Alte Leipziger
ALH Gruppe

Cyber-Versicherung

Glossar zu Fachbegriffen

Nachfolgend werden einige wichtige Fachbegriffe aus dem Cyber-Umfeld erläutert. Sie finden diese Begriffe auch in den Vertragsbestandteilen unserer Cyber-Versicherung.

Administrator

Der Administrator ist ein Verwalter eines Systems (z. B. Netzwerk, Computer). Er ist für die Wartung und Sicherstellung des fortlaufenden Betriebs des Systems sowie die Systemsicherheit zuständig. Dafür besitzt er die erforderlichen Zugriffsrechte und kann die Rechte anderer Systemnutzer einsehen und ggf. auch einschränken.

Back-up (Datensicherung)

Bei einem Back-up werden Daten auf ein separates Medium (z. B. externe Festplatte) kopiert, um im Falle eines Datenverlustes die Originaldaten wiederherstellen zu können.

Botnet (Botnetz)

Bei einem Botnetz handelt es sich um ein zentral von Kriminellen errichtetes und steuerbares Netzwerk infizierter Computer oder internetfähiger Geräte (z. B. Überwachungskameras). Diese mit Schadsoftware infizierten Computer/Geräte werden Bots (von Roboter) genannt, da sie ohne das Einverständnis ihres rechtmäßigen Nutzers von außen gesteuert werden können. Botnetze werden z. B. für DDoS-Attacken eingesetzt und von ihren Betreibern gegen Entgelt an andere Kriminelle vermietet.

Bring Your Own Device (BYOD)

Bring Your Own Device beschreibt die gewollte Einbindung privater mobiler Endgeräte wie Notebooks, Tablets oder Mobiltelefone in Unternehmensnetzwerke zur dienstlichen Nutzung.

Cloud-Computing

Cloud-Computing umfasst ein Netzwerk aus IT-Strukturen und IT-Leistungen (z. B. Rechenleistung, Software oder Speicherplätze), die von entsprechenden Dienstleistern über das Internet bereitgestellt werden. Im Cloud-Computing ist es nicht mehr notwendig, Daten lokal auf dem Rechner zu speichern, da sie online in einer Cloud bearbeitet und gespeichert werden können.

Computervirus/-wurm

Siehe ➔ Virus bzw. ➔ Wurm

Denial-of-Service-Attacke (DoS-Attacke)

Denial of Service (DoS) bedeutet »Verweigerung des Dienstes«. Eine DoS-Attacke ist ein Angriff auf ein mit dem Internet verbundenes System (z. B. Server oder Website) und verfolgt das Ziel, dieses durch eine Vielzahl von Anfragen zu überlasten und somit zu stören oder zu unterbrechen.

Distributed-Denial-of-Service-Attacke (DDoS-Attacke)

Eine DDoS-Attacke ist eine DoS-Attacke, die mittels einer Vielzahl von Computern oder internetfähiger Geräte erfolgt. In der Internetkriminalität wird sie häufig in Botnetzen ausgeführt. Die DDoS-Attacke wird zum gleichen Zeitpunkt von verschiedenen Computern ausgelöst und ist dadurch nur schwer zu orten und noch schwieriger zu unterbinden.

fhs 081.01 – 02.2021

Alte Leipziger Versicherung AG · Alte Leipziger-Platz 1 · 61440 Oberursel · www.alte-leipziger.de
www.gewerbe-neu-entdecken.de/cyber · Produktmanagement Cyber · fhs-pmhs@Alte-Leipziger.de

DSGVO

Die Datenschutz-Grundverordnung (DSGVO) der EU regelt die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen. Sie soll sicherstellen, dass personenbezogene Daten innerhalb der EU geschützt sind, gleichzeitig aber den freien Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleisten.

E-Payment-Serviceprovider

Der elektronische Zahlungsverkehr über das Internet wird als E-Payment bezeichnet. Ein E-Payment-Serviceprovider erbringt entgeltlich Zahlungsdienstleistungen, wie z. B. die Anbindung von Online-Bezahlmethoden bei Online-Shops und die Zahlungsabwicklung.

Firewall

Eine Firewall ist ein zwischen Computern oder Netzwerken installiertes Softwarepaket (manchmal auch im Zusammenhang mit eigener Hardware), das einen kontrollierten und reglementierten Datenaustausch sicherstellt und so unbefugte Zugriffe von oder nach außen verhindert.

Hosting

Als Hosting wird der Betrieb von Softwareapplikations- oder Internetdiensten bezeichnet. Ein Webhosting-Anbieter (Hosting-Provider) bietet und betreibt Hosting-Dienste für Angebote seiner Kunden im Internet, wie z. B. eine E-Commerce-Shopping-Website.

