Besondere Vereinbarung Nr. 000567

Begriffserklärungen zur Cyberversicherung

Bitcoin

Eine virtuelle Währung im Internet auf Basis eines ausschließlich im Internet verfügbaren Zahlungssystems, welches auf Rechner-zu-Rechner-Verbindung fußt. Diese „Internet-Währung“ ist vollkommen unabhängig von Staaten oder Banken und gewährleistet dem Verwender bei Bedarf Anonymität, was die häufige Verwendung bei z.B. Ransomware-Angriffen erklärt.

Code Signing

Die Nutzung einer elektronischen Signatur (z.B. mittels Hash-Algorithmen) von Programmen oder Skript-Code mit dem Ziel sowohl die Authentizität des Erstellers/Versenders als auch die Integrität der signierten Daten zu gewährleisten.

DDoS-Attacke

Eine Distributed Denial of Service Attacke ist ein Angriff auf ein mit dem Internet verbundenes System, der mittels einer Vielzahl von Computern oder internetfähiger Geräte (Bot Netz) durchgeführt wird. Zweck eines solchen Angriffs ist es das Ziel durch Anfragen zu überlasten, damit es seine Arbeit verweigert (denial of service).

E-Payment Service Provider

Die entgeltliche Erbringung von Zahlungsdienstleistungen über das Internet durch sogenannte Zahlungsdienstleister.

Firewall

Ein zwischen Computern oder Netzwerken (LAN, WAN) 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.

IT-Forensik

Ein Teilgebiet der Forensik, das sich mit der Analyse von tatsächlichen oder vermuteten Vorfällen im Zusammenhang mit ITK-Systemen beschäftigt, um Sachverhalte, Ursachen und Verursacher festzustellen.

Malware

Der Englischsprachige Begriff für Schadsoftware.

Netzwerk

Die zu einem System zusammengeschlossenen Computer bzw. netzwerkfähigen Geräte. Man unterscheidet lokale Netzwerke (LAN/WLAN) oder überregionale Netzwerke (WAN).

PCI-DSS

Der Datensicherheitsstandard der Payment Card Industry, einem Zusammenschluss der großen Kreditkartenunternehmen. Sinn und Zweck des PCI Data Security Standards ist es, die Kreditkartenzahlungsprozesse möglichst sicher zu gestalten.

Ransomware

Eine Schadsoftware (Malware) mit dem Ziel von den Opfern Löse-/ Erpressungsgelder zu erhalten. In den vergangenen Monaten standen insbesondere Verschlüsselungstrojaner wie Wannacry im Fokus der Berichterstattung zu Ransomware.

Schadprogramme

Ein Programmcode, der vom Systembesitzer unerwünschte, schädigende Wirkung entfaltet, wenn er auf dessen Systeme gelangt.

Sicherheitspatch

Eine Nachbesserung in Sachen ITK-Sicherheit, die identifizierte Sicherheitslücken schließt. Sicherheitspatches werden von Softwareherstellung in mehr oder weniger regelmäßigen Abständen (patch days) an die Nutzer verteilt und sollten von diesen schnellstmöglich implementiert werden.

Virenscanner

Ein Programm zur Identifizierung (und Eliminierung) von Schadsoftware (Viren, Würmer, Trojaner) auf Systemen. Hierzu ist es in der Regel erforderlich, dass die „Steckbriefe“ zur Identifikation der Schadsoftware durch häufige Updates der Schadprogrammdatenbanken möglichst aktuell gehalten werden.

Kritische Infrastruktur

Als kritische Infrastrukturen im Sinne dieser Versicherung gelten Infrastruktur-Sektoren und Teilsektoren gemäss Bundesamt für Bevölkerungsschutz (BABS), wenn diese von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Als erhebliche Versorgungsengpässe gelten Beeinträchtigungen, die überregionale Auswirkungen haben.

Staatlicher Angriff

Das sind Angriffe die durch einen Staat, im Auftrag oder unter Kontrolle eines Staates verursacht worden sind.
Um einen staatlichen Angriff handelt es sich insbesondere dann, wenn eine IT-forensische Untersuchung des **IT-System des Versicherungsnehmers** oder beim Cyberangriff verwendete Systeme oder Hilfsmittel objektive Hinweise auf die Beteiligung, Urheberschaft oder Steuerung der Ursachen des Angriffs durch einen Staat, im Auftrag oder unter Kontrolle eines Staates ergeben. Das ist unter anderem dann der Fall, wenn eine Beteiligung von Gruppen oder Personen nachgewiesen werden kann, die in der Vergangenheit bereits an entsprechenden Handlungen dieses Staates beteiligt waren.

Zuschreibungen von Cyberangriffen die als staatlicher Angriff gelten:

Bei der Feststellung der Zuschreibung an einen Staat trägt der Versicherer die Beweislast. Ungeachtet dessen können die Parteien alle ihnen zur Verfügung stehenden objektiv angemessenen Beweismittel berücksichtigen. Neben allen rechtlich zulässigen Beweismitteln kann dies auch die formelle oder offizielle Zuschreibung durch staatliche Stellen des Staates, dessen kritische Infrastruktur durch die für den Schaden verantwortliche Ursache beeinträchtigt worden ist, an einen anderen Staat oder zu Gruppen oder Personen, die auf seine Anweisung oder unter seiner Kontrolle handeln, umfassen.

Finanzmarktinfrastruktur

Finanzmarktinfrastruktur umfassen Wertpapierbörsen (security exchanges), zentrale Wertpapierverwahrungsstellen (central securities depository, CSD) und zentrale Gegenpartei-Clearingstellen (central counterparty clearing House, CCP).

Internet-Services

Internet-Services bezeichnet Dienstleistungen, die die Nutzung des Internets ermöglichen, wie z. B.

- Internet-Service-Provider, die für die Bereitstellung von Diensten, Hardware und technischer Ausrüstung für den Zugang zum Internet und dessen Nutzung/Betrieb verantwortlich sind;
- Anbieter von Domänennamensystemen;
- andere Anbieter von Internet- und externen Netzdiensten, die für den Internetzugang zuständig sind, sowie Netzbetreiber; und,
- Betreiber von Kabelnetzen, Satelliten- und Funkkommunikationsnetzen.