Security Duell
Wiki

biometrische Authentifi-zierung

23

Ransomware

12

Schnellsuche in Wiki nach Nummer

1. SQL-Injection

SQL Injection ist ein Security-Exploit, bei dem der Angreifer eine Anfrage über ein Web-Formular per Structured Query Language (SQL) erweitert, um auf Ressourcen zuzugreifen oder Daten zu verändern. Eine SQL-Abfrage ist eine Anforderung, die eine Aufgabe in einer Datenbank ausführt.

2. Sniffer

Bei Netzwerken ist ein Sniffer ein Programm, das Netzwerk-Traffic überwacht und analysiert. Damit lassen sich die Gründe für Performance-Engpässe und andere Probleme entdecken. Mithilfe solcher Informationen können Administratoren das Netzwerk effizient betreiben.

3. Man-in-the-Middle

Bei einem Man-in-the-Middle-Angriff platziert sich der Angreifer logisch oder physisch zwischen dem Opfer und den verwendeten Ressourcen. Er ist dadurch in der Lage, die Kommunikation abzufangen, mitzulesen oder zu manipulieren. Die Ende-zu-Ende-Verschlüsselung ist eine wirksame Gegenmaßnahme gegen eine Man-in-the-Middle-Attacke.

4. Social Engineering

Bei Social Engineering handelt es sich um eine Technik, mit der Cyberkriminelle versuchen, arglose Benutzer dazu zu bewegen, vertrauliche Daten an den Angreifer zu senden, Malware auf dem Computer zu installieren oder einen Link zu einer infizierten Seite zu öffnen.

5. DDOS

Ein DDoS-Angriff versucht durch eine gezielt herbeigeführte Überlastung die Nichtverfügbarkeit eines Internetservices herbeizuführen. Meist werden Botnetze bestehend aus einer Vielzahl einzelner Systeme für den Angriff verwendet. Angriffsziel können Server oder andere Netzkomponenten sein.

6. Dumpster Diving

In der IT versteht man unter Dumpster Diving Techniken, die genutzt werden, um Informationen zu sammeln, mit denen man einen Angriff auf ein Computernetzwerk durchführen kann.

7. Phishing

Phishing beschreibt den Versuch des Diebstahls von Kennungen und Passwörtern per Internet durch den Versand von gefälschten E-Mails oder SMS.

8. Spear-Phishing

Bei Spear-Phishing handelt es sich um eine Betrugsmasche per elektronischer Kommunikation, die auf bestimmte Personen, Organisa-

tionen oder Unternehmen abzielt.

9. Trojanisches Pferd

Ein Trojanisches Pferd ist im Computerumfeld ein Programm, das sich als nützliche Anwendung tarnt. Neben den offensichtlichen Funktionen besitzt es versteckte Funktionen, die vom Anwender unbemerkt ausgeführt werden. Dies können schädliche Aktionen wie das Öffnen von Hintertüren oder das Herunterladen weiterer Malware sein.

10. IP-Spoofing

Beim IP-Spoofing versucht ein Angreifer, durch das Senden von Nachrichten von einer gefälschten IP-Adresse unbefugten Zugang zu einem System zu erlangen. Es soll dabei der Anschein erweckt werden, die Nachricht stamme aus einer vertrauenswürdigen Quelle, wie zum Beispiel von einer Adresse aus dem eigenen internen Computernetzwerk.

11. E-Mail-Spoofing

Die E-Mails, mit denen diese Angriffe gestartet werden, stammen scheinbar von vertrauenswürdigen Absendern wie Kunden, Kollegen oder Vorgesetzten. In Wirklichkeit kommen sie aber von Cyberkriminellen, die sich bewusst tarnen, um Ihr Vertrauen und Ihre Unterstützung zu erlangen und Sie so zu bestimmten Handlungen zu bewegen.

12. Ransomware

Ransomware ist eine Schadsoftware, die die Nutzung von Rechnern oder Daten blockiert und für die Freigabe ein Lösegeld fordert. Es kommen Methoden wie die Verschlüsselung von Dateien zum Einsatz. Bekannte Beispiele für diese Art von Malware sind CryptoLocker, WannaCry oder Locky.

13. Scareware

Scareware ist der Oberbegriff für Schadsoftware-Art, die den Computerbenutzer verängstigen und so zu bestimmten Handlungen bewegen soll.

14. Spyware

Bei Spyware handelt es sich um eine Software, die ohne Wissen des Anwenders Aktivitäten auf dem Rechner oder im Internet ausspioniert und aufzeichnet. Diese Informationen können an Dritte weitergeleitet und für Zwecke wie Werbung missbraucht werden.

