Glossar

Abmelden

Ist der Abmeldevorgang des Benutzers. Damit weist der Benutzer das System an, die aktuelle Sitzung zu beenden.

siehe auch: Anmelden (https://www.ebas.ch/glossary/anmelden/)

Advanced Encryption Standard (AES)

Ist eine Methode zur Verschlüsselung von Daten. AES kann z.B. zur Verschlüsselung der Übertragung in einem WLAN (WPA2, WPA3) verwendet werden. Dadurch wird alles verschlüsselt, was zwischen WLAN-Router und einem drahtlos verbundenen Gerät ausgetauscht wird.

siehe auch: Wi-Fi Protected Access (WPA) (https://www.ebas.ch/glossary/wi-fi-protected-access/) , Wireless Local Area Network (WLAN) (https://www.ebas.ch/glossary/wireless-local-area-network/)

Adware

Setzt sich aus dem englischen Wort «advertisement» (deutsch Reklame, Werbung) und «Software» zusammen und bezeichnet Programme, welche dem Benutzer zusätzlich zur eigentlichen Programmfunktion Werbung anzeigt oder weitere Software installiert, um Werbung anzuzeigen.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

American Standard Code for Information Interchange (ASCII)

Ist eine Zeichenkodierung, welche 95 druckbare und 33 nicht druckbare Zeichen enthält. Die druckbaren Zeichen umfassen das lateinische Alphabet (A-Z, a-z), die zehn arabischen Ziffern (0-9) sowie einige Interpunktionszeichen (Satzzeichen, Wortzeichen) und andere Sonderzeichen.

siehe auch: Unicode (https://www.ebas.ch/glossary/unicode/)

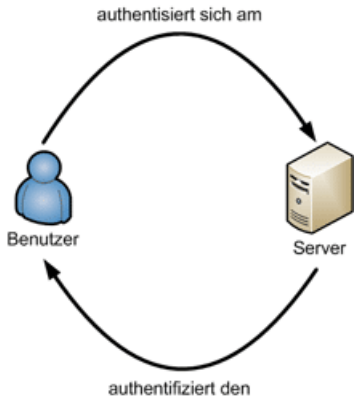
Anmelden

Ist der Anmeldevorgang, z.B. für die Nutzung eines Geräts oder eines Online-Dienstes. In der Regel dient der Vorgang dazu, dem System mitzuteilen, dass nun eine Sitzung beginnt und dass der Benutzer mit einem Benutzerkonto, z.B. dem E-Banking-Konto, verknüpft werden möchte.

siehe auch: Abmelden (https://www.ebas.ch/glossary/abmelden/) , Authentifizierung (https://www.ebas.ch/glossary/authentifizierung/)

Authentifizierung

Ist ein Vorgang, bei dem die vorgegebene Identität einer Person oder eines Geräts an Hand eines oder mehrerer bestimmter Merkmale (z.B. Passwort, Chipkarte oder Fingerabdruck) überprüft wird.



siehe auch: Zwei-Faktor-Authentifizierung (2FA) (https://www.ebas.ch/glossary/zwei-faktor-authentifizierung/) , Autorisierung (https://www.ebas.ch/glossary/autorisierung/)

Autorisierung

Das Zuweisen von Berechtigungen. Auf der Grundlage von Berechtigungen wird die Erlaubnis erteilt, nach einer erfolgreichen Identifizierung und Authentifizierung auf Ressourcen (z.B. Dateien, Software, Zahlungen etc.) zuzugreifen.

siehe auch: Authentifizierung (https://www.ebas.ch/glossary/authentifizierung/)

Backdoor

Das englische Wort für «Hintertür». Bei einer Software bedeutet dies ein meist nicht dokumentierter Zugang, über den der Hersteller (oder Dritte) von aussen auf die Software oder auf die Daten des Benutzers zugreifen kann.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Backup

Datensicherung, bei der elektronische Informationen (Daten) auf ein externes Speichermedium (z.B. auf eine externe Festplatte) kopiert werden. Backups werden in der Regel nach einem regelmässigen Zeitplan durchgeführt.

Benutzername

Ist der Name, mit dem sich ein Benutzer gegenüber einem System authentisiert. Bei der Anmeldung an einem Programm oder einem Dienst (z.B. beim E-Banking) werden in der Regel ein Benutzername und ein Passwort abgefragt. Diese dienen zur Identifikation des berechtigten Benutzers.

siehe auch: Authentifizierung (https://www.ebas.ch/glossary/authentifizierung/) , Anmelden (https://www.ebas.ch/glossary/anmelden/)

Betriebssystem

Ein Programm des Geräts, welches Systemressourcen wie Prozessor, Speicherelemente und die Ein- und Ausgabegeräte verwaltet und diese Ressourcen Anwendungsprogrammen (Software) zur Verfügung stellt. Bekannte Betriebssysteme sind z.B. Windows, macOS, Linux, Android und iOS.

