MARKEL

Sprechen Sie Cyber? Ein Glossar von A bis Z.

Als Makler wissen Sie, dass Cyberrisiken für Unternehmen eine realistische Bedrohung darstellen. Prävention und ein passgenaues Versicherungskonzept bilden die Säulen, mit denen Sie und Ihre Kunden sich schützen können. In der Kommunikation mit IT-Sicherheitsexperten – zum Beispiel im Rahmen von Cyber-Präventionsmaßnahmen, auf die Unternehmen setzen sollten –, doch auch bei der gemeinsamen Definition des Restrisikos oder der Abwicklung im Schadensfall ist es absolut notwendig, sich über potenzielle sowie entstandene Schäden präzise austauschen zu können.

Doch wie? Trojanisches Pferd, Phishing oder Ransomware – Botnetz, Advanced Persistent Threat oder DoS-Attacke: Der Cyber-Jargon der Hackerszene begegnet uns täglich, ist aber nicht immer einfach zu verstehen. Und wer sich mit dem Thema Cybersicherheit auseinandersetzt, sollte wissen, worum es geht. Damit Sie und Ihre Kunden nicht aneinander vorbeireden, wenn es um konkrete Schäden geht, haben wir ein hilfreiches ABC der Cyberwelt für Sie aufgestellt:

A.

ADVANCED PERSISTENT THREAT (APT)
Ein zielgerichteter, höchst professioneller und aufwändiger Angriff auf ausgesuchte Institutionen und Einrichtungen über einen dauerhaften Zugriff zu einem Netz, der auf weitere Systeme ausgeweitet werden kann.

B.

BOT / BOTNETZ
Ein Bot ist ein fernsteuerbares Schadprogramm, das einen ganzen Verbund von Systemen beziehungsweise einen Rechnerverbund (Botnetz) befällt. Der Botnetz-Betreiber (Angreifer) kontrolliert und steuert das betroffene Botnet über einen Command-and-Control-Server (C&S-Server).

C.

CACHE POISONING
Werden manipulierte Daten in den Zwischenspeicher (Cache) eines Computers eingeschleust, der in Folge von anderen Anwendungen und Diensten genutzt werden kann, spricht man von einer Vergiftung des Caches (Cache Poisoning). So lassen sich die Routen von Datenpaketen manipulieren und Anfragen für Webseiten, z. B. einer Bank, auf eine gefälschte URL weiterleiten.

CSRF
Der Cross-Site-Request-Forgery-Angriff richtet sich gegen Nutzer von Webanwendungen, deren Funktionen sich durch den Angreifer im namen des Opfers nutzen lassen. Häufig werden beispielsweise gefälschte Statusnachrichten in sozialen Netzwerken platziert.

CYBERRAUM
Der Cyberraum ist der weltweite virtuelle Raum aller vernetzten und vernetzbaren informationstechnischen Systeme auf Datenebene. Das Internet bildet gleichzeitig die Basis und das öffentliche zugängliche Verbindungsnetz, das um andere Datennetze beliebig erweitert werden kann.

D.

DATENSICHERUNG
Sicherungskopien vorhandener Datenbestände zum Schutz vor Datenverlust. Der Vorgang umfasst sämtliche organisatorischen wie technischen Maßnahmen, welche die Verfügbarkeit Integrität und Systemkonsistenz umfasst. Das schließt auch die auf den entsprechenden Systemen gespeicherten und zum Zweck der Weiterverarbeitung gespeicherten Daten, Prozeduren und Programme ein.

DOS- & DDOS-ATTACKE
Mit einem Denial-of-Service-Angriff (DoS) können Cyberkriminelle Webserver oder Datennetze bewusst überlasten. Noch wirkungsvoller sind DDoS-Angriffe (Distributed-Denial-of-Service-Angriffe). Bei dieser Attacke werden Server lahmgelegt, indem gleich mehrere Computer parallel und im Verbund (Botnetz) eine Webseite oder eine Netz-Infrastruktur angreifen.

E.

ENTSCHLÜSSELUNG
Damit unbefugte Dritte elektronische Daten nicht einsehen können, können diese unter Anwendung mathematischer Algorithmen sowie privater/geheimer Schlüssel „verschlüsselt“ und auf dem gleichen Weg nur durch den Besitzer der Daten wieder in die Originalform überführt werden.