15. Exploit

Exploits sind eine bestimmte Art Schadprogramm. Sie enthalten Daten oder ausführbaren Code, die eine oder mehrere Sicherheitslücken in den Programmen, die auf einem Computer laufen, ausnutzen können.

16. WPA3

Der WLAN-Verschlüsselungsstandard WPA3 (Wi-Fi Protected Access 3) wurde im Juni 2018 als Ergänzung zum bestehenden Standard WPA2 verabschiedet. WPA3 bringt wesentliche Verbesserungen bei der Authentifizierung und Verschlüsselung mit sich. Zudem soll sich die Konfiguration von WLAN-Geräten vereinfachen und die Sicherheit an öffentlichen Hotspots erhöhen.

17. Shoulder Surfing

Shoulder Surfing lässt sich interpretieren mit “Über die Schulter schauen”. Diese triviale Technik, mit der die Computersicherheit ausgehebelt werden kann, dient dem Ausspähen von Passwörtern, der persönlichen Identifikationsnummer (PIN) oder anderen sensitiven Informationen.

18. SSL

Eine SSL-Verbindung (Secure Socket Layer) ist eine verschlüsselte Netzverbindung zwischen einem Server und einem Client (Browser).

19. Firewall

Bei einer Firewall handelt es sich um ein System, das in der Lage ist, Datenverkehr zu analysieren. Sie schützt IT-Systeme vor Angriffen oder unbefugten Zugriffen.

20. Mirror-Server

Ein Mirror (Spiegel) ist eine Webseite oder ein Satz Dateien auf einem Server, der auf einen anderen Server kopiert wurde, damit die Seite oder die Dateien an mehr als einer Stelle verfügbar sind.

21. Restriktiv

beschränkt, begrenzt

22. Cloud

Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können.

23.Biometrische Authentifizierung

Biometrie ist eine Authentifizierungsmethode, die zur Identifikation von Benutzern biologische Merkmale wie Fingerabdruck, Gesicht, Stimme, Retina (Augensignatur) verwendet wird.

24. Software-Patch

Durch einen Software-Patch ist es möglich, Applikationen im Nachhinein zu ändern, Fehler zu beheben oder neue Features hinzuzufügen.

25. Backup

Datensicherung (englisch backup) bezeichnet das Kopieren von Daten in der Absicht, diese im Fall eines Datenverlustes zurückkopieren zu können.

26. DNS-Spoofing

Das DNS-Spoofing beziehungsweise das Cache-Poisoning stellen eine Form der Internetkriminalität dar. Sie umfasst eine Reihe von Methoden, mit denen Cyber-Angreifer Attacken auf Endbenutzer starten. Ziel des DNS-Spoofings ist es, unwissenden Internet-Nutzern Webseiten mit gefälschten oder vorgeblichen Inhalten zu liefern.

27. ID Call Spoofing

Beim Call-ID-Spoofing handelt es sich um eine verbotene Methode, Anrufe von einer vorgetäuschten Nummer aus vorzunehmen.

28. Data Leak

Datenpannen (Data Leak) sind Verstöße gegen die Datensicherheit und den Datenschutz, bei denen Staatsgeheimnisse, Betriebsgeheimnisse oder personenbezogene Daten Unberechtigten vermutlich oder erwiesenermaßen bekannt geworden sind. Es spielt keine Rolle, ob die Daten in analoger oder elektronischer Form vorliegen.

29. Virus

Ein Computervirus ist ein Programmcode, der sich an eine Wirtsdatei anhängt und sich selbständig vervielfacht. Er verändert die Funktionen des infizierten Computers. Meist ist er als Malware programmiert und führt schädliche Funktionen aus oder manipuliert den Rechner und dessen Daten.

30. Ende-zu-Ende Verschlüsselung

Die Ende-zu-Ende-Verschlüsselung sorgt für eine sichere Kommunikation zwischen zwei Partnern. Das Ver- und Entschlüsseln der übertragenen Informationen nehmen direkt die beiden Kommunikationspartner vor.

Andere an der Übertragung beteiligten Stationen können nicht auf die Informationen zugreifen.

31.Zwei-Faktor-Authentisierung

Die Zwei-Faktor-Authentisierung (2FA) bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren). Typische Beispiele sind Bankkarte plus PIN beim Geldautomaten, Fingerabdruck plus Zugangscode in Gebäuden, oder Passphrase und TAN beim Online-Banking.

Quellen

https://www.kaspersky.de
https://www.computerweekly.com
https://www.security-insider.de
https://www.secupedia.info
https://www.itwissen.info
https://de.wikipedia.org
https://aixvox.com/
https://www.seoagentur.de
https://praxistipps.chip.de