Bit

Ist die kleinste Informationseinheit in der elektronischen Datenverarbeitung und entspricht einem ja/nein-Entscheid, oder einer 0/1 in einem digitalen Datensatz.

Blockchain

Eine Reihe von verbunden und mit kryptographischen Verfahren gesicherten Informations-Blöcken. Die bekannteste Blockchain-Anwendung ist Bitcoin, wo die Blockchain das manipulationssichere Kontobuch mit den Transaktionen darstellt.

siehe auch: Kryptowährung (https://www.ebas.ch/glossary/kryptowaehrung/)

Bluetooth

Ist ein Standard für die Funkkommunikation über kurze Distanz. Die Übertragungsleistung beträgt bis zu 2 MBit pro Sekunde bei einer Reichweite von bis zu 100 Metern.

Botnetz

Sind Netzwerke aus meist mehreren Tausend Geräten, welche nach einer Infektion mit Malware zusammengeschlossen werden. Betreiber illegaler Botnetze installieren die Bots meist ohne Wissen der Inhaber auf den Geräten und nutzen die Ressourcen dieser für ihre Zwecke, wie verteilte DDoS-Angriffe, den Versand von Spam-Mails oder dem Schürfen von Kryptowährungen. Die meisten Bots können von einem Botnetz-Operator über einen Kommunikationskanal überwacht werden und Befehle empfangen.

siehe auch: Distributed Denial-of-Service (DDoS) (https://www.ebas.ch/glossary/distributed-denial-of-service/) , Malware (https://www.ebas.ch/glossary/malware/) , Kryptowährung (https://www.ebas.ch/glossary/kryptowaehrung/)

Browser

Spezielles Programm zur Darstellung von Webseiten im World Wide Web (WWW) oder allgemein von Dokumenten und Daten. Die wichtigsten Browser im Bereich des Internets sind Google Chrome, Mozilla Firefox, Microsoft Edge und Apple Safari.

siehe auch: World Wide Web (WWW) (https://www.ebas.ch/glossary/world-wide-web/)

Bundesamt für Cybersicherheit (BACS)

Das Bundesamt für Cybersicherheit (BACS) ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die koordinierte Umsetzung der Nationalen Cyberstrategie (NCS).

Cache

Bezeichnet einen schnellen Zwischenspeicher, um Daten (bei wiederholten Zugriffen) rasch bereitzustellen. Im Kontext des Internets speichern Browser Inhalte von besuchten Webseiten, damit diese bei einem späteren Besuch nicht erneut heruntergeladen werden müssen und die Seite folglich schneller angezeigt werden kann.

Carding

Beschreibt das Handeln, Verbreiten und Verwenden von illegalen Kreditkarten. Die Aktivitäten umfassen auch die Ausnutzung persönlicher Daten und die Geldwäscherei.

Cookie

Sind Textdateien, die beim Aufruf von Webseiten generiert und auf den Geräten der Besucher gespeichert werden. Damit wird es möglich, Besucher bei künftigen Aufrufen wieder zu erkennen. Die Besucher können auf diese Weise etwa automatisch angemeldet oder Artikel im Warenkorb können wiederhergestellt werden.

Cookies werden allerdings auch von Werbenetzwerken dazu verwendet, das Nutzungsverhalten der Benutzer aufzuzeichnen und gezielte Werbung anzuzeigen.

Darknet

Im Darknet können sich Internetnutzer fast komplett anonym bewegen. Dieser Bereich des Internets wird von Menschen genutzt, die viel Wert auf Privatsphäre legen oder in einem repressiven politischen System leben – aber auch sehr oft von Kriminellen.

Digitale Signatur

Ist ein digitales Siegel, das einen eindeutigen und nicht manipulierbaren Zusammenhang zwischen einer natürlichen Person und einem elektronischen Dokument (z.B. E-Mail) herstellt. Aus dem zu signierenden Dokument wird nach einer bestimmten Rechenvorschrift eine Checksumme (Hashwert) berechnet. Die Checksumme wird mit dem geheimen Signaturschlüssel des Senders verschlüsselt und mit dem Originaldokument an den Empfänger gesandt. Dieser erzeugt unter Verwendung der gleichen Rechenvorschrift erneut einen Hashwert aus dem Dokument. Ausserdem entschlüsselt er mit dem öffentlichen Schlüssel des Senders den ihm zugesandten Hashwert, den der Sender zu Beginn erzeugt hat. Sind beide Hashwerte gleich, so kann er davon ausgehen, dass das Dokument unverändert bei ihm angekommen ist und der Sender tatsächlich derjenige ist, den er vorgibt zu sein.

