Cyber-Versicherung

Das Plus für mehr Datensicherheit.

Ihr Fels in der Brandung.

württem
bergische

Das IT-Sicherheitskonzept der Württembergischen.

Tipps und Hinweise

Cyber-Kriminalität - die unsichtbare Bedrohung

Mitarbeiter im Homeoffice, Kundenkommunikation per Videotelefonie und digitale Absatzwege: Die rasanten Entwicklungen der Informations- und Kommunikationstechnik bieten so viele Chancen wie Risiken – branchenübergreifend, über alle Betriebsgrößen hinweg. Sicherheit vor Onlinebetrug und anderen IT-Risiken war nie wichtiger.

Grundsätze und Mindestanforderungen

- Datensicherheit ist Chefsache! Deshalb muss die Verantwortung für dieses Thema in der Geschäftsführung verankert sein.
- Verwenden und aktualisieren Sie regelmäßig Ihre Antivirensoftware. Lassen Sie den Virenscanner im Hintergrund laufen. Dateien werden so bei Zugriff gescannt.
- Verwenden Sie nur Software, die vom Hersteller regelmäßig gepflegt wird.
- Übernehmen Sie sicherheitsrelevante Patches (Updates) der Softwarehersteller über die automatische Update-Funktion.
- Sichern Sie Ihre Daten mindestens einmal wöchentlich auf einem separaten Datenträger. Bewahren Sie mindestens die letzten drei Sicherungen auf.
- Um zusätzliche Sicherheit zu gewährleisten, sollte darüber hinaus je Quartal mindestens eine Vollsicherung auf einem separaten Datenträger durchgeführt werden. Überschreiben Sie die längerfristige Datensicherung frühestens nach vier Quartalen.
- Testen Sie regelmäßig den Notfall: Können die gesicherten Daten auch wieder auf die Anlage zurückgespielt werden?
- IT-Risiken müssen klar kommuniziert werden. Sensibilisieren Sie Ihre Mitarbeiter.
- Darüber hinaus gibt es weitere Ansätze, um Ihre Daten und die Ihrer Kunden vor unliebsamen Überraschungen zu schützen.

Organisatorische Maßnahmen

- Verwenden Sie für jeden Nutzer und Administrator benutzerindividuelle, ablaufende Passwörter. Schützen Sie auch Ihre Daten auf mobilen Geräten mit einem Passwort. Sperren Sie Rechner und mobile Geräte bei Inaktivität automatisch.
- Datenschutz: Achten Sie auf die sichere Entsorgung von Papier und Datenträgern (Festplatten, USB-Sticks etc.).

Präventive Maßnahmen

- Öffentliche WLAN-Netze sind unsicher. Geben Sie keine vertraulichen Daten wie Passwörter und Kontodaten ein, solange Sie einen öffentlichen Netzwerkzugang nutzen.
- Schützen Sie Ihren Server im Idealfall durch eine physische Zutrittsbeschränkung zum Server-Raum.
- Prüfen Sie, ob Sie digitale Medieninhalte (beispielsweise Bilder) veröffentlichen dürfen.

Absicherung des IT-Netzwerkes

Schützen Sie Ihren elektronischen Firmenzugang durch eine für Ihr Unternehmen geeignete Firewall, durch VPN-Zugänge oder ähnliches. Im Idealfall als eigenständige Hardware-Firewall, die nicht im DSL-Router integriert ist.

- Richten Sie für Ihr WLAN mindestens eine WPA2-Verschlüsselung ein.

Umgang mit mobilen Geräten

Schalten Sie bei mobilen Geräten (Smartphone, Tablet, Laptop etc.) die Bluetooth- oder WLAN-Funktion Ihres Endgerätes nur ein, wenn Sie diese bewusst zur Kommunikation einsetzen.

- Schließen Sie keine USB-Sticks, SD-Karten und andere Speichermedien von nicht vertrauenswürdigen Quellen an einen Rechner an.

Tipps zu sicheren Passwörtern

Ein gutes Passwort sollte mindestens acht Zeichen lang sein (je länger, desto sicherer) und aus Groß- und Kleinbuchstaben sowie Sonderzeichen und Ziffern bestehen.

- Es sollte nicht in Wörterbüchern vorkommen, gängige Tastatur- oder Ziffernfolgen sind tabu.
- Die meisten Browser bieten die Möglichkeit, Passwörter für bestimmte Webseiten zu speichern. Darauf sollten Sie und Ihre Mitarbeiter verzichten, denn in der Regel werden die Passwörter unverschlüsselt auf dem Computer gespeichert.
- Den besten Schutz bieten Passwort-Manager. Sie erstellen auf Wunsch zufallsgenerierte Passwörter und speichern diese in einer verschlüsselten Datenbank ab.

