Fachbegriff	Erklärung
Adware	Als Adware werden Programme bezeichnet, die sich über Werbung finanzieren. Auch Schadprogramme, die Werbung für den Autor des Schadprogramms generieren, gehören zu dieser Kategorie.
Backdoors	Backdoor (auch Trapdoor oder Hintertür) bezeichnet einen (oft vom Autor eingebauten) Teil einer Software, der es Benutzern ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Computerprogramms zu erlangen.
BOT-Net	Als Botnet wird ein Verbund von Rechnern (Systemen) bezeichnet, die von einem fernsteuerbaren Schadprogramm (Bot) befallen sind. Die betroffenen Systeme werden vom Botnet-Betreiber mittels eines Command-and-Control-Servers (C&C-Server) kontrolliert und gesteuert.
Bots	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.
Brute-Force-Attack	Bei einer Brute-Force-Attacke handelt es sich um eine Methode, die versucht Passwörter oder Schlüssel durch automatisiertes, wahlloses Ausprobieren herauszufinden. Lange Schlüssel und komplexe Passwörter bieten Schutz gegen die Brute-Force-Methode.
Camfecting	Beim Camfecting verschaffen sich Hacker per Remote-Verbindung Zugriff auf private Webcams in Laptops. Der Eingriff in die Privatsphäre wird durch Trojaner möglich, die sich Nutzer häufig durch das Downloaden kostenloser Software einfangen. Gefährdet sind auch Smart-TVs, die über eine Kamera und ein Mikrofon verfügen.
CEO-Fraud	Der CEO Fraud ist eine Betrugsmasche, bei der Firmen unter Verwendung falscher Identitäten zur Überweisung von Geld manipuliert werden. „CEO“ steht für Chief Executive Officer und bedeutet sinngemäß Geschäftsführer. Fraud ist das englische Wort für Betrug.
Clickjacking	Clickjacking ist eine Technik, bei der ein Computerhacker die Darstellung einer Internetseite überlagert und dann deren Nutzer dazu veranlasst, scheinbar harmlose Mausklicks und/oder Tastatureingaben durchzuführen.
Credentials-Fraud	Es bezeichnet den Diebstahl von Geschäftsgeheimnissen zu Rezepturen beispielsweise bei chemischen Produkten oder auch produktionstechnischen Verfahrensweisen.

Fachbegriff	Erklärung
Crime-as-a-Service	Crime-as-a-Service ist eine Ableitung des Begriffs „Software as a Service“ (SaaS). Während Saas davon ausgeht, dass die gesamte IT oder Teilbereiche bei einem externen IT-Dienstleister betrieben und vom Kunden als Service genutzt werden, werden beim Crime-as-a-Service analog die Dienste Krimineller im Dark Web „eingekauft“, die für eine Straftat benötigt werden.
Cross-Site-Scripting	Cross-Site-Scripting bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden.
Crypto-Mining	Als Crypto-Mining ist das „Abschürfen“ von Einheiten einer Cryptowährung wie Bitcoin zu verstehen. Da solche rein digitalen Währungen nicht von Staaten oder Banken verwaltet und ausgegeben werden, benötigen sie sogenannte Cryptominer, die sämtliche Transaktionen aufzeichnen, verifizieren und verbuchen.
Darknet	Das Darknet ist ein loser Verbund von vielen privaten Computern, die als Peer-to-Peer-Netz untereinander verbunden sind und zwischen denen die Daten häufig verschlüsselt übertragen werden. Der Zugang zum Darknet erfolgt über das TOR-Programm, wobei TOR für The Onion Router (TOR) steht.
Denial-of-Service (DoS)	Denial-of-Service (DoS)-Angriffe richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Wird ein solcher Angriff mittels mehrerer Systeme parallel ausgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig durch eine sehr große Anzahl von Computern oder Servern.
Domain-Hijacking	Unter Domain-Hijacking versteht man die Entführung fremder Domainnamen. Als Domain Hijacking bezeichnet man den Versuch, sich die Domain einer fremden Internetseite (URL) dadurch anzueignen, dass man behauptet, die Domain stehe aufgrund eines eingetragenen Markennamens einem selbst zu.

