Technische und organisatorische Maßnahmen für Alcatel-Lucent OmniPCX Enterprise

Alcatel-Lucent OpenTouch Multimedia Services

Alcatel-Lucent OmniVista 8770 Network Management System

White Paper
Technische und organisatorische Maßnahmen

Alcatel·Lucent
Enterprise

Inhaltsverzeichnis

1. Vorwort

Thema: Dieses Dokument erklärt, mit welchen technischen und organisatorischen Strategien Alcatel-Lucent Enterprise allgemeine und persönliche Daten schützt. Die Maßnahmen gelten für Produkte und Dienstleistungen sowie das Design und die Entwicklung.

Die beschriebenen Schritte sind notwendig, um die Kontrollstandards hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit zu erfüllen. Wir weisen dabei über einen standardisierten Prozess nach, dass wir das für einen effizienten Datenschutz notwendige Niveau erreichen.

Verantwortungsbereich

- **Im Zusammenhang mit Kommunikationsprodukten**: Alcatel-Lucent Enterprise ist der Entwickler und Hersteller des Produkts. Das Produkt kommt jedoch beim Endkunden zum Einsatz.
- Für die Sicherheit hinsichtlich des **physischen Zugangs zum Produkt sowie die Telekommunikationssicherheit ist daher der Endkunde verantwortlich** – beziehungsweise der Auftraggeber, der den Prozess an einen Subunternehmer vergeben hat.

2. Allgemeines Sicherheitskonzept der Alcatel-Lucent Enterprise

A. Thema Sicherheit – Standortbestimmung

A.1 Einleitung

Viele Jahre lang boten moderne Technologien keinerlei Sicherheit. Täglich wurde von neuen Gefahren für die IT-Sicherheit berichtet. Sie gingen auf Schwachstellen im Betriebssystem (OS) oder Lücken in der Anwendungssicherheit zurück: Die Leute konnten einfach nicht mit den ständig neu veröffentlichten Software-Patches Schritt halten. Im Laufe der Zeit sind neue Bedrohungen aufgetaucht, die sämtliche Computer-Komponenten für ein breites Spektrum von Angriffen anfällig machen. Gleichzeitig hat das Zusammenführen mehrerer Geräte und Komponenten in IP-Infrastrukturen dazu geführt, dass diese Bedrohungen nicht mehr nur Personalcomputer oder Server betreffen.

Die Nachfrage ist aufgrund neuer Plattformen wie Tablets und Smartphones und neuer Technologien wie Bring your Own Device (BYOD) gestiegen. Das eröffnet Cyberkriminellen neue Möglichkeiten, in Unternehmensnetzwerke einzudringen. Zwar nutzen die meisten PC-Anwender immer noch Microsoft® Windows. Allerdings hat sich inzwischen ein Großteil der Entwicklung auf andere Plattformen verlagert, etwa auf Webanwendungen und mobile Lösungen. Die Unternehmen müssen deshalb die Sicherheitsrisiken neuer Umgebungen wie etwa Android® mit berücksichtigen.

Größte Schwachstellen und Angriffspunkte für Cyberkriminelle

A.2 Betriebssysteme

Betriebssysteme zählen nicht zu den am häufigsten genutzten Angriffspunkten, ziehen aber die Aufmerksamkeit der Medien auf sich. Das Patch-Management ist dafür verantwortlich, Sicherheitslücken in Betriebssystemen zu schließen.

Da es nur eine begrenzte Anzahl von Betriebssystemen gibt, Sind die Sicherheitslücken überschaubar. Trotzdem kann kein Betriebssystem für sich in Anspruch nehmen, frei von Schwachstellen zu sein.

Es gibt immer mehr BYOD-Lösungen, die auf dem beliebten mobilen Betriebssystem Android mit seinem offenen Ökosystem basieren. Diese Systeme könnten sich aber als besonders attraktives Ziel für Cyberkriminelle erweisen.

A.2.1 Anwendungen

Sicherheitslücken in IT-Systemen beschränken sich nicht nur auf das Betriebssystem. Auch die Anwendungen, die auf dem System laufen, brauchen Sicherheits-Patches. Einige bekannte Anwendungen, für die regelmäßig Patches veröffentlicht werden, sind Frameworks und Geschäftsanwendungen wie Microsoft Office, der Microsoft SQL Server und der Microsoft Exchange Server. Zu dieser Gruppe gehören auch Softwareprodukte unabhängiger Drittanbieter. Außerdem haben die Experten neue Schwachstellen mit Cross-Site-Scripting (XSS)-Lücken ausgemacht. Cyberkriminelle nutzen diese XSS-Schwachstellen aus, um Authentifizierungsnachweise oder Rechnungsdaten von Kunden zu stehlen und sich Kundenidentitäten anzueignen.

A.2.2. Viren

Ein Virus ist ein Programm oder ein Programmcode, der sich selbst vervielfältigt oder in ein anderes Programm, einen Boot-Sektor des Computers oder ein Dokument kopiert. Viren können als Anhang von E-Mail-Nachrichten oder in Datei-Downloads enthalten sein. Auch USB-Sticks oder CD-ROMs sind mögliche Übertragungswege. Die Anbieter von Virenschutzprogrammen erfüllen zwei Schutzfunktionen auf einmal. Sie stellen über ihren Update-Service Patches für Sicherheitslücken bereit, um die sich letztendlich das Patch-Management kümmert.

A.2.3 Würmer

Ein Wurm ist ein Virus, der sich von selbst ausbreitet. Würmer verändern keine Dateien, setzen sich aber im aktiven Speicher fest, wo sie sich vervielfältigen. Würmer verwenden automatische Komponenten des vorliegenden Betriebssystems, die In der Regel für den Benutzer nicht sichtbar sind. Der Nutzer bemerkt die Würmer meist erst dann, wenn die unkontrollierte Vervielfältigung Systemressourcen belegt, wodurch andere Prozesse langsamer ablaufen oder zum Stillstand kommen. Würmer nutzen oft bekannte Fehler oder Schwachstellen in der Software aus.

A.2.4 Spamming

Bei Spam handelt es sich um unerwünschte E-Mail-Nachrichten. Spam-Mails sind eine Art Massenmail, die oft an eine Liste verschickt werden. Die Daten stammen von Spambots oder Unternehmen, die auf die Erstellung von E-Mail-Verteilerlisten spezialisiert sind. Für den Empfänger sieht Spam normalerweise wie Junk-E-Mail aus. Spam-Mails sind vergleichbar mit unerbetenen Anrufen im Telefonmarketing – mit dem Unterschied, dass der Nutzer die Nachricht teilweise mitbezahlt, weil sich alle die Kosten für die Wartung des Internets teilen. Spam-Mails können auch Viren enthalten, die beim Öffnen der Nachricht das System infizieren.

A.2.5 Spyware

Als Spyware werden Technologien bezeichnet, die ohne deren Wissen Informationen zu Personen oder Organisationen sammeln. Im Internet beschreibt der Begriff Spyware Programmzeilen, die Computer infiltrieren, um heimlich Informationen über den Benutzer zu sammeln, um sie an Werbetreibende oder andere Parteien weiterzugeben. Die Spyware kann sich als Software-Virus oder über dei Installation eines neuen Programms Zugang zum Computer verschaffen.

A.2.6 Rootkit

Der Begriff Rootkit bezeichnet in der Regel Schadsoftware, die auf einem System unbemerkt bestimmte Prozesse oder Programme verschleiert und dem Angreifer den umfassenden Zugriff auf einen Computer ermöglicht.

A.2.7 APIs

Sicherheitsgefährdende Exploits nutzen oft mehrere Details einer Komponente, die auf niedriger Ebene laufen. Dazu gehören beispielsweise Layouts von Stack-Frames. Die vorhandenen Software-Analysewerkzeuge können Schwachstellen zwar effektiv identifizieren. Sie können jedoch keine Details niedriger Ebene modellieren und sind daher für die Suche nach Exploits ungeeignet.

Exploits auf der API-Ebene (Application Programming Interface): Softwarekomponenten können anfällig für API-Exploits sein – etwa, wenn eine Abfolge werkseitig zugelassener API-Operationen die Sicherheit der Komponente beeinträchtigt.

A.2.8 Netzwerk-Angriffe

Es gibt aktive und passive Angriffe. Beim aktiven Angriff geht es darum Systemressourcen zu verändern oder ihren Betrieb zu stören. Beim passiven Angriff wird versucht, Informationen aus dem System zu ziehen oder zu nutzen, ohne die Systemressourcen zu beeinträchtigen. Ein Beispiel dafür sind Abhörversuche.

Der Angriff kann von innen oder von außen erfolgen. Den Angriff von innen leitet eine Stelle innerhalb des Sicherheitsperimeters ein. Ein Beispiel dafür wäre der Zugriff über eine Schnittstelle, die Zugang zu Systemressourcen hat. ist, diese aber auf nicht autorisierte Art nutzt. Der Angriff von außen läuft über einen nicht autorisierten oder unrechtmäßigen Benutzer des Systems, der sich außerhalb des Perimeters befindet. Im Internet reicht die Bandbreite potenzieller Angriffe von außen vom Dummejungenstreich über das organisierte Verbrechen bis hin zum internationalen Terrorismus und zu Angriffen durch verfeindete Regierungen.

A.2.9 Angriffe über Mobilgeräte

Es gibt immer mehr BYOD-Systeme, die mit unterschiedlichen Betriebssystemen von iOS bis Android arbeiten. Die meisten Geräte verfügen dabei über keinerlei Malware-Erkennung. Die Unternehmen brauchen deshalb einen besseren Einblick in die Interaktion der Geräten innerhalb ihrer Unternehmensumgebung. Wenn Mobilgeräte gehackt werden, kann das dazu führen, dass Daten geklaut werden oder verlorengehen. Genauso riskant ist es, wenn ein Unternehmen bei Sicherheitsmaßnahmen wie der Identifizierung und Authentifizierung hinterherhinkt oder mobile Malware im Netzwerk verbreitet wurde.

Auswirkungen unterschiedlicher Sicherheitsrisiken

A.3 Computer-Notfallteam

Das Computer Emergency Response Team - Industry, Services and Tertiary (CERT-IST) ist in Notfällen das Sicherheitsnetz für die IT. Das Team ist für die Sicherheit der Wettbewerbsdaten verantwortlich. Es warnt die Administratoren und analysiert, wie durch Angriffe entstandene Fehler zu beheben sind. Das CERT hilft dabei, die Vorfälle in Kategorien einzuteilen.