Industrial Control System (ICS)

Industrial Control System ist ein Oberbegriff für industrielle Steuerungssysteme (Fabrikautomation und Prozesssteuerung) mit einer Infrastruktur aus Hardware, Software und Vernetzungskomponenten.

IT-Forensik

Die IT-Forensik beschäftigt sich mit der Analyse von tatsächlichen oder vermuteten Vorfällen im Zusammenhang mit IT-Systemen, um Sachverhalte, Ursachen und Verursacher festzustellen.

Kompromittieren

Das unberechtigte Eindringen in ein Computersystem und das dortige Ausspähen oder Manipulieren gespeicherter Daten wird als Kompromittieren bezeichnet.

Logdatei

Bei einer Logdatei (auch Logfile genannt) handelt es sich um eine Protokolldatei, in der IT-Systeme Ereignisse in Computersystemen oder Netzwerken eintragen und protokollieren. Die Datei soll helfen, Vorgänge nachvollziehbar zu machen, um so beispielsweise für die Problemanalyse oder die Rekonstruktion von verloren gegangenen Daten herangezogen werden zu können.

Malware

Siehe ➔ Schadsoftware

Netzwerk

Bei einem Netzwerk spricht man (im Bereich der Informationstechnik) von Computern bzw. netzwerkfähigen Geräten, die zu einem System zum Zweck der Datenkommunikation zusammengeschlossen sind. Man unterscheidet lokale Netzwerke (LAN/WLAN) oder überregionale Netzwerke (WAN).

Payment Card Industry Data Security Standard (PCI-DSS)

Der Datensicherheitsstandard der Payment Card Industry, einem Zusammenschluss der großen Kreditkartenunternehmen, ist ein Regelwerk für die Abwicklung von Kreditkartentransaktionen und hat das Ziel, Kreditkartendaten vor Diebstahl und Missbrauch zu schützen. Alle Unternehmen, die Kreditkartenzahlungen akzeptieren und die entsprechenden Daten verarbeiten, müssen die Regelungen erfüllen.

Pharming

Als Pharming wird eine betrügerische Methode beschrieben, mit der Nutzer mittels gefälschter DNS-Abfragen bei Eingabe einer Webadresse automatisch auf eine gefälschte Website

fhs 081.01 – 02.2021

Alte Leipziger Versicherung AG · Alte Leipziger-Platz 1 · 61440 Oberursel · www.alte-leipziger.de
www.gewerbe-neu-entdecken.de/cyber · Produktmanagement Cyber · fhs-pmhs@Alte-Leipziger.de

weitergeleitet werden, um vertrauliche Nutzerdaten ausspionieren zu können. Die Nutzer merken oftmals nicht, dass sie sich auf einer gefälschten Seite befinden, und geben arglos ihre persönlichen Daten ein. Kreditkartenbetrug und die Manipulation von Online-Banking-Zugängen sind hier häufig das Ziel. Die Methode basiert auf der Idee des Phishings.

Phishing

Phishing beschreibt den Versuch, durch falsche Informationen Nutzer dazu zu bringen, persönliche Zugangsdaten wie Benutzernamen und Passwörter im Web preiszugeben. Getarnt werden die Angriffe über gefälschte E-Mail-Links oder Webadressen, um einen seriösen Anschein zu erwecken. Besonders lukrativ und beliebt ist bei Betrügern der Diebstahl von Kontodaten.

Ransomware

Bei Ransomware handelt es sich um eine Schadsoftware, die oft über Phishing-Mails auf das Computersystem der Nutzer gelangt und das Ziel hat, den Zugriff darauf zu blockieren oder die dort gespeicherten Daten zu verschlüsseln, um dann von den Nutzern Löse-/Erpressungsgelder für die Entschlüsselung oder Freigabe zu fordern.

Schadsoftware (Malware)

Als Schadsoftware, Schadprogramme oder Malware werden Computerprogramme bezeichnet, die schädigende und vom Systembesitzer unerwünschte Wirkung entfalten, wenn sie auf dessen Systeme gelangen. Beispiele: Viren, Würmer, Trojaner, Ransomware.

Server

Ein Server ist ein Computerprogramm oder Computer, der über ein Netzwerk anderen Computern oder Programmen (»Clients«) Dienste, Daten oder andere Ressourcen, wie z. B. Speicherkapazität, bereitstellt.

Sicherheitspatch

Sicherheitspatches sind Nachbesserungen, die identifizierte Sicherheitslücken schließen. Sie werden von Softwareherstellern in regelmäßigen Abständen an die Nutzer verteilt und sollten von diesen implementiert werden.

Social Engineering

Beim Social Engineering nutzen Angreifer die Hilfsbereitschaft oder das Vertrauen ihrer Opfer aus, um sie durch geschickte Manipulation beispielsweise dazu zu verleiten, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln oder Schadsoftware zu installieren. Beispielsweise gibt sich der Angreifer als Systemadministrator aus und ruft den Mitarbeiter an, da er angeblich zur Behebung eines Sicherheitsproblems oder Systemfehlers das Passwort des Benutzers benötigt.

