Informationssicherheit, Datenschutz, Urheberrecht

ISDS

Themenübersicht

01
Einführung EU-DSGVO

Datenschutz

erste Schritte EU-DSGVO

Artikel 4

02
Vertiefung EU-DSGVO

Kapitel 1
Art. 1 - 3

Kapitel 2
Art. 5 – 7, 9

Kapitel 3
Art. 12 - 23

Kapitel 4
Art. 25 - 32

03
Grundlagen Sicherheit

Schutzziele

BSI

Grundschutz

Standards

ISMS

ISO 27x

ISIS 12 für KMU

04
Angriff Abwehr

Angriffsvarianten

Layer 8 Problem

Angriffsvorbereitung

Schadsoftware

Sicherheitssoftware

05
Angriff Abwehr

Angriffe auf Serverdienste

Brute Force

DoS & DDoS

Flooding

Tools

IT-Sicherheits-beauftragter

Agenda

- 01 Exploits
- 02 Rootkits
- 03 Brute Force
- 04 DoS, DDoS, DDoS – Reflektion
- 05 Replay Attacken
- 06 TCP/IP Hijacking
- 07 Tools
- 08 IT Sicherheitsbeauftragter

01 Exploits

01 Exploits

- Als *Exploit* bezeichnet man eine Methode oder einen Programmcode, mit dem über eine Schwachstelle in Hard- oder Software-Komponenten nicht vorgesehene Befehle oder Funktionen ausgeführt werden können.
- Je nach Art der Schwachstelle kann mithilfe eines *Exploits* z. B. ein Programm zum Absturz gebracht, Benutzerrechte ausgeweitet oder beliebiger Programmcode ausgeführt werden.

01 Exploits

Exploit-Kit

- *Exploit-Kits* oder *Exploit*-Packs sind Werkzeuge für Cyber- Angriffe und werden auf legitimen Webseiten platziert.
- Mithilfe verschiedener *Exploits* wird automatisiert versucht, eine Schwachstelle im Webbrowser oder dessen *Plug-ins* zu finden und zur Installation von Schadprogrammen zu verwenden.

02 Rootkits

02 Rootkits

- Wie bereits bei den Exploits vernommen, sehen wir den Begriff „Kits“ als Bezeichnung für eine Sammlung von Softwarewerkzeugen
- Als „Root“ wird die Rechteebene der Administratorrechte bezeichnet
- Nach dem Einbruch in einen System, dienen diese Werkzeuge im wesentlichen dazu im Verborgenen agieren zu können
- Belauschen, Ausspionieren, Datendiebstall, Installationen vornehmen, Hintertüren einbauen, umfangreichere Angriffsszenarien vorbereiten

02 Rootkits

Einige Beispiele

- Application Rootkits
- Kernel Rootkits
- Userland Rootkits
- Speicher Rootkits
- Virtualisierungs Rootkits

03 Brute Force

03 Brute Force

Kein direktes Ziel definiert, Maximalprinzip: definierter Einsatz mit größtmöglicher Wirkung

- Bei einem Brute-Force-Angriff handelt es sich um den Versuch, z.B. Zugangsdaten wie Benutzernamen und Passwort zu knacken oder einen Schlüssel zu finden, mit dem Daten verschlüsselt worden.
- Vereinfacht dargestellt, es wird versucht die Zugangsdaten oder Schlüssel zu erraten.
- Auf Grund der vielen Möglichkeiten entwickeln Hacker Werkzeuge, die in der Lage sind viele Möglichkeiten innerhalb einer sehr kurzen Zeit abzufragen.

04 DoS, DDoS, DDoS-Reflected

04 DoS, DDoS, DDoS-Reflection

- ***DoS - Denial* of *Service*** („Verweigerung des Dienstes“)

  Hierbei handelt es sich um die Nichtverfügbarkeit eines Dienstes, für den in der Regel eine Überlastung des Datennetzes verantwortlich ist.
  Eine solche Überlastung kann unbeabsichtigt auftreten, oder durch einen gezielten Angriff herbeigeführt werden.
  Bei einem Angriff durch viele gezielte Anfragen, mit dem Ziel einen mutwilligen Dienstausfall herbeizuführen, bezeichnet man einen solchen Angriff als „Denial of Servive Attack“.

04 DoS, DDoS, DDoS-Reflection

- **DDoS - Distributed-Denial-of-Service**

  Wird ein solcher Angriff nicht von einem Angreifer ausgeführt, sondern von einer Vielzahl von Angreifern, bezeichnet man dieses als „Distributed-Denial-of-Service-Attack“. Da in diesem Fall die Angriffe von einer Vielzahl von Quellen ausgehen, ist es nicht möglich die entsprechenden Angreifer zu blockieren.

  Solche Angriffe haben in den vergangenen Jahren jedoch viel von ihrem Schrecken verloren. Nichts desto trotz, gegenüber unvorbereiteten und schutzlosen Opfern können nach wie vor erhebliche Schäden erzeugt werden.
- Zunehmende Vernetzung von Geräten führt jedoch zu einer Art zweiten Frühling

04 DoS, DDoS, DDoS-Reflection

- **DRDoS - Distributed-Reflected-Denial-of-Service**

  Bei dieser Angriffsvariante stellt der Angreifer Anfragen an reguläre Dienste und nicht direkt an das Ziel. Er versieht seine Anfrage jedoch mir einer anderen „Absenderadresse“, die des eigentlichen Ziels.
  Ein Beispiel dafür wäre eine „DNS Amplification Attacke“, bei der das Domain Name System als „Reflektor“ benutzt wird.
  Durch eine solche Vorgehensweise ist die Ermittlung der eigentlichen Quelle natürlich deutlich schwieriger.

