Bei Anruf Hacking

Virtuelle TK-Anlagen sind in modernen Unternehmen mit weit verzweigten Niederlassungen ein Gewinn. Zu einem Verlust kann das Ganze allerdings werden, wenn Hacker in das System eindringen. Hinzu kommen Spionageangriffe auf TK-Einrichtungen, die laut Verfassungsschutz beträchtliche Schäden anrichten können. Kaum ein Unternehmen kann es sich da noch leisten, seine TK-Anlagen nicht mit den entsprechenden Methoden abzusichern.

Leistung, Freiheit, Perfektion. Ein Blick auf die bunten Werbeauftritte der Anbieter moderner Telekommunikationsanlagen verspricht mit jeder Menge Allgemeinplätzen einiges und suggeriert die grenzenlose Telefonie. In der Tat können virtuelle TK-Anlagen in fortschrittlichen Unternehmen mit weitverzweigten Niederlassungen ein Gewinn sein. Vor allem dank der einfachen Remote- und Managementfunktionen, die diese Systeme bieten. Dazu zählen neben dem zentralen Management der Anlage auch die persönlich konfigurierbaren Einstellungen oder das Wegfallen teurer und komplizierter Hardwarekosten. Im Grunde geht es darum, dass moderne TK-Anlagen in flexible Geschäftsprozesse nahtlos integriert werden können. Und das kabellos über das Internet und aus der Cloud. Vor allem die Cloud-Lösungen werden von fast allen Dienstleistern angeboten, wobei die gängigen Funktionen einer TK-Anlage in Rechenzentren gehostet und vom Anwender via Internet abgerufen werden.

Experten warnen vor Hackern

Ein Verlustgeschäft wird eine TK-Unterstützung dann, wenn Hacker in das System eindringen. Sei es, dass es zu Telefonmissbrauch mit kostenpflichtigen Telefon-Mehrwertdiensten im In- und Ausland kommt oder gleich die komplette TK-Anlage aufgrund von Sabotage ausfällt.

Die Spielwiese möglicher Angriffsziele ist groß und schon der direkte Schaden kann beträchtliche Ausmaße annehmen – vom Imageverlust für das betroffene Unternehmen ganz zu schweigen. Nicht umsonst warnt der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (Bitkom) vor Hackerangriffen auf Telefonanlagen. „Wer seine Telefone nicht schützt oder nur Standard-Passwörter verwendet, riskiert einen beträchtlichen finanziellen Schaden“, sagt Johannes Weicksel, Telekommunikationsexperte des Bitkom.

Hinzu kommen Spionageangriffe auf TK-Einrichtungen, die laut Verfassungsschutz hohe Gefahren bedeuten. Beispielsweise warnt die Niedersächsische Verfassungsschutzbehörde vor schlecht gewarteten Telefonanlagen, die ein deutliches Sicherheitsrisiko darstellten. In einer Wirtschaftsschutz-Info von Ende 2013 heißt es: „Der Wirtschaftsschutz Niedersachsen weist seit längerem auch auf die Gefahren durch Telefonanlagenmanipulationen hin.“

In einem konkreten Fall wurde ein mittelständisches Unternehmen aus dem produzierenden Gewerbe Opfer von Hackern. Dem Unternehmen, das eine Telefonanlage mit 200 Nebenstellen betreibt, entstanden durch den Angriff Telefonkosten in Höhe von mehr als 10.000 Euro. Und das ist kein Einzelfall, sondern nur die Spitze des Eisberges. Hinzu kommt, dass es den Angreifern mit voreingestellten oder nur simpel variierten Passwörtern leicht gemacht wird, in das jeweilige TK-System einzudringen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterscheidet bei der „Gefährdungslage“ einer klassischen TK-Anlage die Risikobereiche

- höhere Gewalt,
- organisatorische Mängel,
- menschliche Fehlhandlungen
- und vorsätzliche Handlungen.

Nichts von der Stange

Gerade im Bereich vorsätzlicher Handlungen sind eine ganze Reihe unerlaubter Eingriffsmöglichkeiten aufgelistet – vom Missbrauch der Fernwartungszugänge über das Abhören von Telefongesprächen bis hin zum Gebührenbetrug und dem Social-Engineering. Darüber hinaus verweist das BSI auf Bereiche, „die über die klassische TK-Anlage hinausgehen“. In diesen Fällen sei eine Umsetzung entsprechender Bausteine zur Absicherung notwendig, wie etwa zu „VoIP“ oder „mobilen und drahtlosen Systemen“.