Distributed Denial-of-Service (DDoS)

Ein DDoS-Angriff ist ein verteilter Angriff auf die Webseite oder die Server eines Unternehmens. Viele Geräte (die meist Teil eines Botnetzes sind) bombardieren dabei das Ziel mit unzähligen Anfragen. Das Resultat: Die Webseite oder die Server gehen wegen Überlastung in die Knie und sind nicht mehr oder nur noch eingeschränkt erreichbar. Hinter DDoS-Angriffen auf Unternehmen steckt oft ein Erpressungsversuch. Wird nicht bezahlt, drohen die Kriminellen, die Angriffe zu wiederholen.

siehe auch: Botnetz (https://www.ebas.ch/glossary/botnetz/)

Domain (Domainname)

Ist der Name, unter dem eine Ressource (wie z.B. eine Webseite) erreichbar ist. Jede Domain besteht aus mehreren Teilen, die durch Punkte voneinander getrennt sind. Die Domain dieser Webseite lautet z.B. www.ebas.ch (http://www.ebas.ch) .

Domain Name System (DNS)

Ist ein Dienst im Internet, welcher einen Domain Namen (z.B. www.ebas.ch) in die zugehörige IP-Adresse (217.26.54.120) umwandelt.

Drive-By-Download

Ist die Infektion eines Geräts mit Malware allein durch den Besuch einer Webseite. Vielfach beinhalten die betroffenen Webseiten seriöse Angebote und sind zwecks Verteilung der Malware zuvor kompromittiert worden. Das alleinige «Ansurfen» einer betroffenen Webseite genügt, um das Gerät zu infizieren.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Dropper und Downloader

Bei einem Dropper (Malware) handelt es sich um ein kleines Programm, dessen einzige Aufgabe darin besteht, eine (meist umfangreichere) Malware auf einem System auszuführen.

Ein Downloader ist ein Dropper, welcher die Malware aus dem Internet nachlädt.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Exploit

Ein **Exploit** (engl. to exploit: ausnutzen) bezeichnet ein Schadprogramm, welches eine bestimmte Schwachstelle gezielt ausnutzt, um ein System zu kompromittieren.

Fingerabdruck

Ist ein Verfahren, mit dem ein kryptografischer Schlüssel überprüft werden kann, ohne den gesamten Schlüssel abgleichen zu müssen. Damit lässt sich z.B. die Echtheit eines Zertifikats überprüfen, das einer TLS/SSL-Verbindung zugrunde liegt. Ein Fingerabdruck wird meist als hexadezimale Zeichenfolge bestehend aus den Buchstaben A-F und den Ziffern 0-9 dargestellt.

Firewall

Ist ein Sicherungssystem, das ein Rechnernetz oder eine einzelnes Gerät vor unerwünschten Netzwerkzugriffen schützt.

Hyperlink

Ist ein Querverweis, z.B. auf Webseiten, der beim Anklicken einen Sprung zu einem anderen elektronischen Dokument oder an eine andere Stelle innerhalb eines Dokuments ermöglicht. Im WWW können die Zieladressen solcher Sprünge auch andere Webseiten sein.

Impersonation

Auftreten unter falscher Identität. Im Kontext des E-Bankings bedeutet dies, dass sich eine Drittperson mit fremden Zugangsdaten und damit unter fremdem Namen bei einem Finanzinstitut anmeldet. Die Drittperson verfügt somit über uneingeschränkten Zugriff auf die Konten. Das Finanzinstitut kann dabei kaum noch unterscheiden, ob es mit dem Kunden selbst, mit einem beauftragten Mittelsmann oder mit einem kriminellen Angreifer kommuniziert. Impersonation wird bei klassischen Phishing-Angriffen (https://www.ebas.ch/phishing/) und beim Zugriff durch Drittanbieter auf Bankkonten (https://www.ebas.ch/zugriff-durch-drittanbieter-auf-bankkonten/) verwendet.

Internet der Dinge, Internet of Things (IoT)

Sammelbegriff für Technologien, welche es ermöglichen, physische oder virtuelle Gegenstände zu vernetzen und miteinander kommunizieren zu lassen. Die Geräte verfügen im Allgemeinen über Sensoren, um Information aus ihrer Umgebung aufzunehmen, und eingebettete Software, um Daten mit anderen Geräten und Systemen zu verknüpfen und auszutauschen. Typische Beispiele sind Haussteuerung (Heizung), Gesundheitsmonitoring (Sportuhren) oder Umweltüberwachung (Wetterstationen).

