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.