Hacker, Einzeltäter oder Organisationen nehmen inzwischen auch die Kommunikation, Dienste und Geräte von Unternehmen ins Visier. Sie verwenden dabei dieselben Sicherheitslücken und Exploits wie in IT-Netzwerken. Alcatel-Lucent Enterprise behält die vom CERT identifizierten potenziellen Gefahrenquellen im Auge. Wir kümmern uns mit unseren Sicherheitsmaßnahmen und -prozessen um die Schwachstellen.

A.3.1 Datensammlung

Bei einem Angriff zur Datensammlung scannt der Angreifer ständig Ihre Systeme – mit dem Ziel, auf dem Netzwerk oder Server verfügbare Dienste zu entdecken. Der Angreifer kundschaftet also die Umgebung aus. Damit verfolgt er zwei klar umrissene Ziele:

- Er will herausfinden, ob das Ziel existiert und dessen Netzwerktopologie durchleuchten. Außerdem möchte er herausfinden, wohin die aus der Umgebung verschickten Daten laufen.
- Er möchte in seinem Ziel oder dessen Umgebung Schwachstellen aufdecken.

A.3.2 Zugriffsversuche

Diese Art von Angriff dient Unbefugten dazu, sich Zugriff auf Server zu verschaffen – um Dienste zu nutzen oder Daten zu extrahieren. Der Angreifer kann dabei unterschiedliche Ziele verfolgen:

- Er will sich sensible Informationen oder Vermögenswerte aneignen.
- Er möchte Lizenzen oder Software-Aktivierungscodes stehlen.
- Er will sich widerrechtlich Zugang zu den Diensten auf den Servern verschaffen.

A.3.3 Telefonie- und VoIP-Angriffe

Welche Absicht ein Angriff auf Telefondienste verfolgt, ist leicht nachzuvollziehen. Dies sind die verschiedenen Kategorien von VoIP-Angriffen:

- Lahmlegen des Service
- Diebstahl von Identitäten und Diensten
- Abhörversuch
- Vishing (VoIP-Phishing)
- Einschleusen von Viren und Malware, die auf Softphones abzielen (eingebettete Software von IP-Tischtelefonen)
- Denial-of-service (DoS)/Distributed denial-of-service (DDoS)
- PIT
- Anrufmanipulation und Man-in-the-Middle-Angriffe
- Gebührenbetrug

A.3.4 Gebührenbetrug

Bei der unbefugten gebührenfreien Nutzung verwenden nicht autorisierte Personen das Dial-through-System eines Unternehmens für kostenlose Ferngespräche. Die Betrüger sitzen oft außerhalb des Unternehmens.

Solche Betrugsversuche können erhebliche wirtschaftliche Konsequenzen haben. In der Vergangenheit waren hauptsächlich größere Unternehmen mit teuren und leistungsfähigen Telefonsystemen Ziel der Betrüger. Heute haben sie auch kleinere und mittelständische Unternehmen im Visier.

A.3.5 Denial-of-Service

Es gibt verschiedene Varianten von Denial-of-Service-Angriffen. Das Hauptziel ist jedoch immer, Server, Netzwerke und Anwendungen so zu stören, dass sie auf die Anfragen der Benutzer nicht mehr oder nur noch unzureichend reagieren.

Die Mehrzahl der Denial-of-Service-Angriffe erfolgen anonym, da der Server dafür keine Informationen zum Angreifer zurücksenden muss.

Beim Distributed-Denial-of-Service (DDoS) handelt es sich um einen Angriff, der von mehreren Stellen aus gestartet wird. Bei einem verteilten Angriff sind die angreifenden Computer-Hosts oft sogenannte Zombie-Systeme, die über Breitbandverbindungen durch Viren oder

Trojanerprogramme kompromittiert wurden. Der Täter kann dadurch den Rechner fernzusteuern und den Angriff lenken. Dafür Verwendet er oft ein Botnetz – eine Ansammlung von Programmen, die mit dem Internet verbunden sind und mit anderen ähnlichen Programmen kommunizieren, um bestimmte Aufgaben auszuführen. Wenn genügend Slave-Hosts vorhanden sind, lassen sich damit sogar die Dienste der größten und am besten vernetzten Websites lahmlegen.

A.3.6 Würmer und Viren

Ein Virus ist ein bösartiges Programm, das sich automatisch reproduzieren kann. Der Virus ist in eine Anwendung, ein Programm oder eine andere ausführbare Datei eingebettet und läuft oft unbemerkt im Hintergrund.

Ein Wurm ist ein eigenständiges Programm, das sich über eine Netzwerkverbindung von Computer zu Computer oder Server zu Server verbreitet. Die Weitergabe führt häufig dazu, dass die Netzwerke überlastet werden.

A.3.7 Verdächtige Aktivitäten

Zu verdächtigen Aktivitäten zählen Zwischenfälle und Datenübertragungen, die nicht mit den erwünschten Aktivitäten in einem Netzwerk, auf einem Server oder in einer Anwendung in Verbindung stehen.

Ein Zwischenfall kann je nach Unternehmen unterschiedliche Konsequenzen haben. Wie stark sich der Zwischenfall auf das Unternehmen auswirkt, hängt vom Geschäftsumfeld ab. Das gilt es beim Aufsetzen der Sicherheitspolitik für das Unternehmen zu berücksichtigen.

B. Alcatel-Lucent Enterprise im Dienste der Sicherheit

„Sicherheit ist ein Prozess, kein Produkt.[1]“

Heutzutage muss das IT-System eines Unternehmens gut geschützt sein – von der Infrastruktur über den Server bis hin zu den Anwendungen. Die Sicherheit ist kein greifbares Produkt oder Merkmal, sondern vielmehr ein Prozess, bei dem eine Organisation Maßnahmen zum Schutz von Informationssystemen vor nicht autorisiertem Zugriff einführt.

Sicherheitsfragen sind ein zentraler Bestandteil globaler Lösungsarchitekturen. Es muss immer wieder die richtige Balance zwischen dem Wert der zu schützenden Daten und den Kosten der Schutzmaßnahmen gefunden werden. Sensible Daten müssen als wertvolles Gut identifiziert und geschützt werden.

Beim Ermitteln des richtigen Sicherheitskonzeptes ist auch der Nutzer mit einzubeziehen. Zu viele Sicherheitsmaßnahmen können den erfolgreichen Einsatz technologischer Lösungen beeinträchtigen. Außerdem kann eine zu hohe Komplexität die Kommunikation mit Kunden und Auftraggebern erschweren.

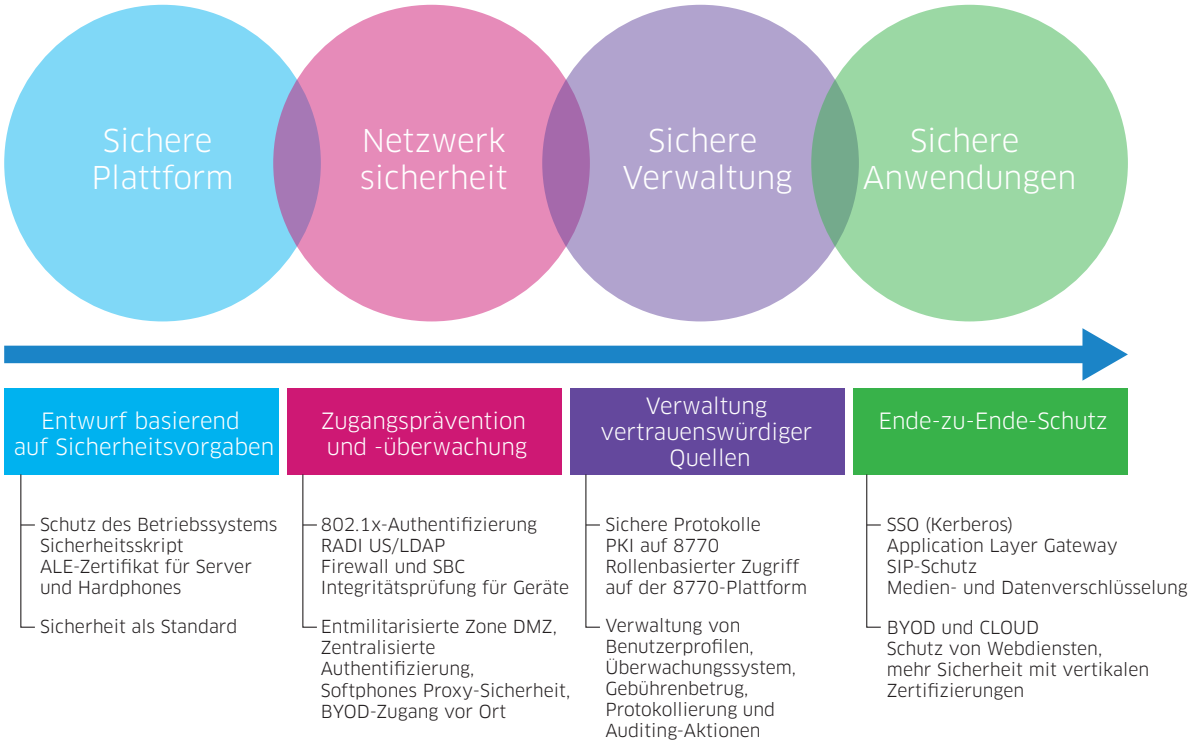
B.1 Tiefgreifende Schutzmaßnahmen

Wer das Herzstück des IT-Systems und damit die Lösung und das Netzwerk schützen will, muss sich auf allen Ebenen mit den Themen Sicherheit und potenzielle Schwachstellen befassen. Alcatel-Lucent Enterprise bietet einen ganzheitlichen Sicherheitsansatz, den wir im folgenden Modell c wollen.

Unsere tiefgreifenden Schutzmaßnahmen umfassen ein Information Assurance (IA)-Konzept, bei dem mehrere Schichten von Sicherheitskontrollen (Verteidigungsmaßnahmen) über ein komplettes IT-System verteilt sind. Die Absicht ist es, Redundanz zu erreichen und dadurch das Personal, die Prozesse, die technischen und physischen Elemente im System zu unterstützen – für den Fall, dass eine Sicherheitskontrolle ausfällt oder jemand eine Schwachstelle ausnutzt.

