VHV CYBER-LEXIKON

VHV VERSICHERUNGEN

WIE GUT SPRECHEN SIE CYBERANISCH?

Beim Schutz Ihrer Netzwerke und Daten werden Sie früher oder später mit hoch spezialisierten IT-Experten sprechen.

Und die haben ihre ganz eigene Art, sich auszudrücken: Deren Sprache besteht aus technischen Abkürzungen („CSRF"), englischen Fachbegriffen („Zero-Day-Exploit") und dem Insider-Jargon der Hackerszene. Letztere ist im Erfinden neuer Wörter äußerst kreativ und bereicherte die IT-Sprache u. a. um „Phishing", „Nicknapping" oder „Fuzzing".

Auch wenn sich dieses „Cyberanisch" etwas sonderbar anhört: Es ermöglicht Ihnen, sich über Computerschäden hochpräzise zu verständigen. Darum hat die VHV die wichtigsten Begriffe hier für Sie gesammelt und leicht verständlich erklärt.

Dieses Taschenwörterbuch hilft Ihnen, die Welt der Cyberrisiken zu verstehen und gibt Ihnen mehr Sicherheit im Gespräch mit Fachleuten.

Gleichzeitig hoffen wir, dass Sie keinen der Fachausdrücke je benutzen müssen und Ihr IT-System immer störungsfrei läuft!

DAS KLEINE ABC DER CYBERWELT

A.

ADBLOCKER

Ein „Adblocker" ist eine Anwendung, die verhindern soll, dass Werbung auf Websites angezeigt wird. Sie erkennen einen Großteil der im Internet geschalteten Werbeanzeigen und blenden diese aus. Einige Adblocker können jedoch auch Spyware beinhalten.

ADVANCED PERSISTENT THREAT (APT)

„Advanced Persistent Threats" (APT) sind zielgerichtete Cyber-Angriffe auf ausgewählte Institutionen und Einrichtungen, bei denen sich ein Angreifer dauerhaften Zugriff zu einem Netz verschafft und diesen in der Folge auf weitere Systeme ausweitet. Hierzu sind hohe Ressourceneinsätze und erhebliche technische Fähigkeiten aufseiten der Angreifer nötig.

B.

BOTNETZE

Als „Botnetz" wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnetz-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.

C.

CACHE POISONING

Unter „Cache Poisoning“ versteht man das Einschleusen von manipulierten Daten in einen Zwischenspeicher „Cache“, der dann von anderen Anwendungen oder Diensten genutzt wird. Ein Angreifer kann so z. B. allgemein die Routen von Datenpaketen ändern oder gezielt Anfragen für Webseiten einer Bank auf eine gefälschte Seite umleiten.

CSRF

„Cross-Site-Request-Forgery“ ist eine weitere Angriffsform, die sich gegen Benutzer von Webanwendungen richtet. Mit dieser Vorgehensweise lassen sich Funktionen einer Webanwendung von einem Angreifer im Namen des Opfers nutzen. Ein Beispiel ist die Versendung einer gefälschten Statusnachricht in einem sozialen Netzwerk: Ein Angreifer formuliert die Nachricht und schiebt sie dem Opfer beim Abruf einer Webseite unter. Wenn der Angriff gelingt und das Opfer während des Angriffs parallel im betreffenden sozialen Netzwerk angemeldet ist, wird die Nachricht des Angreifers im Namen des Opfers veröffentlicht.

CHOSEN-PLAINTEXT-ATTACKE

Kryptografischer Angriff, in dem der Angreifer Zugriff auf Chiffrate zu von ihm gewählten Klartexten erhalten kann.

CYBERRAUM

Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.

D.

DATENSICHERUNG

Bei einer Datensicherung werden zum Schutz vor Datenverlust Sicherungskopien von vorhandenen Datenbeständen erstellt. Datensicherung umfasst alle technischen und organisatorischen Maßnahmen zur Sicherstellung der Verfügbarkeit, Integrität und Konsistenz der Systeme einschließlich der auf diesen Systemen gespeicherten und für Verarbeitungszwecke genutzten Daten, Programme und Prozeduren.

