Alle wichtigen Begriffe auf einen Blick.

Der Bereich Cyber ist sehr komplex und etliche Begrifflichkeiten aus dem IT-Bereich sind vielen nicht bekannt. Daher haben wir hier die wichtigsten Begriffe für Sie alphabetisch aufgelistet und kurz erläutert. Von A wie Advanced Persistent Threat (APT) bis Z wie zielgerichtete Angriffe.

Advanced Persistent Threat (APT)

APT bezeichnet einen sehr komplexen, zielgerichteten, aufwendig vorbereiteten und durchgeführten Cyber-Angriff.

Bitcoin

Die Merkmale von Bargeld und elektronischen Überweisungen vereinen sich im Bitcoin, einer neuen Form des Geldes, das ausschließlich über ein Computernetzwerk geschöpft wie auch verwaltet wird. Bitcoin ist von Banken und vom Staat unabhängig und wird absolut anonym gehandelt.

Cloud-Computing

Im Bereich der Informationstechnologie (IT) ermöglicht Cloud-Computing neue Verfahren zur Bereitstellung von IT-Ressourcen, d. h. solchen Ressourcen, die Unternehmen bei der elektronischen Datenverarbeitung (EDV) unterstützen. Beispiele hierfür sind Server oder Softwareanwendungen. Anstatt IT-Ressourcen in unternehmenseigenen Rechenzentren zu betreiben, können diese bedarfsorientiert bei einem Cloud-Anbieter reserviert, genutzt und wieder freigegeben werden.

Cyber-Kriminalität

Als Cyber-Kriminalität werden kriminelle Aktivitäten bezeichnet, die den Cyber-Raum als Quelle, Ziel und/oder Werkzeug nutzen.

Cyber-Sicherheit

Die Cyber-Sicherheit verfolgt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gegen Bedrohungen aus dem Cyber-Raum.

Denial of Service (DoS)

Denial of Service (DoS) sind Dienstverweigerungen, die im Internet zur Beeinträchtigung von Webservices führen. Eine DoS-Attacke kann einen angegriffenen Server oder eine Webseite außer Betrieb setzen.

Home Banking Computer Interface (HBCI) als Online-Banking-Standard

Das Home Banking Computer Interface (HBCI) ist ein sicheres Übertragungsprotokoll für Finanztransaktionen in offenen Netzen wie dem Internet. Somit dient es als Kommunikationssystem zwischen Bank- und Kundenrechner. Das HBCI ist das derzeit sicherste Verfahren für Onlineüberweisungen.

IT-Forensik

Die IT-forensische Vorfallsbearbeitung behandelt die Aufklärung von Sicherheitsvorfällen, beginnend bei Sofortmaßnahmen, Spurensicherung, Analyse des Hergangs, der Ursache und des Umfangs des Schadens bis hin zur Aufbereitung der gewonnenen Erkenntnisse.

IT-Systeme

IT-Systeme im Sinne dieser Bedingungen sind der Verbund elektronischer, datenverarbeitender Systeme. Darunter fallen sämtliche vom Versicherungsnehmer genutzte stationäre und mobile Hard- und Softwaresysteme einschließlich Netzwerkkomponenten. Als IT-Systeme im Sinne dieser Bedingungen gelten auch industrielle Steuerungsanlagen wie z. B. Informationstechnologien zur Steuerung oder zur Kontrolle technischer Prozesse, eingebettete Systeme (Embedded Systems) und SCADA-Systeme (Supervisory Control and Data Acquisition Systems).

Patch-Management

Ein Patch, auch Bugfix, ist eine Korrekturauslieferung für Software oder Daten, um Sicherheitslücken zu schließen, Fehler zu beheben oder bislang nicht vorhandene Funktionen nachzurüsten. Bei einigen Herstellern heißen diese Aktualisierungen auch Service-Pack, wenn sie aus mehreren zusammengefassten Patches bestehen. Unter Patch-Management versteht man die Organisation rund um die Installation der Patches/ Service-Packs.

Pharming

Unter Pharming versteht man eine Methode zum Betrug im Internet. Die Opfer werden beim Pharming auf manipulierte Webseiten gelenkt. Ziel ist, in Betrugsabsicht an persönliche Informationen, z. B. Bankdaten, zu kommen.

Phishing

Beim Phishing wird dem Opfer in der Regel eine E-Mail geschickt. Das Opfer wird dazu verleitet, mit der Webseite des Angreifers Kontakt aufzunehmen. Über den Link in der E-Mail wird die Webseite des Angreifers angesteuert. Es handelt sich hierbei um eine Nachahmung des Designs einer vertrauenswürdigen Webseite. Ziel ist, an persönliche Zugangsdaten wie z. B. Benutzernamen oder Passwörter zu gelangen.

Punitive Damages (auch Exemplary Damages)

In den USA und Kanada gebräuchlicher Strafschadenersatz, der dort besonders im Bereich der Produkthaftpflicht (Produkthaftpflichtversicherung) gewährt wird. Der Strafschadenersatz kann erheblich über den Ausgleich des materiellen und immateriellen Schadens des Geschädigten hinausgehen. Voraussetzung für die Festsetzung von Punitive Damages ist die besondere Verwerflichkeit des schädigenden Verhaltens (bösartig oder rücksichtslos).

Schadsoftware

Als Schadprogramm, auch Malware, bezeichnet man Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenenfalls schädliche Funktionen auszuführen. Malware ist damit ein Oberbegriff, der unter anderem Computerviren, Trojaner und Würmer umfasst.

Trojaner:
Programm, das einen schädlichen Programmcode einschleust und im Verborgenen unerwünschte Aktionen ausführt.

Virus:
Ein Computervirus ist eine nicht selbstständige Programmroutine, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

Wurm:
Ein Computerwurm ist ein Schadprogramm mit der Eigenschaft, sich selbst zu vervielfältigen, nachdem es einmal ausgeführt wurde. In Abgrenzung zum Computervirus verbreitet sich der Wurm, ohne fremde Dateien mit seinem Code zu infizieren. Die Vervielfältigung/Verbreitung erfolgt oftmals mittels eines auf dem IT-System vorhandenen E-Mail-Programms.

Zielgerichtete Angriffe

Ein zielgerichteter Angriff im Sinne der ERGO Vesicherungsbedingungen ist ein Angriff auf die IT-Systeme des Versicherungsnehmers, der sich direkt gegen den Versicherungsnehmer oder ein mitversichertes Unternehmen oder die Branche des Versicherungsnehmers richtet.

Quellen: http://www.business-on.de/, http://wirtschaftslexikon.gabler.de, http://www.itwissen.info, https://www.internet-sicherheit.de/