Internetprotokoll-Adresse

Ist eine Adresse in Computernetzwerken, die auf dem Internetprotokoll (IP) basiert. Sie wird Geräten zugewiesen, die an das Netz angebunden sind, und macht die Geräte so adressierbar und damit erreichbar.

siehe auch: Transmission Control Protocol/Internet Protocol (TCP/IP) (https://www.ebas.ch/glossary/transmission-control-protocol-internet-protocol/) , Domain Name System (DNS) (https://www.ebas.ch/glossary/domain-name-system/)

Investment Fraud

Investment Fraud, auch Anlagebetrug genannt, bezeichnet eine Form des Betrugs, bei der Investoren durch falsche oder irreführende Informationen dazu verleitet werden, in Projekte oder Produkte zu investieren. Diese Investitionsmöglichkeiten sind oft fiktiv, stark überbewertet oder ihre Risiken werden bewusst verschleiert. Das Ziel dieser Täuschung ist es, Geld von den Investoren zu erhalten, wobei die versprochenen Renditen oder Vorteile oft unrealistisch hoch sind.

Jailbreak

Nicht-autorisiertes Entfernen von Nutzungsbeschränkungen besonders bei Smartphones. Mittels entsprechender Software wird bei einem «Jailbreak» das Betriebssystem modifiziert, um Zugriff auf interne Funktionen sowie das Dateisystem zu erhalten. Dadurch kann die Sicherheit und die Stabilität des Betriebssystems wesentlich beeinträchtigt werden.

Java

Ist eine objektorientierte und plattformunabhängige Programmiersprache. Zur Ausführung von Java-Programmen muss auf dem Computer die Java-Laufzeitumgebung installiert sein.

JavaScript

Ist eine Skriptsprache zur dynamischen Gestaltung von Webseiten. Mit JavaScript können Inhalte verändert oder nachgeladen werden und so z.B. Suchvorschläge bereits während der Eingabe angezeigt werden.

Keylogger

Malware, welche die Tastatureingaben des Benutzers protokolliert, in der Hoffnung, dort Anmeldedaten wie z.B. Passwörter zu ergattern.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Krypto-Mining

Beim Krypto-Mining werden Einheiten (Coins) einer Kryptowährung (z.B. Bitcoin) erzeugt und neue Transaktionen verifiziert. Weil Kryptowährungen im Allgemeinen nicht von einer übergeordneten Instanz ausgegeben werden, benötigen sie sogenannte Krypto-Miner, die sämtliche Transaktionen aufzeichnen, verifizieren und verbuchen

siehe auch: Kryptowährung (https://www.ebas.ch/glossary/kryptowaehrung/)

Krypto-Wallet

Kryptowährungen werden digital in sogenannten Wallets (deutsch: Brieftasche) aufbewahrt und in diesen mit Zugangscodes geschützt.

siehe auch: Kryptowährung (https://www.ebas.ch/glossary/kryptowaehrung/)

Kryptographie

Wissenschaft der Verschlüsselung, um Informationen geheim zu übertragen und abzuspeichern.

Kryptowährung

Kryptowährungen sind digitale Tausch- bzw. Zahlungsmittel bzw. Vermögenswerte, welche kryptografische Verfahren nutzen, um die Sicherheit des Zahlungssystem zu gewährleisten. Werden Systeme durch Schadsoftware lahmgelegt, verlangen Cyberkriminelle in der Regel eine Bezahlung in einer Kryptowährung (z.B. Bitcoins), um eine Nachverfolgbarkeit zu verunmöglichen.

Local Area Network (LAN)

Ist ein lokales Netzwerk. In einem solchen sind die Arbeitsstationen, Server und Zusatzgeräte über eine Entfernung von bis zu wenigen hundert Metern miteinander verbunden, in der Regel innerhalb eines Gebäudes oder eines Gebäudekomplexes.

siehe auch: Wireless Local Area Network (WLAN) (https://www.ebas.ch/glossary/wireless-local-area-network/)

Makro

Einige Programme (z.B. Microsoft Office, Adobe Acrobat) erlauben es den Benutzern, gewisse Tätigkeiten mit kleineren Programmen – sogenannten Makros, Aktionen oder Skripte – zu automatisieren. Diese werden allerdings von Angreifern gerne auch verwendet, um unscheinbar aussehende Dokumente mit bösartigem Code (Malware) zu versehen.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Malware

Setzt sich aus den englischen Begriffen «malicious» (bösartig) und «Software» zusammen. Malware ist der Oberbegriff für Software, die schädliche Funktionen auf einem Gerät ausführt (wie z.B. Viren, Würmer, Trojaner, Ransomware).