F.

FAKE PRESIDENT
Auch als Enkeltrick bekannt ist diese weit verbreitete Betrugsmethode, bei der E-Mails im Namen des Firmenchefs an Mitarbeiter versendet werden, die Handlungsaufforderungen oder Transaktionsanordnungen enthalten. Der Angriff ist relativ einfach, da E-Mail-Adressen in der Regel öffentlich zugänglich sind.

G.

GEHEIMER SCHLÜSSEL
Diese werden im Zusammenhang mit sogenannten symmetrischen Kryptoalgorithmen verwendet. Anders als bei asymmetrischen Kryptoalgorithmen privater Schlüssel ist in diesem Fall das gesamte Schlüsselmaterial allen Kommunikationspartnern bekannt.

H.

HINTERTÜR (Backdoor)
Bei Hintertüren handelt es sich um Schadprogramme mit dem Ziel, einen unbefugten Zugang zu einem IT-System offen zu halten, um einen Systemeinbruch unbemerkt zu ermöglichen. Gleichzeitig sollte dieser Zugang möglichst weitgehende Zugriffsrechte aufweisen, um etwa Angriffsspuren verstecken zu können.

HTTPS
Das „Hypertext Transfer Protocol Secure“ ist ein Protokoll zur sicheren Datenübertragung im Internet, das häufig zur Kommunikation zwischen Webbrowser (über URL) und Webserver verwendet wird. Ein SSL-Zertifi kat stellt die Verbindung sicher. Das HTTP-Protokoll hingegen ist unverschlüsselt.

I.

IDENTITÄTSDIEBSTAHL
Verschafft sich ein unbefugter Dritter Zugang zu Identifi kations- und Authentisierungsdaten wie Benutzernamen, Passwörter oder Bank- bzw. Kreditkarteninformationen, spricht man von Identitätsdiebstahl.

INTERNET OF THINGS (IOT)
Gemeint sind sogenannte intelligente Gegenstände, sprich Gegenstände mit intelligenten Funktionen, die an bestehende Datennetze angeschlossen und üblicherweise drahtlos auf das Internet zugreifen oder darüber erreicht werden.

IT-FORENSIK
Ein Bereich, der sich mit der Untersuchung, Analyse und Aufklärung von Cyberangriffen beziehungsweise Sicherheitsvorfällen im Zusammenhang mit IT-Systemen befasst.

K.

KEYLOGGER
Als Keylogger bezeichnet man Hard- oder Software zum Mitschneiden von Tastatureingaben. Es werden alle Tastatureingaben aufgezeichnet, 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 zum Beispiel den sich erhöhenden Schutzbedarf eines IT-Systems infolge einer Kumulation mehrerer (z. B. kleinerer) Schäden auf einem IT-System, die zu einem insgesamt höheren Gesamtschaden führen.

L.

LEITLINIE ZUR INFORMATIONSSICHERHEIT
Diese Leitlinie ist ein zentrales Dokument für die Informationssicherheit einer Institution oder eines Unternehmens. Sie beschreibt, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der Institution hergestellt werden soll, beinhaltet die von der Institution angestrebten Informationssicherheitsziele sowie die verfolgte Sicherheitsstrategie. Damit beschreibt die Sicherheitsleitlinie auch das über die Sicherheitsziele angestrebte Sicherheitsniveau in einer Behörde oder einem Unternehmen.

M.

MALWARE
Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig als Synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus „Malicious Software“ und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistens schädliche Funktionen auszuführen. Beispiele für Malware sind Computerviren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

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. Als erstes leitet der Angreifer eine Verbindungsanfrage des Senders zu sich um. Im nächsten Schritt baut der Angreifer eine Verbindung zu dem eigentlichen Empfänger der Nachricht auf. Wenn ihm das gelingt, kann der Angreifer unter Umständen alle Informationen, die der Sender an den vermeintlichen Empfänger sendet, einsehen oder manipulieren, bevor er sie an den richtigen Empfänger weiterleitet. Auf die Antworten des Empfängers kann der Angreifer wiederum ebenfalls zugreifen, wenn nicht entsprechende Schutzmechanismen wirksam sind.