Schutz vor Schadsoftware

Verwenden Sie Software und Links nur aus vertrauenswürdigen Quellen. Gehen Sie mit Downloads von Programmen, Bildschirmschonern und Daten-Dateien aus dem Internet sorgsam um. Diese können Trojaner und Viren enthalten.

Sicherung der Daten

Die Sicherungsdatenträger müssen eindeutig gekennzeichnet sein und der Zeitpunkt der Datensicherung nachvollziehbar dokumentiert werden.

- Die Sicherungsdatenträger sollten mit einem Passwort geschützt werden. Die Sicherungsdatenträger sollten nur zur Datensicherung mit dem Netzwerk verbunden werden und ansonsten vom Netzwerk getrennt sein.
- Lagern Sie Ihre Sicherungsdatenträger in einem anderen Gebäude oder in einem geeigneten Datensicherungsschrank.

Sicherheitsnetz mit der Cyber-Police

Die Einhaltung dieser Maßnahmen verringert zwar die Möglichkeit einer Cyber-Attacke, völlig ausschließen lässt sich diese Gefahr jedoch nicht. Die Cyber-Police der Württembergischen schützt Unternehmen vor den Folgen von Cyber-Risiken – sowohl finanziell als auch mit Rat und Tat an unserem Cyber-Service-Telefon.

Glossar zur Cyber-Police.

Administrator	Der Administrator ist für die Verwaltung des Netzwerkes innerhalb einer Einheit verantwortlich. Zu den Verantwortlichkeiten gehören unter anderem die Netzwerksicherheit, Installationen, die Wartung und Aktivitätsüberwachung.
Anti-Viren-Software	Eine Anti-Viren-Software ist eine Software, die verschiedene Formen schädlicher Software (auch bekannt unter der Bezeichnung „Malware“) erkennen und entfernen kann und vor ihnen Schutz bietet, unter anderem auch vor Viren, Würmern oder Trojanern.
Anwendung	Als Anwendung zählen alle erworbenen oder benutzerspezifischen Softwareprogramme oder Programmgruppen, einschließlich sowohl interne als auch externe (z. B. Web-) Anwendungen.
Backup-Medien	Backup-Medien sind die zur Speicherung von elektronischen Daten eingesetzten Speichermedien. Die auf Speichermedien gesicherten Daten werden als Sicherungskopien bezeichnet. Medien sind jegliche Materialien und Gegenstände (andere als Papier), auf welchen Daten in einer Weise gespeichert werden, dass sie durch einen Computer gelesen oder verarbeitet werden können.
Benutzerindividuelle Kennung	Die benutzerindividuelle Kennung ist eine Zugangsberechtigung und basiert auf einem eindeutigen, nur einer Person zugewiesenen, Benutzernamen beispielsweise einer USER-ID.
Betriebssystem	Betriebssystem ist die Software eines Computersystems, die für Verwaltung und Koordination aller Aktivitäten, einschließlich der Verteilung von Computerressourcen, verantwortlich ist. Beispiele für Betriebssysteme sind u.a. MS Windows, Mac OS, Linux und Unix.
Bluetooth	Bluetooth ist eine Kommunikationstechnologie für drahtlose Datenübertragungen über kurze Distanzen.
Botnet	Ein Botnet (von englisch robot „Roboter) ist eine Gruppe von automatisierten Computerprogrammen, die auf vernetzten Rechnern laufen und deren Netzwerkanbindung sowie lokale Ressourcen und Daten nutzen. Betreiber illegaler Botnets installieren die Schadsoftware ohne Wissen der Inhaber und missbrauchen die Rechner bspw. für Spam-Versand und für Attacken auf andere Computer.
Compliance-Regeln	Compliance ist die Anforderung an die Einhaltung von gesetzlichen Bestimmungen und regulatorischen Standards in Unternehmen sowie vom Unternehmen selbst gesetzter Standards. Die Anforderungen an die Unternehmen variieren je nach Branche.
Computer	Ein Computer ist ein Gerät oder eine Gruppe von Geräten, welche(s) durch die Beeinflussung von elektronischen, magnetischen, optischen oder elektromechanischen Impulsen in der Lage ist, durch ein Computerprogramm Daten zu verarbeiten.
Computersystem	Als Computersystem gilt Computerhardware und -software sowie a. die darauf gespeicherten Daten, b. daran angeschlossene Ein- und Ausgabegeräte, c. daran angeschlossene Speichermedien, d. Netzwerkequipment, e. Firmware und f. Geräte, die der Datensicherung („Back-up“) dienen, inklusive aller Systeme, auf die über das Internet, Intranets, Extranets und Virtual Private Networks zugegriffen werden kann.
Datenschutzbeauftragter	Der Datenschutzbeauftragte hat unter anderem auf die Einhaltung der für das Unternehmen relevanten Datenschutzbestimmungen hinzuwirken. Er muss in Unternehmen und Vereinen bestellt werden, wenn personenbezogene Daten (z.B. Arbeitnehmerdaten in der Personalabteilung, Kunden- und Interessentendaten) automatisiert verarbeitet werden und mehr als neun Personen Zugriff auf diese Daten haben. Diese Grenze entfällt bei besonderen Risikosituationen wie z.B. Adressdatenhandel sowie Markt- und Meinungsforschung.

