Cyberversicherung: Schutz gegen Internetkriminalität

Anke Nickel-Fiedler, Rechtsanwältin,
Dr. Friedhelm G. Nickel, Rechtsanwalt und Fachanwalt für Versicherungsrecht,
Kanzlei für Versicherungsnehmer,
Edermünde bei Kassel

Einleitung

Cyberversicherung ist eine neuartige Verbindung von Sach- und Rechtsversicherungen in der Weise, dass Schäden, die der Versicherungsnehmer selbst erleidet, etwa durch Datenverlust und Betriebsausfall, im Rahmen einer Sachversicherung versichert sind und die Schäden, die durch eine Informationssicherheitsverletzung (ISV) etwa beim Kunden entstehen, durch die Haftpflichtversicherung von der Deckung erfasst werden. Cyberversicherungen stehen in einem engen Zusammenhang mit der IT-Deckung und einer Vertrauensschaden-Versicherung. Die Cyberversicherung ist mit ihrer Kombination von Sach- und Rechtsversicherung ein einheitlicher Vertrag und nicht Bündelung zweier selbständiger Verträge.

Cyberrisiko ist das Risiko einer Datenveränderung durch Vernetzung. Datenveränderungen sind Daten-Verfügbarkeitsänderungen, das Löschen und das Abhandenkommen von Daten. *Cybercrime* ist vorsätzliche Datenveränderung. *Cyberspace* ist das Internet einschließlich der Daten in Sende- und Empfangseinrichtungen.

Spams und *Adware* werben illegal. Das Unternehmen wird ausspioniert. Im *Advanced Persistent Threat (APT)* werden Unternehmensdaten gestohlen. Exploits, also bekannte Schwachstellen eines Programms, verhelfen zum Gelddiebstahl durch Bankzugriff. Die gestohlenen Daten werden verkauft.

Denkbar sind auch religiös oder politisch motivierte Angriffe oder einfach „Spaßmacher". Oder im sog. *social engineering* psychologische Angriffe auf die Ethik des Angegriffenen, der erben soll, seine Angebote im Anhang finden oder den Auftrag bestätigen soll.

Botnets nutzen Netzwerkanbindungen, Ressourcen und Daten ohne Kenntnis des Berechtigten. *Hijacker Browser* leiten Suchanfragen um. *Denial-of-service* kennzeichnet die fehlerhafte Nichtverfügbarkeit eines Internetdienstes. Ransomware verhindert den Zugriff des Berechtigten auf dessen Daten. *Rootkits* verbergen Anmeldungen des Hackers und „verstecken" dessen Daten.

Trojaner sind Scheinprogramme mit unbekannten schadenstiftenden Anwendungen. *Viren* kennzeichnen ein Schadprogramm, das sich selbst verbreitet und Daten des Berechtigten infiziert. *Würmer* kennzeichnen ein Schadprogramm, das sich selbst verbreitet, ohne Daten des Berechtigten zu infizieren.

Gegenstand der Deckung

Gegenstand der Versicherung nach Maßgabe des Basis-Bausteins A1 der Musterbedingungen des GDV sind Vermögensschäden durch Informationssicherheitsverletzungen (ISV). ISV sind Daten-Beeinträchtigungen, unabhängig davon, ob sich die Daten beim VN oder bei einem externen Dienstleister befinden. Die Datensicherheitsverletzung beeinträchtigt die Verfügbarkeit, die Integrität oder die Vertraulichkeit von elektronischen Daten und wird bewirkt durch Eingriffe, Angriffe, unberechtigte Zugriffe, datenschutzwidrige Handlungen sowie Schadprogramme.

Unter Vermögensschäden versteht die Deckung selbständige Vermögensschäden, nicht aber solche als Folge eines Personen- oder Sachschadens.