N.

NACHWEIS/NACHWEISDOKUMENT GEMÄß §8a (3) BSIG
Ein Nachweis gemäß § 8a (3) BSIG ist die Bescheinigung eines unabhängigen Dritten über die Einhaltung eines angemessenen Sicherheitsniveaus (gemäß § 8a (1) BSIG) durch den Betreiber. Die Umsetzung der angemessenen und wirksamen Maßnahmen kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Das Nachweisdokument ist eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel, sowie der zur Bearbeitung erforderlicher Informationen.

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. In der Vergangenheit wurden z. B. Twitter-Konten im Namen von Politikern erstellt, um darüber Falschmeldungen im Namen des Politikers zu verbreiten.

O.

ÖFFENTLICHER SCHLÜSSEL
Ein öffentlicher Schlüssel ist der Teil eines kryptographischen Schlüsselpaares, der öffentlich bekannt und frei zugänglich ist. Er ist meist Teil eines Zertifikates und wird neben der Prüfung digitaler Signaturen auch verwendet, um Daten für eine bestimmte Person zu verschlüsseln. Diese können im Anschluss mit dem zugehörigen, nur dieser Person bekannten, privaten Schlüssel wieder entschlüsselt werden.

OPERATIONELLE RISIKEN
Bei den operationellen Risiken handelt es sich um die ursprünglichste Form der Risiken: hierbei handelt es sich um Risiken, die aus dem Prozessablauf heraus entstehen. Dabei ist es unerheblich, welche Prozesse ausgeführt werden. Typischerweise werden zu den operationellen Risiken fehlerhaftes Verhalten, Unkenntnis, Betrug, Naturkatastrophen, IT-Risiken und auch die Risiken im Bereich Informationssicherheit gezählt.

P.

PAIRING
Um miteinander kommunizieren zu können, benötigen zwei Bluetooth-fähige Geräte wie Handys oder Tablets einen gemeinsamen Verbindungsschlüssel. Dieser wird berechnet, nachdem auf beiden Geräten eine gleichlautende PIN eingegeben wurde. Die „besondere Vertrauensbeziehung“ zwischen den beiden Geräten bezeichnet man als „Pairing“.

PHARMING
Wie beim Phishing sind auch beim Pharming meist Zugangsdaten das Ziel eines Angriffs. Der Unterschied zum Phishing besteht darin, dass beim Pharming die Infrastruktur so manipuliert wird, dass das Opfer auch dann auf einer gefälschten Webseite landet, wenn er die korrekte Adresse des Dienstes eingeben hat. Technisch geschieht das in der Regel durch eine Manipulation der DNS-Einträge in der lokalen Host-Datei, an einem Zwischenspeicher oder an der zentralen DNS-Infrastruktur.

PHISHING
Der Begriff ist eine Zusammensetzung aus „Password“ und „Fishing“ (nach Passwörtern angeln). Bei dieser Methode wird etwa 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 unter Umständen selbst unwissentlich in unberechtigte Hände. Bekannte Beispiele sind Phishing-Angriffe gegen Bankkunden, die in einer E-Mail aufgefordert werden, ihre Zugangsdaten auf der Webseite der Bank einzugeben und validieren zu lassen. Mit dem gleichen Verfahren werden aber auch Nutzer von E-Commerce-Anwendung angegriffen, z. B. Online Shops oder Online-Dienstleister. Angreifer setzen zunehmend Schadprogramme statt klassischem Phishing als Mittel zum Identitätsdiebstahl ein. Andere Varianten des Phishings setzen auf gefälschte Near Field Communication (NFC)-Tags oder Barcodes, die vom Opfer eingelesen werden und auf eine Phishing-Seite weiterleiten.

R.

RANSOMWARE
Unter diesem Begriff fungieren Schadprogramme, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (englisch „ransom“) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.

REPLAY-ANGRIFFE
Diese Attacken beschreiben Angriffe, bei denen ein Informationsaustausch zuerst aufgezeichnet wird, bevor die gewonnenen Informationen im Anschluss 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
Unter Sanitarisierung versteht man die Bereinigung einer Meldung von schutzbedürftigen Informationsanteilen. Ziel der Sanitarisierung 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.