Datensicherung	Bei einer Vollsicherung werden alle Daten/Dateien kopiert und gespeichert. Ob sich Daten seit der letzten Datensicherung geändert haben, bleibt dabei unberücksichtigt. Bei einer Teilsicherung werden immer nur die Daten/Dateien gesichert, die sich gegenüber der letzten Sicherung geändert haben oder neu hinzugekommen sind.
Datenträger	Datenträger sind Speichermedien, die mit elektronischen Geräten gelesen oder beschrieben werden.
Denial of Service-Angriff (DoS)	DoS ist ein Angriff, der auf ein IT-System, wichtige IT-Dienste oder Netzwerke erfolgt, um deren Betrieb zu verzögern oder zu unterbrechen.
Deep-Linking	Deep-Linking ist ein Verweis (Verlinkung) auf urheberrechtlich geschützte digitale Inhalte eines Anbieters dergestalt, dass durch direkten Verweis auf „tief“ in dessen Webseite veröffentlichte Inhalte (bspw. eine Datei) eine technische Maßnahme des Anbieters, seine Inhalte zu schützen, umgangen wird.
Drive-by-Exploits/ Drive-by-Download	Drive-by-Exploits bezeichnen die automatisierte Ausnutzung von Sicherheitslücken auf einem PC. Dabei werden beim Betrachten einer Webseite ohne weitere Nutzerinteraktion Schwachstellen im Webbrowser oder im Betriebssystem ausgenutzt, um Schadsoftware unbemerkt auf dem PC zu installieren.
Flüchtiger Speicher (Arbeitsspeicher)	Ein flüchtiger Speicher (auch Arbeitsspeicher genannt) ist die Bezeichnung für den Speicher, der die gerade auszuführenden Programme/Programmteile und die dabei benötigten Daten enthält.
Firewall	Die Firewall ist eine Hardware- und/oder Softwaretechnologie, die Netzwerkressourcen vor unerlaubten Zugriffen schützt. Eine Firewall lässt Datenverkehr zwischen Netzwerken mit verschiedenen Sicherheitsebenen auf Grundlage einer Reihe von Regeln und anderen Kriterien entweder zu oder lehnt diesen ab.
Framing	Framing ist die Einbindung digitaler Inhalte Dritter in das eigene Webangebot durch Verweis (Verlinkung) mittels der Funktionalität von HTML-Frames, dass der Eindruck entstehen kann, die Inhalte Dritter seien Teil des eigenen Angebots.
Hardware	Die Hardware bezeichnet die Gesamtheit der technischen, physisch vorhandenen Maschinen-Elemente (Geräte, Teile) eines Computersystems oder Netzwerks wie beispielsweise Zentraleinheit, Datenspeicher und Leitungsverbindungen. Die Funktionen der Hardware werden durch Programme ausgelöst, gesteuert und kontrolliert.
Hardware-Firewall	Als Hardware-Firewall bezeichnet man eine dem internen Netzwerk vorgeschaltete Hardware-Komponente, welche stellvertretend für den einzelnen Rechner des Netzwerks die ausgehende und eingehende Kommunikation mit dem Internet übernimmt.
HBCI-Verfahren	Home-Banking-Computer-Interface. Sicherheitsverfahren für elektronisches Banking für Firmenkunden. Notwendige Voraussetzungen: – HBCI-Finanzsoftware – HBCI-Chipkarte – HBCI-Chipkartenleser
Hosting-Anbieter	Hosting-Anbieter bieten Web-Speicher, Datenbanken, E-Mail-Adressen und weitere Produkte im Internet an. Die Anbieter legen bspw. auf ihren Webservern die von Kunden hochgeladenen Webseiten ab.
Informationssicherheit	Schutz von Informationen zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit.
IP-Adresse	Die IP-Adresse wird auch als „Internetprotokolladresse“ bezeichnet. Die IP-Adresse ist ein Zahlencode, mit dem ein bestimmter Computer (Host) im Internet eindeutig identifiziert wird.
IT-System	IT-Systeme sind sämtliche Hard- und Software-Systeme sowie Endgeräte, die dazu geeignet sind, Daten zu erfassen, zu speichern oder zu verarbeiten.

