IT-Sicherheit

Angreifer-Typen und Typische Angriffe

Prof. Dr. Dominik Merli, Prof. Dr. Lothar Braun

Sommersemester 2020

Hochschule Augsburg - Fakultät für Informatik

Interpretation von Angriffen

https://www.xkcd.com/932/

Eigenschaften von Angriffen

- Ziel
  - Wer oder was wurde angegriffen?
  - Gab es Kollateralschäden?
- Angreifer
  - Wer ist für den Angriff verantwortlich?
  - Kann er überhaupt jemandem zugeschrieben werden?
- Motivation
  - Warum wurde der Angriff durchgeführt?
  - In welchem größeren Zusammenhang steht er?
- Datum und Zeit
  - Was wissen wir über den zeitlichen Verlauf des Angriffs?
- Umsetzung
  - Wie wurde der Angriff auf technischer Ebene durchgeführt?
  - Gab es Social Engineering Komponenten?

Cyber Kill Chain

Reconnaissance	1	
	2	Weaponization
Delivery	3	
	4	Exploitation
Installation	5	
	6	Command & Control
Actions on Objectives	7	

(siehe Cyber Kill Chain von Lockheed Martin)

Angreifer-Typen

Ohne Angreifer keine Angriffe!

Mögliche Kriterien für Klassifikation von Angreifern

- Motivation bzw. Beweggründe
- Fähigkeiten
- Einsatz von Zeit
- Einsatz von Ressourcen

Typische Angreifer

- Hacker
- Cracker
- Penetration Tester und Security Researcher
- Skript Kiddies
- Kriminelle Gruppen
- Böswillige Insider
- Automatisierte Malware
- Nation State Attacker / Advanced Persistent Threat Gruppen

Angriffs-Typen

Es gibt sehr viele verschiedene Angriffsarten!

Und kontinuierlich tauchen neue Angriffe auf!

Ausnutzen von Schwachstellen/Vulnerabilities

- Ziel(e)
  - Manipulation von IT-Systemen
  - Abgreifen oder Manipulation von Daten auf dem System
  - Übernahme der vollständigen Kontrolle über ein System

- Umsetzung(en)
  - Identifikation von Schwachstellen in Software oder Geräten
  - Ausnutzen der Schwachstelle mittels *Exploits*

(Distributed) Denial-of-Service (DoS / DDos)

- Ziel(e)
  - System/Dienst ist nicht mehr erreichbar
  - Störung von (Sicherheits-)Prozessen
  - Bloßstellen von (Sicherheits-)Institutionen

- Umsetzung(en)
  - Botnet
  - Reflection-Angriffe mit gefälschter IP Quelladresse
  - Lokaler Zugriff, der Manipulation erlaubt

Malware: Virus / Trojan Horse / Ransomware / Adware / ...

- Ziel(e)
  - Ausführen von Code auf fremden Geräten
  - Evtl. Weiterverbreitung auf andere Geräte
  - Ausspionieren von Nutzern und deren Daten
  - Verändern von Dateien und dem Geräte-Verhalten
  - Verschlüsseln von Dateien und Lösegeldforderung
  - Zeigen von unerwünschter Werbung

- Umsetzung(en)
  - Nutzer erhält (obfuszierte) ausführbare Datei per E-Mail, Webseite, App Store, USB-Stick, etc.
  - Nutzer muss dazu gebracht werden, die Datei auszuführen

Phishing

- Ziel(e)
  - Abgreifen von Nutzerdaten, Passwörter, Bank TANs, etc.
- Umsetzung(en)
  - Bereitstellung einer gefälschten Webseite, Benutzer-Oberfläche, App, etc.
  - Nutzer muss dazu gebracht werden, Daten einzugeben
  - Sehr spezifisches/gezieltes Phishing: Spear Phishing

Social Engineering

- Ziel(e)
  - Menschen überzeugen Dinge zu tun oder zu sagen, die dem Angreifer helfen
  - Zugriffsrechte geben, Zugriffe für Angreifer durchführen, Prozesse in Gang setzen, etc.
  - Aushändigen von (vertraulichen) Informationen
- Umsetzung(en)
  - Psychologische Tricks, z.B. am Telefon, per E-Mail, bei persönlichen Treffen, etc.

