GLOSSAR FÜR PRIVAT- UND FIRMENKUNDEN

	Wissenswertes von A bis Z
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.
Botnetze	Sind mit Schadsoftware infizierte Computer oder andere mit dem Internet verbundene Geräte, die von Kriminellen ferngesteuert und beispielsweise für Spam-Versand und für Attacken auf andere Systeme missbraucht werden. Auf diese Weise „gekaperte" Geräte können vom Nutzer unbemerkt auf ferngesteuerte Befehle von Kriminellen reagieren und zum Beispiel Spam versenden.
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 Software-Anwendungen. 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 das Internet als Quelle, Ziel und/oder Werkzeug nutzen.
Cyber-Mobbing	Mit den aus dem Englischen kommenden Begriffen Cyber-Mobbing, auch Internet-Mobbing, Cyber-Bullying sowie Cyber-Stalking genannt, werden verschiedene Formen der Diffamierung, Belästigung, Bedrängung und Nötigung anderer Menschen oder Firmen mit Hilfe elektronischer Kommunikationsmittel über das Internet, in Chatrooms, beim Instant Messaging und/oder auch mittels Mobiltelefonen bezeichnet. Dazu gehört auch der Diebstahl von (virtuellen) Identitäten, um in fremden Namen Beleidigungen auszustoßen oder Geschäfte zu tätigen usw. Opfer werden durch Bloßstellung im Internet, permanente Belästigung oder durch Verbreitung falscher Behauptungen gemobbt. Die Täter werden in diesem Zusammenhang auch als Bullies bezeichnet.
DDoS-Attacke	DDoS steht für Distributed Denial of Service. Bei dieser Form des Cyber-Angriffs wird das Zielsystem mit einer großen Anzahl von automatisierten Anfragen konfrontiert. Sind es so viele Anfragen, dass das Zielsystem die Anfragen nicht mehr abarbeiten kann, so werden reguläre Anfragen nicht mehr beantwortet. Die automatisierten Anfragen können zusätzlich noch auf Schwachstellen in der Software zielen, die dann zu einem kompletten Ausfall (Absturz) des Zielsystems führen. DDoS-Attacken werden mittlerweile von Cyber-Kriminellen zum Verkauf angeboten, so dass auch technisch nicht versierte Personen solche Attacken veranlassen können, beispielsweise um Konkurrenten zu schädigen.
E-Reputation	Als Schädigung der „E-Reputation" gilt die Verletzung des allgemeinen Persönlichkeitsrechts, zum Beispiel durch Beleidigung, üble Nachrede und Verleumdung mithilfe von Fotografien, Texten, Videos oder öffentlichen Erklärungen, die über einen Blog, ein Diskussionsforum, ein soziales Netzwerk oder eine Webseite verbreitet werden.
Firewall	Eine Firewall ist ein System aus Soft- und Hardware-Komponenten, das ein Rechnernetz oder einen einzelnen Computer vor unerwünschten Netzwerkzugriffen schützt.
Hacking	Ein Fremder verschafft sich Zugang zu einem Computersystem ohne notwendige Autorisierung durch den Nutzer oder den Eigentümer.
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, um online Überweisungen zu tätigen.
Identitätsmissbrauch	Ein Identitätsmissbrauch liegt vor, wenn der handelnde Dritte zur Nutzung personenbezogener Daten der versicherten Personen weder selbst berechtigt noch von der versicherten Person bevollmächtigt wurde und er diese Daten rechtswidrig zur Veranlagung eines Vermögensvorteils oder zum Zwecke der Bereicherung nutzt.

