SICHERHEIT/TECHNIK

IT-Sicherheit - Abhörschutz und Notfallpläne

Sicherheit und Gefahrenabwehr in der Telekommunikation (TK) und Informationstechnik (IT) waren Hauptthemen eines Simedia-Seminars am 4. und 5. April 2000 in Frankfurt.

Der Brand in der Vermittlungsstelle der deutschen Telekom am 1. August 1998 in Reutlingen verursachte nicht nur Schäden durch Feuer und Löschwasser: 54.000 digitale Telefonanschlüsse waren "tot". In der ersten Woche nach dem Brand konnten erst 12.000 Anschlüsse auf analoger Basis wieder hergestellt werden. Der Schaden durch den Ausfall der Telefonleitungen war enorm.

Nicht nur Brände in Vermittlungsstellen und technische Defekte verursachen große Schäden in der Telekommunikation; sondern auch Sabotage. Gruppen wie Keine Verbindung e.V. und K.A.B.E.L.S.C.H.N.I.T.T. verübten 1995 und 1996 Anschläge auf Glasfaserkabel auf dem Gelände des Frankfurter Flughafens. In Seligenstadt trennten Unbekannte im Dezember 1999 in einer Vermittlungsstelle Kabelstränge durch; 15.000 Anschlüsse waren betroffen.

Notfallpläne

Vermittlungsstellen und TK-Anlagen sollten ähnlich wie Rechenzentren vor dem Zutritt Unbefugter und gegen Gefahren durch Brand, Wasser, Stromausfall und Überspannung geschützt werden, erläuterte Dkfm. Harald Seiffert von Simedia. Notfallpläne müssten erstellt werden.

Diese Pläne sollten auf Abhängigkeitsanalysen aufbauen: Für wen ist es in einem Katastrophenfall erforderlich, schnellstmöglich zu telefonieren und zu faxen, und zwar unter der gewohnten Rufnummer? Wer kann auf Telefon und Telefax zumindest kurzfristig verzichten? Ein Irrtum sei es zu glauben, Handys könnten eine ausgefallene drahtgebundene Anlage ersetzen. Das Netz könnte überlastet sein, es könnte nicht gefaxt werden. Bei dem in manchen Sparten herrschenden Konkurrenzdruck könnten Aufträge schon dadurch verloren gehen, dass der Gesprächs-partner nicht unter der gewohnten Rufnummer erreicht werden kann.

Manipulation

Die Leistungsmerkmale von Telekommunikationsanlagen ermöglichen auch Missbrauch und Manipulation. Durch Deaktivierung von Sperren können Gebührenbetrüger Schaden anrichten. Durch die Funktion "Freisprechen" in Verbindung mit der Funktion "direktes Ansprechen" können Räume abgehört werden ("Babyfon"-Funktion). Telefongespräche können durch einfache Manipulation der Konferenzschaltung mitgehört werden oder durch die Zeugenschaltung (silent monitoring). Faxe können dadurch mitgelesen werden, dass der Ruf um- und erst dann weitergeleitet wird. Kommunikationsprofile können erstellt werden, um herauszufinden, wer mit wem wie lange gesprochen, gefaxt oder Daten ausgetauscht hat. Daraus können Rückschlüsse gezogen werden über Kunden, Vertriebswege und Konkurrenzangebote. Gesteuert werden digitale TK-Anlagen über den D-Kanal; die eigentliche Gesprächsverbindung läuft über den B-Kanal.

Öffentliche Sicherheit, Ausgabe 06/2000

Die Steuerbefehle werden auch zur Fernwartung eingesetzt. Prinzipiell ist es möglich, Schaden stiftende Befehle zu übermitteln. Dafür sind allerdings hohe Fachkenntnisse erforderlich. Schützen kann man sich durch einen D-Kanal-Filter, der die einlangenden Befehlspakete mit vorgegebenen Einstellungen vergleicht. Die Sicherheit der Datenübermittlung gegen Abhören kann durch Verschlüsselung erhöht werden. Wichtig ist, sich mit den verschiedenen Anzeigen am Display des Telefons vertraut zu machen, um sehen zu können, ob nicht Funktionen zugeschaltet sind, die die Vertraulichkeit des Gesprächs gefährden. Auch sollte Warntönen entsprechende Aufmerksamkeit gewidmet werden; es lohnt sich, die Bedienungsanleitung genau zu studieren.

