

Erläuterungen zur Cyberversicherung.

An dieser Stelle wollen wir Ihnen verschiedene Begriffe erläutern, die im Zusammenhang mit der elektronischen Datenverarbeitung und Kommunikation verwendet werden, insbesondere solche, die wir im Rahmen unseres Produkts Cyberversicherung verwenden. Die Erläuterungen dienen dabei aber nur einem allgemeinen Verständnis und vermitteln kein tieferes Wissen.

Auftragsdatenverarbeitung

kurz ADV, ist die weisungsgebundene Verarbeitung von personenbezogenen Daten durch einen externen Dienstleister (Auftragnehmer). Der Auftraggeber bleibt dabei der Hauptverantwortliche für den Datenschutz, da ihn der Auftragnehmer bei seiner Arbeit nur unterstützt.

Beispiele für eine ADV sind:

- Die Nutzung von Cloud Computing
- Beauftragung eines externen Rechenzentrums mit der Lohn- und Gehaltsabrechnung
- Ein Callcenter erhebt Daten bei den Kunden des Auftraggebers.
- Eine Marketingagentur verarbeitet Kundendaten, um Statistiken oder einen Newsletter zu erstellen.

Betriebssystem

nennt man das grundlegende Programm zur Steuerung eines Computersystems oder Endgeräts. Das Betriebssystem ermöglicht die Ansteuerung von Prozessoren und Speichern und ist die Basis für die Arbeit der Anwendungsprogramme.

Bring Your Own Device

abgekürzt BYOD, bedeutet auf Deutsch: „Bring dein eigenes Gerät mit!“ BYOD steht für die berufliche Nutzung privater (mobiler) Geräte in jeglicher Form. Erfolgt die Einbindung eines privaten Geräts ohne Beachtung bestimmter Sicherheitsstandards, kann dies ein hohes Risiko für das Unternehmen bedeuten.

Cloud Computing

bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software. (Quelle: BSI)

Computersabotage

ist ein Vergehen, das in § 303b Strafgesetzbuch mit Freiheitsstrafe bis zu 5 Jahren oder mit Geldstrafe bewehrt ist. Computersabotage begeht, wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert oder Daten in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt. Strafbar macht sich danach auch, wer eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert.

Cyber

ist eine Vorsilbe, die sich für verschiedenste computer- bzw. Internetbezogene Themen eingebürgert hat. Abgeleitet wurde sie von Kybernetik, der Wissenschaft der Steuerung, Regelung und Nachrichtenübertragung. Beispiele: Cyberspace, Cybermoney, Cyberangriff.

Datenschutzverletzung

Eine Datenschutzverletzung ist die Verletzung von anwendbaren in- und ausländischen gesetzlichen Regelungen zum Datenschutz (z. B. EU-Datenschutz-Grundverordnung, Bundesdatenschutzgesetz) in Bezug auf elektronische Daten Dritter.

Datenvertraulichkeitsverletzung

Eine Datenvertraulichkeitsverletzung ist eine Verletzung der Vertraulichkeit elektronischer Daten Dritter. Unter Vertraulichkeit versteht man die Eigenschaft von Nachrichten oder Informationen, nur für einen bestimmten Empfängerkreis bestimmt zu sein. Vertrauliche Daten müssen also gegenüber Personen, die nicht diesem Kreis angehören, geheim gehalten werden.

Denial-of-Service-Attacke

im Computer-Englisch DDoS (Distributed Denial of Service) nennt man das Überfluten eines Internetdienstes mit Anfragen, das zu einer Nichtverfügbarkeit dieses Dienstes führt. Schäden an Software und Daten werden dabei in der Regel nicht verursacht, aber der Betrieb zeitweise unterbrochen oder stark behindert.

DNS

bedeutet Domain Name System und ist sozusagen das Telefonbuch des Internets. Es organisiert die Zuordnung lesbarer Domainnamen wie z. B. hdi zu der IP-Adresse des Servers, auf dem der entsprechende Dienst zur Verfügung gestellt wird. Dieses System ist hierarchisch aufgebaut. Top-Level-Domains haben die Namensendungen .com, .org, .net oder länderbezogen .de, .at, .ch usw. Darunter sind dann die jeweiligen Namen als Second-Level-Domain aufgegliedert, wie z. B. talanx.com. Darunter befinden sich weitere Ebenen.

Ein großes Sicherheitsproblem ergibt sich, wenn dieses System von Hackern beeinflusst wird (siehe Pharming).

Domain

ist ein abgegrenzter Bereich des Internets, der unter einem bestimmten Namen, wie z. B. hdi.de, von einer Suchmaschine angesprochen werden kann.

ERP

bedeutet Enterprise Resource Planning. ERP-Software unterstützt einen Unternehmer bei der Aufgabe, Ressourcen wie Kapital, Personal, Betriebsmittel, Material, Informations- und Kommunikationstechnik und IT-Systeme im Sinne des Unternehmenszwecks rechtzeitig und bedarfsgerecht zu planen und zu steuern.

Hardware

sind physisch vorhandene technische Geräte oder Bestandteile zur Datenverarbeitung oder Datenübertragung. Ihre Funktionen werden in der Regel durch Software ausgelöst oder dienen der Ansteuerung von Software (z. B. Tastatur, Maus, Touchpad). Als Hardware bezeichnet man auch die Gesamtheit aller Geräte eines IT-Systems.

ICS

steht für Industrial Control System und bezeichnet IT-Systeme, die der Fabrikautomation und Prozesssteuerung in der Produktion und Logistik dienen.