1 Dieses Zitat wird Bruce Schneier zugeschrieben, den der Economist als „Sicherheitsguru“ bezeichnet.

Ein umfassender Schutz des Systems ist die beste Verteidigung



Sicherheit ist keine einfache Funktion, die auf einer einzelnen Ebene implementiert wird. Die Maßnahmen müssen auf allen Ebenen des Netzwerks implementiert werden. Sie müssen dazu in der Lage sein, verschiedene potenzielle Schwachstellen über eine Vielzahl umgebungsbedingter Einschränkungen hinweg zu beheben.

Dieser Sicherheitsansatz ist in die Sicherheitspolitik für Kommunikationsprodukte eingebettet, die darauf abzielt, dem Kunden sichere Kommunikationslösungen bereitzustellen. So muss beispielsweise die Fabrikhalle eines Lieferanten über alle Arbeitsschritte und Meilensteine hinweg gut geschützt sein. Im Rahmen der Produktentwicklung haben wir die folgenden Kategorien definiert: Sicherheit in der Entwicklung, Sicherheit als Standard und Sicherheit bei der Umsetzung.

B.2 Produktsicherheits-Richtlinien

B.2.1 Sicherheit in der Entwicklung

Im Zusammenhang mit Kommunikationsprodukten versuchen wir mit den Sicherheitsmaßnahmen im Entwicklungsprozess Probleme so früh wie möglich zu beheben. Das erreichen wir, indem wir die Entwickler entsprechend schulen. Die Experten müssen lernen, Programmierschnittstellen zu vermeiden, die bekanntermaßen anfällig für Sicherheitslücken sind.

B.2.2 Sicherheit als Standard

Kommunikationsprodukte müssen vor der Installationsphase über werkseitig aktivierte Sicherheitsfunktionen verfügen.

B.2.3 Sicherheit in der Umsetzung

Im praktischen Einsatz müssen die Kommunikationsprodukte weiterhin sicher bleiben – auch im Angesicht ständig neuer Bedrohungen. Cyberkriminelle entdecken ständig neue Schwachstellen und Möglichkeiten für Angriffe. Deshalb ist es wichtig, die Eindringlinge immer

wieder mit neuen Strategien zu bekämpfen. Damit die Sicherheitsvorgaben weiterhin genau befolgt werden können, müssen innerhalb kurzer Zeit Sicherheits-Patches entwickelt werden, die etwaige Schwachstellen beheben. Darüber hinaus müssen wir alle Nutzer alarmieren und dazu auffordern, die Patches zu installieren. Außerdem muss sichergestellt sein, dass sich die Community auf die Qualität der Korrektur-Codes verlassen kann.

Kontrollfunktionen vorheriger Produktversionen müssen in nachfolgenden Versionen neu bewertet werden. Andernfalls kann das die Sicherheit beeinträchtigen. Wenn veröffentlichte Produkte mit den Sicherheitsentwicklungen Schritt halten, ist gewährleistet, dass die implementierte Version die Sicherheitsstandards erfüllt.

Es gibt keinen Kontrollmechanismus, der über einen längeren Zeitraum wirksam bleibt. Daher müssen wir mehrere Sicherheitskontrollen übereinanderschichten. So stellen wir potenziellen Angreifern mehrere Hürden auf einmal in den Weg.

Eine Firewall ist eine gute Maßnahme, um ein Unternehmen in der Peripherie zu schützen. Als einzige Schutzstrategie reicht sie allerdings nicht aus. Wir müssen ein Intrusion-Detection-System (IDS) an der Peripherie installieren, das durch die Firewall geschützt ist. Dadurch werden die Administratoren zumindest gewarnt, wenn ein Angriff aus dem Internet die Firewall umgangen hat oder von einem Punkt innerhalb des LAN ausgeht.

Ein wirksamer mehrschichtiger Ansatz ist eine Schutzmaßnahme, die Angriffe unterbindet – gestützt durch Schutzmechanismen, die erfolgreiche Angriff erkennen und die Administratoren alarmieren. In Umgebungen mit erhöhten Sicherheitsanforderungen kann eine dritte Schutzebene helfen, die Folgen erfolgreicher Angriffe abzudämpfen.

Das oben erwähnte IDS ist nicht ausreichend, wenn stringente Sicherheitsmaßnahmen erforderlich sind. Damit Durchbrüche der Firewall an der Peripherie möglichst wenig Schaden verursachen, müssen die zentralen LAN-Router so konfiguriert sein, dass sie alle nicht ausdrücklich erlaubten Datenübertragungen zurückweisen – zum Beispiel Daten, die aus dem Internet von privaten IP-Adressen oder von nicht zugewiesenen privaten Adressen stammen.

Wenn wir dieses Prinzip lokal auf ein System anwenden, können wir über die Zugriffskontrolle des Dateisystems die Schäden begrenzen, die erfolgreiche Angriffe anrichten.

Eine weitere wichtige Sicherheitsebene ist eine Sicherheitskontrolle zur Abschreckung, die potenzielle Angreifer darauf aufmerksam macht, dass ihr beabsichtigtes Ziel bereit ist, sich mit allen möglichen Mitteln zu schützen – einschließlich strafrechtlicher Verfolgung.

Letztlich kann es in vielerlei Hinsicht helfen, wenn die Aktionen der Nutzer und Administratoren zurückverfolgt werden können. Das ist nicht nur bei der Verfolgung der Täter hilfreich, sondern auch bei forensischen Analysen von Verstößen. Auf dieser Grundlage können wir Korrekturmaßnahmen ergreifen, um erneute Übergriffe zu verhindern.

B.2.4 Sicherheit bei der Entsorgung

Diese letzte Sicherheitsphase greift, wenn der Kunde ein oder mehrere Kommunikationsprodukte oder -lösungen außer Betrieb nimmt und das Material sicher entsorgt werden muss. Das größte Sicherheitsproblem besteht darin, dass vertrauliche oder personenbezogene Daten versehentlich offen gelegt werden könnten. Diesem Problem begegnet man in der Regel dadurch, dass man die physischen Speichermedien vernichtet.

B.2.5 Product Security Incident Response Team (PSIRT)

Wir wissen, wie wichtig es für unsere Kunden ist, dass sie sich auf sichere Produkte und Lösungen verlassen können. Bei der Entwicklung der ALE-Produkte achten wir darauf, dass alle notwendigen Schutzmaßnahmen berücksichtigt werden. Dies sind die Eckpunkte unseres umfassenden Sicherheitsprogramms:

- Bewährte Verfahren, Prozesse und Werkzeuge zur sicheren Software-Entwicklung
- Einhalten strengster Anforderungen an die Produktsicherheit
- Validierung und Überprüfung der Sicherheit vor der Freigabe

Trotz dieser Sicherheitsstrategien und der damit verbundenen Maßnahmen kann es in den Softwarekomponenten unserer Produkte Schwachstellen geben, die Angreifer ausnutzen können und die den Schutz unserer Produkte bei Einsatz in einem Kundennetzwerk beeinträchtigen können.

Das Product Security Incident Response Team (PSIRT) kümmert sich um Sicherheitsfragen. Das PSIRT-Team beschäftigt sich ausschließlich mit Anfragen, Nachforschungen und Berichten zu Schwachstellen oder technischen Problemen, die sich auf ALE-Produkte und -Lösungen auswirken.

Mehr über das PSIRT erfahren Sie unter: https://www.al-enterprise.com/en/support/security-advisories

B.2.6 Melden möglicher Sicherheitslücken

Wenn Sie Einzelpersonen oder in Ihrer Organisation ein technisches Sicherheitsproblem mit einem ALE-Produkt oder einer ALE-Lösung entdecken, sollten Sie sich an das ALE PSIRT wenden. Beachten Sie dabei bitte die folgenden Regeln:

1. Besorgen Sie sich den öffentlichen ALE PSIRT PGP-Schlüssel. Nur so können wir gewährleisten, dass die Kommunikation vertraulich abläuft. Die vertrauliche Behandlung der Anfrage ist in dieser Phase ein zentraler Aspekt im Sinne Ihrer Sicherheit als Kunde. Die Behandlung Ihrer Anfrage berührt unsere Richtlinien zur Offenlegung Ihrer Daten.
2. Füllen Sie den Vulnerability Summary Report (VSR) aus.
3. Schicken Sie den ausgefüllten Bericht per E-Mail an: psirt@al-enterprise.com
4. Schicken Sie unter Umständen die E-Mail mit dem Bericht zusammen mit dem öffentlichen PGP-Schlüssel der Organisation, die das Problem gemeldet hat, und schützen Sie bei Bedarf die Nachricht mit dem öffentlichen PGP-Schlüssel des ALE PSIRT.

PSIRT hält sich beim Austausch mit den Beteiligten, die das Problem gemeldet haben, an den unten beschriebenen Ablauf: Die Kommunikation mit allen beteiligten Parteien ist ein Schlüsselfaktor bei der Behebung der Schwachstelle.

Andere Kanäle zur Kontaktaufnahme mit Alcatel-Lucent Enterprise

Als Kunde können Sie mutmaßliche Sicherheitslücken auch gern über die üblichen Support-Kanäle melden. Je nach Wartungsvertrag können Ihnen die unten aufgeführten Ansprechpartner bei weniger spezifischen Problemen weiterhelfen:

- Technischer Support zur Feststellung, ob überhaupt ein Sicherheitsproblem besteht
- Konfigurieren eines ALE-Produkts für bestimmte Sicherheitsfunktionen
- Fragen zu einem angekündigten Sicherheitsproblem mit einem ALE-Produkt
- Implementieren bestimmter behelfsmäßiger Lösungen für Schwachstellen

Bitte beachten: Handelt es sich um Sicherheitsvorfälle, die „live“ in bereitgestellten Netzwerken und Lösungen auftauchen, wenden Sie sich bitte NICHT an das PSIRT-Team, um den Vorfall zu melden und einen Support anzufordern. Solche Vorfälle sind über die bekannten Kanäle des Kunden-Supports zu melden.

.