Schutzmaßnahmen

Dipl. Ing. Harald Kelter vom deutschen Bundesamt für Sicherheit in der Informationstechnik (BSI) berichtete unter anderem über Lauschabwehr: technische Schutzmaßnahmen sowie Maßnahmen bei Organisation und Personal.

Die Anforderungen an den Schutzbedarf sind abhängig von den Schutzklassen. Die Klasse 1 (mittlerer Schutzbedarf) ist dadurch gekennzeichnet, dass der Betroffene in seinem Ansehen geschädigt wird; darunter fallen typische personenbezogene Daten wie Name, Anschrift, Einkommensverhältnisse. Es wird davon ausgegangen, dass der Angreifer geringes Fachwissen hat (Hobby-Hacker) und finanzielle sowie technische Mittel nur eingeschränkt vorhanden sind.

In der Schutzklasse 2 müssen bereits Angriffe mit qualifizierten Mitteln verhindert werden. Die Angreifer sind Experten, denen umfangreiche finanzielle und technische Mittel zur Verfügung stehen. Typische personenbezogene Daten dieser Schutzklasse sind Personalaktendaten oder medizinische Daten. Der Betroffene wird in seiner sozialen Existenz geschädigt. In diese Schutzklasse fällt beispielsweise die Abwehr von Aktivitäten der organisierten Kriminalität.

In der Schutzklasse 3 müssen Angriffe mit hoch qualifizierten Mitteln, durch Angreifer mit Wissen auf Entwickler-Niveau, verhindert werden. Dem Betroffenen droht Gefahr an Leib und Leben. Es handelt sich beispielsweise um Daten von Personen, die einem Zeugenschutzprogramm unterliegen oder von V-Leuten. Je nach Schutzklasse müssen die noch fehlenden Maßnahmen ergänzt werden, jeweils aus den Gesichtspunkten der Verfügbarkeit, Vertraulichkeit und Integrität der übermittelten Daten.

Drahtlose Telekommunikation

Schnurlostelefone, die zunehmend innerhalb von Firmen verwendet werden, um sich Leitungsverlegungen zu ersparen, sind zumindest für Entscheidungsträger nicht sicher, warnte Lauschabwehr-Experte Manfred Fink: "Die Chefs müssen immer an die Leine genommen werden." Bei D- und E-Netz-Handys ist das tatsächliche Abhörrisiko auf der Luftschnittstelle mit großem Aufwand verbunden und daher nicht sehr wahrscheinlich; die Ausrüstung dafür ("IMSI-Catcher") ist sehr teuer.

Im Normalfall liegt die Gefahr eher in der unbedachten Nutzung sicherheitskritischer Leistungsmerkmale, wie etwa von Freisprecheinrichtungen oder der automatischen Rufannahme. Es können versehentlich reguläre Funktionen ausgelöst werden wie die Wahlwiederholung oder die Wahl-aus-Speicher-Funktion. In Sonderelektronik-Geschäften sind Akkus mit eingebautem Sender zum Abhören von Räumen für alle gängigen Handy-Modelle erhältlich.

Öffentliche Sicherheit, Ausgabe 06/2000

Handys sollten deshalb niemals unbeaufsichtigt liegen gelassen werden: Der Akku könnte ausgetauscht oder die Konfigurationen verändert werden. Basisstationen und Ladegeräte stehen üblicherweise auf dem Schreibtisch und werden ständig mit Strom versorgt; sie eignen sich daher ideal als "Container" für Abhörgeräte. Manfred Fink rät, Handys für sicherheitskritische Verwendungsbereiche in einem zufällig ausgewählten Fachgeschäft zu kaufen – anonym gegen Barzahlung und original verpackt. Teile sollten mit einer unverwechselbaren Markierung versehen und Ladegeräte nicht in sensiblen Räumen aufgestellt werden.

Auf sicherheitskritische Leistungen wie mobile Freisprecheinrichtung sollte verzichtet und die Tastatursperre aktiviert werden. Mobiltelefone sollten niemals unbeaufsichtigt liegen gelassen werden. Ein Handy-Verbot in Konferenzräumen kann mit einem einem elektronischen Detektor ("Mobifinder") überwacht werden.

Kurt Hickisch