Die Liste möglicher Bedrohungen zeigt, dass es nicht „die“ Schutzvorrichtung im Umgang mit modernen TK-Anlagen gibt. Erschwerend wirkt die Bandbreite an technischen Lösungen und Anwendungen, die

je nach Unternehmen sehr unterschiedlich und komplex ausfallen. Und in diesem Kontext stellen Cloud-basierte Lösungen Sicherheitsexperten vor weitere Herausforderungen. Vor allem die Tatsache, dass Telefonie ein integraler Bestandteil von Geschäftsprozessen ist und mit neuen (mobilen) Business-Anwendungen verzahnt sind, macht den Spagat zwischen mehr Technik und mehr Sicherheit nicht einfacher.

Grundsätzlich sind Risiken im Umgang mit TK-Anlagen und allen IT/TK-Lösungen nicht komplett zu verhindern. Vielmehr geht es darum, bestehende Gefahren mithilfe organisatorischer sowie technischer Vorkehrungen zu verringern sowie Chancen zu erkennen. Wichtig hier sind Standards und eine klare Strategie bei den internen Prozessen und der Wahl der richtigen Methoden der Risikoüberwachung und -bewertung. Und diese fallen unterschiedlich aus – je nach Branche, Größe, Vernetzung und Komplexität der jeweiligen Organisation sowie der eingesetzten TK-Lösungen. Expertenverbände wie die unabhängige Interessenvertretung RMA setzen beim Risikomanagement auf einen hohen Reifegrad der Prozesse und durchgängige Strategien und Lösungen. Im Klartext heißt das: Organisationen müssen sich aktiv um wirkungsvolle Abwehrmechanismen im Risikomanagement bemühen. Hierzu gehört, dass die Verantwortlichen Sicherheitsstrukturen und Verhaltensregeln regelmäßig hinterfragen und gegebenenfalls neu einstellen – in der gesamten Organisation und über alle Hierarchiestufen hinweg. Dies bedeutet auch, Risiken und deren Bewertungen in die Unternehmensplanung und das Controlling zu integrieren. Damit lassen sich beispielsweise Insellösungen im „Lösungspark“ vermeiden und ein Gesamtkonzept zur Risikosteuerung aufbauen. Diese Vorgehensweise erscheint im Bereich der TK umso wichtiger, als die technologischen Herausforderungen mit vernetzten Strukturen und neuen Risikofaktoren gleichfalls neue Wege im Organisationsdenken erfordern – ein Knackpunkt vor dem Hintergrund neuer Cloud-Technologien sowie mobiler Lösungen, die sowohl das Sicherheitsdenken als auch das Arbeitsumfeld stetig verändern.

Ein gangbarer Weg liegt in einem einheitlichen Sicherheitskonzept im TK-Bereich, das von der Planung und dem Konzept bis zur Umsetzung und dem Betrieb – inklusive eines Notfallmanagements – klare Maßnahmen vorsieht. Bei-

Max Schroeder,
Entwicklungsleiter, Starface:

„Die höchste Priorität hat beim Anwender die Zuverlässigkeit der Telefonanlage. Am wichtigsten ist das Vermeiden von Gesprächsabbrüchen, aber auch die möglichst hundertprozentige Funktionsfähigkeit der Anlage. Telefonische Erreichbarkeit ist für viele Kunden von existenziellem Interesse. Hinzu kommt bei vielen Kunden die – berechtigte – Angst vor Viren, Trojanern und Dialern.“

funkschau EXPERTENKOMMENTAR

Bild: MPC Service

Mirko Mach,
Geschäftsführer, MPC Service

Lausch- und Dialerangriff – die Achillesfersen von IP-Centrex

Viele Unternehmen hegen beim Thema IP-Centrex Bedenken bezüglich Sicherheit. Und tatsächlich gibt es bei der TK-Anlage im Netz vor allem zwei reale Gefahren, gegen die sich Unternehmen wappnen sollten: Lausch- und Manipulationsangriffe.