Passwort Brute Forcing

- Ziel(e)
  - Finden des korrekten Passworts durch (geschicktes/automatisiertes) Ausprobieren
  - Zugriff auf Daten/Konten mit legitimen Passwörtern
  - Identitätsdiebstahl

- Umsetzung(en)
  - Über ein Netzwerk, z.B. Brute Forcing von SSH Logins
  - Mit Passwort-Hashes und Cracking Tools, z.B. hashcat

Man-in-the-Middle (MitM)

- Ziel(e)
  - Belauschen von Kommunikation
  - Evtl. Manipulation des Kommunikationsinhalts
  - Wertvolle Daten aus der Kommunikation extrahieren
  - Verfälschte Informationen in Kommunikation einbringen

- Umsetzung(en)
  - Sich als Gerät/Dienst/Nutzer ausgeben, Kommunikation umleiten, anschließend zum rechtmäßigen Empfänger weiterleiten
  - Spezielle physikalische Position im Netzwerk ausnutzen um Datenverkehr zu analysieren bzw. zu manipulieren

QUIZ: Angriffe (twbk.de)

Ein Unternehmen stellt fest, dass sich vor 6 Monaten Unbekannte Zugriff zur Produktionsdatenbank verschafft haben. Es ist bekannt, dass der Datenbank-Administrator zuvor mit einer gefälschten E-Mail auf eine Website gelockt wurde, die der Firmenseite täuschend ähnlich sah. Um welche Art Angriff handelt es sich vermutlich?

A) Phishing

B) Social Engineering

C) Man-in-the-Middle

QUIZ: Angriffe (twbk.de)

Ein Angreifer tarnt sich als Service-Techniker und gelangt so in den Serverraum eines mittelständischen Unternehmens. Er findet einen großen Switch und kann nach mehrmaligem Ausprobieren verschiedener Ports Teile des Netzwerkverkehrs mitlesen. Um welchen Angriff handelt es sich?

A) Brute-Force Angriff

B) Denial-of-Service

C) Man-in-the-Middle

Key Logger

- Ziel(e)
  - Gedrückte Tasten auf einem Gerät aufzeichnen
  - Passwörter und persönliche Daten abgreifen

- Umsetzung(en)
  - Malware als Key Logger
  - USB-Gerät, das zwischen PC und Tastatur gesteckt wird

Evil Maid Attack

- Ziel(e)
  - Malware-Installation bei Zugriff auf ausgeschaltetes Gerät (z.B. im Hotel)
  - Erlangen des Passworts/Schlüssels für Festplatten-Verschlüsselung
  - Abgegriffene Daten an Angreifer senden/übergeben
- Umsetzung(en)
  - Installation eines manipulierten Bootloaders
  - Speichern oder übertragen der verwendeten Passwörter/Schlüssel

Abgreifen von Geräten (engl. interdiction)

- Ziel(e)
  - Gerät wird auf dem Weg zum Empfänger manipuliert
  - Installation von Malware vor der ersten Benutzung
  - Ändern von Grundeinstellungen des Geräts

- Umsetzung(en)
  - Unterbrechen der Zustellung, z.B. bei Liefer-Unternehmen
  - Manipulation des Geräts ohne Spuren zu hinterlassen

Reverse Engineering

- Ziel(e)
  - Analyse von proprietärer Hardware/Software
  - Aufbau von Wissen
- Umsetzung(en)
  - Geschicktes Ausprobieren
  - Nutzung von Reverse Engineering Tools, z.B. radare, IDA Pro
  - Detaillierte und zeitaufwendige Handarbeit

Seitenkanalangriffe (engl. side-channel attacks)

- Ziel(e)
  - Extraktion von vertraulichen Daten, z.B. kryptographische Schlüssel, PINs, Passwörter, etc.

- Umsetzung(en)
  - Während der Ausführung von kryptographischen Algorithmen: Aufnahme von Stromverbrauch, Laufzeit, elektro-magnetischer Abstrahlung, Geräuschen, optische Ausstrahlung, etc.
  - (Statistische) Analyse der aufgenommenen Daten

QUIZ: Angriffe (twbk.de)

Der CTO eines Augsburger Unternehmens erklärt Ihnen, dass das firmeneigene Protokoll ein gut gehütetes Geheimnis ist und auch Angreifer mit physikalischem Zugriff auf das Produkt keine Kenntnis davon erlangen können. Welcher Gedanke kommt Ihnen in den Sinn?

