

Glossar DMB Rechtsschutz Cyber-Check

Anti-Virus SW

Spezial Software, die Personal-Computer vor dem Befall von Computer-Viren schützt (Forderung der Datensicherheit)

App

App ist die Kurzform von Applikation. Die beliebten Anwendungen auf Smartphones haben viele Vorteile. Sie sind klein, laden schnell und sind einfacher zu navigieren als Websites. Sie sind außerdem in der Lage, native Smartphone-Funktionen wie GPS, Kameras, Telefonieren etc. effizient für die Zwecke der App zu nutzen

Bluetooth

Bluetooth ist ein in den 1990er Jahren durch die Bluetooth Special Interest Group entwickelter Industriestandard für die Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik. Dabei sind verbindungslose sowie verbindungsbehaftete Übertragungen von Punkt zu Punkt möglich. Bluetooth wird genutzt, um drahtlos beispielsweise Kontakt zu Headsets, Kopfhörern, Lautsprecher oder Druckern herzustellen. In Autos wird Bluetooth genutzt, um das Handy mit Freisprechanlage und Autoradio zu verbinden, Sportler verwenden es, um die Aufzeichnungen von Smartphones mit dem PC abzugleichen.

BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist eine in der Bundesstadt Bonn ansässige zivile obere Bundesbehörde im

Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat, die für Fragen der IT-Sicherheit zuständig ist. Der Leitsatz des BSI lautet: „Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.“.

Bully

Der Begriff umschreibt das Phänomen, dass ein einzelnes Opfer von einem oder mehreren in seiner Gruppe schikaniert und terrorisiert wird. Bullying ist identisch mit dem Phänomen Mobbing, da es weitreichende Parallelen in den Definitionen und in der Phänomen Beschreibung gibt. So wird etwa von Bullying wie von Mobbing auch im Cyber-Kontext gesprochen.

Cloud Computing

Der Begriff Cloud (deutsch Wolke) ist die Kurzform von Cloud Computing. Im Allgemeinen spricht man davon, etwas „in der Cloud zu speichern“.

Damit ist im Regelfall gemeint, Daten auf einem entfernten Internet-Server abzulegen. Die Übertragung vom Endgerät des Nutzers (PC, Tablet, Smartphone) erfolgt hierbei über das Web. Wurden die Dateien einmal in einer Cloud gespeichert, so können sie später auch mit beliebigen anderen Geräten wieder abgerufen und genutzt werden.

Typische Beispiele für ein Cloud sind Onedrive, GoogleDrive, DropBox oder iCloud.

Glossar DMB Rechtsschutz Cyber-Check

Cyberbullying

Der Begriff wird wie Cybermobbing verwendet.

Cybermobbing

Unter Cybermobbing oder Cyberbullying versteht man die Beleidigung, Bedrohung, Bloßstellung oder Belästigung von Personen mithilfe von Kommunikationsmedien wie Smartphones, E-Mails, Websites, Foren, Chats und Communities.

Cyber-Sicherheit

Der Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der Informationssicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationstechnik mit ein. Häufig wird bei der Betrachtung von Cyber-Sicherheit auch ein spezieller Fokus auf Angriffe aus dem Cyber-Raum gelegt.

Cyberstalking

Der Begriff Cyberstalking bezieht sich auf Stalking, das im Internet stattfindet. E-Mails und Nachrichten über Messenger werden als Mittel missbraucht, um eine Person zu stalken. Auch mithilfe von Beiträgen oder sozialen Netzwerken sowie

digitalen Medien setzen sich Stalker mit ihren Opfern in Verbindung.

Cyber-Versicherung

Eine Cyber-Versicherung ist eine fakultative Zusatzversicherung für Unternehmen, die Schäden im Zusammenhang mit Hacker-Angriffen oder sonstigen Akten von Cyberkriminalität absichert.

Defender

Der Windows „Defender“ (zuvor Windows AntiSpyware genannt) ist eine von Microsoft für dessen Windows entwickelter Virenschutz zur Erkennung von potenziell unerwünschter Software (vorwiegend Malware wie Computerviren und Spyware).

Doxing

Doxxing (oder Doxing) bedeutet, dass jemand im Internet private Informationen über andere Personen veröffentlicht. Die Informationen sind persönlich zuzuordnen und daher sensibel.

