ÜBERBLICK

DIE GÄNGIGSTEN ARTEN VON CYBERANGRIFFEN

PHISHING

Diese Art von Angriff zielt darauf ab, Benutzer dazu zu bringen, vertrauliche Informationen preiszugeben, indem sie sich als legitime Einrichtungen, Unternehmen oder Personen ausgeben. Phishing erfolgt häufig über gefälschte E-Mails, Websites, SMS oder Instant Messages und kann darauf abzielen, Benutzernamen, Passwörter, Kreditkartendaten oder andere sensible Informationen zu stehlen. Auch bemühen sich Cyberkriminelle, durch Phishing-Maßnahmen Nutzer dazu zu verleiten, auf Links zu klicken, um auf diese Weise Schadsoftware einzuschleusen.

MALWARE

Schadsoftware umfasst verschiedene Arten von schädlicher Software wie Viren, Trojaner, Ransomware und Spyware. Malware wird normalerweise über infizierte E-Mail-Anhänge, Downloads, unsichere Websites oder ausgenutzte Schwachstellen verbreitet und kann dazu führen, dass das angegriffene System oder Netzwerk beschädigt oder kompromittiert wird.

DOS- & DDOS-ANGRIFFE

Denial-of-Service (DoS)- und Distributed-Denial-of-Service (DDoS)-Angriffe zielen darauf ab, ein System, Netzwerk oder eine Website zu überlasten, indem sie einen enormen Datenverkehr generieren oder die verfügbaren Ressourcen erschöpfen. Dadurch wird der Dienst für legitime Benutzer unzugänglich gemacht.

BEDROHUNG DURCH INSIDER

Cyberangriffe, bei denen jemand innerhalb einer Organisation, wie ein Mitarbeiter, Auftragnehmer oder Partner, böswillig oder unbeabsichtigt sensible Informationen oder Systeme gefährdet.Die Bedrohung durch Insider ist besonders herausfordernd, da Insider oft über legitimen Zugriff auf Systeme und Informationen verfügen, was es schwierig macht, ihre böswilligen Handlungen zu erkennen und zu stoppen.

SQL-INJECTION

SQL steht für "Structured Query Language". Es handelt sich dabei um eine spezielle Daten-Abfrage-Sprache, die entwickelt wurde, um Datenbanken zu verwalten und zu abzufragen. Diese Art von Angriff wird gegen Websites oder Anwendungen verwendet, die eine Datenbank verwenden. Ein Angreifer fügt schädlichen SQL-Code in Eingabefelder ein, um die Datenbankabfragen zu manipulieren und unautorisierten Zugriff auf Daten zu erlangen oder diese zu modifizieren.

SPOOFING

Beim Spoofing gibt der Angreifer vor, jemand oder etwas anderes zu sein. Spoofing-Angriffe zielen darauf ab, die Authentizität von Informationen oder Identitäten zu täuschen, um Zugang zu sensiblen Daten zu erhalten, Phishing-Angriffe durchzuführen, Verbindungen zu verschleiern oder Sicherheitsmechanismen zu umgehen.

CROSS-SITE-SCRIPTING

Cross-Site-Scripting (XSS) ist eine Sicherheitslücke, bei der Angreifer schädlichen Code in eine vertrauenswürdige Website einschleusen. Dadurch kann der Angreifer bösartigen Code an die Browser von Besuchern senden und deren vertrauliche Daten stehlen oder deren Browsersitzungen übernehmen. XSS-Angriffe können verheerende Auswirkungen haben und erfordern eine sorgfältige Absicherung von Webanwendungen.

SESSION HIJACKING

Bezeichnet eine Methode, bei der ein Angreifer die Kontrolle über eine laufende Sitzung zwischen einem Benutzer und einem System übernimmt. Dabei erlangt der Angreifer Zugriff auf die Sitzungsdaten und kann sich als der legitime Benutzer ausgeben, um auf vertrauliche Informationen zuzugreifen oder schädliche Handlungen auszuführen. Dieser Angriff erfolgt oft durch das Abfangen und Manipulieren von Netzwerkpaketen, um die Sitzung zu übernehmen und die Sicherheitsmechanismen zu umgehen.

BRUT-FORCE-ANGRIFFE

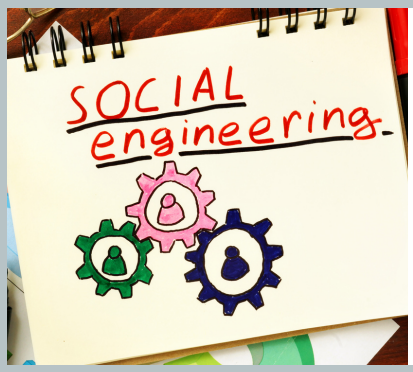
"Passwortangriffe" im Bereich Cybercrime beziehen sich auf verschiedene Methoden, die von Angreifern verwendet werden, um unautorisierten Zugriff auf Benutzerkonten zu erlangen, indem sie versuchen, Passwörter zu erraten, zu knacken oder zu umgehen. Das Ziel eines Passwortangriffs besteht darin, die Kontrolle über ein Benutzerkonto zu erlangen, um Zugriff auf persönliche Informationen, vertrauliche Daten oder Systeme zu erhalten.

WATERING-HOLE-ANGRIFF

Ein Watering-Hole-Angriff ist eine gezielte Cyber-Angriffsmethode, bei der Angreifer eine legitime Website oder Plattform infizieren, die häufig von den Zielbenutzern besucht wird. Das Ziel besteht darin, die Besucher der Website mit Malware zu infizieren und Zugriff auf ihre Systeme oder Informationen zu erhalten.

MAN IN THE MIDDLE

Bei einem MitM-Angriff versucht ein Angreifer, den Kommunikationsfluss zwischen zwei Parteien abzufangen, zu überwachen oder zu manipulieren, ohne dass die Parteien dies bemerken. Dadurch kann der Angreifer sensible Informationen wie Passwörter, Kreditkarteninformationen oder vertrauliche Daten stehlen.



SOCIAL ENGINEERING

Social Engineering bezieht sich auf die manipulative Nutzung psychologischer und sozialer Techniken, um Menschen zu überreden, vertrauliche Informationen preiszugeben, unerlaubten Zugriff auf Systeme zu gewähren oder bestimmte Handlungen auszuführen, die den Zielen des Angreifers dienen. Es geht darum, menschliche Schwachstellen auszunutzen, um an sensible Informationen oder Zugang zu gelangen.

STALKING PER APPLE AIRTAG

"Stalking per Apple Airtag" bezieht sich auf den missbräuchlichen Einsatz von Apple Airtags, kleinen Geräten zur Ortung von Gegenständen, um heimlich Personen zu verfolgen oder ihre Privatsphäre zu verletzen. Dies kann durch das unbemerkte Anbringen eines Airtags an einer Person oder deren persönlichen Gegenständen geschehen, um ihre Bewegungen zu überwachen oder sie unerwünscht zu verfolgen.

FRAGEN ZUM THEMA INFORMATIONSSICHERHEIT?

Wir sind nur einen Anruf oder eine Mail weit entfernt:
0221 82 95 910 | info@optiqum.de