Log-File	Eine Log-File oder auch Log-Datei enthält das automatisch geführte Protokoll aller oder bestimmter Aktionen/Prozessen auf einem Computersystem. Es werden alle Aktionen mitgeschrieben, die für eine spätere Untersuchung (Audit) erforderlich sind oder sein könnten.
Online-Handel (Internethandel)	Online-Handel ist der Einkaufsvorgang, bei welchem der Kauf- und Bezahlvorgang von Waren und/oder Dienstleistungen online abgewickelt werden.
Netzwerk	Ein Netzwerk (Computer-Netzwerk) ist ein Verbund mehrerer Rechner oder Rechnergruppen zum Zweck der Datenkommunikation.
Patch	Ein Patch ist ein Update für eine vorhandene Software, um zusätzliche Funktionalitäten zu installieren oder Fehler zu korrigieren.
Payment Card Industry	Dies bezeichnet die Zahlungskartenbranche, das heißt die Geschäftsbanken und Zahlungsprozessoren (wie z.B. Visa, American Express etc.) die im Bereich kartengestützter Bezahlsysteme am Zahlungsprozess beteiligt sind.
PCI Datensicherheitsstandard	Um Kreditkartendaten vor Missbrauch zu schützen, haben die Kreditkartenorganisationen einen gemeinsamen Standard, den Payment Card Industry (PCI) Data Security Standard (PCI DSS), entwickelt. Dies ist ein Regelwerk für den Zahlungsverkehr und enthält Anforderungen an die Rechnernetze und den Umgang mit den Daten für alle Unternehmen, die Kreditkartendaten verarbeiten, speichern oder weiterleiten (z. B. Händler, Geschäftsbanken oder sonstige Dienstleister).
PCI Level 1, 2, 3, 4	Unternehmen die Kreditkarten-Transaktionen speichern, übermitteln, oder abwickeln, müssen die Regelungen des PCI-Datensicherheitsstandards erfüllen und dies über eine Zertifizierung nachweisen. In Abhängigkeit vom Transaktionsvolumen erfolgt eine Einstufung in vier Level. – Level 1: > 6 Mio. Transaktionen p.a. und /oder ein Datendiebstahl vorgefallen; – Level 2: 1 Mio. bis 6 Mio. Transaktionen p.a. – Level 3: 20.000 bis 1 Mio. Transaktionen p.a. – Level 4: Alle anderen Je nach Level müssen zur Erlangung der Zertifizierung unterschiedlich strenge Anforderungen erfüllt werden.
Personenbezogene Daten	Personenbezogene Daten sind gemäß § 3 Abs. 1 Bundesdatenschutzgesetz Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person. Hierzu zählen beispielsweise: a. Persönliche Identifikationsnummern, insbesondere Versicherungsnummern, Sozialversicherungsnummern, Krankenversicherungsnummern, Fahrerlaubnisnummern, Steuernummern (E-tin), Chipkartennummern oder Geburtsdaten; b. Konto- und Depotnummern von Kreditinstituten und sonstigen Finanzdienstleistern; c. Kredit-, Debit- oder Zahlungskartennummern oder d. sämtliche Informationen über das Angestelltenverhältnis einer in Diensten eines versicherten Unternehmens stehenden natürlichen Person.
PIN/TAN-Verfahren	Persönliche Identifikationsnummer (PIN)/Transaktionsnummer (TAN). Sicherheitsverfahren für elektronisches Banking.
Remote-Zugriff	Der Remote-Zugriff ist der Zugriff auf Computernetzwerke von einem externen Standort. Verbindungen für den Remote-Zugriff gehen entweder von dem internen unternehmenseigenen Netzwerk oder von einem externen Standort außerhalb des Unternehmensnetzwerks aus. Eine Technologie, die Remote-Zugriff unterstützt, ist bspw. VPN.
Router	Der Router ist eine Hard- oder Software, die eine Verbindung zu einem oder mehreren Netzwerken herstellt.
Schadsoftware/ Malware	Als Schadsoftware/Malware bezeichnet man Software, mit der ein Computersystem ohne Wissen oder Zustimmung des Eigentümers infiltriert bzw. beschädigt werden kann und die mit der Absicht eingesetzt wird, die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten, Anwendungen oder Betriebssysteme des Eigentümers zu gefährden. Dazu zählen bspw. Viren, Würmer sowie Trojaner.