DoS-ATTACKE

Eine künstlich herbeigeführte Überlastung eines Webservers oder Datennetzes – gesteuert von Cyberkriminellen. Im Gegensatz zu einer einfachen Denial-of-Service-Attacke („DoS“) haben Distributed-Denial-of-Service-Attacken („DDoS“) eine immense Schlagkraft. Mehrere Computer greifen dabei gleichzeitig und im Verbund („Botnetze“) eine Webseite oder eine ganze Netzinfrastruktur an. Dies kann sehr schnell zum Ausfall der Server führen.

E.

ENTSCHLÜSSELUNG

Vorgang, bei dem unter Verwendung mathematischer Algorithmen und privater oder geheimer Schlüssel elektronische Daten wieder les- bzw. verarbeitbar gemacht werden. In verschlüsselter Form sind die Daten von unbefugten Dritten nicht einsehbar. Die Daten können nur vom Besitzer des entsprechenden privaten oder geheimen Schlüssels wieder in die Originalform überführt werden.

F.

FUZZING

„Fuzzing“ ist eine automatisierte Testmethode für Software, bei der ein Programm eine Vielzahl automatisch generierter Eingabedaten verarbeiten muss, ohne dabei eine Fehlfunktion zu zeigen. Findet ein Hacker durch Fuzzing ein Eingabemuster, das eine Fehlfunktion erzeugt, muss überprüft werden, ob sich der gefundene Fehler als Sicherheitslücke ausnutzen lässt.

FAKE PRESIDENT

Bezeichnet eine Betrugsmethode („Enkeltrick“), bei welcher E-Mails mit angeblichen Transaktionsanordnungen bzw. Aufforderung zu bestimmten Handlungen im Namen des Firmenchefs an Mitarbeiter des Unternehmens geschickt werden. Diese Betrugsmethode kommt sehr häufig vor, weil die E-Mail-Adressen im Internet öffentlich zugänglich sind.

G.

GEHEIMER SCHLÜSSEL

Geheime Schlüssel werden im Zusammenhang mit symmetrischen Kryptoalgorithmen verwendet. Im Gegensatz zu den bei asymmetrischen Kryptoalgorithmen eingesetzten privaten Schlüsseln ist das gesamte Schlüsselmaterial allen Kommunikationspartnern bekannt.

H.

HTTPS

„HTTPS“ bzw. „Hypertext Transfer Protocol Secure“ ist ein Protokoll zur sicheren Datenübertragung im Internet. Beispielsweise wird es zur Kommunikation zwischen Webbrowser und Webserver verwendet. Bekannt ist die Buchstabenfolge „HTTPS“ den meisten aus der Adresszeile im Webbrowser: Hier wird sie vor jeder sicheren Webseite als „https://“ angezeigt. Die Verbindung wird über ein erworbenes SSL-Zertifikat sichergestellt.

HTTP

Das „Hypertext Transfer Protocol“ HTTP ist im Gegensatz zu HTTPS nicht verschlüsselt. Daten, die mit diesem Protokoll übertragen werden, können leicht von Dritten gelesen oder manipuliert werden. Wenn Sie schützenswerte Informationen über das Internet austauschen, ist eine verschlüsselte Verbindung (z. B. HTTPS) sehr empfehlenswert.

I.

IT-FORENSIK

Die „IT-Forensik“ befasst sich mit der Untersuchung, Analyse und Aufklärung von Sicherheitsvorfällen im Zusammenhang mit IT-Systemen.

K.

KEYLOGGER

Als „Keylogger“ wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern filtern.

KUMULATIONSEFFEKT IM IT-GRUNDSCHUTZ

Der Kumulationseffekt beschreibt, dass sich der Schutzbedarf eines IT-Systems erhöhen kann, wenn durch Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System ein insgesamt höherer Gesamtschaden entstehen kann. Ein Auslöser kann auch sein, dass mehrere IT-Anwendungen bzw. eine Vielzahl sensitiver Informationen auf einem IT-System verarbeitet werden, sodass durch Kumulation von Schäden der Gesamtschaden höher sein kann.

M.