Deckungsvoraussetzungen

Der Versicherungsnehmer muss aktiv Datensicherung betreiben. Vorgeschrieben sind dabei getrennte Benutzungsebenen, Passwörter, Administratorenvorbehalte und Sicherungssysteme, wie Firewalls, Authentifizierungen, Verschlüsselungen und Diebstahlsicherungen. Was heißt das?

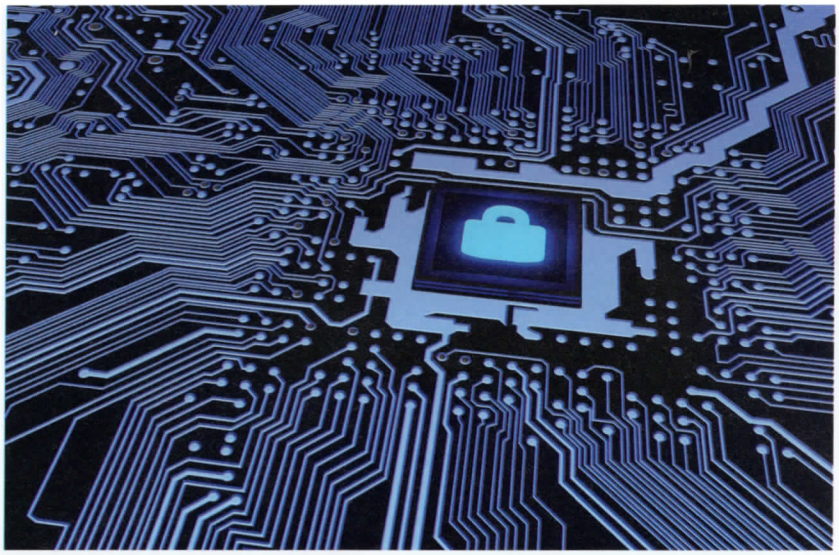
Backup-Systeme bewirken Datensicherung insbesondere durch Kopieren von Daten mit dem Ziel, die kopierte Datei im Schadenfall durch die Kopie zu ersetzen. Das Speichermedium wird redundant.

Aktive Datensicherung wird auf der Basis der typischen Betriebssysteme Windows, Mac OS oder Linux betrieben mit Antivirenprogrammen, Virenscanner oder Virenschutz-Programmen, also mit einer Software, die Schadprogramme wie z. B. Computerviren, Computerwürmer oder Trojanische Pferde ermitteln, behindern und beseitigen soll.

Bestandteil eines effektiven Schutzprogramms ist dabei eine Firewall. Sie soll vor unberechtigten An- oder Eingriffen Dritter in das Netzwerk des Angegriffenen schützen.

Schadprogramme oder *junkware* verursachen schädliche Funktionen innerhalb der Hardware, insbesondere im Rechner sowie in der Software, also allen nicht dreidimensionalen Teilen eines Rechners, aber auch im Rahmen der Firmware, also den *embedded* Software-Systemen, die typischerweise in Flash-Speichern, EPROM, EEPROM oder ROMs gespeichert werden und kaum austauschbar sind.

Gefordert wird alternativ eine Datenverschlüsselung. Verschlüsselung ist die Konvertierung von lesbaren Daten in ein verschlüsseltes Format. Und umgekehrt.



Mit der *2-Faktor-Authentifizierung* müssen sich Anwender in zwei aufeinanderfolgenden Schritten authentifizieren.

Stufe 1: Persönliche Information, etwa das Passwort.

Stufe 2: Authentifizierung etwa durch SMS- oder E-Mail-basierte Verifizierungscodes.

Angreifer benötigen also neben dem Passwort eines Anwenders Zugriff auf dessen Handy oder E-Mail-Account. Ein Passwort enthält eine unique Zeichenfolge, durch welche die Identität des berechtigten Benutzers bestätigt wird.

