Dienstanweisung

über IT-Sicherheitsmaßnahmen beim Betrieb individueller Datenfernübertragungseinrichtungen (Modems, ISDN-Karten, etc.)

Quelle: Bundeskriminalamt Wiesbaden

1. Gegenstand

(1) Gegenstand dieser Dienstanweisung sind IT-Sicherheitsmaßnahmen bei individuellen Datenfernübertragungen. Individuelle Datenfernübertragungen sind Datenfernübertragungen (DFÜ), die nicht im Rahmen allgemeiner Aufgabenzuweisung (z.B. DFÜ-Operating im Rechenzentrum, Fernmeldebetriebsstelle, Zugriff auf externe Datenbanken über zentralen Kommunikationsserver) oder im Rahmen speziell geregelter Verfahren, sondern in der Regel vom Bedarfsträger selbst von einem APC aus durchgeführt werden. Sofern in bereichsspezifischen Dienstanweisungen (bspw. für die Nutzung von mobilen APC (Laptops/Notebooks)) abweichende Regelungen getroffen sind, gilt die bereichsspezifische Regelung.

(2) Bei DFÜ in öffentlichen Wählnetzen sind Vorkehrungen gegen folgende Gefahren zu treffen:

- Unbefugte Kenntnisnahme der übertragenen Daten (Verlust der Vertraulichkeit)
- Abfangen und Verändern der übertragenen Daten (Verlust der Integrität)
- Blockieren der Übertragungswege und/oder der zur Übertragung genutzten Rechner (Verlust der Verfügbarkeit)
- Unbefugtes Eindringen in die zur Übertragung genutzten und die ggf. mit diesen verbundenen Computer
- Einbringen von Schadensprogrammen (z. B. Viren) in die zur Übertragung genutzten und ggf. die mit diesen verbundenen Computer.

2. Maßnahmen

Mit folgenden Maßnahmen sollen die in Nr. 1 Abs. 2 genannten Gefahren minimiert werden. Diese Maßnahmen sind bei individueller DFÜ über öffentliche Wählnetze zu beachten.

(1) Beschaffung

1. Vor Beschaffung von individuellen DFÜ-Einrichtungen sind die für TK-Planung sowie die für IT-Koordination jeweils zuständige Organisationseinheiten und der IT-Sicherheitsbeauftragte zu beteiligen.
2. Für individuelle DFÜ beschaffte Geräte müssen folgende Sicherheitsfunktionen unterstützen:
   - Automatischer Paßwortschutz (bei häufiger Kommunikation mit demselben Kommunikationspartner): Hierbei tauscht das Modem bei jeder ankommenden Verbindungsanforderung Sicherheitsdaten mit dem rufenden Modem aus. Das antwortende Modem läßt den Verbindungsaufbau nur zu, wenn aufgrund der übersandten Daten das rufende Modem eindeutig identifiziert wurde.
   - Manueller Paßwortschutz (bei wechselnder Kommunikation mit mehreren Kommunikationspartnern): Hierbei müssen die entfernten Benutzer zum Aufbau einer Verbindung das passende Paßwort übersenden.

- ´Call-Back-Funktion´: Hierbei bricht das Modem nach erfolgreicher Prüfung des Paßwortes die Verbindung ab und wählt die Rufnummer, die zu dem in einer (internen) Liste gefundenen Paßwort gehört. Wird kein passender Eintrag gefunden, kommt keine Verbindung zustande.
- Darüber hinaus müssen die automatische Entgegennahme von Anrufen ("Auto-Answer") und die Möglichkeit zur Fernkonfiguration abgeschaltet werden können.