B.2.7 Product Security Incident Response Process

1. Melden Sie die Schwachstelle unter psirt@al-enterprise.com.
2. Alcatel-Lucent Enterprise bestätigt dem Sender der Meldung, dass der VSR empfangen wurde.
3. Das PSIRT-Team analysiert, wie relevant das Problem ist. Die Bericht erstattenden Parteien werden regelmäßig über den Stand der laufenden Untersuchungen zur Schwachstelle informiert.
4. Das ALE PSIRT gibt die Ergebnisse der Analyse an die Bericht erstattenden Parteien weiter.
5. Bei Auswirkungen auf die Sicherheit unternimmt Alcatel-Lucent Enterprise die folgenden Schritte:
   - Koordination der Problembehebung und der Folgenabschätzung
   - Festlegen eines Zeitrahmens für Korrekturen, Benachrichtigungspläne und Meldungen an öffentliche Organisationen wie mitre.org und Organisationen des Community Emergency Response Team (CERT).

B.2.8 Schutz der Anwendungen von Drittanbietern

Das ALE PSIRT arbeitet zur Koordination mit Drittanbietern zusammen, um Meldungen zu Schwachstellen zu verwalten. Dazu gehören Organisationen wie das CERT-IST, die National Vulnerability Database (NVD) und das US-CERT. Die Meldungen können über Softwarelösungen von Drittanbietern eingereicht werden, die in ALE-Produkte und -Lösungen eingebettet sind oder darin verwendet werden.

Die Berichte sind durch eine eindeutige CVE-Nummer (Common Vulnerabilities and Exposures) gekennzeichnet. Unsere ALE-Teams nehmen alle CVE-Fälle unter die Lupe, um eine angepasste Risikobewertung zu erstellen. Dieser können Sie entnehmen, welche Auswirkungen sich für unsere Produkte tatsächlich ergeben.

Zur Umsetzung von Sicherheitspatches geben wir neue Releases heraus, die Upgrades für Komponenten und Schwachstellen beinhalten. Diese gelten auch für ursprünglich nicht auf ALE aufgebaute Systeme (Non-ALE Originating Systems, kurz: NAOS) und freie Open-Source-Software (FOSS).

Das ALE PSIRT verwendet Version 3.0 des Common Vulnerability Scoring System (CVSS), um die gemeldeten und analysierten Schwachstellen auszuwerten. Der numerische CVSS-Score liefert Standardinformationen über das geschätzte Risiko für eine bestimmte Schwachstelle.

Wenn eine oder mehrere der folgenden Bedingungen vorliegen, gibt Alcatel-Lucent Enterprise eine öffentliche Sicherheitsanweisung heraus:

- Ein Prozess zur Reaktion auf einen Vorfall wurde abgeschlossen. Dabei wurde festgestellt, dass Software-Patches oder Ersatzlösungen zur Behebung der Schwachstelle existieren, oder es ist eine spätere öffentliche Bekanntgabe von Code-Fixes geplant, um Schwachstellen mit hohem bis kritischem Schweregrad zu beheben.

- Es wurde beobachtet, dass Schwachstellen aktiv ausgenutzt wurden, was zu einem erhöhten Risiko für unsere Kunden führen könnte. Unter Umständen veröffentlichen wir vorläufige Sicherheitsanweisungen, bevor wir Patches oder Korrekturen herausbringen, um unsere Kunden über die potenziellen Risiken zu informieren.

- Die Veröffentlichung von Informationen zur Schwachstelle kann unsere Kunden einem potenziell erhöhten Risiko aussetzen. Unter Umständen veröffentlichen wir vorläufige Sicherheitsanweisungen, bevor wir Patches oder Korrekturen herausbringen, um unsere Kunden über die potenziellen Risiken zu informieren.

Weitere Informationen finden Sie unter:
http://enterprise.alcatel-lucent.com/?content=ALEPSIRT&page=overview

C. Erfüllung von Sicherheitsstandards

Alcatel-Lucent Enterprise bietet umfassende Lösungen, die die Einhaltung gesetzlicher Bestimmungen gewährleisten:

- Sarbanes-Oxley (SOX)
- Gramm-Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- BALE II
- Payment Card Industry Data Security Standard (PCI DSS)
- MIFID2
- ISO 17799 und BS 7799

Der HIPAA und der PCI DSS sehen vor, dass bei der Verarbeitung sensibler Daten im medizinischen Umfeld, beim Banking oder im Bereich von Zahlungssystemen der Datenschutz und die Vertraulichkeit gewährleistet sind. Das System Alcatel-Lucent OmniPXC® Enterprise (OXE) kann diese strenge Anforderung erfüllen, indem es die gesamte Kommunikation über das Netzwerk auf Grundlage der IP Premium Security-Funktion oder der nativen Verschlüsselung verschlüsselt.

Bei ISO/IEC 17799 handelt es sich um eine Datenschutznorm, die im Juni 2005 die Internationale Organisation für Normung (ISO) und die Internationale Elektrotechnische Kommission (IEC) veröffentlicht haben. Die Norm wurde im Juli 2007 umbenannt zu ISO/IEC 27002:2005.

Die ISO/IEC 27002 enthält Empfehlungen für Best Practices beim Management der Informationssicherheit – genauer gesagt bei der Initiierung, Implementierung oder Wartung von Managementsystemen für die IT-Sicherheit (ISMS). Die Informationssicherheit wird in der Norm im Kontext der C-I-A-Triade definiert:

Vertraulichkeit

Im Sinne der Norm ISO 27002 setzt die Vertraulichkeit von Datenquellen eine strenge Zugriffskontrolle für die betreffenden Quellen voraus. Es sind alle in die Lösung integrierten Funktionen und Mechanismen zu berücksichtigten, um strenge Authentifizierungs- und Autorisierungsebenen in Abhängigkeit von Benutzerprofilen zu gewährleisten.

ALE-Kommunikationsprodukte befassen sich auf Verwaltungs- und Systemebene mit diesen unterschiedlichen Problemen.

Integrität

Es ist unerlässlich, dass die Informationen und Verarbeitungsmethoden akkurat und vollständig sind. In die ALE-Kommunikationsprodukte sind spezielle Funktionen integriert, mit denen wir die Integrität sowohl der System- als auch der Datenbankdateien gewährleisten.

Verfügbarkeit

Die Architektur der ALE-Kommunikationsprodukte sorgt für eine hohe Verfügbarkeit der Dienste und Ressourcen. Das System basiert auf verschiedenen Mechanismen auf Serverebene (Redundanz) und auf Ebene der Telefoniedienste (Overflow von öffentlich zu privat).

Die Common Criteria (ISO 15408) stellen sicher, dass Produkte für die IT-Sicherheit rigoros spezifiziert, entwickelt und evaluiert werden. Die Bewertungssicherheitsstufe (Evaluation Assurance Level, kurz: EAL) besteht in einer numerischen Einschätzung eines Produktes. Sie gibt wieder, welche Sicherheitsanforderungen während der Evaluation nach den Common Criteria (CC)

erfüllt wurden. Die CC führen sieben Stufen auf. EAL1 ist die niedrigste und EAL7 die höchste Stufe. Die Stufen EAL1 bis EAL4 sind für Produkte im zivilen Kontext gedacht. Die Stufen EAL5 bis EAL7 sind Produkten im militärischen Kontext vorbehalten.

Die IP-Telefonielösung von Alcatel-Lucent Enterprise ist nach den Common Criteria als System der Stufe EAL2+ zertifiziert. Der Zielperimeter umfasst unsere IP-PBX-Lösung Alcatel-Lucent OmniPCX Enterprise Communication Server und das Netzwerkmanagement-System Alcatel-Lucent OmniVista® 2500 zur Verwaltung/Konfiguration. Diese Zertifizierung bewertet, inwiefern bestimmte Sicherheitslösungen angemessen sind. Das Verhältnis zwischen den verbreiteten Sicherheitsbedrohung en für Kommunikationslösungen (IP-Telefonanlagen inklusive Verwaltungsplattform) und den Schutzmechanismen und -funktionen muss stimmen. Zu diesen Sicherheitsmaßnahmen zählen die Entwicklung, Validierung, Lieferung und Installation der Produkte. Dieser Zertifizierungsprozess wurde unter Aufsicht der französischen Regierungsagentur Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) durchgeführt. Die staatliche Agentur ist in Frankreich für die Validierung von ALE-Produkten und die Bereitstellung der Zertifikate zuständig.

D. Empfehlungen zu bewährten Praktiken für Nutzer

Alcatel-Lucent Enterprise ist verantwortlich für die Gestaltung der Nutzerzugriffskontrollen. Außerdem müssen wir unsere Endkunden über die bewährten Praktiken informieren, die für die Zugriffsverwaltung gelten, wenn der Nutzer Zugang zu bestimmten Prozessen und Daten hat.

Diese Praktiken sind im folgenden Dokument ausführlicher beschrieben: TBE025 - OXE (OmniPCX Enterprise) Suite for MLE Security Guideline ed9a.pdf (Kapitel 13). Die Anleitung können unsere Vertriebspartner im ALE- Business Partner Portal aufrufen.

Die Sicherheit ist für jedes moderne Netzwerk von entscheidender Bedeutung. Wenn wir zu einem bestehenden IP-Netzwerk Telefoniedienste hinzufügen, hat das Auswirkungen, die sowohl für das Netzwerk als auch für die Sprachanwendung sorgfältig abgewogen werden müssen. Die Interaktion mit Anwendungen, die sich in einer Cloud-Infrastruktur befinden, kann zusätzliche Herausforderungen hinsichtlich der globalen Sicherheit mit sich bringen.

Nachfolgend finden Sie eine Reihe von Empfehlungen für eine sichere VoIP-Implementierung. Betrachten Sie diese Empfehlungen als Ergänzung bestehender Sicherheitsrichtlinien, die Ihr Unternehmen bereits definiert hat oder die für Sie formuliert wurden. Die folgenden Empfehlungen sind für die Installation von Kommunikationsprodukten in keiner Weise vorgeschrieben. ALE empfiehlt aber dringend, sich bei jedem VoIP-Projekt daran zu halten.

Die IP (Internet Protocol)-Technologie hat die Effektivität vieler Unternehmen erhöht und ihnen über E-Business-Anwendungen neue Einnahmequellen erschlossen. Meistens erfordern diese Anwendungen hochzuverlässige Netzwerke, die den Datentransfer in Echtzeit abwickeln. Sie müssen skalierbar sein, damit das System auch eine steigende Zahl an Anwendungen und Benutzern unterstützt. Außerdem müssen sie gegen ein breites Spektrum potenzieller Bedrohungen resistent sein.

Das Netzwerk muss gegen die unterschiedlichen Bedrohungen gewappnet sein. Und es muss dafür gesorgt werden, dass Kundenanwendungen nicht beeinträchtigt werden. Daher müssen beim modernen Netzwerkdesign die Sicherheitstechnologien im Mittelpunkt stehen.