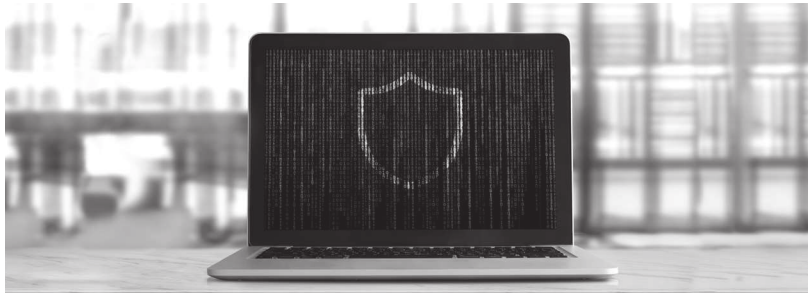
MAN-IN-THE-MIDDLE-ANGRIFF

Ziel bei einem „Man-in-the-Middle-Angriff“ ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehreren Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte“ der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt.

N.

NICKNAPPING

Personen treten im Internet mit ihrem realen Namen oder unter der Verwendung eines Pseudonyms oder Nicknames auf. Als „Nicknapping“ bezeichnet man einen Cyberangriff, bei dem der Angreifer unter einem bekannten Namen oder Pseudonym auftritt. Dadurch versucht der Angreifer, gegenüber Dritten den Eindruck zu erwecken, er sei der eigentliche/ursprüngliche Inhaber des Namens oder des Pseudonyms. Gelingt dies, kann der Angreifer in begrenztem Maße als der eigentliche/ursprüngliche Inhaber agieren.



P.

PAIRING
Zwei bluetoothfähige Geräte wie z. B. Smartphone und Kopfhörer benötigen einen gemeinsamen Verbindungsschlüssel, um miteinander kommunizieren zu können. Dieser wird berechnet, nachdem auf beiden Geräten eine gleichlautende PIN eingegeben wurde. Die „besondere Vertrauensbeziehung" zwischen den beiden Geräten bezeichnet man als „Pairing".

PHARMING
Ist eine Betrugsmethode, die auf der Grundidee des Phishings beruht. Dabei wird der Benutzer durch die Nutzung von Systemmanipulationen auf gezielt gefälschte Webseiten umgeleitet, ohne dass er dies bemerkt. Dadurch ist es möglich, an persönliche Informationen wie z. B. Bankdaten zu gelangen.

PHISHING
Beim „Phishing" wird z. B. mittels gefälschter E-Mails und/oder Webseiten versucht, Zugangsdaten für einen Dienst oder eine Webseite zu erlangen. Wird diese Manipulation vom Opfer nicht erkannt und die Authentizität einer Nachricht oder Webseite nicht hinterfragt, gibt das Opfer seine Zugangsdaten u. U. selbst unwissentlich in unberechtigte Hände.

R.

RANSOMWARE
Als „Ransomware" werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch: „ransom") wieder freigegeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

REPLAY-ANGRIFFE
„Replay-Angriffe" beschreiben allgemein Angriffe, bei denen ein Informationsaustausch zuerst aufgezeichnet wird und die gewonnenen Informationen im Anschluss daran missbräuchlich wiederverwendet werden. Anhand eines aufgezeichneten Login-Vorgangs kann ein Angreifer beispielsweise versuchen, sich selbst unberechtigt Zugang zu dem jeweiligen System zu verschaffen.

S.

SANITARISIERUNG
Die Bereinigung einer Meldung von schutzbedürftigen Informationsanteilen. Ziel ist die Wahrung der berechtigten Schutzinteressen der am Informationsaustausch Beteiligten bei gleichzeitigem Erhalt der relevanten Informationen.

SCHADFUNKTION
Mit Schadfunktion wird eine vom Anwender ungewünschte Funktion bezeichnet, die die Informationssicherheit unbeabsichtigt oder bewusst gesteuert gefährden kann.

SCAREWARE

„Scareware“ ist eine Form von Schadsoftware, die der Nutzer selbst auf seinem System installiert. In den meisten Fällen wird dem Nutzer beim Surfen im Internet durch Täuschung oder Ausnutzen von technischem Unverständnis suggeriert, dass ein Problem mit seinem Computer besteht. Häufig wird dazu eine Infektion mit Schadsoftware gemeldet, eine angebliche Fehlfunktion des Betriebssystems erkannt oder mit einem wichtigen Sicherheits-Update geworben. Vertraut ein Anwender auf diese Meldungen und installiert die angebotene Software, hat er selbst dadurch das System im ungünstigsten Fall mit einer Schadsoftware infiziert.