DSGVO

Die Datenschutz-Grundverordnung (DSGVO; Französisch Règlement général sur la protection des données RGPD, englisch General Data Protection Regulation GDPR) ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch Datenverarbeiter, sowohl private wie öffentliche, EU-weit vereinheitlicht werden. Dadurch soll einerseits der

Glossar DMB Rechtsschutz Cyber-Check

Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt, und auch andererseits der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Firewall Software

Eine Firewall (von englisch firewall, Brandwand oder Brandmauer) ist ein Sicherungssystem, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt. Weiter gefasst ist eine Firewall auch ein Teilaspekt eines Datensicherheitskonzepts. Jedes Firewall-Sicherungssystem basiert auf einer Softwarekomponente. Die Firewall-Software dient dazu, den Netzwerkzugriff zu beschränken, basierend auf Absender oder Ziel und genutzten Diensten. Sie überwacht den durch die Firewall laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden oder nicht. Auf diese Weise versucht sie, unerlaubte Netzwerkzugriffe zu unterbinden. Diese Systeme sind vor allem auch für den Schutz besonders schutzwürdiger Daten in einer Arztpraxis, Klinik und Krankenhaus, speziell auch nach dem DSGVO von hoher Priorität.

Hausnetz

Als Hausnetz bezeichnet man die elektrische Grundinstallation eines Hauses. Der Begriff wird häufig im Zusammenhang mit einer „Smart Home“ Installation verwendet.

Internet of Things

Das „Internet der Dinge“ ist eine Technologie, die es uns ermöglicht, ein Objekt (z. B. Häuser, Fahrzeuge, elektronische Anlagen, Dächer, Beleuchtungen usw.) mit einem Gerät auszustatten, das Umweltparameter messen, zugehörige Daten erzeugen und diese über ein Kommunikationsnetz übertragen kann. Das IoT basiert auf dem Einsatz verschiedener Sensoren.

IoT

Gebräuchliche Abkürzung für das „Internet of Things“

IT-System

IT-Systeme sind technische Anlagen, die der Informationsverarbeitung dienen und eine abgeschlossene Funktionseinheit bilden. Typische IT-Systeme sind Server, Clients, Mobiltelefone, Smartphones, Tablets, IoT-Komponenten, Router, Switches und Firewalls.

Onlinebanking

Der Begriff Onlinebanking bezeichnet die Abwicklung von Bankgeschäften über das Internet. Kriminelle versuchen, Konto- und Kreditkartendaten der Nutzer auszuspähen und mit ihrer Hilfe an das Geld der Bankkunden zu kommen. Onlinebanking ist wegen der bequemen Nutzung mittlerweile für viele Menschen eine Selbstverständlichkeit geworden. Nach Angaben des BITKOM Verbands erledigen über 70% der Bundesbürger ihre Bankgeschäfte online.

Glossar DMB Rechtsschutz Cyber-Check

Passwort

Mit der Eingabe eines Passwortes weist der Benutzer nach, dass er zu dem geschlossenen System eine Zugangsberechtigung hat. Dies kann zum Beispiel die Anmeldung an einem Client oder die Eingabe der Geheimzahl am Geldautomaten sein. "Passwort" stellt dabei einen Oberbegriff dar und beinhaltet Passwörter, PINs oder auch Passphrasen (Folge von aneinandergereihten Wörtern).

Personal Firewall

Eine Personal Firewall unterscheidet sich von einer herkömmlichen Firewall durch ihren Funktionsumfang. Eine Personal Firewall schützt in der Regel nur den Computer, auf dem sie installiert ist. im Gegensatz zu einer herkömmlichen Firewall, die in der Regel auf einer bestimmten Schnittstelle zwischen zwei oder mehreren Netzen installiert wird, z. B. einem Router oder Proxy-Server.

Phishing

Unter dem Begriff Phishing (Neologismus von fishing, engl. für ‚Angeln‘) versteht man Versuche, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen und damit Identitätsdiebstahl zu begehen. Ziel des Betrugs ist es, mit den erhaltenen Daten beispielsweise Kontoplünderung zu begehen und den entsprechenden Personen zu schaden. Es handelt sich dabei um eine Form des Social Engineering, bei dem die Gutgläubigkeit des Opfers ausgenutzt wird.

Der Begriff ist ein englisches Kunstwort, das sich aus password harvesting (Passwörter sammeln) und fishing (Angeln, Fischen) zusammensetzt und bildlich das Angeln nach Passwörtern mit Ködern verdeutlicht. Schutzmaßnahmen gegen Pishing können wirksam mit Awareness-Training z.B. vom BSI und einem professionellen Datenschutz-Konzept umgesetzt werden (siehe Firewall, Cyber Security etc.)

