

## Informationssicherheit im TecCom Verbund

Bei der Erstellung der TecCom Software und der TecCom Infrastruktur wird größte Aufmerksamkeit auf die Sicherheit der Daten im TecCom-Verbund gelegt. Dieses reicht bis hin zur Schnittstelle zu dem jeweiligen TecCom Teilnehmer. Im Folgenden sind neben den existierenden TecCom Software- und Provider-Sicherheitsmaßnahmen auch die Maßnahmen dargestellt, die auf TecCom Geschäftspartnerseite (Besteller, Lieferant) ergriffen werden müssen.

### Darstellung der TecCom-Providersicherheit

- Den Geschäftspartnern (Besteller, Lieferanten) von TecCom wird mit dem TecCom-Verbund ein Netz zur Verfügung gestellt, das höchsten Anforderungen bezüglich Datensicherheit im Netzwerkbereich erfüllt.
- Die Anmeldung am TecCom Applikation Server geschieht durch ein gesondertes Passwort, das vom Geschäftspartner möglichst häufig geändert werden sollte.
- Die Verbindung kann über Internet hergestellt werden. Der komplette Datenverkehr wird mit HTTPS abgewickelt. Dadurch werden nur verschlüsselte Daten (per SSL: Secure Socket Layer) übertragen; ein zufälliges oder vorsätzliches Aufzeichnen des Datenstromes kann nur mit Hilfe des dazugehörigen Schlüssels wieder nutzbar gemacht werden.
- Ein direkter Verbindungsaufbau zwischen Besteller und Lieferanten, Lieferanten zu Lieferanten, bzw. Besteller zu Besteller ist nicht möglich. Der gesamte Datenverkehr wird grundsätzlich über einen TecCom Applikation Server abgewickelt. In den Applikationsservern gibt es kein Routing von Nachrichten, sondern die Nachrichten werden bearbeitet und entsprechend den Geschäftsvorfällen wird eine logische Verbindung zu den notwendigen Stellen im Netz hergestellt.
- Geschäftsprozessdaten werden in einem speziellen Format (Tecform) im TecCom-Verbund transportiert.
- In der Applikation sind alle Passwörter verschlüsselt.
- Der Zugang zu den Datenbanken des Anwenders ist verschlüsselt.
- Der Zugang zum TecCom-Verbund vom Internet ist mit einem Firewall durch den Betreiber des Verbundes geschützt. In diesem Firewall ist nur das Protokoll HTTPS (Port 443) freigeschaltet. Über diesen Port (443) werden über einen Filter nur Tecform Nachrichten angenommen.
- Die im TecCom-Netz verfügbaren WIN2003-Server werden nach neuesten Sicherheitsrichtlinien regelmäßig getestet, um sicherheitsrelevante Schwachstellen bereits frühzeitig zu erkennen.
- Alle TecCom Komponenten werden in Sicherheitsbereichen (Zugangsschutz, Brandschutz, Notstromversorgung) betrieben.
- Alle Mitarbeiter haben die Verpflichtungen auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz (BDSG) und auf Geschäfts- und Dienstgeheimnis unterschrieben. Sie werden regelmäßig über Änderungen informiert.
- Der TecCom-Verbund Betreiber ist ISO 9001 zertifiziert.

**Um die Sicherheit sowohl bei dem Betreiber des TecCom-Verbundes als auch auf der Teilnehmerseite zu erhalten, müssen alle Geschäftspartner folgende Grundsätze einhalten:**

#### **Maßnahmen bei den Bestellern**

- Ein Geschäftspartner (Besteller) mit direkter Einwahl von einem PC ohne eigenem Netzwerk sollte die externe Rufannahme an seinem Modem oder ISDN-Adapter ausschalten. Dieses kann eventuell auch an seiner Telefonanlage realisiert werden. Dadurch werden unberechtigte Zugriffe von außen auf diesen PC verhindert. Wenn die Verbindung zum TecCom-Verbund nicht mehr benötigt wird, sollte sie abgebaut werden.
- Ein Geschäftspartner (Besteller) mit eigenem Netzwerk und Router, über den mehrere PC's sich am TecCom-Verbund anmelden, muss im Router eine „extended accesslist“ auf IP Basis einsetzen. Dadurch ist es möglich, den Datenverkehr auf ein IP-Adresspärchen zu beschränken.
- Die Verbindung zum TecCom-Verbund erfolgt über eine NIC-IP Adresse oder eine vom TecCom Verbund vergebene RFC-Adresse (incl. Netz-Adress-Umsetzung), die dem Teilnehmer bei der Einrichtung vom Betreiber des Verbundes mitgeteilt wird. Der Teilnehmer kann alle TecCom-Dienste über diese eine IP-Adresse erreichen.
- Im Router sollte nur das Protokoll HTTPS (Port 443) freigeschaltet werden. Dadurch werden nur HTTPS Nachrichten bis zum lokalen Netzwerk zugelassen.

#### **Maßnahmen bei den Lieferanten**

- Ein Geschäftspartner (Lieferant) mit eigenem Netzwerk und Router, über den mehrere PC's sich am TecCom-Verbund anmelden, muss im Router eine „extended accesslist“ auf IP Basis einsetzen. Dadurch ist es möglich den Datenverkehr auf ein IP-Adresspärchen zu beschränken.
- Die Verbindung zum TecCom-Verbund erfolgt über eine NIC-IP Adresse oder eine vom TecCom Verbund vergebene RFC-Adresse (incl. Netz-Adress-Umsetzung), die dem Teilnehmer bei der Einrichtung vom Betreiber des Verbundes mitgeteilt wird. Der Teilnehmer kann alle TecCom-Dienste über diese eine IP Adresse erreichen.
- Der Teilnehmer muss mit dem Betreiber einen Hostnamen und ein Passwort vereinbaren. Durch das PPP- Protokoll (mit CHAP) tauschen die beteiligten Router Nachrichten aus und erst bei Übereinstimmung dieser Daten wird der Datenverkehr ermöglicht.
- Im Router darf nur das Protokoll HTTPS (Port 443) freigeschaltet werden
- Ein Geschäftspartner mit eigener Firewall sollte die gleichen Regeln wie oben beachten. In der Firewall sollten alle Möglichkeiten der Filterung genutzt werden.