Daten im Darknet und die kriminellen Folgen

- Fabian Diener-Fürmetz/ IT Security Analyst
- NSIDE ATTACK LOGIC GmbH
- E: fdiener@nsideattacklogic.de
T: +49 89 89 082 110

Über mich

Penetrationstester bei NSIDE ATTACK LOGIC

Expertise:

- Web App Security
- Social Engineering
- OSINT
- Netzwerksicherheit
- AI Security

Über NSIDE

- 2014 in München gegründet
- 100 % im privaten Besitz
- knapp 25 Mitarbeiter
- Komplett deutschsprachiges Team
- Firmensitz: München

Referenzen

- Tätig für 14 DAX Unternehmen
- Vodafone: Gewinner „2016 Pentest Benchmark”; Mitglied der Hall of Fame für herausragende Leistungen
- Bücher (z.B. Cybersecurity Best Practices) und Artikel in zahlreichen Zeitungen und Zeitschriften (z.B. iX, FAZ, SZ, Manager Magazin, Handelsblatt)
- Live Hackings auf Messen/Konferenzen (it-sa, Bullet Proof, DuD, IKT Sicherheitskonferenz etc.)

Unsere Expertise / Leistungsspektrum

Security Consulting

- Red und Purple Teaming
- Tactical Information Gathering & Strategic Cyber Security
- Penetration Tests & Web Application Hacking
- Managed Pentest Service (extern)
- CISO Tech Team
- (I)IoT, SCADA & Hardware Hacking
- Social Engineering
- Technische Konzeptberatung
- Cloud und DevOps Security
- Source Code Audits

Security Tools (intern)

- **NSIDE PHISHING FRAMEWORK** - Professional Toolkit für Phishing-Simulationen
- **NVOKE** - Taktisches Command & Control (C2) Framework

Security Training

- Hands-on Trainings
- Security Workshops
- Awareness Trainings
- Live Hacking / Vorträge

Disclaimer

Ich bin kein Jurist, sollten während des Vortrags rechtliche Fragen auftauchen beantworten wir diese aber gerne im Rahmen unserer Möglichkeiten.

Dafür leite ich Ihre Anfrage gerne intern an unsere Geschäftsführung bzw. entsprechende Ansprechpartner weiter.

Bitte wenden Sie sich dazu per E-Mail an:

fdiener@nsideattacklogic.de

Was ist das Darknet?

Clear Web

Öffentlich, indexiert (über Suchmaschiene, etc.)

Deep Web

Nicht öffentlich, nicht indexiert (z. B. Intranet)

Darknet

Anonymer Teil des Deep Web – Zugang über z. B. Tor

Was ist das Darknet?

Nutzung des Darknets:

- Legitime Zwecke: Whistleblowing, Pressefreiheit, Zensurumgehung
- Kriminelle Nutzung: Anonymisierter Handel mit Drogen, Waffen oder Daten

Datenhandel im Detail: Was wird verkauft?

- Kreditkarten- & Bankdaten
- Persönliche Identitätsdaten
- Kompromittierte Firmendaten
- Zugangsdaten

Herkunft der Daten

- Datenlecks durch Sicherheitslücken & Hacks
- Interne Leaks / Insider
- Phishing & Social Engineering
- Malware & Infostealer

Zugangsdaten im Darknet - was genau ist gemeint?

- Klassische Kombinationen: Nutzername + Passwort
  - Zugang zu Mails, Tools, Accounts
- API-Tokens & Zugriffsschlüssel
  - Zugriff auf Schnittstellen & Cloud-Ressourcen
- VPN-, RDP-, Citrix-Zugangsdaten
  - Direkter Zugang zu internen Infrastrukturen!
- 2FA-Bypass durch gestohlene Session-Cookies / Tokens
  - Umgehung von Zwei-Faktor-Authentifizierung!

Session Hijacking - die alternative Tür ins System

- Was ist Session Hijacking?
  - Die Übernahme aktiver Logins durch gestohlene Session-Tokens

- Warum ist das so gefährlich?
  - Kein Passwort nötig
  - MFA wird umgangen
  - Tokens sind oft lange gültig
  - Nutzer merkt meist nichts

Risiken & Folgen für Unternehmen

- Geschäftliche Folgen
  - Vertrauensverlust bei Kunden & Partnern
  - Imageschäden durch Berichterstattung
  - Finanzielle Auswirkungen

- Sicherheitsbedrohungen
  - Missbrauch der Daten
  - Nachfolgeangriffe: Ransomware, Erpressung, usw.

Fallbeispiel – Der Cyberangriff auf Change Healthcare

- Initial Access (Feb 2024)
  - Angriff durch BlackCat / ALPHV Ransomware-Gruppe
  - Zugang via öffentlich bekanntem Citrix-Login eines Support-Mitarbeiters

- Folgen
  - Exfiltration sensibler Daten:
    - Krankenversicherungsinfos
    - Behandlungs- & Abrechnungsdaten
    - Sozialversicherungsnummern, Finanzdaten
  - Systemverschlüsselung -> Betrieb über Monate gestört

Fallbeispiel – Der Cyberangriff auf Change Healthcare

- Kosten & Schaden
  - Lösegeldzahlung: 22 Mio. USD
  - Gesamtschaden: ca. 2,5 Mrd. USD
  - Kein Rückerhalt der Daten trotz Zahlung

Wie erkennt man, dass man Betroffen ist?

- Monitoring durch Threat Intelligence Provider
- Abgleich mit Leaks (z. B. HIBP, internes Monitoring)

Welcher Sicherheitsvorkehrungen sind notwendig?

- Sicherheitsbewusstsein stärken
  - Jeder Mitarbeitende ist potenzielles Ziel
  - Phishing, Session Hijacking & BYOD gezielt ansprechen
- Angriffsvektoren minimieren
  - Systemhärtung & Schwachstellenprüfung
  - Least Privilege: Nur nötige Rechte
  - BYOD klar regeln, gemeinsame Geräte absichern
- Schutz kompromittierter Daten
  - Monitoring auf geleakte Credentials
  - Automatische Sperrlisten & erzwungene Passwortänderung bei Verdacht

Welcher Sicherheitsvorkehrungen sind notwendig?

- Awareness & Reaktion
  - Schulungen & simulierte Angriffe
  - Klare Meldewege intern definieren
- Bewährte Frameworks nutzen
  - TIBER: Red-Teaming zur Schwachstellenaufdeckung
  - DORA: Digitale Resilienz durch organisatorische Prozesse
- Cybersicherheit als Daueraufgabe
  - Regelmäßige Evaluation & Anpassung
  - Sicherheit als Teil der Unternehmenskultur begreifen

Offensive IT-Security ist unsere Spezialität:

Penetrationstest, Red-Team-Assessments, Phishing-Simulationen oder taktische Informationsbeschaffung & OSINT.

www.nsideattacklogic.de

info@nsideattacklogic.de

Landshuter Allee 8, 80637 München

+49 89 89 082 110