Fachbegriff	Erklärung
Drive-by-Exploits	So genannte Drive-By-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC und zählen zu den Hauptinfektionsquellen von Rechnern. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Browser, in Browser-Plugins oder im Betriebssystem ausgenutzt, um Schadsoftware wie Trojaner unbemerkt auf dem PC zu installieren.
Fuzzing	Fuzz-Testing oder Fuzzing ist eine Methode zum Testen von Software, mit der Programmierfehler und Sicherheitslöcher in Anwendungen, Betriebssystemen und Netzwerken entdeckt werden sollen. Ihre Eingabeschnittstellen werden dabei mit zufälligen Daten, genannt Fuzz, überflutet, um sie zum Abstürzen zu bringen.
Hacking	Hacking ist ein Begriff, der auch als Synonym für „clevere Programmierer“ verwendet wird. Ein Ausdruck für Personen, die versuchen in Computer-Systeme einzubrechen.
Injection-Attack	Der Angreifer versucht dabei, über die Anwendung, die den Zugriff auf die Datenbank bereitstellt, eigene Datenbankbefehle einzuschleusen. Sein Ziel ist es, Daten auszuspähen, in seinem Sinne zu verändern, die Kontrolle über den Server zu erhalten oder einfach größtmöglichen Schaden anzurichten.
Jamming	Eine Jamming-Attacke ist eine Art DoS-Attacke, bei der ein Kanal von Hackern so belegt wird, dass er von anderen Nutzern nicht mehr zur Kommunikation verwendet werden kann. Besonders gängig ist dabei der Angriff auf Radio Frequenzen.
Malware	Unter „Malware“ versteht man eine Software (wie z. B. Viren, Würmer usw.), die in Computersysteme eindringt und dort Störungen oder Schäden verursachen kann.
Man-in-the-Middle	Phishing-Betrügern gelingt es mithilfe von Malware, sich in den Kommunikationsweg zwischen Bankkunde und Bank zwischenzuschalten (Man-in-the-Middle-Angriff) und Daten abzugreifen, die in Folge nie bei der Bank ankommen. Der Umweg, den Bankkunden über das Versenden einer E-Mail zur Preisgabe seiner Zugangsdaten zu verleiten, ist damit nicht mehr notwendig.
Nicknapping	Eine besondere Form des Identitätsdiebstahls stellt das Nicknapping dar: Das Auftreten im Internet unter dem Namen oder Pseudonym eines anderen Diskussionsteilnehmers oder Benutzers.

Fachbegriff	Erklärung
Pharming	Es ist eine Weiterentwicklung des klassischen Phishings, bei der nicht nur die Website, sondern auch die Internetadresse gefälscht ist, sodass Nutzer auch mit korrekt eingegebenen Internetadressen gefälschte Websiten aufrufen. Sie basiert auf einer Manipulation der DNS-Anfragen von Webbrowsern (beispielsweise durch DNS-Spoofing), um den Benutzer auf gefälschte Webseiten umzuleiten.
Phishing	Das Wort setzt sich aus den Begriffen „password“ und „fishing“ zusammen und bedeutet soviel wie „nach Passwörtern angeln“. Angreifer versuchen dabei, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internetnutzers zu gelangen und diese für ihre Zwecke zu missbrauchen – meist zulasten des Opfers.
Poisoning	Poisoning ist ein IT-Sicherheitsangriff auf das Domain Name System, um die Zuordnung zwischen einem Domainnamen und der zugehörigen IP-Adresse zu fälschen. Der Zweck ist es, Datenverkehr unbemerkt zu einem anderen Computer zu lenken.
Ransom	Als Ransomware werden Schadprogramme bezeichnet, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. „ransom“) wieder freigeben. Es handelt sich dabei um einen Angriff auf das Sicherheitsziel der Verfügbarkeit und eine Form digitaler Erpressung.
Replay Attack	Ein Replay Attack basiert auf der Wiedereinspielung von vorher gesammelten Daten für die Authentifizierung und die Zugriffskontrolle. Der Angreifer arbeitet mit Identitätsdiebstahl und benutzt dabei die erfassten Daten mit denen er eine fremde Identität vortäuscht, um damit auf Ressourcen und Datenbestände zugreifen zu können.
Reverse Engineering	Reverse Engineering bezeichnet die Umkehrung des Entwicklungs- bzw. Produktionsprozesses vom Produkt hin zur Konstruktionszeichnung bzw. zum Quellcode. Einsatzgebiete des Reverse Engineerings sind die Produktentwicklung, die Qualitätsprüfung und die Fehlersuche.
Rootkits	Der Begriff Rootkit beschreibt Schadprogramme, die PCs infizieren und dem Angreifer erlauben, verschiedene Programme darauf zu installieren, die ihm dauerhaften Zugriff auf den Computer ermöglichen. Das Schadprogramm wird üblicherweise tief im Betriebssystem versteckt und ist so programmiert, dass es die Entdeckung durch Antivirus-Software und andere Security-Lösungen erschwert.

