OFFENSIVE SECURITY (PENETRATION TESTING)

Projektverlauf Penetration Testing

1 AUFKLÄREN & SCANNEN

- Internet- und Serveradressen und Komponenten
- Prüfung der IP-Adressen auf Aktivitäten
- Domänen der Internetpräsenz
- Analyse der Betriebssysteme, Protokolle und Ports
- Schwachstellen identifizieren

Maßnahmenkatalog & Umsetzungsplan

2 EINDRINGEN & BEREINIGEN

- Zielsystem angreifen
- Zugang zum System verschaffen
- Zugriffsrechte im System erweitern
- Nach Abschluss der Tests: Wiederherstellung des ursprünglichen Zustandes
- Erstellte Accounts löschen
- Konfigurationen zurücksetzen

Abnahmebericht

3 BERICHTSERSTELLUNG & MASSNAHMENKATALOG

- Vorgehen und Testfälle
- Identifizierte Sicherheitslücken
- Risikobewertung je Schwachstelle
- Bewertung mit CVSS
- Maßnahmen der System-härtung

Nachweisführung (Security Case)

4 UMSETZUNG SYSTEMHÄRTUNG

- Unterstützung beim Schließen der Sicherheits-lücken
- Bei Bedarf: Definition alternativer Maßnahmen (z. B. bei Bestandstechnik)

Betriebsführungskonzept

Penetration Testing & Vulnerability Analysen für IACS und Operational Technology

IEC 62443-4-1: IT-Sicherheit als Teil des Produktlebenszyklus
Penetrationstests für Verifikations- und Validierungsprüfungen der IT-Sicherheit

- Certified Ethical Hacker
- Dokumentiertes Vorgehensmodell
- OT SecLAB
- Suite mit über 600 Tools im Einsatz

OT SecLAB am Standort Berlin

Hardware Security Tests

Operational Technology (OT) Attacks

- Erprobung von Angriffen auf OT - Komponenten
- Angriffe auf häufig verwendete Technologien
- Security Überprüfung von industriell genutzten Systemen

Skillset immer up to date

Hacking - Challenges

- HackTheBox.eu
- root-me.org
- HackOn.com
- TryHackMe.com

LiveHack Workshops

Zertifizierungen

- CEH
- CISSP
- COSP
- u.a.

Referenzen

- DB Netze: iLBS Security Testing, seit Q1/21
- Informatik Consulting Systems GmbH: Systemexterner Penetration Test, Q2/21
- Deutscher Hersteller: ETCS-OBS Penetration Test, seit Q2/21

PATRIC BIRR
M. Sc., CISSP
Head of Business Center Security
Mobile: +49 172 728 05 80
E-Mail: Patric.Birr@ics-gmbh.de