Software as a Service (SaaS)

Bei Software as a Service (SaaS) werden die Software und die IT-Infrastruktur bei einem externen Dienstleister betrieben und vom Anwender als entgeltliche Dienstleistung über das Internet als Cloud-Anwendung genutzt.

Trojaner

Ein Trojaner (Trojanisches Pferd) ist eine Software, die sich – offiziell als nützliches Anwendungsprogramm getarnt – auf dem Computersystem unbemerkt einschleicht und im Hintergrund unbemerkte Funktionen ausführt, um den Anwender und sein System zu schädigen.

Update

Als Update wird die Aktualisierung von Datenbanken oder Softwareanwendungen bezeichnet. Die regelmäßig angebotenen Updates dienen meist dazu, Sicherheitslücken zu schließen oder die Software um neue Funktionalitäten und Verbesserungen zu erweitern. Spezielle Sicherheitsupdates gibt es vor allem für Betriebssysteme, Firewalls oder Antivirenprogramme.

fhs 081.01 – 02.2021

Alte Leipziger Versicherung AG · Alte Leipziger-Platz 1 · 61440 Oberursel · www.alte-leipziger.de
www.gewerbe-neu-entdecken.de/cyber · Produktmanagement Cyber · fhs-pmhs@Alte-Leipziger.de

Verschlüsselung

Bei der Verschlüsselung von Daten werden diese in ein unleserliches Format umgewandelt, um sie vor unbefugtem Zugriff zu schützen. Erst nach der Entschlüsselung mit einem geheimen Schlüssel (z. B. Passwort) können die Daten wieder gelesen werden. Die Verschlüsselung ist daher eine der wichtigsten Voraussetzungen, um die Datensicherheit gewährleisten zu können. Dies gilt besonders für den Versand datenschutzrelevanter Daten (z. B. beim Online-Banking). Bei der zertifikatsbasierten Verschlüsselung kommen innerhalb einer Sicherheitsinfrastruktur, der sogenannten Public-Key-Infrastruktur (PKI), digitale Zertifikate zur Anwendung, um einen sicheren Austausch von Daten zwischen Kommunikationspartnern im Internet zu gewährleisten. Das digitale Zertifikat ist ein elektronischer Echtheitsnachweis, der von einer Zertifizierungsstelle ausgestellt wird und die vergleichbare Funktion eines Personalausweises besitzt.

Virenscanner

Ein Virenscanner, auch Antiviren- oder Virenschutz-Programm genannt, ist ein Programm, das Schadsoftware (Viren, Würmer, Trojaner) auf Systemen identifizieren und gegebenenfalls auch eliminieren soll. Wichtig ist dabei, den Virenscanner durch regelmäßige Updates möglichst aktuell zu halten, sodass ihm die »Steckbriefe« zur Identifikation der Schadsoftware vorliegen.

Virtual Private Network (VPN)

Ein Virtual Private Network bezeichnet ein privates virtuelles Netzwerk, das bereits in einem bestehenden Kommunikationsnetzwerk integriert ist und die Teilnehmer eines Netzes an ein anderes bindet. So können z. B. Mitarbeiter über ein VPN als Firmennetzwerk nicht nur am Arbeitsplatz im Unternehmen, sondern auch von zu Hause aus auf dieses zugreifen.

Virus

Ein Computervirus ist ein Schadprogramm, welches sich im Computersystem ausbreitet. Es benötigt eine Nutzeraktion für seine Verbreitung. So gelangt der Virencode z. B. durch das Öffnen einer infizierten Datei auf weitere Systeme und infiziert diese.

WLAN

Ein WLAN (Wireless Local Area Network) bezeichnet ein drahtloses lokales Netzwerk, das einen kabellosen Internetzugriff ermöglicht.

WPA

Bei WPA (Wi-Fi Protected Access) handelt es sich um eine Technik zur Datenverschlüsselung im Bereich von WLAN. Die Nachfolger WPA2 und WPA3 wenden einen anderen Verschlüsselungsalgorithmus an.

Wurm

Ein Computerwurm ist ein Schadprogramm, das sich selbstständig in Netzen verbreitet, ohne dabei Dateien zu infizieren.

Zwei-Faktor-Authentifizierung

bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (z. B. Passwort und PIN).

fhs 081.01 – 02.2021

Alte Leipziger Versicherung AG · Alte Leipziger-Platz 1 · 61440 Oberursel · www.alte-leipziger.de
www.gewerbe-neu-entdecken.de/cyber · Produktmanagement Cyber · fhs-pmhs@Alte-Leipziger.de