Server	Ein Server ist ein Computer, der anderen Computern Dienste zur Verfügung stellt, z. B. Kommunikationsverarbeitung, Dateispeicherung oder Zugriff auf eine Druckeinrichtung. Zu den Servertypen gehören z.B. Web-, Datenbank-, Anwendungs- oder Authentifizierungsserver.
Standardprogramme	Ein Standardprogramm bezeichnet ein Programm, das für gleichartige Anwendungen in unterschiedlichen Bereichen oder Betrieben erstellt wird und mit relativ geringem Aufwand an individuelle Anforderungen angepasst werden kann.
Trojanische Pferde (kurz: Trojaner)	Trojanische Pferde bezeichnet Programme, die neben ihrer eigentlichen Funktion, die dem Anwender bekannt ist, noch weitere Funktionen ausführen, von denen der Anwender nichts weiß und deren Ausführung er regelmäßig nicht bemerkt. Ein Spezialfall von Trojanischen Pferden sind logische Bomben (d. h. Programme mit verdeckter Schadensfunktion, die aber in Abhängigkeit von äußeren Bedingungen gestartet werden, z. B. Uhrzeit, Datum).
Update	Ein Update ist eine Produktaktualisierung wie z.B. die erweiterte und/oder verbesserte Version eines Softwareproduktes oder von Daten einer Datenbank.
USB-Stick	Ein USB-Stick ist ein kleines, wechsel- und tragbares Speichermedium, das über den Universal Serial Bus (USB) mit einem anderen Gerät (z.B. Computer) verbunden werden kann.
URL	URL (Uniform Resource Locator) wird im allgemeinen Sprachgebrauch als Web- oder Internetadresse bezeichnet.
VPN-Zugang	Um Daten sicher über ungeschützte Netze übertragen zu können, werden sogenannte Virtuelle Private Netze (VPN) gebildet, deren Daten in einem Tunnel das Internet durchqueren um bspw. verschiedne Standorte zu verbinden.
Verschlüsselung	Eine Verschlüsselung ist ein Prozess zum Konvertieren von Informationen in ein unleserliches Format, ausgenommen für Inhaber eines spezifischen kryptographischen Schlüssels (bspw. Kennwort). Durch die Verschlüsselung werden Informationen vor unerlaubten Freigaben geschützt.
Viren	Viren oder ähnliche Instrumente bezeichnen Programmcodes, Programmierungsanweisungen oder eine Reihe vorsätzlich entwickelter Instruktionen zum Zwecke der Beschädigung, Störung oder andersartigen nachteiligen Beeinflussung von Computerprogrammen, Dateien oder Rechenoperationen unabhängig davon, ob Viren oder ähnliche Instrumente sich selbst replizieren oder nicht. Die Definition von Viren oder ähnlicher Instrumente beinhalten u. a. Trojanische Pferde und Würmer.
Web-Filtersystem	Web-/Content-Filter werden vor allem in Unternehmensnetzwerken und bei Internetprovidern eingesetzt. Meist wird dadurch versucht, illegale, anstößige oder jugendgefährdende Webseiten zu sperren.
WLAN	WLAN steht für „Wireless Local Area Network“ (drahtloses lokales Netzwerk) und ist ein lokales Netzwerk, das zwei oder mehr Computer oder Geräte kabellos miteinander verbindet.
WPA/WPA2	WPA/WPA2 ist ein Sicherheitsprotokoll zur Sicherung drahtloser Netzwerke. WPA ist der Nachfolger von WEP. WPA2 wurde als nächste Generation von WPA veröffentlicht.
Würmer	Würmer bezeichnen selbstständige, sich selbst reproduzierende Programme, die sich in einem System, insbesondere Netz, ausbreiten.
Zero-Day-Exploits	Bei Zero-Day-Exploits wird eine Sicherheitslücke bereits zum Zeitpunkt der Entdeckung durch Kriminelle ausgenutzt. Daher bleibt Anwendern wenig Zeit für die Einleitung von Gegenmaßnahmen.
Zwei-Faktor-Authentifizierung	Die Zwei-Faktor-Authentifizierung ist eine Methode zur Authentifizierung eines Benutzers, bei der zwei oder mehrere Faktoren überprüft werden.