A) Mit physikalischem Zugriff kann das Gerät immer per Seitenkanalangriff gebrochen werden...

B) Einer starken Evil Maid Attacke würde auch dieses Produkt nicht lange standhalten...

C) Reverse Engineering mit hoher Motivation wäre auf jeden Fall eine Bedrohung...

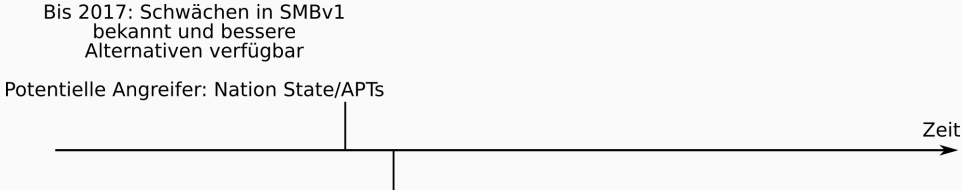
Bewertung von Angriffen und Angreifern

Schutzmaßnahmen gegen Angriffe und Angreifer

- **Ein Ziel der IT-Sicherheit ist Umsetzung von Schutzmaßnahmen gegen Angriffe**
  - Planung und Umsetzung von Maßnahmen benötigt Wissen über Angriffe
  - Maßnahmen kosten Geld → nicht jeder Angriff kann abgewehrt werden
- **Risikoabwägung: gegen welche Angriffe werden Maßnahmen implementiert**
- **Risiko und Bewertungen können sich über die Zeit ändern**
  - Anpassung der Entscheidungen können notwendig werden

Fall-Beispiel: EternalBlue / CVE-2017-0144

- *Vulnerability* in Microsoft Windows Implementierung des SMBv1-Protokolls
- Entwicklung durch NSA, späterer Leak und Ausnutzung durch Malware



Informationen über Angriffe

Lage der IT-Sicherheit in Deutschland

- Bericht
  - https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html
- Inhalt
  - Häufige Bedrohungen und Angriffe
  - Aktuelle Sicherheitssituation behördlicher Einrichtungen
  - IT-Sicherheit von kritischen Infrastrukturen

Presse mit Fokus auf IT-Sicherheit

- Heise Security
  - https://www.heise.de/security
- ThreatPost
  - https://threatpost.com/
- The Register
  - https://www.theregister.co.uk

- Inhalt
  - Neuigkeiten zu Malware und Angriffen, die in der IT-Öffentlichkeit diskutiert werden

Blogs der Anti-Viren Firmen

- Symantec
  - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence
- McAfee / Intel
  - https://www.mcafee.com/blogs/other-blogs/mcafee-labs/
- Kaspersky
  - https://www.kaspersky.de/blog/category/threats/

- Inhalt
  - Neuigkeiten zu Malware und Angriffen
  - Gute Einblicke auf Grund großer Anzahl von Samples
  - Erfahrene Software Reverse Engineering Experten

Schwachstellen-Datenbanken

- Exploit-DB
  - https://www.exploit-db.com/
- Full Disclosure Mailing List
  - https://seclists.org/fulldisclosure/

- Inhalt
  - Berichte und Diskussionen zu entdeckten Schwachstellen
  - Bezieht sich oft auf aktuell verfügbare Produkte/Software

Konferenzen

- Chaos Communication Congress
  - https://events.ccc.de/congress/
- BlackHat USA
  - https://www.blackhat.com/usa/
- DefCon
  - https://www.defcon.org/
- BSides Konferenzen
  - http://www.securitybsides.com
- Inhalt
  - Technische Details neuer Schwachstellen und neuer Angriffstechniken
  - Tutorials und Vorträge die Einstieg in bestimmte Thematik ermöglichen
  - Manche Konferenzen bieten Videos mit Vorträgen an

Informieren Sie sich über Angriffe
und versuchen Sie sie zu verstehen!

https://www.schneier.com/
https://krebsonsecurity.com/
viele mehr ...