In puncto Abhörsicherheit kann es verschiedene wunde Punkte geben: Hacker könnten theoretisch an mehreren Stellen zwischen Kundentelefon und Centrex-Zentralsystem eindringen. Um dies zu verhindern, muss der Kunde in jedem Fall sein LAN durch eine aktuell gewartete Firewall absichern. Außerdem empfiehlt es sich, die Strecke zwischen Kunden-CPE zum RZ des Providers über ein geschlossenes IP-Netz, zum Beispiel MPLS, zu realisieren. Eine zusätzliche Erhöhung der Sicherheit kann durch die Verschlüsselung der Gespräche per Secure-Real-Time-Protocol (SRTP) erreicht werden, was bisher allerdings nur von wenigen Providern angeboten wird. Firmen sollten in diesem Zusammenhang jedoch auch grundsätzlich die eigenen Ansprüche an die Datensicherheit hinterfragen – wird doch in vielen Fällen bisher nicht einmal der E-Mail-Verkehr verschlüsselt.

Hoher wirtschaftlicher Schaden droht Unternehmen, die einer Manipulation der Telefonanlage zum Opfer fallen. Um das Risiko von Dialer-Angriffen zu minimieren, müssen verschiedene Schutzmechanismen ineinandergreifen. Zu den präventiven Maßnahmen auf Kundenseite gehören hier neben der Firewall die Verwendung sicherer Passwörter bei Mailboxsystemen. Auf Providerseite sollten Fraud-Tools für eine automatische Überwachung sämtlicher Systemaktivitäten sorgen, auffälliges Telefonieverhalten registrieren und bei Erreichen eines Schwellwertes Alarm auslösen.

Nicht zuletzt spielt beim Thema Sicherheit natürlich auch der Standort des Rechenzentrums des Anbieters eine Rolle. Vor dem Hintergrund strenger Datenschutzrichtlinien und -gesetze empfiehlt sich die Wahl eines Providers, dessen Rechenzentrum in Deutschland steht. Eine hohe Ausfallsicherheit sollte durch den redundanten Betrieb mit möglichst geografisch getrennten Servern gewährleistet sein. *(DK)*

spielsweise sprechen sich Experten dafür aus, dass während der Installation einer TK-Anlage die voreingestellten Passwörter geändert werden und Schnittstellen abzusichern sind. Nach der Formel „Keep it simple“ sollten sämtliche Funktionen, die nicht den Zielen des TK-Betriebs in der eigenen Organisation dienen, abgeschaltet werden.

Risikomanagement: steuern, überwachen, Kultur aufbauen

Gefordert sind zunächst Vorstände und Aufsichtsräte, die eine klare Risikomanagementstrategie in der eigenen Organisation positionieren müssen. Durch die vielfältigen Modifikationen der gesetzlichen Rahmenbedingungen, wie zuletzt beim Bilanzrechtsmodernisierungsgesetz (BilMoG), hat sich die Verantwortung von Firmenverantwortlichen im Rahmen des Risikomanagements kontinuierlich verschärft. Das betrifft große Konzerne und mittelständische Unternehmen gleichermaßen. Die besondere Verantwortung des Aufsichtsrats im Zusammenhang mit dem BilMoG erklärt sich aufgrund der regelmäßigen Prüfungspflichten. Es reicht nicht aus, von der Geschäftsführung auferlegte Sicherheitsstrukturen zu etablieren und sich selbst zu überlassen. Kern ist das Steuern und Überwachen der Prozesse sowie vor allem auch der Wirksamkeit der jeweiligen Strukturen im Bereich des Informationssicherheitsmanagements.

Trotz aller internen Richtlinien nimmt im Bereich der Risikokultur das „wahre Leben“ hinter allen Regeln, Normen und Vorkehrungen einen großen Stellenwert ein. Sicherheitsdenken im Sinne der Organisation fängt im Kopf jedes einzelnen Mitarbeiters an. Nicht umsonst sieht das BSI bei den Risiken für den Betrieb einer klassischen TK-Anlage das menschliche Fehlverhalten als einen wesentlichen Faktor. Und dabei stehen Ausfälle der TK-Anlage durch eine Fehlbedienung ebenso im Zentrum der Überlegungen wie die „fehlerhafte Administration von Zugangs- und Zugriffsrechten“ oder der IT-Systeme.