Der erste Schritt zur Entwicklung eines sicheren Netzwerks besteht darin, effiziente Sicherheitsvorschriften mit den folgenden Vorgaben zu formulieren:

1. Nur sichere Geräte dürfen an das Netzwerk angeschlossen werden.
   - Alle PC-Server müssen konfiguriert und gut geschützt sein, bevor sie mit anderen an das Netzwerk angeschlossenen Geräten interagieren.
   - Die Netzwerk-Clients müssen so konfiguriert sein, dass potenzielle Angreifer sie so wenig wie möglichst für ihre Zwecke ausnutzen können.
2. Die Netzwerkumgebung sollte effiziente Funktionen zur Authentifizierung, Eindämmung und Isolation bieten. Außerdem muss sie effiziente Schutzfunktionen enthalten, die Angriffe vermeiden oder eindämmen.
3. Alle Verwaltungssysteme müssen rigoros geschützt und kontrolliert werden.
4. Die Interaktionen der Kunden müssen so gut geschützt werden, wie es die Sensibilität und der Stellenwert der von ihnen verwalteten Medien gebietet. (Je sensibler die Spracheingaben/Daten, umso aggressiver muss die Schutzmaßnahme sein.)

Warum muss die Infrastruktur für die Spracheingabe gesichert werden?

Ohne gezielte Sicherheitsmaßnahmen ist jeder Teil des Netzwerks potenziell anfällig für Angriffe oder nicht autorisierte Prozesse. Hacker und eigene Mitarbeiter können die Router, Switches und IP-Hosts von inner- und außerhalb des Netzwerks kompromittieren. Will der IT-Ingenieur die besten Möglichkeiten zum Schutz eines Voice-over-IP-Projekts ermitteln, das in einem Kundennetzwerk gehostet wird, muss er die verschiedenen Technologien und Strategien kennen, mit denen er Angriffe eindämmen kann.

D.1. Bewährte Praktiken beim Thema Sicherheit

Wie jede interne Ressource im LAN müssen auch ALE-Produkte vor externen Netzwerken und dem Internet geschützt werden – durch die passenden Strategien bei der Inbetriebnahme und Maßnahmen zur Sicherung der Netzwerkgrenzen wie etwa Session Border Controller (SBC), Reverse Proxy oder Firewall. Diese Technologien können externe Bedrohungen abwehren.

Eine vorrangige Maßnahme besteht darin, OmniPCX Enterprise, den Alcatel-Lucent OpenTouch® Multimedia Server (OTMS) oder andere ALE-Lösungen ohne diese Sicherheitselemente nicht direkt dem Internet auszusetzen. (Diese Regel gilt natürlich nicht für die Komponenten zur Sicherung der Netzwerkgrenzen.)

Zusätzlich zu den unten beschriebenen Geräten wird dringend empfohlen, geeignete Firewall-Systeme zu installieren. Damit lassen sich interne Angriffe (und Netzwerk-Scanning-Versuche) verhindern, die auf ALE-Server und Geräte im Netzwerk des Kunden abzielen.

Firewalls sind wertvolle Warnsysteme, anhand derer Administratoren unerwartete oder verdächtige ein- und ausgehende Datenübertragungen erkennen können.

D.2. Sicherheit der physischen Infrastruktur

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen die folgenden Maßnahmen, um Ihr System optimal gegen physische Bedrohungen abzusichern:

- Kommunikationsserver, IP-Media-Gateways und alle anderen Telefoniekomponenten sollten in gesicherten IT-Umgebungen mit ausreichenden physischen Zugangsbeschränkungen untergebracht sein. Verwenden Sie falls möglich abschließbare Schränke/Anlagen, um den physischen Zugang weiter einzuschränken.
- Kommunikationsserver, IP-Media-Gateways und alle anderen Telefoniekomponenten sollten mit einer ausreichenden Notstromversorgung ausgestattet sein. Dies gilt auch für die Ressourcen des Datennetzes.

- Falls möglich sollten alle Kommunikationsserver und andere Telefoniekomponenten über redundante Systeme verfügen. Für einen optimalen Schutz sollten redundante Komponenten an geographisch getrennten Orten platziert werden.

Empfehlungen zur Umsetzung

- Vermeiden Sie es nach Möglichkeit, redundante Komponenten an ein und dieselbe Netzwerkinfrastruktur anzuschließen. Redundante Kommunikationsserver sind sinnlos, wenn sie im Datenzentrum alle an einen gemeinsamen Ethernet-Switch oder eine Stromversorgungseinheit (PSU) angeschlossen sind.

D.3. Logische Segmentierung von Netzwerken

Mit gemeinsamen Netzwerkinfrastrukturen können Sie die Effizienz enorm steigern und Kosten stark reduzieren. Solche Systeme bieten Ihnen außerdem bessere Zugriffsmöglichkeiten. Das kann je nach Situation ein positiver und/oder negativer Aspekt sein.

Es kann gefährlich sein, unterschiedliche Arten der Datenübertragung miteinander zu vermischen. Um die Quality of Service (QoS) zu erhalten, die Verwaltung zu vereinfachen und die Sicherheit zu gewährleisten, sollten Sprachnachrichten und Datenübertragungen nach Möglichkeit in der IT-Logik getrennt werden.

Der Datentransfer kann über 802.1p und PBR (Policy-based Routing) priorisiert werden, ohne die Übertragung in mehrere Broadcast-Domänen (VLANs) aufzusplitten. Trotzdem ist es weitaus einfacher, QoS-Schemata zu entwickeln, umzusetzen und zu verwalten, die eine Segmentierung des Datenverkehrs verwenden.

Vom Standpunkt der Sicherheit aus bietet die Trennung des Datenverkehrs in verschiedene Ethernet-Übertragungsdomänen eine bessere DoS-Resilienz. Diese Maßnahme ermöglicht es außerdem, die Netzwerkgrenzen durch starke Maßnahmen zu schützen. Der Schutz der Netzwerkgrenzen kann ganz einfach über Switch-/Router-basierte Zugriffskontrolllisten (ACL) oder komplexere Lösungen erfolgen, die auf spezifischen Hardware-Anwendungen basieren. Dazu gehören die Angriffserkennung, Paketinspektionen und VPNs. In beiden Fällen ist die Trennung des Datenverkehrs in der IT-Logik der Schlüssel für eine effektive Kontrolle der Netzwerkgrenzen.

Eine der größten Bedrohungen für VoIP-Systeme ist der DoS-Angriff. VoIP-Systeme sind oft nicht das direkte Ziel von DoS-Angriffen, da die Plattformen und Endgeräte aufgrund ihrer stabilen Architektur schwer zu infizieren sind. Wenn ein VoIP-System komplett vom IP-Netzwerk abhängig ist, wird es dadurch allerdings zu einem großen direkten Ziel. Daher ist es sehr wichtig, die Datenübertragung in Echtzeit vom Datenverkehr zu trennen, der nicht in Echtzeit abläuft. Dies kann durch einen eigens eingerichteten Switch-Port und ein dynamisches VLAN erreicht werden.

Um die VLAN-Verwaltung zu vereinfachen, hat Alcatel-Lucent Enterprise die automatische VLAN-Zuweisung implementiert. Der Mechanismus wirkt sich automatisch auf die per VLAN geschickten Sprachdaten auf IP-Tischtelefonen aus. Der Mechanismus basiert auf einer doppelten DHCP-Abfrage.

Segmentieren und Filtern des Datenverkehrs – Empfehlungen zum Aufbau

Wenn ein Informationsaustausch zwischen den verschiedenen logischen Netzwerken erforderlich ist, sollte zusätzlich zur VLAN-Segmentierung eine Sicherheitsrichtlinie eingeführt werden, um den Datenfluss zwischen VLANs mit Hilfe der Zugriffskontrollliste zu überwachen. Diese Sicherheitsrichtlinien können auf Endnutzer-Adressen und IP-Flows basieren, die Nutzer oder VLAN-Instanzen verwenden.

Mit Firewall-Geräten können Sie die Filterregeln zwischen VLANs verwalten und sicherstellen, dass nur zugelassene Netzwerkelemente mit sensiblen Sprach-Servern kommunizieren können.

Eine Proxy-Komponente kann speziell für Softphone-Anwendungen installiert werden, die auf einem SIP-Protokoll zur Anrufsteuerung basieren. Einige dieser Proxy-Softphones unterstützen auch TLS und SRTP für sichere Softphone-Anrufe.

D.4. Filtern/Überwachen des Netzwerkverkehrs

Das Filtern und Überwachen des Netzwerkverkehrs gehört zu den Aufgaben, die grundsätzlich die Firewall übernimmt – je nach gewähltem Modell und Typ in verschiedenen Analysestufen. Andere Geräte wie Router können den Datenverkehr zwischen IP-Subnetzen filtern.

Eine Firewall ist ein System, das den unbefugten Zugriff auf oder aus einem privaten Netzwerk verhindert. Firewalls können sowohl in die Hardware als auch die Software integriert werden – oder in beide Komponenten. Firewalls werden häufig dazu genutzt, unbefugten Internet-Nutzern den Zugang zu privaten Netzwerken – insbesondere Intranets – zu verwehren. Alle Nachrichten, die ins Intranet gelangen oder es verlassen, passieren die Firewall, die jede Nachricht prüft und alles blockiert, was nicht den angegebenen Sicherheitskriterien entspricht.

Eine Firewall gilt als erste Verteidigungslinie zum Schutz privater Informationen. Um die Sicherheit zu steigern, können die Daten verschlüsselt werden.

Firewalls arbeiten grundsätzlich nach der Regel „Es ist alles verboten, was nicht ausdrücklich erlaubt ist." Einige Anwendungen wie VoIP machen es erforderlich, dass bestimmte spezifische TCP- und UDP-Ports geöffnet werden. Unabhängig vom Typ der Firewall verwendet der Filterprozess immer eine ACL.

Die ACL ist ein Verfahren zum Testen von Paketen, die das Netzwerk durchqueren. Die Komponente stellt fest, ob die Pakete an ihr Ziel weitergeleitet oder verworfen werden müssen. Eine ACL kann Parameter wie die Quelle und/oder das Ziel einer IP-Adresse, die Quelle und/oder das Ziel eines TCP/UDP-Ports und spezifische Protokolle überprüfen.