Der *Systemadministrator* richtet ein, verwaltet und beendet Computersysteme mit weitgehenden Zugriffsrechten auf das System. Befugnisebenen weisen dem Benutzer Zugriffsmöglichkeiten auf Ebenen zu, die es etwa ermöglichen, das Tagesgeschäft zu erledigen oder – auf anderer Ebene – Systemverwaltung zu betreiben.

Software-Versionsnummern sind die Programm-Indices zur Versionsunterscheidung. Die Nummernfolge weist regelmäßig Hauptversionsnummer, Nebenversionsnummer und Revisionsnummer aus.

Die Hauptversionsnummer indiziert dabei wesentliche Änderungen – wie etwa ein neu geschriebenes Programm mit gleichem Namen.

Nebenversionsnummern bezeichnen dagegen zumeist die Funktionserweiterungen der Software. Revisionsnummern bezeichnen zumeist die Anzahl von Fehlerbehebungen.

Das vom Versicherer geforderte Patchmanagement dient der Fehlerbehebung. Patches beseitigen Fehler der Software und dienen damit der Datensicherung nach Bekanntwerden von Sicherheitslücken. Im Code *Signing* bestätigen digitale Signaturen den Autor der Software.

Ausschlüsse

Ausgeschlossen sind vorvertragliche Schäden und alle Versicherungsfälle oder Schäden aufgrund des Ausfalls einer gesamten Infrastruktur, die etwa dann vorliegt, wenn Gebietskörperschaften oder ganze Stadtteile vom Ausfall betroffen sind.

Fremdschäden

Der Drittschadenbaustein der Cyberversicherung ist eine Vermögensschaden-Haftpflichtversicherung.

Die Leistung des Versicherers umfasst die Prüfung der Haftpflichtfrage, die Abwehr unberechtigter Ansprüche sowie die Freistellung des Versicherungsnehmers von berechtigten Schadenersatzansprüchen.

Auf Antrag mitversichert werden können Vertragsstrafen wegen der Verletzung eines Payment Card Industry (PCI) Daten-Sicherheitsstandards sowie Schäden oder Aufwendungen im Vertrauen auf die ordnungsgemäße Vertragserfüllung und Verzugsschäden.

Der *Payment Card Industry Data Security Standard* ist ein Regelwerk für Kreditkartentransaktionen.

Ausgeschlossen von der Deckung bleibt der Rückruf von Erzeugnissen, bleiben Ansprüche untereinander sowie Ansprüche innerhalb des Versicherungsnehmer-Konzerns.

Eigenschäden

Der Eigenschadenbaustein der Cyberversicherung ist eine von den Regeln der Sachversicherung ausgehende Deckung für Vermögensschäden mit einer Anschlussdeckung für Betriebsunterbrechungen und sieht demgemäß für den Fall einer Informationssicherheitsverletzung zunächst sowohl die Wiederherstellung der von der ISV betroffenen Daten, als auch die Entfernung der Schadsoftware vor.

Versichert ist die Betriebsunterbrechung im Rahmen der versicherten Haftzeit in Höhe eines vereinbarten Tagessatzes. Eine Betriebsunterbrechung liegt vor, wenn infolge der ISV Daten nicht mehr zur Verfügung stehen und die übliche Leistung nicht erbracht werden kann.

Als Unterbrechungsschaden gelten der ausfallende Betriebsgewinn und die fortlaufenden Kosten.

Kein Versicherungsschutz besteht für den Zeitraum einer geplanten Abschaltung oder durch eine geplante Datenlöschung sowie durch die Einführung neuer informationsverarbeitender Systeme. Nicht versichert ist der Einsatz ungetesteter oder unberechtigter Software.

Nicht versichert sind außergewöhnliche Ereignisse, behördliche Betriebsbeschränkungen, das Fehlen finanzieller Mittel um die Gesamtstruktur der innerbetrieblichen Datenverarbeitung wiederherzustellen, für Verbesserungen des Systems sowie für Sach- und Personenschäden. ■

GVNW – immer gut informiert