SCHADPROGRAMM/SCHADSOFTWARE
Siehe bitte MALWARE.

SPAM
Unter Spam versteht man unerwünschte Nachrichten, die massenhaft und ungezielt per E-Mail oder über andere Kommunikationsdienste versendet werden. In der harmlosen Variante enthalten Spam-Nachrichten meist unerwünschte Werbung. Häufig enthält Spam jedoch auch Schadprogramme im Anhang, Links zu verseuchten Webseiten oder wird für Phishing-Angriffe genutzt.

SPEAR-PHISHING
Spear-Phishing ist eine Spezialform eines Phishing-Angriffs, bei dem nicht breitflächig, sondern nur ein kleiner Empfängerkreis (häufig Führungskräfte oder Wissensträger auf Leitungsebene) attackiert wird. Voraussetzung für einen erfolgreichen Angriff ist eine gute Vorbereitung und die Einbettung des Angriffs in einen für das Opfer glaubwürdigen Kontext. Spear-Phishing richtet sich in der Regel nicht gegen allgemein nutzbare Dienste wie Online-Banking, sondern gegen Dienste, die für Angreifer einen besonderen Wert haben.

SPOOFING
Spoofi ng (von 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.

SPYWARE
Damit sind Programme gemeint, 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, fälschlicherweise häufig 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 Wirtsprogrammes für seine Installation durch den Benutzer.

V.

VERSCHLÜSSELUNG
Bei der Verschlüsselung (Chiffrieren) wird ein Klartext in Abhängigkeit von einer Zusatzinformation, die „Schlüssel“ genannt wird, in einen zugehörigen Geheimtext (Chiffrat) transformiert, der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation – die Zurückgewinnung des Klartextes aus dem Geheimtext – wird Entschlüsselung genannt.

VIREN
Die klassische Form von Schadsoftware, die sich selbst verbreitet und unterschiedliches Schadpotenzial in sich tragen kann (von gar keiner 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.

W.

WURM
Computer-, Internet- oder E-Mail-Würmer bezeichnen eine Schadsoftware, die, ähnlich einem Virus, sich selbst reproduziert und durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet.

Z.

ZERO-DAY-EXPLOIT
Hierbei handelt es sich um die Ausnutzung einer Schwachstelle, die nur dem Entdecker bekannt ist. Die Öffentlichkeit und insbesondere der Hersteller des betroffenen Produkts erlangen in der Regel erst dann Kenntnis von der Schwachstelle, wenn Angriffe entdeckt werden, die auf dieser Schwachstelle basieren. Der Begriff Zero-Day leitet sich also davon ab, dass ein entsprechender Exploit bereits vor dem ersten Tag der Kenntnis der Schwachstelle durch den Hersteller existierte – also an einem fiktiven „Tag Null". Der Hersteller hat somit keine Zeit, die Nutzer vor den ersten Angriffen zu schützen.

ZUGRIFF
Ein Zugriff beschreibt die Nutzung von Daten oder Informationen. Über entsprechende Zugriffsberechtigungen wird geregelt, welche Personen im Rahmen ihrer Funktionen oder welche IT-Anwendungen bevollmächtigt sind, Informationen, Daten oder auch IT-Anwendungen, zu nutzen oder Transaktionen auszuführen.

Quelle: Bundesamt für Sicherheit in der Informationstechnik.
Dort finden Sie auch weitere spannende wie komplexe Begriffserläuterung rund um das Thema Cyber-Sicherheit.

SICHER VON A BIS Z

Sicherheit ist trügerisch. Trotz bester EDV-Technik, teurer Systeme und aufgeklärter Mitarbeiter bleibt immer ein Restrisiko, das ein passgenaues Versicherungskonzept absichert. Markel Pro IT schützt Ihre Kunden umfassend und passgenau vor Schäden an Computersystemen und digitalen Archiven sowie bei technischen Defekten, kriminellen Angriffen oder Untreue. Markel Pro Cyber, eine gezielte Cyber-Versicherung für Endkunden und Vermittler, rundet das Sicherheitspaket sinnvoll ab. Beide Produkte enthalten das kostenfreie Cyber-Präventionspaket in der Basis-Variante, womit sich Ihre Kunden zum Thema Cybersicherheit präventiv schulen können.