Firewalls können auch Application Layer Gateways (ALGs) implementieren. Ein ALG kontrolliert die Protokollkonformität, um jede Art von Fuzzing-Angriff zu vermeiden. Mit dem System können Sie auch Paketmanipulationen (für NAT-Operationen oder dynamische Pinholing-Operationen) durchführen. Das Gateway wendet Schutzmechanismen auf bestimmte Protokolle wie FTP oder HTTP an. ALGs können Sie auch für VoIP-spezifische Protokolle wie H323, SIP und CSTA implementieren.

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfiehlt:

- Verwenden Sie Firewalls, die eine „Stateful Packet Inspection" erlauben, mit „VoIP aware" gekennzeichnet und mit den Umgebungen von Kommunikationsprodukten kompatibel sind.
- Erzwingen Sie die Zugriffskontrolle mithilfe einer ACL, um den Zugriff zwischen Sprach- und Daten-VLANs zu beschränken und die Ausbreitung von DoS-Angriffen aus dem Datennetzwerk zu verhindern.

Empfehlungen zur Umsetzung

Die Firewall- und ACL-Implementierungen sowie die Wahl der Topologie gehören zur Sicherheitsstrategie des Kunden und liegen in seiner Verantwortung.

D.5. Private Adressen und NAT

Die Implementierung von Network Address Translation (NAT) oder Network Address Port Translation (NAPT) ermöglicht die Kommunikation zwischen einem privaten Netzwerk (nicht fürs Internet-Routing ausgelegter privater IP-Adressplan) und dem öffentlichen Netzwerk (fürs Internet-Routing ausgelegte Adressen).

Das NAT/NAPT-Schema bietet zusätzliche Sicherheit, indem es das private Netzwerk vor dem Internet verbirgt. Wenn Pakete die Domain-Grenze überschreiten müssen (NAT-Router), müssen Sie einige Änderungen an den Paket-Headern vorgenommen werden – zur Anpassung an die temporäre Zuordnung (Quell-IP, Ziel-IP und Port-Nummer). Dieses Verfahren ist für Daten uneingeschränkt anwendbar. Bei Voice over IP ist das allerdings nicht der Fall. Einige Anwendungen beinhalten Adress-Informationen innerhalb ihrer Nutzdaten (z. B. H.323 und SIP), und genauso verhält es sich bei VoIP-Systemen. Beispielsweise können UDP-Ports der H.245-Sitzungen, die in den IP-Nutzdaten enthalten sind, von einem generischen NAPT-Router nicht problemlos interpretiert werden. Infolgedessen ist keine Synchronisierung von UDP-Sitzungen möglich.

In den meisten Fällen funktioniert VoIP nicht, wenn ein NAT/NPAT-Router zwischen VoIP-Komponenten installiert ist.

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfehle folgende Maßnahmen, wenn bereits ein NAT/NPAT-Router im Netzwerk vorhanden ist:

- Umgehung des NAT/NPAT-Routers für den gesamten VoIP-Verkehr
- Verwendung des Bridged-Modus im VPN-Tunnel über das WAN
- Installation einer Remote Access Point (AP)-Lösung , um eine Verbindung über das Internet mit einem IP-Tischtelefon oder WLAN-Telefon zu ermöglichen, das ein Mitarbeiter im Homeoffice verwendet
- Empfehlung einer auf einem SBC basierenden Lösung für SIP-Nutzung im Remote-Betrieb (Hardphone und Softphone), um NAT-Probleme zu lösen

D.6. Integration von Infrastrukturdiensten

Zusammen mit den Kommunikationsnetzen haben sich auch die Erfinder bösartiger Programme weiterentwickelt. Die IT-Sicherheit ist ein ständiges Tauziehen, mit einem ständigen technologischen Schlagabtausch zwischen Netzwerkbetreibern und Angreifern: Jeder versucht, die Technologiesprünge optimal für sich auszunutzen.

In den frühen Tagen der Viren- und Wurmprogrammierung bestand das Ziel letztendlich darin, die Daten auf Großrechnern und/oder privaten Computern zu kompromittieren. Die Hersteller von Betriebssystemen, Softwareanbieter und Netzwerkadministratoren reagierten auf diese Bedrohungen, indem sie den Angreifern das Leben schwer machten. Dies führte dazu, dass die Zahl der Angriffe auf Datensammlungen abnahm, während die Fälle von Denial-of-Service-Angriffen stark zunahmen.

Die Programmierer von Schadsoftware und Netzwerk-Hacker profitieren einerseits von den genannten Technologiesprüngen. Andererseits verschieben sie ständig den Fokus ihrer Angriffe. Sie sind eine Art technologischer Opportunisten, die den Weg des geringsten Widerstandes suchen. Sie bewerten oft sorgfältig die Umgebung eines oder mehrerer Zielnetzwerke, um festzustellen, wie sie mit dem geringsten Aufwand den größten Schaden anrichten können. Eine Tendenz, die sich in den letzten Jahren herauskristallisiert hat, ist die starke Vorliebe der Hacker für Elemente der Netzwerk-Infrastruktur, die schlecht geschützt sind, leicht erobert werden können und dem Netzwerk kritische Dienste bereitstellen. Zu diesen neuen Zielen gehören VPN-

Gateways, Core-IP-Router, Drucker-Spooler/Server, Datenbanksysteme und DHCP-Ressourcen. Die Beseitigung oder Beeinträchtigung jedes dieser Infrastrukturdienste kann ein ansonsten gesundes Netzwerk außer Gefecht setzen oder ernsthaft behindern.

Mit den oben erwähnten Veränderungen im Angriffsverhalten sind die Netzwerkadministratoren zunehmend sensibler geworden, was die Konfiguration der Schutzmaßnahmen für Infrastrukturdienste betrifft. Dokumente zur Unternehmenssicherheitspolitik enthalten jetzt routinemäßig Abschnitte, in denen definiert wird, wie Infrastrukturdienste genutzt und wie neue Dienste in das Netzwerk eingeführt werden können – und welche Strategien weniger erfolgversprechend sind. Das setzt voraus, dass zusätzliche DHCP- und TFTP-Server zum Netzwerk hinzugefügt werden.

Früher wurde in diesem Zusammenhang die Routerkonfiguration angepasst, um die Erkennung und Weiterleitung zu ermöglichen. Diese Strategie gilt aber inzwischen nicht mehr als geeignete Maßnahme.

OmniPCX Enterprise kann zwar DHCP- und TFTP-Dienste für IP-Telefonie-Geräte und Media-Gateways hosten. Die Nutzung dieser eingebetteten Dienste ist aber nicht zu empfehlen, wenn die Umgebung gut geschützt sein soll. Die OmniPCX Enterprise-Lösung kann und sollte so eingesetzt werden, dass die vorhandenen Netzwerkinfrastruktur-Dienste und die bereits vorhandenen Redundanzen und Schutzvorkehrungen genutzt werden.

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen die folgenden Maßnahmen, wenn Sie Ihren Infrastrukturdienst optimal vor DoS-Angriffe schützen wollen:

- Überprüfen Sie, ob die vorhandene DHCP-Server-Ausrüstung, „herstellerspezifische Attribute“ nutzen kann, um Ihre IP-Tischtelefone mit angemessenen und vollständigen Konfigurationsinformationen zu versorgen und sicherzustellen, dass Schemata wie AVA (Automatic VLAN Assignment) praktikabel sind.
- Überprüfen Sie, ob die vorhandenen TFTP-Server-Geräte BINÄR- und CONFIG-Datei-Uploads vom OmniPCX Enterprise Communication Server empfangen und hosten können, um einen transparenten Betrieb mit OmniPCX Enterprise zu gewährleisten.
- Die Nutzung vorhandener DHCP- und TFTP-Infrastrukturdienste für sprachbezogene Aktivitäten steigert den Bedarf an Redundanz und Angriffsresistenz. Netzwerkadministratoren sollten über diese Anforderung informiert werden, um beurteilen zu können, ob zusätzliche Schutzmaßnahmen erforderlich sind oder nicht.

Empfehlungen zur Umsetzung

Integration von Infrastrukturdiensten zur Maximierung der Systemsicherheit:

- Netzwerk-Router und ACL-Filterpunkte sollten DHCP- und TFTP-Anforderungen an den Kommunikationsserver kontrollieren, um sogenannten Sättigungsangriffen einen Riegel vorzuschieben.
- AVA-Dienste sollten auf bestehenden DHCP-Servern in Übereinstimmung mit den Richtlinien konfiguriert werden, wie sie im Dokument „Automatic VLAN Assignment – PreSales Communication“ definiert sind.

D.7. Authentifizierungsrahmen (allgemeine Geheimhaltung)

D.7.1. Allgemeine Authentifizierungselemente

Integration der Authentifizierungsinfrastruktur – Empfehlungen zum Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen die folgenden Maßnahmen, wenn Sie ein benutzerfreundliches und einfach zu verwaltendes System bereitstellen und gleichzeitig das höchstmögliche Maß an Netzwerksicherheit aufrechterhalten wollen:

- Verwenden Sie für den Netzwerkaufbau über den gesamten Sprach- und Datenverkehr hinweg gemeinsame Serverelemente zur Netzwerkauthentifizierung. Verwenden Sie für die 802.1X-Authentifizierung von IP-Desktop-Telefonen und anderen Endpunkten dieselben RADIUS-Server, mit denen Sie auch die Anforderungen für den Remote-VPN-Zugriff und den Zugriff über Wählleitungen authentifizieren.
- Es ist wichtig, dass ALLE Elemente des Netzwerks an einem strukturierten Authentifizierungsschema beteiligt sind. IP-Telefone, PC-Clients, drahtlose Clients und alle anderen Endpunkte MÜSSEN mit eingebunden sein. In den meisten Fällen bedeutet dies, dass alle Clients die 802.1X-Authentifizierung unterstützen müssen. Die Netzwerkinfrastruktur muss darüber hinaus in der Lage sein, mehrere 802.1X-Anforderungen pro Ethernet-Switch-Port zu authentifizieren.
- In den empfohlenen Authentifizierungssysteme müssen die notwendigen Redundanzen vorgesehen sein, damit sie nicht für Denial-of-Service-Angriffe missbraucht werden können.