Frank Bauer,
Leiter Portfoliomanagement und Support,
Mitel Deutschland:

„Schutz fängt bei der eigenen Mailbox oder so genannten DISA-Zugängen an: Passwörter wie ‚12345‘ oder ‚00000‘ sollten gleich bei Inbetriebnahme des Telefons durch sichere Zahlenkombination ersetzt werden. Zusätzlich schützen Sperrlisten in der TK-Anlage vor Missbrauch, so dass bestimmte Ländervorwahlen oder Dienste nicht angerufen werden können.“

Und diese Fehlerquellen steigen mit jeder technischen Neuerung. Eine gelebte Risikomanagement- und Unternehmenskultur kann diesen Denkprozess maßgeblich mitbestimmen und im Sinne einer ausgebildeten Awareness-Strategie lenken.

Mit anderen Worten: Ein loyaler und gut geschulter Mitarbeiter kann sich vom Sicherheitsrisiko zum Sicherheitsfaktor wandeln. Für Hacker heißt das: Kein Anschluss unter dieser Nummer. *(DK)*

Prof. Dr. Roland Franz Erben,
Vorsitzender des Vorstands, Risk Management Association e. V. (RMA)

Tipps zur Sicherung der TK-Systeme

Umfassende Schutzkonzepte können aufgrund der Vielfalt der Technologien und Anwendungen nur unternehmensspezifisch ausfallen und gegebenenfalls entsprechend komplexe Anforderungen darstellen. In vielen Fällen lässt sich das Schutzniveau allerdings schon mit relativ einfachen Maßnahmen deutlich erhöhen. Die Tipps für sichere TK-Systeme vom LKA NRW, Bitkom und VAF:

- **Passwortschutz für TK-System**: Für persönliche Sprachboxen (integrierte Anrufbeantworter) müssen immer vom Nutzer individuelle Passwörter vergeben werden. Keinesfalls dürfen werksseitige Voreinstellungen belassen werden. Sensibilisierung aller Nutzer ist notwendig! Sind im TK-System so genannte DISA-Nebenstellen mit Durchwahlmöglichkeit vorhanden? Die DISA-Funktion dient der Anbindung von Heimarbeitsplätzen oder als Einwahlmöglichkeit für TK-Servicetechniker. Sie muss ebenfalls geschützt werden, wie auch Administratorenzugänge. Wenn ein Zugang für Fernwartung vorgesehen ist, sollten klare Regelungen über die sichere Nutzung mit der supportgebenden Fachkraft oder Fachfirma zugrunde gelegt werden.

- **Einrichtung von Sperrlisten:** Die Erreichbarkeit von nicht benötigten Zielrufnummern und Rufnummerngruppen, wie zum Beispiel Vorwahlen bestimmter Länder oder Dienste, kann durch Eintrag in eine Sperrliste im TK-System verhindert werden. Rufnummernsperren können auch beim Anschlussnetzbetreiber beauftragt werden. Die Einrichtung muss auf die individuellen Erfordernisse des Unternehmens ausgerichtet und gegebenenfalls an sich ändernde Verhältnisse angepasst werden. Sperrlisten bieten zusätzlichen Schutz, sind aber als isolierte Maßnahme nicht ausreichend.

- **Frühwarnzeichen erkennen:** Auch kann es sich empfehlen, das Verbindungsaufkommen regelmäßig (zum Beispiel wöchentlich) auf Auffälligkeiten zu überprüfen. Unter Umständen lassen sich so Angriffsversuche rechtzeitig erkennen und verhindern oder Schäden zumindest begrenzen.

- **Pflege der TK-Software:** Verbesserte Softwareversionen (Patches) mit Sicherheitsbezug sollten unverzüglich nach Herstellerfreigabe eingespielt werden. Die Sicherheitshinweise des Herstellers gilt es zu beachten.

- **Fachkundige Betreuung sicherstellen:** In manchen Fällen fanden Angreifer völlig ungeschützte TK-Systeme vor. Planung, Installation, Administration und Instandhaltung von TK-Systemen erfordern für die jeweilige Aufgabe spezifische Kompetenzen. Potenziell sicherheitsrelevante Arbeiten sollten nur durch Fachkräfte beziehungsweise geschultes Personal erbracht werden.

- **Sicherheit im Internet:** Wenn das TK-System über direkte oder indirekte Verbindung zum Internet verfügt, erfordern Schutzkonzepte auch die Berücksichtigung spezifischer IT-Sicherheitsmechanismen. *(DK)*

Quelle: TK-Anlagen-Schutz-Flyer des LKA NRW, Bitkom und VAF / Herausgeber: VAF Bundesverband Telekommunikation e.V.