PIN / TAN

PIN-TAN-sind Begriffe des Homebankings zur Berechtigungsprüfung von Nutzern. Eine Persönliche Identifikationsnummer (personal identification number, PIN, Geheimzahl) ist eine nur dem autorisierten Verbraucher bekannte Zahl, mit der sich dieser gegenüber einer IT-Maschine authentifizieren können.

Proxy

Ein Proxy ist eine Art Stellvertreter in Netzen. Er nimmt Daten von einer Seite an und leitet sie an eine andere Stelle im Netz weiter. Mittels eines Proxys lassen sich Datenströme filtern und gezielt weiterleiten.

Proxy Server

Ein Proxy-Server fungiert als Gateway zwischen Ihnen und dem Internet. Bei ihm handelt es sich um einen vermittelnden Server, der die Endbenutzer von den Websites, die sie sich ansehen, trennt. Proxy-Server bieten ein unterschiedliches Maß an Funktionalität, Sicherheit und

Glossar DMB Rechtsschutz Cyber-Check

Datenschutz, je nach Ihrem Anwendungsfall, Ihren Bedürfnissen oder Ihren Unternehmensrichtlinien.

Ransomware

Ransomware ist ein gefährlicher Bereich der Cyberkriminalität geworden. Der Angreifer verschafft sich Zugang zum PC über eine Internetverbindung und verschlüsselt die Daten der Opfer. Anschließend verlangt er ein Lösegeld für den privaten Schlüssel zum Dekodieren der Daten. Ransomware wird unter anderem via E-Mail-Anhang, infizierte Programme und kompromittierte Websites verteilt. Security-Experten bezeichnen ein Ransomware-Malware-Programm manchmal auch als Kryptovirus, Kryptotrojaner oder Kryptowurm.

Risikoanalyse

Als Risikoanalyse wird der komplette Prozess bezeichnet, um Risiken zu beurteilen (identifizieren, einschätzen und bewerten) sowie zu behandeln.

Risikoanalyse bezeichnet nach den einschlägigen ISO-Normen ISO 31000 und ISO 27005 nur einen Schritt im Rahmen der Risikobeurteilung, die aus den folgenden Schritten besteht:

- > Identifikation von Risiken (Risk Identification)
- > Analyse von Risiken (Risk Analysis)
- > Evaluation oder Bewertung von Risiken (Risk Evaluation)

Im deutschen Sprachgebrauch hat sich allerdings der Begriff Risikoanalyse für den kompletten Prozess der Risikobeurteilung und Risikobehandlung etabliert.

Router

Ein Router ist die wesentliche Komponente für das Surfen im Internet über einen Computer. Das System ermöglicht die Kommunikation zwischen einem lokalen Netz und dem Internet. Der Router hat in der Regel die Form einer Box mit grünen und roten Leuchtsignalen, die während des Betriebs blinken und eingeschaltet bleiben. Der Router besteht aus vier Komponenten: Eingangsanschlüsse, Ausgangsports, Schaltmatrix und Prozessor. Router für das Hausnetz haben 5 oder 6 Eingangsanschlüsse, Profi-Router für Unternehmen haben ein Vielfaches davon.

Sandboxing

Im Cybersecurity-Kontext ist eine Sandbox-Umgebung eine isolierte virtuelle Maschine, in der potenziell unsichere Software ausgeführt werden kann, ohne Netzwerkressourcen oder lokale Anwendungen zu beeinträchtigen oder zu schädigen. In Windows 10 / 11 ist die Sandbox bereits fester Bestandteil des Betriebssystems.

Schadprogramm / Schadsoftware / Malware

Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware oder Malware werden häufig 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 sind Computerviren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte

Glossar DMB Rechtsschutz Cyber-Check

Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.

Schnellstart

Bezeichnung von Modulen für unterschiedliche Zielgruppen im digitalen MCSS-Ökosystem. Die Module listen wesentliche Schritte auf, wie die Systeme eingesetzt werden sollten (wie eine „Roadmap“).

Segmentierung

Segmentierung im Kontext von Cybersicherheit bedeutet Netzwerksegmentierung. Es ist ein Netzwerksicherheitsverfahren, bei dem ein Netzwerk in kleinere, separate Subnetzwerke unterteilt wird, der meist im gewerblichen Bereich verwendet wird.