siehe auch: Adware (https://www.ebas.ch/glossary/adware/) , Backdoor (https://www.ebas.ch/glossary/backdoor/) , Botnetz (https://www.ebas.ch/glossary/botnetz/) , Drive-By-Download (https://www.ebas.ch/glossary/drive-by-download/) , Keylogger (https://www.ebas.ch/glossary/keylogger/) , Ransomware (https://www.ebas.ch/glossary/ransomware/) , Rootkit (https://www.ebas.ch/glossary/rootkit/) , Scareware (https://www.ebas.ch/glossary/scareware/) , Session-Riding (https://www.ebas.ch/glossary/session-riding/) , Spyware (https://www.ebas.ch/glossary/spyware/) , Trojanisches Pferd (https://www.ebas.ch/glossary/trojanisches-pferd/) , Virus (https://www.ebas.ch/glossary/virus/) , Wurm (https://www.ebas.ch/glossary/wurm/)

Man-in-the-Middle (MitM)

Bei einem Man-in-the-Middle-Angriff greift eine Drittperson oder eine Malware in die E-Banking-Sitzung ein, indem sie sich unbemerkt zwischen das Gerät des Benutzers und den Server des Finanzinstituts schaltet und so die Kontrolle über den Datenverkehr übernimmt.

siehe auch: Phishing (https://www.ebas.ch/glossary/phishing/) , Pharming (https://www.ebas.ch/glossary/pharming/)

Media-Access-Control-Adresse (MAC-Adresse)

Ist die individuelle Identifikationsnummer eines Netzwerkgeräts (z.B. WLAN-Anschluss). Die Kennung wird in der Regel ab Werk eingestellt. Sie ist vergleichbar mit der Fahrgestellnummer eines Autos.

Money Mule

Als Money Mules (https://www.ebas.ch/money-mules-finanzagenten/) (auch Finanzagenten genannt) werden Personen bezeichnet, welche gegen Entschädigung Gelder über ihre eigenen Bankkonten empfangen und ins Ausland weiterleiten. Die Gelder stammen fast immer aus illegalen Geschäften. Rekrutiert werden Money Mules meist über lukrative Jobangebote, welche rasche und hohe Verdienstmöglichkeiten versprechen. Wer sich an solchen «Geschäften» beteiligt, riskiert ein Strafverfahren wegen Gehilfenschaft zu Geldwäscherei.

Nationales Zentrum für Cybersicherheit (NCSC)

Das Nationale Zentrum für Cybersicherheit (NCSC) heisst seit dem 1.1.2024 Bundesamt für Cybersicherheit (BACS).

Online-Banken

Internetbanken bieten ihre Produkte ausschliesslich über das Internet an. Internetbanken haben keine physischen Filialen, wodurch die Gebühren für die angebotenen Produkte vergleichsweise niedrig sind. Durch die eingeschränkte Kontaktmöglichkeit kann sich der Support bei Problemen stark zu demjenigen von herkömmlichen Finanzinstituten unterscheiden.

Passwort

Dient zur Authentifizierung. Hierbei wird eine Zeichenfolge vereinbart und benutzt, durch die sich jemand, meist eine Person, ausweist und dadurch die eigene Identität bestätigt.

Ein gutes Passwort (https://www.ebas.ch/4-schuetzen-der-online-zugaenge/) sollte mindestens 12 Zeichen lang sein und aus Ziffern, Gross- und Kleinbuchstaben sowie Sonderzeichen bestehen.

siehe auch: Authentifizierung (https://www.ebas.ch/glossary/authentifizierung/)

Patch

Ist eine Programmkorrektur, welche Bugs (Fehler) von Software repariert. Die meisten Patches werden von den Software-Herstellern auf ihren Webseiten kostenlos zum Download angeboten oder automatisch verteilt.

siehe auch: Upgrade (https://www.ebas.ch/glossary/upgrade/)

Pharming

Gehört wie das klassische Phishing zur Gruppe der Man-in-the-Middle-Angriffe. Beim Pharming erfolgt eine Umleitung auf eine gefälschte Webseite durch eine Manipulation der Zuordnung von IP-Adresse und Domain.

siehe auch: Man-in-the-Middle (MitM) (https://www.ebas.ch/glossary/man-in-the-middle/)

Phishing

Setzt sich aus den Wörtern «Password» und «Fishing» zusammen. Mittels Phishing (https://www.ebas.ch/phishing/) versuchen Kriminelle an vertrauliche Daten von ahnungslosen Internetbenutzern zu gelangen. Dabei kann es sich z.B. um Anmeldeinformationen fürs E-Banking oder Kontoinformationen von Online-Shops handeln. Die Täter nutzen die Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie etwa als Mitarbeiter vertrauenswürdiger Finanzinstitute auftreten.

Neben dem klassischen Phishing via E-Mail existieren weitere Varianten wie Vishing (Voice-Phishing oder auch Phone-Phishing), Smishing (SMS-Phishing) und QR-Phishing.

siehe auch: Man-in-the-Middle (MitM) (https://www.ebas.ch/glossary/man-in-the-middle/)

Provider

Ist der Anbieter des Internetzuganges, sprich die Organisation oder Firma, die den Benutzern den Anschluss ihres Geräts ans Internet ermöglicht.