	Wissenswertes von A bis Z
Informationssicherheitsverletzung	Informationssicherheitsverletzung ist eine Beeinträchtigung der - Verfügbarkeit - Integrität - Vertraulichkeit von elektronischen Daten des Versicherungsnehmers oder von informationsverarbeitenden Systemen, die er zur Ausübung seiner betrieblichen oder beruflichen Tätigkeit nutzt. Dabei ist es unerheblich, ob sich die elektronischen Daten/die informationsverarbeitenden Systeme des Versicherungsnehmers in dessen unmittelbarem Verfügungsbereich befinden oder der Versicherungsnehmer sich eines externen Dienstleisters bedient.
Integrität	Unter der Integrität von Daten versteht man die Nachvollziehbarkeit von vorgenommenen Änderungen an diesen. Daten stehen immer einem gewissen Kreis von autorisierten Personen zur Verfügung. Bei den täglich anfallenden Geschäftsprozessen werden diese Daten natürlich verändert. Änderungen in den Dateien - seien dies Word-, Excel- oder andere Dokumente - müssen für jede zugriffsberechtigte Person nachvollziehbar sein. Dies kann zum Beispiel durch eine Versionsverwaltung sichergestellt werden.
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-Sicherheit	Die IT-Sicherheit verfolgt den Schutz der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen gegen Bedrohungen aus dem Internet.
IT-Systeme	IT-Systeme sind der Verbund elektronischer datenverarbeitender Systeme. Darunter fallen sämtliche vom Versicherungsnehmer genutzte stationäre und mobile Hard- und Softwaresysteme einschließlich Netzwerkkomponenten. Als IT-Systeme 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).
Keylogger	Als Keylogger wird Hard- oder Software zum Mitschneiden von Tastatureingaben bezeichnet. Sie zeichnen alle Tastatureingaben auf, um sie möglichst unbemerkt an einen Angreifer zu übermitteln. Dieser kann dann aus diesen Informationen für ihn wichtige Daten, wie z. B. Anmeldeinformationen oder Kreditkartennummern, filtern.
Man-in-the-Middle Attacke oder Fake President	Ziel bei einem Man-in-the-Middle-Angriff ist es, sich unbemerkt in eine Kommunikation zwischen zwei oder mehr Partnern einzuschleichen, beispielsweise um Informationen mitzulesen oder zu manipulieren. Hierbei begibt sich der Angreifer „in die Mitte“ der Kommunikation, indem er sich gegenüber dem Sender als Empfänger und gegenüber dem Empfänger als Sender ausgibt. Gelingt es dem Angreifer, erfolgreich in die Kommunikation einzudringen, kann er evtl. sämtliche gesendeten Informationen einsehen oder auch manipulieren, bevor er sie an den richtigen Empfänger weiterleitet.
Netzwerksicherheitsverletzung	Eine Netzwerksicherheitsverletzung ist jedes von einem Dritten geltend gemachte behauptete oder tatsächliche pflichtwidrige Tun oder Unterlassen von Versicherten, das einen Netzwerkeingriff zur Folge hat.
Patch	Unter einem Patch versteht man ein Update für Programme oder Betriebssysteme, die Sicherheitslücken schließen, Fehler beheben oder kleinere Funktionserweiterungen enthalten.
PCI-Standard (Payment Card Industry Data Security Standard)	Beim PCI-Standard handelt es sich um ein umfangreiches Regelwerk zur Abwicklung von Kreditkartenzahlungen. Unternehmen, die Kreditkarten-Transaktionen speichern, übermitteln oder abwickeln, müssen diese Regelungen einhalten. Andernfalls drohen Strafgebühren und andere Sanktionen.
Personenschäden	Personenschäden sind Schäden, die durch den Tod, die Körperverletzung oder die Gesundheitsschädigung eines Menschen entstanden sind.
Pharming	Pharming ist eine Betrugsmethode, bei der sich der Täter durch das Umleiten des Internetnutzers auf gefälschte Webseiten durch Manipulation des Webbrowers (beispielsweise durch DNS Spoofing - gefälschte Zuordnung zwischen URL und der zugehörigen IP-Adresse) vertrauliche Zugangs- und Identifikationsdaten von arglosen Dritten verschafft. Mit den gewonnenen Daten nimmt der Täter unter der Identität des Inhabers im Online-Verkehr unerlaubte Handlungen vor.

	Wissenswertes von A bis Z
Phishing	Mit Phishing werden Versuche bezeichnet, über gefälschte Webseiten, E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen. Mit den erhaltenen Daten werden beispielsweise Kontoplünderungen begangen. 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 an „fishing“ (angeln, fischen) anlehnt.
Ransom-Ware (Erpressungssoftware)	Hierbei handelt es sich um eine Schadsoftware, die den Nutzer von seinen Daten aussperrt und dann ein Lösegeld fordert, um den Zugang wieder freizugeben. In einfacheren Varianten (z. B. der bekannte „BKA-Trojaner“) wird lediglich der Systemstart manipuliert, so dass der Nutzer immer ein entsprechendes Hinweisfenster im Vordergrund hat.
Sachschaden	Als Sachschaden bezeichnet man die Zerstörung, die Beschädigung oder das Abhandenkommen versicherter Sachen.
Schadprogramm / Schadsoftware / Malware	Die Begriffe Schadfunktion, Schadprogramm, Schadsoftware und Malware werden häufig synonym benutzt. Malware ist ein Kunstwort, abgeleitet aus „Malicious software“ und bezeichnet Software, die mit dem Ziel entwickelt wurde, unerwünschte und meistend schädliche Funktionen auszuführen. Beispiele sind Computer-Viren, Würmer und Trojanische Pferde. Schadsoftware ist üblicherweise für eine bestimmte Betriebssystemvariante konzipiert und wird daher meist für verbreitete Systeme und Anwendungen geschrieben.
Schwachstelle	Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.
Skimming	Ist ein illegales Ausspähen der Daten von Kreditkarten oder Bankkarten. Meist werden dabei an echten, aber heimlich präparierten Geldautomaten die Kartendaten ausgelesen und die PIN abgegriffen.
Spam	Missbrauch von elektronischen Sendediensten (z. B. E-Mails, SMS) zum Versand von nicht erwünschten und unaufgeforderten Massennachrichten, die entweder Werbung für dubiose Produkte enthält oder versucht, zum Beispiel über einen Link oder einen Anhang Schadsoftware zu installieren.
Trojanisches Pferd (Trojaner)	Programm, welches sich als nützliches Werkzeug tarnt, jedoch schädlichen Programmcode einschleust und im Verborgenen unerwünschte Aktionen ausführt.
Verfügbarkeit	Dem Benutzer stehen Dienstleistungen und Funktionen eines IT-Systems sowie Daten und Informationen zum geforderten Zeitpunkt zur Verfügung.
Vermögensschäden	Vermögensschäden sind solche Schäden, die weder Personenschäden noch Sachschäden sind, noch sich aus solchen - von dem Versicherungsnehmer oder einer Person, für die er einzutreten hat, verursachten - Schäden herleiten.
Vertraulichkeit	Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
Virenschutzprogramm	Ein Virenschutzprogramm ist eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.
Virus	Ein Computer-Virus ist eine Schadsoftware, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen am System vornimmt.
Wurm	Ein Computer-Virus, der sich auch ohne Ausführung selbst reproduziert und sich im System (vor allem in Netzen) ausbreitet.

FK 282 (01/2018)