  Hinweis: Wenn Sie innerhalb eines Netzwerkdesigns nur einen RADIUS-Server verwenden, wird dieser zu einem Single Point of Failure, was bei Unterbrechung zu massiven Ausfällen im gesamten Netzwerk führen kann.
- Bei Multi-Site-Designs sollten lokale Authentifizierungsressourcen oder Backup-Authentifizierungsressourcen an jedem Standort vorgesehen sein. Damit verhindern Sie, dass einfache WAN-Ausfälle den Betrieb des Telefonsystems erheblich beeinträchtigen.

Integration der Authentifizierungsinfrastruktur – Empfehlungen zum Aufbau

- Vermeiden Sie es nach Möglichkeit, redundante Komponenten an gemeinsam genutzte Netzwerkinfrastrukturen anzuschließen. Redundante RADIUS-Server bringen nur wenig, wenn sie alle an einen gemeinsamen Ethernet-Switch im Rechenzentrum angeschlossen sind, der ausgefallen ist.

D.7.2. Starke Authentifizierungslösungen

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen die folgenden Maßnahmen, um die Sicherheit von Netzwerk- und Telefonieanwendungen durch eine starke Authentifizierung zu erhöhen:

- Die Zwei-Faktor-Authentifizierung sollte nach Möglichkeit immer dann eingesetzt werden, wenn solche Lösungen und Richtlinien für den Einsatz innerhalb eines Kundennetzwerks existieren. Aufgrund der komplexen Bereitstellung ist es jedoch selten ratsam, ein Token-System ausschließlich für die Verwendung mit einem IP-Telefoniesystem vorzuschlagen.
- Definieren Sie klar, wo die Zwei-Faktor-Authentifizierung verwendet werden kann und sollte (z. B. in der Systemadministration und beim administrativen Zugriff auf das Alcatel-Lucent OmniVista® 8770 Network Management System). Legen Sie auch klar fest, wo sie NICHT verwendet werden kann und sollte (z. B. bei automatisierten 8770-Zugriffen, bei der 802.1X-Terminal-Authentifizierung und zur Validierung von Nutzer-PIN-Codes).

Empfehlungen zur Umsetzung

- Für die Zuverlässigkeit des Systems ist es entscheidend, dass die Elemente des RADIUS- und Token-Authentifizierungsservers über ausreichende Redundanzen verfügen, um die Verfügbarkeit zu gewährleisten.
- Bei Multi-Site-Designs sollten an jedem Standort lokale Authentifizierungsressourcen, Backup-Authentifizierungsressourcen oder On-Demand-Netzwerklinks als Backups vorgesehen sein. Damit verhindern Sie, dass einfache WAN-Ausfälle den Betrieb des Telefonsystems erheblich beeinträchtigen, indem sie den Zugriff auf die Authentifizierungsserver blockieren.

D.7.3. Authentifizierung von Anwendungen

In den vorherigen Abschnitte haben wir uns mit den Netzwerkzugangskontrollen und der Authentifizierungsinfrastruktur befasst. Es ist aber auch sehr wichtig, den Wert und die Bedeutung einer starken Anwendungsauthentifizierung und die Durchführbarkeit von Single-Sign-On-Lösungen zu berücksichtigen.

Ein einziges Passwort zur Verwaltung aller Zugriffsanfragen ist logischerweise ungünstig. Wenn jemand dieses Passwort manipuliert, ist auch der Zugang zu allen anderen Anwendungen mit demselben Passwort gestört. Separate Passwörter sind also allgemein die bessere Lösung – aber nur bis zu einem gewissen Punkt. Muss sich der Benutzer zu viele Passwörter merken, wird er irgendwann Passwortlisten anlegen, nur noch einfache Passwörter verwenden oder andere Schritte ergreifen, die gegen die Integrität und den Schutz der Passwörter verstoßen. Es ist daher wichtig, die richtige Balance zu finden.

Viele Netzwerkadministratoren gruppieren ihre Anwendungen nach Riskostufen in drei oder vier Kategorien. In den meisten Fällen ist es möglich, für Anwendungen innerhalb ein und derselben Risiko-Kategorie einen Zugriff auf Basis einer einzigen Authentifizierungsanfrage oder Single Sign-On (SSO) zu ermöglichen. Ein Beispiel für ein SSO wäre eine einzelne Authentifizierungsabfrage für einen PC-Client, der dem Nutzer Zugang zum physischen Netzwerk (802.1X), zu Microsoft/Linux/Novell-Netzwerkdomänen und verschiedenen anderen Anwendungen wie Internet-Proxy-Dienste und Instant-Messaging-Clients gewährt.

Einige Anwendungen sind immer als kritisch zu betrachten. Bei diesen Anwendungen müssen Sie separate Authentifizierungsabfragen und/oder separate Anmeldedaten für die Nutzer vorsehen. In vielen Unternehmen fallen E-Mails und der Zugang zu Online-Bewerbungsunterlagen in diese Kategorie.

Die Entscheidung, welche Anwendungen Authentifizierungsdaten gemeinsam nutzen dürfen, sollten Sie wenn möglich dem Kunden überlassen. Die Anwendungen sollten nach Möglichkeit die gemeinsame Konto-Authentifizierung und/oder das Single Sign-On unterstützen.

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen die folgenden Maßnahmen für Ihre Telefonie-Anwendungen, mit denen Sie bei der Authentifizierung die Sicherheit erhöhen und die Koordination verbessern:

- Sie sollten Ihre Telefonie-Anwendungen in eindeutige Risikostufen einteilen, um die Authentifizierungsdienste besser aufeinander abzustimmen.
- Wir raten dringend davon ab, Verwaltungsanwendungen wie OmniVista 8770 NMS in Single-Sign-On-Operationen zu integrieren.

D.7.4 Authentifizierung von IP-Tischtelefonen

Die Endpunkt-Authentifizierung wird seit vielen Jahren sowohl in Sprach- als auch in Datennetzen verwendet. In Sprachsystemen – besonders bei älteren nicht IP-basierten

Plattformlösungen – wurden nur selten Systeme zur Authentifizierung eingesetzt. Eine Ausnahme bildet der Zugriff auf Anwendungen wie Voicemail sowie spezifische Ersatz- und Verwaltungsfunktionen. Fassen wir die vorherigen Abschnitte kurz zusammen:

- Die Authentisierung ist ein wertvolles Sicherheits-Tool, solange Sie es universell nutzen.
- Lücken in Authentifizierungslösungen werden häufig auch genutzt.

Terminal-Authentifizierung – Empfehlungen zum Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen die folgenden Maßnahmen, um die Sicherheit von Netzwerk- und Telefonieanwendungen durch die Authentifizierung zu erhöhen:

- Die Netzwerkinfrastruktur (Ethernet-Switches) sollte dazu in der Lage sein, an jedem Switch-Port mehrere 802.1X-Clients zu authentifizieren.
- Für das Protokoll 802.1X ist ein Authentifizierungsserver (RADIUS) erforderlich, der die Übereinstimmung zwischen den vom Terminal gesendeten Anmeldedaten (Login/Passwort oder digitales X509-Zertifikat) und der Identitätsdatenbank überprüft, die an den Authentifizierungsserver angeschlossen oder zur globalen Nutzung im Unternehmen zentral angelegt ist.

D.8 Überlegungen zu drahtlosen Netzwerken

Für ein sicheres VoWLAN ist es erforderlich, Sprache und Daten voneinander zu trennen. Dadurch vermeiden Sie Angriffe aus dem Datennetz aufs Sprachnetz. Zur Umsetzung brauchen Sie unterschiedliche SSIDs für die Sprachverarbeitung und die Daten. Jede SSID ist mit einem WLAN beziehungsweise mit einem VLAN verbunden.

Wenn Sie die SSID-Übertragung verbieten, führen Sie damit keine zusätzliche Sicherheitsstufe ein, weil dies größere Verzögerungen bei der Verbindungsübergabe mit drahtlosen Telefonen nach sich zieht.

Die Verschlüsselung ist eine ausgezeichnete Methode, um den drahtlosen Datenaustausch vor Abhörangriffen zu schützen. Es gibt inzwischen verschiedene Lösungen für die Verschlüsselung. Während WEP als eine sehr schwache Lösung angesehen wird, bietet WPA PSK auf der Grundlage von TKIP ein ausreichendes Maß an Sicherheit. Der Standard WPA2 PSK, der auf dem AES-Algorithmus (802.11i-Standard) basiert, stellt die höchste Sicherheitsstufe dar.

Bei der Rogue-Erkennung handelt es sich um ein Sicherheitsschema, das bei drahtlosen Verbindungen Angriffe oder die Umleitung des Datenverkehrs zu einem Rogue AP erkennen und blockieren kann. Dieser Abwehrmechanismus wird durch die WLAN-Infrastruktur bereitgestellt.

Die Authentisierung ist ein zusätzlicher Sicherheitsprozess, mit dem Sie den Zugang zum WLAN filtern. Whitelisting und Blacklisting stellen eine erste Ebene der Authentifizierung dar. WPA und WPA2 bieten eine höhere Authentifizierungsstufe als ein Verschlüsselungscode, der dem AP zugeordnet werden muss. Firewall-Regeln (falls auf dem WLAN-Switch verfügbar) filtern den Zugriff auf das WLAN.

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen die folgenden Maßnahmen, um die Sicherheit auf WLAN-Ebene zu erhöhen:

- Weisen Sie den Sprachdaten und den anderen Daten getrennte SSIDs zu, um den Datenfluss zu splitten. Behalten Sie dabei aber die SSID-Übertragung bei, um Verzögerungen beim Roaming mit Alcatel-Lucent 81x8-WLAN-Telefone-WLAN-Handsets zu minimieren.

- Zum Schutz vertraulicher Inhalte empfiehlt Ihnen Alcatel-Lucent Enterprise, zur Sprachverschlüsselung WPA oder idealerweise WPA2 zu verwenden. Diese Verschlüsselungsverfahren bringen auch eine starke Authentifizierung mit sich.

Empfehlungen zur Umsetzung

Unterbinden Sie mithilfe der WLAN-Switch-Konfiguration Übergriffe von Sprach- auf Datennetze:

- Weisen Sie eine SSID für die Sprachverarbeitung zu. Verbinden Sie die SSID mit einem Sprach-WLAN und dann mit einem Sprach-VLAN. Lassen Sie außerdem SSID-Übertragungen zu. Verwenden Sie eine separate SSID für den Datenverkehr.
- Verwenden Sie WPA oder vorzugsweise WPA2 zur Verschlüsselung und Authentifizierung.
- Verwenden Sie die Rogue-Erkennung und Firewall-Regeln auf dem WLAN-Switch, um den Zugriff auf das Sprach-WLAN/VLAN einzuschränken
- Als zusätzliche Sicherheitsoption bietet das RF Protection (RFP)-Modul Ihnen Unterstützung bei der Erkennung/Prävention von Netzwerksondierungen, Client-Imitationen, DoS-Angriffen und nicht autorisierten Geräten.

