Telefonanlage im Unternehmen

Wichtige Hinweise für den Schutz Ihres Telekommunikationssystems

vor Hackern und Gebührenbetrügern

BITKOM

POLIZEI Nordrhein-Westfalen Landeskriminalamt Cybercrime

VAF Bundesverband Telekommunikation

Ihre Telefonanlage ist zum Angriffsziel geworden

»Sie haben am Wochenende 800 Gespräche nach Asien, Afrika und Osteuropa geführt.« Solche Benachrichtigungen an ein nichts ahnendes Unternehmen irgendwo in Deutschland sind inzwischen keine Ausnahme mehr. Mit der nächsten Telefonrechnung kommen dann auf die betroffene Firma mitunter erhebliche Forderungen für Verbindungsentgelte zu. Typisch sind einige Tausend Euro, die Beträge können aber auch drastisch höher sein. Jedes Unternehmen kann zum Angriffsziel werden, ob Freiberufler, Handwerksbetrieb oder Anwaltskanzlei, ob Mittelständler oder Großunternehmen.

»Sie haben am Wochenende 800 Gespräche nach Asien, Afrika und Osteuropa geführt?«

Meistens erfolgen die Angriffe am Wochenende, wenn niemand im Unternehmen ist. Kriminelle Hacker verschaffen sich Zugang über das Telefonnetz oder – je nachdem welche Telefontechnologie verwendet wird – auch über das Internet. Ist der Einbruch in das Telekommunikationssystem (TK-System) der Firma erst einmal gelungen, so werden automatisiert möglichst viele, kurze Verbindungen zu beispielsweise Mehrwertdienste-Nummern im Ausland aufgebaut. Zu oft können die Täter tatsächlich abkassieren und verstecken sich hinter kurzlebigen Briefkastenfirmen in verschiedensten Teilen der Welt.

Nachlässigkeit spielt den Tätern in die Hände

Besonders leicht ist es für die Angreifer, wenn bei den persönlichen Sprachboxen (integrierte Anrufbeantworter) werksseitig voreingestellte Passwörter (z. B. »0000«) nicht geändert oder in zu leichte Varianten geändert wurden (z. B. »1234«) und aus diesen Boxen Verbindungen nach außen aufgebaut werden können. Genau danach suchen

Persönliche Sprachboxen sind weitverbreitet

Wie viele gibt es in Ihrem Unternehmen?

Sind alle geschützt?

viele der Angreifer und tätigen mit automatisierter Software abends und nachts deutschlandweit massenhaft kurze Testanrufe (Ping-Calls). Nach dem Zufallsprinzip werden ganze Rufnummernblöcke von Unternehmen nach Schwachstellen durchsucht. Wenn die Software auf keine Pass-

> ***Mitunter berichten Reinigungskräfte, dass sie abends ein vielfaches, kurzes Klingeln aus den Büros gehört haben – ein klares Zeichen, dass gerade versucht wird, ins TK-System einzubrechen.***

worthürde trifft oder eine zu schwache Hürde überwindet, kann der Angriff sofort beginnen. Um unentdeckt maximal abschöpfen zu können, erfolgt der Angriff jedoch oft erst ab dem folgenden Freitagabend bis montags früh. Eine besondere Gefährdung besteht an verlängerten Wochenenden, wie beispielsweise zu Ostern.

Sie können sich schützen!

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.

Unsere Tipps:

Passwortschutz für Ihr TK-System

Für persönliche Sprachboxen (integrierte Anrufbeantworter) müssen immer vom Nutzer individuelle Passwörter vergeben werden. Keinesfalls dürfen werksseitige Voreinstellungen belassen werden. Sensibilisieren Sie alle Nutzer!

Sind im TK-System sogenannte 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 ggfs. 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 (z. B. 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. Beachten Sie die Sicherheitshinweise des Herstellers.

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 bzw. 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.

Vernetzte Welten

Noch nie waren die Vielfalt und die Innovationsgeschwindigkeit in der Telekommunikation so groß wie heute. Neben klassischen Bauformen von TK-Systemen (analoge Technik, ISDN) ist heute weitgehend Voice-over-IP (VoIP) verbreitet. Mobile Endgeräte (Laptops, Tablets, Smartphones) werden mit TK-Systemen verbunden, und internetbasierte Anwendungen werden in TK-Konzepte integriert. Zunehmend wachsen Telekommunikation, Internet, Informationstechnik und Mobilkommunikation zusammen. Damit ergeben sich zahlreiche neue Anwendungsmöglichkeiten für Unternehmen.

Zugleich wandeln sich mit den technischen Entwicklungen die Schutzanforderungen für TK-Systeme, und Anwender werden sich auch auf neue Angriffsszenarien einstellen müssen. Das Bewusstsein für diese Zusammenhänge ist darum eine wesentliche Voraussetzung für die künftige Sicherstellung von hohen Schutzniveaus.

»Wir haben erst lernen müssen, dass diese Firewall Löcher hat.«

Nicht jede Firewall erkennt VoIP-Daten. Wird über VoIP telefoniert, erfordert dies angepasste Sicherheitseinrichtungen, z. B. den Einsatz »VoIP-fähiger« Firewalls.

Es informieren:

Nach Erkenntnissen des Landeskriminalamts NRW sind steigende Schäden durch Hackerangriffe auf TK-Anlagen zu verzeichnen. Daraus folgt ein erhöhter Handlungsbedarf zur Abwehr der Täter. Diese Informationsschrift soll einen Beitrag zur Bewusstmachung und Prävention bilden. Für den Fall eines versuchten oder vollendeten Angriffs auf eine TK-Anlage im Unternehmen steht das Cybercrime-Kompetenzzentrum des LKA NRW mit seiner Zentralen Ansprechstelle Cybercrime und seinem Single Point of Contact rund um die Uhr (24/7) zur Verfügung.

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49, 40221 Düsseldorf

Zentrale Ansprechstelle Cybercrime
Telefon: 0211 939-4040
Telefax: 0211 939-194040
E-Mail: cybercrime.lka@polizei.nrw.de

www.lka.nrw.de

BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V.
Albrechtstraße 10 A, 10117 Berlin-Mitte
Kontakt: Johannes Weicksel
Telefon: 030 27576-250
E-Mail: j.weicksel@bitkom.org

www.bitkom.org

VAF Bundesverband Telekommunikation e.V.
Otto-Hahn-Straße 16, 40721 Hilden
Kontakt: Martin Bürstenbinder
Telefon: 02103 700-252
E-Mail: buerstenbinder@vaf-ev.de

www.vaf-ev.de

Herausgeber:

VAF Bundesverband Telekommunikation e.V.
Otto-Hahn-Straße 16
40721 Hilden
Telefon: 02103 700-250
E-Mail: info@vaf-ev.de
www.vaf-ev.de

Layout:

Uwe Klenner, Layout & Gestaltung

Bildnachweise:

Seite 1: © iStockphoto.com/hidesy
Seite 2 und 4: © iStockphoto.com/Minerva Studio
Seite 3: © mybreev.com