Sicherheit im Datenverkehr [1]

Einen vertrauenswürdigen und sicheren Umgang mit Kunden- und Personendaten setzen Geschäftspartner im gegenseitigen Verständnis stets voraus, nur selten wird es hinterfragt. Bereits im Grundsatz müssen wir für die uns anvertrauten Daten klare Regeln für den Umgang haben. Unser Qualitätsmanagementhandbuch schreibt Prozessabläufe und Arbeitsanweisungen vor, um „Das geistige Eigentum des Kunden sowie die von uns erstellte Übersetzung“ richtig zu lenken und zu verwahren. Besteht Dokumentenschutz wird das Projekt als CONFIDENTIAL eingerichtet.

Nun muss glücklicherweise nicht alles wie unter Geheimschutzbetreuung mit Verschlusssachen in Stahlschränken aufbewahrt werden. Dennoch dürfen wir keinesfalls leichtsinnig oder unbedacht werden oder uns gar wie auf einem Markplatz bewegen.

Doch nun zum Datenverkehr: der Versand einer Mail über das Internet entspricht nicht einem Brief, sondern einer Postkarte. Ohne Vorkehrungen sind die Daten sehr einfach zu lesen, sei es bei der Übertragung über Kabel oder WiFi und beim Provider. Verschlüsselungsprotokolle wie SSL/TLS zur „sicheren“ Datenübertragung im Internet, also für den Transport, SMIME/PGP in der Anwendung (E-Mail Client) und die entsprechenden Zertifikate von Zertifizierungsstellen sichern Vertraulichkeit, Authentizität und mehr.

In der Realität schickt über die Hälfte unserer Kunden ihre Dokumente per unverschlüsselter E-Mail, etwa 40 % per SSL/TSL-Verschlüsselung und weniger als 10 % per SMIME bzw. PGP, ohne sich Gedanken zu machen, dass dann eine eventuelle Geheimhaltungsvereinbarung keinen Sinn ergibt.

TTS versendet E-Mails immer per SSL/TSL über unseren Provider delink, wenn seitens Empfänger möglich, auch PGP-verschlüsselt. Oder aber die Daten werden über SFTP-Server (bei TTS im Hause, Zugang können wir Ihnen gerne einrichten) oder über unsere Server-Plattform bei Cryptshare (hier würde TTS bei jedem Transfer ein individuelles Passwort schicken) ausgetauscht, was gerade bei großen Dateien sinnvoll ist.

Gerne würden wir als Ihr Partner den Datenaustausch mit Ihnen noch sicherer gestalten. Lassen Sie sich bei Ihrer nächsten Anfrage doch einfach den PGP-Schlüssel unseres Mitarbeiters schicken und ab dann kommunizieren wir mit Sicherheit sicher.

[1] War bereits Thema im Newsletter vom November 2017

Angriffsarten:

Malware: (malicious software; zu Deutsch: bösartige Software) Oberbegriff für alle im Internet verbreiteten Programme, die schädliche Funktionen ausführen. Dazu gehören u.a. Trojaner, Viren, Würmer.

Ransomware: (ransom; zu Deutsch: Lösegeld) Ransomware gehört zur Familie der Trojaner und bezeichnet Schadprogramme, die meist durch Öffnen eines E-Mail-Anhangs auf den Rechner gelangen und dort Daten auf der Festplatte verschlüsseln. Bei Neustart erscheint ein Fenster mit der Aufforderung, Geld für die Entschlüsselung der Daten zu zahlen.

(D)DoS: DoS und DDoS: bezeichnen in der Informationstechnik die durch einen Angriff herbeigeführte Nichtverfügbarkeit eines Internetdienstes, der eigentlich verfügbar sein sollte. Dies kann unterschiedliche Ursachen haben. Bei DDoS-Attacken (Distributed Denial of Service) werden durch gezielte Vielanfragen die Server eines Dienstes überlastet, so dass er nicht mehr funktionstüchtig ist. Es ist also eine absichtlich herbeigeführte Blockade eines Dienstes.

Wichtig ist, dass Sie neben regelmäßigen System-Updates, Sicherheits-Patches und Logdatenprüfungen an zentraler Stelle Ihres Netzwerks eine Firewall einrichten.

+49 (0) 40 409409
www.ttsnet.de