SPOOFING

„Spoofing“ (englisch: „to spoof“, zu Deutsch: manipulieren, verschleiern oder vortäuschen) nennt man in der Informationstechnik verschiedene Täuschungsversuche zur Verschleierung der eigenen Identität und zum Fälschen übertragener Daten. Das Ziel besteht darin, die Integrität und Authentizität der Informationsverarbeitung zu untergraben.

SPYWARE

Als „Spyware“ werden Programme bezeichnet, die heimlich, also ohne darauf hinzuweisen, Informationen über einen Benutzer bzw. die Nutzung eines Rechners sammeln und an den Urheber der Spyware weiterleiten. Spyware gilt häufig nur als lästig, es sollte aber nicht übersehen werden, dass durch Spyware auch sicherheitsrelevante Informationen wie Passwörter ausgeforscht werden können.

T.

TROJANISCHES PFERD

Ein „trojanisches Pferd“, oft auch (fälschlicherweise) kurz „Trojaner“ genannt, ist ein Programm mit einer verdeckten, nicht dokumentierten Funktion oder Wirkung. Ein trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogramms für seine Installation durch den Benutzer.

TLS (TRANSPORT LAYER SECURITY)

„SSL“ ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. SSL wurde nach der Version 3.0 unter dem neuen Namen TLS „Transport Layer Security“ weiterentwickelt. Das „SSL-Protokoll“ stellt auf der Transportschicht einen sicheren „Tunnel“ zwischen Sender und Empfänger her, durch den die transportierten Daten gegen Kenntnisnahme und Veränderung geschützt werden.

V.

VERTEILUNGSEFFEKT
Der „Verteilungseffekt“ kann sich auf den Schutzbedarf relativierend auswirken, wenn zwar eine Anwendung einen hohen Schutzbedarf besitzt, ihn aber deshalb nicht auf ein betrachtetes IT-System überträgt, weil auf diesem IT-System nur unwesentliche Teilbereiche der Anwendung laufen.

VIREN
Klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (keine Schadfunktion bis hin zum Löschen der Daten auf einer Festplatte). „Viren“ treten in Kombination mit einem Wirt auf, z. B. einem infizierten Dokument oder Programm.

Z.

ZERO-DAY-EXPLOIT
Die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist, charakterisiert man mit dem Begriff „Zero-Day-Exploit“. Die Öffentlichkeit und der Hersteller des betroffenen Produkts merken in der Regel erst dann die Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Hersteller hat keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

ZUGRIFF
Bezeichnet die Nutzung von Informationen bzw. Daten. Über Zugriffsberechtigungen wird geregelt, welche Personen oder IT-Anwendungen bevollmächtigt sind, Informationen oder Daten zu nutzen oder Transaktionen auszuführen.

VHV CYBERPROTECT

Die IT-Versicherung der VHV schützt Ihren Betrieb umfassend vor Schäden an Computersystemen und digitalen Archiven – bei technischen Defekten, kriminellen Angriffen von außen oder Untreue der eigenen Mitarbeiter.

Optimaler Schutz bei Hackerangriffen
Unser Produkt schützt Sie gegen Best Practices der Hacker und versichert Sie gegen durch Informationssicherheitsverletzung verursachte Vermögensschäden.

Auch bei nicht gezielten Angriffen
VHV CYBERPROTECT hilft sowohl bei gezielten als auch bei nicht gezielten Angriffen auf Ihr Unternehmen, z. B. gegen Schadsoftware, DDoS-Angriffe, unberechtigte Aneignung von Zugangscodes sowie Computer-Sabotage.

VHV Soforthilfe
Die IT-Experten stehen Ihnen rund um die Uhr an 365 Tagen telefonisch und persönlich zur Verfügung, damit Ihr Geschäftsbetrieb schnellstmöglich wieder aufgenommen werden kann.

Inklusive Drittschäden
Falls Dritte Ihnen gegenüber aufgrund einer Informationssicherheitsverletzung Schadenersatzansprüche geltend machen, sorgen wir für die Abwehr unberechtigter und die Erfüllung berechtigter Ansprüche.

Quellen: Bundesamt für Sicherheit der Informationstechnik und VHV Versicherungen

VHV CYBERPROTECT – RUNDUMSCHUTZ GEGEN IT-ANGRIFFE!

400.0031.56 Stand 03.2018 Druck 03.2018