05 Replay Attacken

05 Replay Attacken

- **Ein Replay Angriff dient der Vortäuschung von Authentizität**
- **Vorangegangen ist in der Regel eine sogenannte „man in the middle“ Attacke**
- Beispiel:
  A und B kommunizieren und verifizieren ihre Identität, z.B. mit einer Hash Funktion. Beide Seiten vergleichen den Hash Code und entsprechende Berechnung. C belauscht den Vorgang und zeichnet den Prozess auf. C kommuniziert im Anschluss mit B, gibt sich für A aus und benutzt die Aufzeichnung zur Authentifizierung

06 TCP/IP Hijacking

06 TCP/IP Hijacking

- Auch bei dieser Angriffsform spielt das Ausspähen eine zentrale Bedeutung
- Im Fokus liegen hier TCP Pakete
- Ein Angreifer belauscht den Datenverkehr einer ausgewählten Verbindung und klinkt sich mit manipulierten Paketen in die Kommunikation ein
- Hubs waren eine „freundliche“ Hardwareunterstützung für diese Angriffsform

07 Tools

07 Tools

Werkzeuge der Angreifer sind ebenso Werkzeuge der Abwehr

Auch wenn viele Tools frei zugänglich sind, sie unautorisiert / unerlaubt außerhalb einer eigenen Testumgebung (Laborumgebung) zu nutzen ist eine STRAFTAT ! ! !

Grauzone für ITler § 202c Abs. 2
https://www.gesetze-im-internet.de/stgb/__202c.html

07 Tools

Brute Force Werkzeuge (Beispiele)

- Gobuster
- BruteX
- Dirsearch
- SSB
- THC-Hydra
- Burp Suite
- Patator
- Pydictor
- Ncrack
- Hashcat

07 Tools

DDoS Tools (Beispiele)

- HOIC
- LOIC
- ByteDOS
- PyLoris

07 Tools

Weitere Tools (Beispiele)

- Wireshark
- Nmap
- Aircrack-ng
- Owasp ZAP

07 Tools

Tool Sammlungen (Beispiele)

- Parrot
- Kali Linux
- Black Arch

08 IT-Sicherheitsbeauftragter

08 IT-Sicherheitsbeauftragter

Aufgaben

- In der Regel als Stabsstelle angelegt
- Die Abstimmung der IT-Sicherheitsziele mit den Zielen der Institution, Behörde oder dem Unternehmen
- Erstellung einer IT-Sicherheitsrichtlinie (Policies)
- Aufbau, Betrieb und Weiterentwicklung der IT-Sicherheitsorganisation
- Erstellung eines IT-Sicherheitskonzepts (ISMS) und dessen Anpassung an neue gesetzliche Gegebenheiten
- Unterrichtung der Unternehmensleitung zum Status quo der IT-Sicherheit

08 IT-Sicherheitsbeauftragter

Aufgaben

- Sicherstellung des Informationsflusses für das IT-Sicherheitsmanagement
- Dokumentation der IT-Sicherheitsmaßnahmen sowie Kontrolle dieser Maßnahmen
- Durchführung von Schulungsmaßnahmen zum Thema IT-Sicherheit
- Leitung der Analyse und Nachbearbeitung von IT-Sicherheitsvorfällen
- Verwaltung der für die IT-Sicherheit zur Verfügung stehenden Ressourcen
- Der IT-Sicherheitsbeauftragte ist Ansprechpartner auf dem Gebiet der IT-Sicherheit für Kollegen, aber auch für externe Geschäftspartner und Kunden.

08 IT-Sicherheitsbeauftragter

Gesetzliche Grundlage

- Es gibt keine vergleichbare gesetzliche Regelung wie beim Datenschutzbeauftragten
- Lediglich im Telekommunikationsgesetz wird im § 109 Abs. 4 Satz 1 gefordert, dass Betreiber von öffentlichen oder öffentlich zugänglichen Telekommunikationsnetzen einen IT-Sicherheitsbeauftragten benennen müssen und dass ein Sicherheitskonzept erstellt wird
- Zudem werden im IT-Sicherheitsgesetz 2.0 die Betreiber sogenannter „kritischer Infrastrukturen“ verpflichtet einen IT-Sicherheitsbeauftragten zu beschäftigen

08 IT-Sicherheitsbeauftragter

IT-Sicherheitsgesetz 2.0

- Seit dem 28.05.2021 in Kraft
- Mehr Pflichten für Betreiber, mehr Befugnisse für den Staat
- Die Rechtsverordnung für kritische Infrastrukturen, KRITIS-Verordnung 2.0, konkretisiert das IT-Sicherheitsgesetz und beschreibt die Schwellenwerte

VIELEN DANK!

Quellen

- Grafiken:
- https://storyset.com