Informationssicherheitsverletzung

ist ein Sammelbegriff für verschiedene Tatbestände, die den Versicherungsfall in der Cyberversicherung von HDI darstellen. Eine Informationssicherheitsverletzung im Sinne der Bedingungen der HDI Cyberversicherung ist eine

- Datenschutzverletzung;
- Datenvertraulichkeitsverletzung;
- Netzwerksicherheitsverletzung.

IP-Adresse

ist eine Adresse in Computernetzen, die alle Geräte in diesem Netzwerk individuell bezeichnet, sodass diese für alle anderen Geräte erreichbar sind. Sie basiert auf dem Internetprotokoll (IP), also dem technischen Regelwerk, auf dem das Internet aufgebaut ist.

IT

IT steht für Englisch „Information Technology“, auf Deutsch „Informationstechnologie bzw. -technik“ und ist ein Oberbegriff für die (elektronische) Übertragung und Verarbeitung von Informationen und Daten mithilfe technischer Geräte und Systeme. Hier werden sowohl die Kommunikation (Telefon, Fax, E-Mail) als auch die elektronische Datenverarbeitung (EDV) zusammengefasst.

IT-Systeme

sind sämtliche Software- und Hardware-Systeme sowie Netzwerke und ihre Endgeräte, die für die elektronische Datenverarbeitung und -übertragung genutzt werden.

Netzwerk (Computer-N.)

ist ein Verbund von Geräten, z. B. Laptop, PC, Drucker, Server, zur Übertragung von Informationen über ein Übertragungsmedium (Kabel, Lichtleiter, Funk). Netzwerke können auch ineinander verschachtelt sein (z. B. Heimnetzwerk nimmt am Internet teil).

Netzwerksicherheitsverletzung

ist ein Sammelbegriff für verschiedene Formen von Angriffen auf ein Computer-Netzwerk, die zu einem Versicherungsfall in der Cyberversicherung von HDI führen.

Nutzer und Befugnisebenen

Während man in den Urzeiten des PCs einfach den Einschaltknopf drücken und dann loslegen konnte, verlangt heute jedes Betriebssystem, dass man mindestens einen Nutzer einrichtet und dessen Zugang auch mit einem Passwort sichert. Sicher wird die Nutzung dann, wenn jede Person, die ein Gerät nutzt, als Nutzer registriert ist und sich bei der Nutzung dann auch unter ihrem Namen anmeldet. Wenn alle Nutzer gemeinsam einen Zugang nutzen, kann man bei einer unbefugten Handlung nachher nicht feststellen, wer sie begangen hat. Wenn verschiedene Nutzer unterschiedliche Berechtigungen haben, z. B. nur lesen (Gast), normal arbeiten (Nutzer), Programme verändern (Administrator), so spricht man von unterschiedlichen Befugnisebenen.

Patch

bedeutet auf Deutsch „Flicken“ und ist ein Software-Paket, mit dem eine Software, z. B. ein Betriebssystem, nachgebessert wird. Ziel kann sowohl das Ausmerzen erkannter Fehler als auch eine allgemeine Verbesserung sein.

Patch-Management-Verfahren

ist ein Verfahren, mit dem sichergestellt wird, dass von einem Softwarehersteller gelieferte Patches auf den Systemen des Anwenders eingepflegt werden.

Pharming

ist allgemein gesprochen eine verfeinerte Form des Phishings. Die DNS-Adresse wird manipuliert, sodass trotz Eingabe der richtigen Adresse eine gefälschte Website angesteuert wird.

Phishing

ist eine Kombination aus „fishing“, dem englischen Wort für „Fischen, Angeln“ und dem „P“ aus Passwort. Es bezeichnet den Versuch des Identitätsdiebstahls mithilfe gefälschter Websites, E-Mails oder Kurznachrichten. Das Opfer wird durch Vortäuschen eines vertrauenswürdigen Empfängers dazu veranlasst, Zugangsdaten und Passwörter an Unberechtigte preiszugeben.

Ransomware

ist eine Schadsoftware, mit deren Hilfe Hacker Datenspeicher, Endgeräte oder ganze Computersysteme verschlüsseln und damit eine Nutzung durch die Berechtigten verhindern. Dies dient der Erpressung von Lösegeld für eine Wiederfreischaltung.

Router

ist eine Hardwarekomponente in Netzwerken, die Daten von den angeschlossenen Netzwerkteilnehmern entgegennimmt und diese mithilfe der IP-Adresse an den richtigen Empfänger weiterleitet.

Software

bezeichnet alle nicht körperlichen Bestandteile eines Computers oder IT-Systems, insbesondere die Programme.

Schadsoftware (Malware)

ist Software, die dem Zweck dient, unbefugt auf IT-Systeme einzuwirken, meist mit dem Zweck, Daten zu nutzen, zu verändern oder zu löschen.

Schutz gegen Schadsoftware

bezeichnet Programme, die dazu dienen, Schadsoftware zu erkennen, deren Installation oder Anwendung auf IT-Systemen zu verhindern und vorhandene Schadsoftware zu entfernen. Ein Beispiel dafür sind Antivirenprogramme bzw. Virens Scanner.

Zusätzlicher Schutz gegen unbefugten Zugriff

Server oder Geräte, die über das Internet erreichbar sind, sind dort einem allgemeinen und ständigen Angriffsrisiko ausgesetzt. Sie benötigen zusätzlichen Schutz. Mögliche Schutzmaßnahmen sind:

- Zusätzliche Firewalls – die betriebssystemeigene Firewall reicht nicht
- Zwei-Faktor-Authentifizierung
- Zertifikatsbasierte Anmeldung
- Ähnliche Maßnahmen, die einen Fernzugriff erschweren

HDI Versicherung AG

HDI-Platz 1

30659 Hannover

www.hdi.de/cyberversicherung