Administratoren können diese Subnetzwerke dann voneinander abschotten und Sicherheitskontrollen und Services speziell für jedes Subnetzwerk bereitstellen.

Smart Home

Der Bereich Smart Home umfasst alle vernetzten Geräte, die in der Wohnung genutzt werden können. Dazu gehören Systeme, die automatisch Fenster, Türen und Rollläden öffnen bzw. schließen und sogenannte Hausautomatisierungstechnik. Zum Smart Home zählen auch Haushaltsgeräte wie Kühlschränke, mit digitalen Inhaltsmeldungen, Smart-TVs, vernetzte Lautsprecherboxen.

Smartphone

Als Smartphones bezeichnet man ein Mobiltelefon mit umfangreichen Computer-Funktionalitäten und Konnektivitäten. Der Begriff dient zur Abgrenzung von herkömmlichen Mobiltelefonen. Die Einführung des iPhones im Jahr 2007 durch Apple führte zu einer neuen Zeitrechnung im Mobiltelefon-Markt. Heute sind die meisten verkauften Mobiltelefone Smartphones. Durch den permanent mitgeführten Internetzugang löste dies einen Wandel im Internet-Nutzungsverhalten aus. Das gilt besonders bei sozialen Netzwerken und ermöglichte neue Kommunikationsformen über Dienste wie WhatsApp, Twitter und Instagram.

Social Engineering

Der Begriff Social Engineering wird in unterschiedlichen Zusammenhängen genutzt. Im Kontext der Sicherheit bedeutet der Begriff zwischenmenschliche Beeinflussungen mit dem Ziel, bei Personen bestimmte Verhaltensweisen hervorzurufen, sie zum Beispiel zur Preisgabe von vertraulichen Informationen, zum Kauf eines Produktes oder zur Freigabe von Finanzmitteln zu bewegen („soziale Manipulation“).

Kriminelle spionieren beispielsweise persönliche Daten der Opfer aus, täuschen falsche Identitäten vor oder nutzen Verhaltensweisen wie Autoritätshörigkeit aus, um geheime Informationen oder unbezahlte Dienstleistungen zu beschaffen. Als Social Hacking bezeichnet man das Eindringen in ein fremdes Computersystem, um sensible Daten einzusehen.

Glossar DMB Rechtsschutz Cyber-Check

Social Media

Unter Social Media, übersetzt „soziale Medien“, werden alle digitalen Medien verstanden, die ihre Nutzer über Kanäle in der gegenseitigen Kommunikation und im interaktiven Austausch von Informationen unterstützen. Es handelt sich um eine Gruppe von Internetanwendungen, die auf den technologischen Grundlagen des Web 2.0 aufbauen. Gemeint sind hiermit die sogenannten sozialen Netzwerke „Social Media“ wie Facebook, Twitter, Instagram, YouTube, Snapchat, WhatsApp und viele andere dieser Medien.

Spoofing

Spoofing nennt man in der Informationstechnik verschiedene Täuschungsmethoden in Computernetzwerken zur Verschleierung der eigenen Identität. Personen werden in diesem Zusammenhang auch gelegentlich als „Spoofers“ bezeichnet.

Spoofing ist ein häufig angewendetes Instrument in der Cyber-Kriminalität. Es wird häufig auch im Zusammenhang mit „Phishing“ genannt. Spoofing umfasst alle Methoden, mit denen sich Authentifizierungs- und Identifikationsverfahren untergraben lassen, die auf der Verwendung vertrauenswürdiger Adressen oder Hostnamen in Netzwerkprotokollen beruhen.

Virus

Computerviren verbreiten sich auf Rechnersystemen mit verschiedenen Konzepten und Techniken. Ein Virus

verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese so anpasst, dass das Virus mit ausgeführt wird, wenn das Wirtsprogramm gestartet wird.

Zu den Dateien, die durch ein Virus infiziert werden können, zählen normale Programmdateien, Programmbibliotheken, Skripte, Dokumente mit Makros oder anderen ausführbaren Inhalten.

Virenschutz

Siehe Anti-Virus-SW

WLAN

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden. Der Begriff steht für „Wireless Local Area Network“.

Wurm

Bei (Computer-, Internet-, E-Mail) Würmern handelt es sich um Schadsoftware, ähnlich einem Virus, die sich selbst reproduziert und sich durch Ausnutzung der Kommunikationsschnittstellen selbstständig verbreitet. Dadurch besteht die Gefahr, das ganze Rechnernetze infiziert werden.