Quick Response-Code (QR-Code)

Ursprünglich wurde der QR-Code (https://www.ebas.ch/qrcode) zur Markierung von Baugruppen und Komponenten in der Automobilproduktion entwickelt. Inzwischen werden QR-Codes auf Rechnungen (QR-Rechnung (https://www.ebas.ch/qr-rechnung/)) sowie im Publikationswesen und im Marketing verwendet, um von physischen Objekten (Produkte, Printmedien, Plakate etc.) in die Online-Welt zu verlinken und so weiterführende Informationen bereit zu stellen. Da der Inhalt von QR-Codes von Menschen nicht ohne weiteres dekodiert werden kann, muss der QR-Code, z.B. mit dem Smartphone, eingescannt werden.

Benutzer können vor dem Einlesen eines QR-Codes in der Regel nicht erkennen, welche Informationen in diesem kodiert wurden. Man sollte deshalb nach Möglichkeit einen QR-Code-Scanner (App) verwenden, der zunächst die decodierten Inhalte anzeigt und nachfragt, ob man etwa einen Link besuchen oder eine bestimmte Aktion ausführen möchte.

Beispiel des QR-Codes von «eBanking – aber sicher!»

Ransomware

Ist eine Malware, welche Dateien auf einem Gerät sowie auf allfällig verbundenen Netzlaufwerken und Speichermedien (z.B. externe Festplatten, Cloud-Speicher) verschlüsselt und danach Lösegeldzahlungen fordert.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Remote Desktop- und Terminalserver-Anwendungen (RDP)

Anwendungen, die es Benutzern ermöglichen, Computersysteme aus der Ferne zu bedienen. In erster Linie geht es darum, Bildschirmanzeige, Tastatureingaben und Mausbewegungen über längere Distanzen zwischen dem System und dem Benutzer zu transportieren.

Rootkit

Ist eine Software mit dem Ziel, bestimmte Dateien, Ordner, Prozesse oder Systemeinträge vor dem Benutzer und oft auch vor Sicherheitsprogrammen (Virenschutzprogrammen) zu verbergen. Ein Rootkit alleine ist noch nicht «schädlich», aber ein Indiz dafür, dass sich Malware auf dem Computer befindet.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Scamming

Frei übersetzt heisst Scamming «Betrügen», was in unterschiedlichen Kontexten im Internet praktiziert wird. Primäres Ziel ist es dabei, Menschen um ihr Geld zu erleichtern. Eine weit verbreitete Form ist z.B. das Romance-Scamming. Hierbei wird durch vorgegaukelte Liebe eine Beziehung aufgebaut und dann nach Geld gefragt.

siehe auch: Phishing (https://www.ebas.ch/glossary/phishing/) , Money Mule (https://www.ebas.ch/glossary/money-mule/) , Social Engineering (https://www.ebas.ch/glossary/social-engineering/)

Scareware

Setzt sich aus den englischen Begriffen «Scare» (Schrecken) und «Software» zusammen. Aufgrund von irreführenden Warnmeldungen z. B. bezüglich einer Infektion des Geräts soll der Benutzer so verängstigt und verunsichert werden, dass dieser z.B. zum Kauf von fragwürdigen «Virenschutzprogrammen» (welche nutzlos sind) gedrängt wird.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Secure Sockets Layer (SSL)

Ist die Vorgängerbezeichnung der Transport Layer Security (TLS).

siehe auch: Transport Layer Security (TLS) (https://www.ebas.ch/glossary/transport-layer-security/)

Service Set Identifier (SSID)

Ist der Name eines WLANs.

siehe auch: Wireless Local Area Network (WLAN) (https://www.ebas.ch/glossary/wireless-local-area-network/)

Session-Riding

Im Gegensatz zu Phishing und Pharming handelt es sich beim Session-Riding nicht um einen Man-in-the-Middle-Angriff. Anstatt Anmeldeinformationen über einen Angreifer umzuleiten, wird beim Session-Riding die Kommunikation mit dem Finanzinstitut noch auf dem Gerät des Opfers manipuliert. Für die Manipulation der Kommunikation ist Malware verantwortlich, die das Gerät des Opfers infiziert hat.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Sicherheitslücke

Eine Sicherheitslücke bezeichnet eine festgestellte Schwachstelle in einer Hard- oder Software, welche unter bestimmten Bedingungen ein unvorhergesehenes, ungewolltes Systemverhalten auslöst.

siehe auch: Vulnerability (https://www.ebas.ch/glossary/vulnerability/)

Social Engineering

Ist ein Angriff, der weniger auf technischem, dafür auf psychologischem Weg erfolgt. Es ist eine verbreitete Methode zum Ausspionieren von vertraulichen Informationen. Angriffsziel ist dabei immer der Mensch. Um an vertrauliche Informationen zu gelangen, wird sehr oft die Gutgläubigkeit und die Hilfsbereitschaft aber auch die Unsicherheit einer Person ausgenutzt. Von fingierten Telefonanrufen über Personen die sich als jemand anderes ausgeben bis hin zu Phishing-Attacken ist vieles möglich.