3. Die Nutzung privater Modems zu dienstlichen Zwecken ist nicht gestattet.

(2) Einrichtung

1. DFÜ-Einrichtungen für öffentliche Wählnetze dürfen nur an APC im Stand-alone-Betrieb angeschlossen werden. APC dürfen also nicht gleichzeitig mit dem LAN und externen Netzen verbunden sein.
2. Auf dem APC sollen für die Nutzer der DFÜ persönliche paßwortgeschützte Kennungen eingerichtet sein.
3. Auf dem mit einer DFÜ-Einrichtung ausgestatteten APC dürfen sich keine besonders schutzbedürftigen Daten befinden, es sei denn, sie sind kryptiert gespeichert oder der Verbindungsaufbau zum APC ist nur kryptiert möglich. Der Schutzbedarf der Daten wird vom Bedarfsträger unter Beteiligung des IT-Sicherheitsbeauftragten festgestellt.
4. Ein für den Betrieb und die IT-Sicherheit der DFÜ-Einrichtung und des Stand-alone-APC verantwortlicher Mitarbeiter wird ebenso wie der Einsatzzweck der DFÜ-Einrichtung sowie deren Standort, Typ und genutzte Anschlußnummer gegenüber dem IT-Sicherheitsbeauftragten schriftlich benannt.
5. DFÜ-Einrichtungen müssen vor dem Zugriff durch Unbefugte geschützt werden. Bei dauernder Nutzung sind sie in einem abschließbaren Raum zu installieren. Dieser Raum ist beim Verlassen zu verschließen. Bei nur gelegentlicher Nutzung sind die DFÜ-Einrichtungen nur zur Datenübertragung an den APC anzuschließen und ansonsten verschlossen aufzubewahren.
6. Die Konfiguration der DFÜ-Einrichtung erfolgt grundsätzlich durch das zuständige IT-Referat in Absprache mit der für TK-Planung oder -Einrichtung zuständigen Organisationseinheit.
7. Eine evt. Möglichkeit der Fernkonfiguration der DFÜ-Einrichtung muß deaktiviert sein.
8. Wenn eine automatische Entgegennahme von Datenübertragungen erforderlich ist, ist zum Schutz vor unberechtigten Anrufern die Call-Back-Funktion in Verbindung mit Paßwort-Überprüfung zu aktivieren; wenn nicht, sollen die "Auto-Answer"-Funktion abgeschaltet und die Anrufe manuell entgegengenommen werden.
9. Berechtigte Kommunikationspartner müssen festgelegt werden; nur diesen darf die Rufnummer für die DFÜ bekanntgegeben werden.
10. Auf den für die DFÜ genutzten APC wird das jeweils vom IT-Sicherheitsbeauftragten bereitgestellte Virensuchprogramm installiert. Empfangene Daten sind vor Weiterverarbeitung, insbesondere vor Einspielen in APC, die an das LAN angebunden sind, auf Viren zu überprüfen. Werden Viren festgestellt, dürfen die Daten nicht übernommen werden. Der IT-Sicherheitsbeauftragte ist zu informieren.

(3) Datenübertragung

1. Datenübertragungen, die über die TK-Anlage abgewickelt werden, werden automatisch protokolliert. Für andere Anschlüsse, von denen Daten übertragen werden, erfolgt die Protokollierung über Einzelverbindungsnachweis.
2. Die Übertragung besonders schutzbedürftiger Daten darf nur verschlüsselt erfolgen. Dies kann entweder durch eine Off-Line-Verschlüsselung der Daten vor der Übertragung erfolgen oder durch Einsatz von Kryptomodems bzw. separaten Verschlüsselungsgeräten, die für den angeschlossenen APC gleichzeitig einen erhöhten Zugriffsschutz bieten. Die Auswahl, Beschaffung und Konfiguration von Kryptoprodukten erfolgt durch die dafür zuständige Organisationseinheit unter Beteiligung des IT-Sicherheitsbeauftragten.
3. Die Übertragung von Verschlußsachen, die VS-VERTRAULICH oder höher eingestuft sind, ist grundsätzlich nicht gestattet. Ausnahmen sind mit dem COMSEC-Beauftragten abzustimmen.
4. Es ist darauf zu achten, daß beim Abbruch der Verbindung auf Anwendungsebene auch die Verbindung auf Leitungsebene abgebrochen wird und umgekehrt, damit nicht ein Unberechtigter sich in eine noch bestehende Leitungsverbindung einwählen kann.
5. Der IT-Sicherheitsbeauftragte kann in begründeten Einzelfällen einer Abweichung von den vorstehenden Regeln zustimmen.

3. Inkrafttreten

Die Dienstanweisung tritt am ..... in Kraft.