endpoint, Browser, Cloud…)
- Notfallpläne (Restore)



Bernd Koberwein
Head of Security Services
bernd.koberwein@bearingpoint.com
+43 664 81 61 874



Georg Lerchbaum
Security Engineer
georg.lerchbaum@bearingpoint.com
+43 316 8003 1180

BearingPoint®

bearingpoint.com/store/
besecure@bearingpoint.com

Deutsche Messe
Technology Academy

**Quellen/Links:**
Allianz Risk Barometer 2021
AV-Test New Malware
Verizon Data Breach Investigation Report
Cybercrime Magazine Ransomware Statistics
Google Safe Browsing
Google Hacking Database
Shodan