Spam

Ist der Überbegriff für unerwünschte E-Mails, welche häufig Werbung beinhalten. Phishing-Mails, welche das Entwenden persönlicher Daten des Empfängers zum Ziel haben, werden ebenfalls dazu gezählt.

siehe auch: Spamfilter (https://www.ebas.ch/glossary/spamfilter/)

Spamfilter

Filtert unerwünschte Spam-Mails aus dem Posteingang.

siehe auch: Spam (https://www.ebas.ch/glossary/spam/)

Spyware

Ist eine Malware, die Informationen über das Gerät und das Online-Verhalten des Benutzers ohne dessen Wissen aufzeichnet und weiterleitet. Die Empfänger der Informationen können dann z.B. die Gewohnheiten des Benutzers beim Surfen oder beim Online-Shopping nachvollziehen. Meistens richten sich solche Spionageprogramme während dem Installieren von Shareware- oder Freeware-Programmen auf dem Gerät ein.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Transaktionsnummer (TAN)

Ist eine Art Einmalkennwort, welches zusätzlich zu einem Passwort oder einer PIN verwendet wird. TAN können auf verschiedene Arten erzeugt und dem Benutzer angezeigt werden – z.B. die mobile TAN (mTAN), welche als SMS vom Finanzinstitut zum Benutzer übertragen wird oder die Photo-TAN, welche durch die Entschlüsselung eines farbigen Mosaiks angezeigt wird.

Transmission Control Protocol/Internet Protocol (TCP/IP)

Ist eine Protokollfamilie, die die grundlegenden Kommunikationsprotokolle des Internets umfassen. Diese werden häufig auch innerhalb eines privaten Netzwerks verwendet.

Transport Layer Security (TLS)

Ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet.

siehe auch: Secure Sockets Layer (SSL) (https://www.ebas.ch/glossary/secure-sockets-layer/)

Trojanisches Pferd

Malware, die sich im Vordergrund als nützliches Programm oder als Spiel tarnt, aber im Hintergrund in Wahrheit andere Zwecke verfolgt. Trojaner können z.B. Passwörter und andere vertrauliche Daten ausspähen, verändern, löschen oder an den Angreifer übermitteln.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/)

Unicode

Ist ein internationaler Standard, in dem langfristig für jedes Sinn tragende Schriftzeichen oder Textelement aller bekannten Schriftkulturen und Zeichensysteme ein digitaler Code festgelegt wird. Ziel ist es, die Verwendung unterschiedlicher und inkompatibler Kodierungen in verschiedenen Ländern oder Kulturkreisen zu beseitigen. Unicode wird ständig um Zeichen weiterer Schriftsysteme ergänzt.

siehe auch: American Standard Code for Information Interchange (ASCII) (https://www.ebas.ch/glossary/american-standard-code-for-information-interchange/)

Uniform Resource Locator (URL)

Die Adresse einer Webseite – z.B. https://www.ebas.ch (https://www.ebas.ch) . Im Gegensatz zur Domain umfasst die URL auch das Protokoll (z.B. https://) und ggf. weitere Angaben wie den Port (z.B. :80)

siehe auch: Domain (Domainname) (https://www.ebas.ch/glossary/domain/)

Update

Programmaktualisierung, welche oft auch Bugs (Fehler) von Software repariert. Die meisten Updates werden von den Software-Herstellern auf ihren Webseiten kostenlos zum Download angeboten oder automatisch verteilt.

siehe auch: Patch (https://www.ebas.ch/glossary/patch/) , Upgrade (https://www.ebas.ch/glossary/upgrade/)

Upgrade

Ausbau/Erweiterung eines Systems oder Software. Zunächst wurde der Begriff «Upgrade» nur für den hardwareseitigen Ausbau verwendet, inzwischen ist er (fast) gleichbedeutend mit Update. Manche Softwarehersteller unterscheiden zwischen einem kostenfreien Update (welches in der Regel Fehler etc. behebt) und einem kostenpflichtigen Upgrade (welches in der Regel auch zusätzliche Funktionen enthält).

siehe auch: Patch (https://www.ebas.ch/glossary/patch/)

Virtual Private Network (VPN)

Bezeichnet ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz. VPN wird in der Regel eingesetzt, um ein Gerät über ein bestehendes (unsicheres) Netzwerk, z.B. Internet, an ein anderes (sicheres) Netzwerk, z.B. das Firmennetz, auf sichere Art und Weise anzubinden. Dabei werden die Inhalte auf dem Transportweg mittels Verschlüsselung geschützt (Ende-zu-Ende-Verschlüsselung).

