Glossar

VGH CyberSchutz

fair versichert
VGH

Wissenswertes von A bis Z

Bedrohung	Übertragen in die Welt der IT ist eine Bedrohung ein Umstand oder Ereignis, der oder das die Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Informationen beeinträchtigen kann, wodurch dem Besitzer bzw. Benutzer der Informationen ein Schaden entstehen kann.
Botnetze	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.
Cyber-Kriminalität	Als Cyber-Kriminalität werden kriminelle Aktivitäten bezeichnet, die das Internet als Werkzeug oder Ziel verwenden.
Cyber-Mobbing	Cyber-Mobbing ist das systematische Anfeinden, Schikanieren oder Diskriminieren mithilfe von elektronischen Kommunikationsmitteln über das Internet. Hierzu gehört auch die unberechtigte Nutzung einer virtuellen Identität, um in fremdem Namen Cyber-Mobbing zu betreiben.
DoS-/DDoS-Attacke	Denial-of-Service (DoS)-Angriffe beeinträchtigen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. 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. Im Falle eines DoS-Angriffs gehen alle diese Anfragen von einer einzigen Quelle aus, z. B. dem Rechner eines Cyberkriminellen. Bei einem Distributed-Denial-of Service-Angriff (DDoS) senden sehr viele unterschiedliche Quellen Anfragen. Oft handelt es sich bei diesen Quellen um Rechner in aller Welt, die ein kriminelles Botnetz bilden – ohne das Wissen ihrer Eigentümer.
E-Reputation	Als Schädigung der „E-Reputation“ des Versicherungsnehmers gilt die Verletzung des allgemeinen Persönlichkeitsrechts, unter anderem 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 Website verbreitet werden. Dem Ansehen des Versicherungsnehmers kann dadurch erheblicher Schaden zugefügt werden.
Fake President Angriff	Hierbei geben sich die Täter als Führungskräfte aus und üben hohen Druck auf Angestellte aus, dringende Zahlungen auf Konten der Täter anzuweisen.
Fake-Shop	Fake-Shops sind gefälschte Internet-Shops, hinter denen sich Betrüger verbergen. Nach Erhalt des Geldbetrages wird keine Ware ausgeliefert.
Firewall	Die Firewall besteht aus Hard- und Software, die den Datenfluss zwischen dem internen und externen Netzwerk kontrolliert. Alle Daten, die das Netz verlassen, können ebenso überprüft werden wie die, die hineinwollen. So wird das eigene Netzwerk vor ungewünschten Zugriffen geschützt.
Hardware	Als Hardware werden die materiellen Teile des PCs bezeichnet (z. B. die Festplatte). Auch ein Drucker oder die Tastatur ist Hardware. Auf der Hardware läuft die Software.

Identitätsmissbrauch	Ein Identitätsmissbrauch liegt vor, wenn der handelnde Dritte zur Nutzung personenbezogener Daten der versicherten Personen weder selbst berechtigt ist noch von der versicherten Person bevollmächtigt wurde und er diese Daten rechtswidrig zur Erlangung eines Vermögensvorteils oder zum Zwecke der Bereicherung nutzt.
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	Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Der Verlust der Integrität von Informationen kann bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden.
IT-Forensik	Die IT-Forensik 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).
Man-in-the-Middle Attacke	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 sämtliche gesendeten Informationen einsehen oder auch manipulieren, bevor er sie an den richtigen Empfänger weiterleitet.
Mediation	Mediation ist ein Verfahren zur freiwilligen, außergerichtlichen Konfliktbeilegung, bei dem die Parteien des Konflikts mit Hilfe der Moderation eines neutralen Dritten, des Mediators, eine eigenverantwortliche Problemlösung erarbeiten.
Patch	Unter einem Patch versteht man ein Update für Programme oder Betriebssysteme, das Sicherheitslücken schließt, Fehler behebt oder kleinere Funktionserweiterungen enthält.
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.
Pharming	Pharming ist eine Betrugsmethode, bei der sich der Täter durch das Umleiten des Internetnutzers auf gefälschte Webseiten durch Manipulation des Webbrowsers 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.

Phishing	Phishing ist eine Betrugsmethode, bei der sich der Täter mit Hilfe gefälschter E-Mails vertrauliche Zugangs- und Identifikationsdaten von Dritten verschafft, wobei der Täter typischerweise unter einer falschen Identität ein Vertrauensverhältnis aufbaut und dieses anschließend ausnutzt. Mit den gewonnenen Daten nimmt der Täter unter der Identität des Inhabers im Online-Verkehr unerlaubte Handlungen vor.
Ransomware (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 wird lediglich der Systemstart manipuliert, so dass der Nutzer immer ein entsprechendes Hinweisfenster im Vordergrund hat.
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 meistens 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 oder einer Institution. 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	Skimming ist eine Betrugsmethode, bei der der Täter, beispielsweise am Bankautomaten, Kartendaten und die PIN ausspäht. Mit den gewonnenen Daten nimmt der Täter unter der Identität des Inhabers im Bankverkehr unerlaubte Handlungen vor.
Social Engineering	Bei Cyber-Angriffen durch Social Engineering versuchen Kriminelle ihre Opfer dazu zu bringen, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder selbstständig Schadprogramme auf ihren Systemen zu installieren. Cyber-Kriminelle nutzen vermeintliche menschliche Schwächen wie Neugier oder Angst aus, um Zugriff auf sensible Daten und Informationen zu erhalten.
Software	Software ist ein Sammelbegriff für Betriebssysteme, Anwendungs- und Dienstprogramme u. ä.
Spam	Es handelt sich um Missbrauch von elektronischen Sendediensten (z. B. E-Mails, SMS) zum Versand von nicht erwünschten und unaufgeforderten Massennachrichten, die entweder Werbung enthält oder versucht, beispielsweise über einen Link oder einen Anhang Schadsoftware zu installieren.
Trojanisches Pferd (Trojaner)	Ein Trojanisches Pferd, oft auch kurz Trojaner genannt, tarnt sich durch ein nützliches Programm, während es im Hintergrund unerwünschte Anwendungen ausführt. Ein Trojanisches Pferd verbreitet sich nicht selbst, sondern wirbt mit der Nützlichkeit des Wirtsprogrammes für seine Installation durch den Benutzer.
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 (Tötung, Verletzung des Körpers oder Schädigung der Gesundheit von Menschen) noch Sachschäden (Beschädigung, Verderben, Vernichtung oder Abhandenkommen von Sachen) sind, noch sich aus solchen – von dem Versicherungsnehmer oder einer Person, für die er einzutreten hat, verursachten – Schäden herleiten. Als Sachen gelten auch Geld und geldwerte Zeichen. Als Vermögensschäden gelten auch Schäden aus dem Verlust, der Veränderung oder der Nichtverfügbarkeit von elektronischen Daten Dritter sowie Schäden aus der Verletzung von Persönlichkeitsrechten.

Vertraulichkeit	Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
Virus	Unter einem Computer-Virus ist eine nicht selbstständige Programmroutine zu verstehen, die sich selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt. Zusätzlich können programmierte Schadensfunktionen des Virus vorhanden sein.
Virenschutzprogramm	Bei einem Virenschutzprogramm handelt es sich um eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.
Wurm	Ein Wurm ist ein Computer-Virus, der sich auch ohne Ausführung selbst reproduziert und im System (vor allem in Netzen) ausbreitet.

M1 1.583 (06.21)