Fachbegriff	Erklärung
Scareware	Scareware (Das Wort setzt sich aus engl. scare „erschrecken“ und „Software“ zusammen) ist ein Schadprogramm, das Computerbenutzer verängstigen und so zu bestimmten Handlungen bewegen soll. Sie gilt als automatisierte Form des Social Engineering.
Skimming	Beim Skimming werden illegal Kartendaten erlangt, indem Daten von Magnetstreifen ausgelesen und auf gefälschte Karten kopiert werden.
Social Engineering	Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Sowohl im Bereich der Cyber-Kriminalität als auch bei der Spionage gehen die Täter geschickt vor, um vermeintliche menschliche Schwächen wie Neugier oder Angst auszunutzen und so Zugriff auf sensible Daten und Informationen zu erhalten.
Spam	„Spam“ sind 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	Eine neuere Variante des Phishing wird als Spear-Phishing bezeichnet, worunter ein gezielter Angriff zu verstehen ist. Hierbei beschafft sich der Angreifer z. B. über die Studentenvertretung einer Hochschule die Mailadressen der dort eingeschriebenen Studenten, um an diese gezielt eine Phishing-Mail einer lokal ansässigen Bank oder Sparkasse zu übersenden. Die „Trefferquote“ bei dieser Art von Phishing-Attacken ist höher als bei normalen Angriffen, da die Wahrscheinlichkeit, dass ein Student seine Bankverbindung bei diesem Institut unterhält, sehr groß ist.
Spoofing	Spoofing nennt man verschiedene Täuschungsversuche in Computernetzwerken zur Verdeckung bzw. Verschleierung der eigenen Identität.
Spyware	„Spyware“ sind Schnüffel- oder Ausspähprogramme. Sie werden auf den Rechner oder das Smartphone geschleust, um Informationen zu sammeln und weiterzuleiten. Spyware wird vom Nutzer oft unbemerkt mit einem Programm installiert.

Fachbegriff	Erklärung
Trojaner	Bei einem Trojaner handelt es sich um ein getarntes Computerprogramm. Während die nützliche Anwendung im Vordergrund läuft, wird das Schadprogramm im Hintergrund aktiv. Es versteckt sich vor dem Nutzer, der in den meisten Fällen nichts von den Hintergrundaktivitäten mitbekommt. Häufig wird der Begriff auch synonym zum Computervirus verwendet.
Viren	Unter Computerviren versteht man selbst verbreitende Computerprogramme, welche sich in andere Computerprogramme einschleusen und damit reproduzieren.
Watering Hole Attack	Ein Watering Hole Attack ist ein Security Exploit, bei dem ein Cyberkrimineller eine bestimmte Gruppe an Endanwendern anvisiert. Dabei werden Websites infiziert, von denen Angreifer wissen, dass die Mitglieder der Zielgruppe sie immer wieder aufsuchen. Das Ziel ist es, den Computer eines Opfers zu infizieren und sich damit Zugriff auf das Netzwerk an dessen Arbeitsstelle zu verschaffen.
Whaling	Der Begriff „Whaling“ ist ein Wortspiel, das sich darauf bezieht, dass eine wichtige Person gerne als „dicker Fisch“ – oder in unserem Fall „Phish“ – bezeichnet wird. Whaling trägt alle Merkmale von Phishing, es wird jedoch kein großes Netz ausgeworfen, sondern der Betrug richtet sich gezielt gegen einen ganz bestimmten Endnutzer, etwa einen ranghohen Manager, einen Datenbankadministrator oder einen Prominenten.
Würmer/Wurm	Ein Computerwurm (im Computerkontext kurz Wurm) ist ein Schadprogramm (Computerprogramm oder Skript) mit der Eigenschaft, sich selbst zu vervielfältigen, nachdem es einmal ausgeführt wurde. In Abgrenzung zum Computervirus verbreitet sich der Wurm, ohne fremde Dateien oder Bootsektoren mit seinem Code zu infizieren.