Virus

Obwohl der Begriff jedem Benutzer nach wie vor bekannt ist, gibt es heute eigentlich kaum noch echte (Computer-)Viren. Der klassische (Computer-)Virus infiziert bestehende Dateien auf einem Gerät und hofft darauf, dass eine davon einem anderen Benutzer weitergegeben wird. Wenn die Malware keine Anstrengungen unternimmt, sich selbst aktiv zu verbreiten, spricht man von einem Virus. Wenn die Malware aber auch in der Lage ist, sich automatisch z.B. via E-Mail zu verbreiten, spricht man von einem Wurm.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/) , Wurm (https://www.ebas.ch/glossary/wurm/)

Vulnerability

Eine **Vulnerability** (engl. für: Verletzlichkeit) bezeichnet eine festgestellte Schwachstelle in einer Hard- oder Software, welche unter bestimmten Bedingungen ein unvorhergesehenes, ungewolltes Systemverhalten auslöst.

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access ist eine Verschlüsselungsmethode für Drahtlosnetzwerke (WLAN), welche im Gegensatz zu WEP durch dynamische Schlüssel zusätzlichen Schutz bietet. WPA2 ist der Nachfolger von WPA, jedoch sind sowohl für WPA als auch WPA2 Schwachstellen bekannt. Aufgrund verschiedener Angriffe gegen das WPA- und WPA2-Verfahren ist die Nutzung des Nachfolgers WPA3 zu bevorzugen.

siehe auch: Advanced Encryption Standard (AES) (https://www.ebas.ch/glossary/advanced-encryption-standard/) , Wireless Local Area Network (WLAN) (https://www.ebas.ch/glossary/wireless-local-area-network/)

Wireless Local Area Network (WLAN)

Ist ein kabelloses, lokales Netzwerk beziehungsweise ein Funknetzwerk. Oft wird dafür synonym auch der Begriff Wi-Fi verwendet.

siehe auch: Advanced Encryption Standard (AES) (https://www.ebas.ch/glossary/advanced-encryption-standard/) , Local Area Network (LAN) (https://www.ebas.ch/glossary/local-area-network/) , Service Set Identifier (SSID) (https://www.ebas.ch/glossary/service-set-identifier/) , Wi-Fi Protected Access (WPA) (https://www.ebas.ch/glossary/wi-fi-protected-access/)

World Wide Web (WWW)

Das WWW wurde 1993 am europäischen Forschungszentrum für Kernphysik (CERN) in Lausanne (Schweiz) als Hypermedia-System für das Internet entwickelt. An der Entwicklung war ausserdem das NCSA (National Center for Supercomputing Applications, University of Illinois, USA) beteiligt. Inzwischen erfolgt die Weiterentwicklung durch das WWW Consortium (W3C).

siehe auch: Browser (https://www.ebas.ch/glossary/browser/)

Wurm

Auch der Wurm ist wie der Virus eine heute nicht mehr so verbreitete Malware. Ein Wurm ist ein kleines Programm, das von sich selbst Kopien weiterverbreitet, z.B. via E-Mail, SMS oder über Sicherheitslücken.

siehe auch: Malware (https://www.ebas.ch/glossary/malware/) , Virus (https://www.ebas.ch/glossary/virus/)

Zero-Day-Lücke

Eine Sicherheitslücke in einer Software, die dem Hersteller noch nicht bekannt ist und es deshalb auch noch keinen Patch gibt. «Zero-Day» bedeutet, dass zwischen der Entdeckung dieser Sicherheitslücke und dem ersten Angriff «Null Tage» liegen.

siehe auch: Exploit (https://www.ebas.ch/glossary/exploit/) , Malware (https://www.ebas.ch/glossary/malware/) , Patch (https://www.ebas.ch/glossary/patch/) , Ransomware (https://www.ebas.ch/glossary/ransomware/) , Sicherheitslücke (https://www.ebas.ch/glossary/sicherheitsluecke/) , Vulnerability (https://www.ebas.ch/glossary/vulnerability/)

Zwei-Faktor-Authentifizierung (2FA)

Bei der sogenannten Zwei-Faktor-Authentifizierung wird beim Anmelden zusätzlich zum ersten Sicherheitselement (meistens ein Passwort) ein zweites, unabhängiges Sicherheitselement abgefragt. Dies kann z.B. ein Code sein, der auf ein Mobiltelefon geschickt oder direkt auf diesem generiert wird.

siehe auch: Anmelden (https://www.ebas.ch/glossary/anmelden/) , Authentifizierung (https://www.ebas.ch/glossary/authentifizierung/)