D.9 Überprüfung der Systemintegrität

Sie können bei Ihren Kommunikationsprodukten über verschiedene Mechanismen die Daten- und Konfigurationskonsistenz des Systems sicherstellen. Diese Funktionen sind direkt als Administrationsdienste eingebettet, oder sie werden von ALE-Applikationspartnern bereitgestellt. Sie gewährleisten die Verifizierungsintegrität der auf Servern installierten Software-Releases. Sie protokollieren den Zugriff auf und die Änderung von Datenbanken und ermöglichen es Ihnen, die Konsistenz der Systemkonfiguration zu überprüfen.

Auf dem Kommunikationsserver finden Sie einen Mechanismus, um die Prüfsumme der Binärdateien im dynamischen Patch vor der Installation zu prüfen. Der Systemadministrator kann auch jederzeit kontrollieren, ob die Linux-Distributionspakete während des Installationsvorgangs installiert werden. Es ist eine Verlaufsdatei verfügbar, die alle Versionsaktualisierungen oder Änderungen an der Systemkonfigurationsdatei protokolliert.

D.10 Schutz von Kommunikationsdaten

In puncto Sicherheit ist insbesondere in einer VoIP-Umgebung der Schutz der Kommunikationsdaten ein Schlüsselfaktor. Hacker können sich bei internen oder externen Angriffen schnell sensible Informationen aneignen.

Zu den Risiken im IP-Umfeld gehören Denial-of-Service-Angriffe, die sich unter Umständen auf die Verfügbarkeit des Systems auswirken. Eine weitere Gefahr ist das Abhören von Gesprächen.

Da es sich bei IP-Netzwerken um gemeinsam genutzte Netzwerke handelt, kann der IP-Datenverkehr entweder direkt vom Pfad oder durch Umleitung des Datenstroms zu einem Sniffer abgegriffen werden. Hierbei kommen die sogenannte Man-in-the-Middle-Technik und das Identitäts-Spoofing zum Einsatz. Das Risiko wird dadurch erhöht, dass die zur Durchführung dieser Angriffe erforderlichen Werkzeuge leicht im Internet zu finden sind. So wird jeder Nutzer mit einem PC zur potenziellen Bedrohung für die Kommunikationsdaten.

Es gibt Lösungen, mit denen Sie das Risiko der Erfassung von IP-Kommunikationsströmen über IP auf der Ebene des Infrastrukturnetzes einschränken können. Dazu zählen das LAN-Switching, die VLAN-Partitionierung von Sprach- und anderen Daten sowie der Schutz vor Gratuitous ARPs auf IP-Desktop-Telefonen. Die VoIP-Verschlüsselung (sprich: die Sicherung auf Anwendungs- statt auf Netzwerkebene) ist die am besten geeignete Lösung, um Daten zu schützen. Die Technologie fügt der Netzwerkschicht eine zusätzliche Sicherheitsebene hinzu. Selbst, wenn der Datenfluss erfasst wird, ist es dann nicht mehr möglich, ihn zu entschlüsseln.

In TDM-Umgebungen erfordert die Ende-zu-Ende-Verschlüsselung von Sprache spezielle Geräte. Sie kommt daher nur bei ausgewählten Nutzern zum Einsatz. Die VoIP-Verschlüsselung ermöglicht einen nativen Schutz der Kommunikationsdaten. Das System ist damit stärker als bei Standard-TDM-Telefonen.

Um Daten zu schützen und die Abhörsicherheit zu gewährleisten, müssen Sie sowohl die Sprachdaten als auch die Steuersignalströme verschlüsseln. Die Integrität der Anrufsteuerungssignale ist nur zu erreichen, wenn die Nachrichten nicht verändert und Man-in-the-Middle-Angriffe vermieden werden.

Empfehlungen für den Aufbau

Alcatel-Lucent Enterprise empfiehlt Ihnen dringend, die IP Premium Security -Lösung zu implementieren, um die Daten vor Unbefugten und vor Verlust zu schützen und die Authentifizierung sicherzustellen:

- Mit der gegenseitigen Authentifizierung von VoIP-Elementen verhindern Sie das Identitätsspoofing.
  - Einsatz von werkseitigen oder standortspezifischen Zertifikaten (leicht zu implementieren und zu verwalten)
- Mit der Echtzeit-Verschlüsselung (<1ms Verzögerung)des Datenverkehrs verhindern Sie Lauschangriffe.
  - IPSec und TLS mit SRTP (mit 128 Bit AES) zum Schutz der digitalen Signalverarbeitung als auch der Sprach-Nutzdaten
- Über digitale Signaturen von Binärdateien und Konfigurationsdateien bauen Sie Manipulationen vor.
  - Schutz vor schädlichen Änderungen an der Konfiguration
  - Schutzmaßnahme, um das Deaktivieren/Umgehen der Verschlüsselung zu verhindern
- Setzen Sie Komponenten und Software-Elemente in Form von Modulen ein.
  - Zweckgebundene Verarbeitungsleistung und feine Abstimmung von Datenübertragung und Kosten
  - Volles Ausschöpfen eingebetteter Prozessoren/Firmware ALLER aktuellen IP Premium-Tischtelefone

3. Technische und organisatorische Maßnahmen auf Produktebene

OmniPCX Enterprise (OXE)

OmniPCX Enterprise (OXE) ist eine PBX-Telefonanlage, die Benutzer zur Unterstützung von Gesprächen miteinander verbindet. Ein Netzwerk von OXEs kann Telefoniedienste für größere Einsatzbereiche bereitstellen. OXE basiert auf einem angepassten Linux-Betriebssystem. Alcatel-Lucent Enterprise hat weder Zeit noch Mühe gescheut, um die Linux-Betriebssystemumgebung für OXE noch mehr zu stabilisieren. Wir haben das Betriebssystem stark gestrafft und nur die für den Betrieb wichtigen Dienste beibehalten. Beispielsweise bleibt Telnet Teil der ALE-Distribution von Linux. Das Tool wird aber standardmäßig deaktiviert, weil es ungesichert ist. Es wird durch SSH ersetzt.

Datenschutz

Zugriffssteuerung

Passive Zugangskontrolle

Passive Beschränkung des Zugangs zu Ressourcen:

- Die Anzahl der allgemeinen Systemkonten wird auf ein Minimum reduziert.
- Sicherheit durch Standardaufbau: Bei der Erstinstallation des Produkts aktivieren wir die Sicherheitsmaßnahmen. Gleichzeitig erzwingen wir standardmäßig die Aktivierung der Passwortverwaltung für das System (der Zugriff auf Konten). Die Passwörter für die Benutzer (root, mctl, swinst und adfexc) müssen vom Kunden geändert werden.
- Es ist nicht möglich, den „root"-Zugang direkt über SSH zu nutzen. Der Zugriff ist nur direkt über den Konsolenport möglich, und der Benutzer muss physisch vor Ort sein.
- Zeitlich begrenzte Passwörter: Wir aktivieren die zeitliche Begrenzung der Passwörter. Für die Laufzeit eines Passwortes kann eine maximale Dauer konfiguriert werden. Danach sperrt das System den Zugriff aufs Konto. Fünf Tage vor dem Ablaufdatum wird bei jeder Anmeldung die Warnung angezeigt, dass das Passwort in x Tagen abläuft.
- OXE verwaltet die Passwort-Richtlinie. Die Kennwörter werden mit SHA2-512-Hash verschlüsselt gespeichert.
- Vertrauenswürdige Host-Verwaltung: Standardmäßig wird der Fernzugriff für alle unbekannten IP-Adressen verweigert (Whitelisting).

Kontrolle aktiver Zugriffe

Aktive Beschränkung des Zugangs: Authentifizierung für den Zugriff auf Daten, die Verarbeitung, die Protokolle und die Verwaltung:

- Der Zugriff auf OXE-Ressourcen (Betriebssystem, Protokolle, Tabellen, Datenverarbeitung und Ports) ist durch ein Login/Passwort beschränkt.

Überwachung

- Der Zugriff auf OXE kann protokolliert und überwacht werden

Schutz von Kommunikationsdaten

- Verschlüsselung: OXE unterstützt die native Verschlüsselung für die Kommunikation zwischen Nutzern und zwischen OXE-Servern im Netzwerk (SIP TLS 1.2 sowie DTLS 1.2 und SRTP)

Integrität

Systemintegrität

Sie können in OXE über verschiedene Funktionen die Daten- und Konfigurationskonsistenz des Systems sicherstellen. Diese Funktionen sind direkt als Administrationsdienste eingebettet, oder sie werden von ALE Applikationspartner bereitgestellt. Sie gewährleisten die Verifizierungsintegrität der auf Servern installierten Software-Releases. Sie protokollieren den Zugriff auf und die Änderung von Datenbanken und ermöglichen es Ihnen, die Konsistenz der Systemkonfiguration zu überprüfen.

Eingabesteuerung

Nur der Administrator kann auf OXE zugreifen. Telefonie-Nutzer haben keine Zugriffsmöglichkeit. Der Administrator kann alle MAC-Operationen (Verschieben/Hinzufügen/Ändern) überwachen, die auf verwalteten Systemen durchgeführt werden.

Verfügbarkeit

Sicherstellung der Verfügbarkeit durch den Aufbau

Die lokalen und geographischen Redundanzfähigkeiten zählen zu den Backup-Funktion von OXE.

Sicherstellung der Verfügbarkeit durch Prozesse

Ob ein Business Continuity Plan (BCP) und Disaster Recovery Plan (DRP) vorhanden sind, und wie effektiv diese sind, hängt von den Verfahren der Kunden/Partner ab.

OpenTouch Multimedia Server (OTMS)

Der OpenTouch Multimedia Server ist eine Unternehmenslösung, die Dienste für die Zusammenarbeit bereitstellt (Telefonie- und Benutzeranwesenheitsstatus, Instant Messaging, gemeinsame Nutzung von Dokumenten, Desktop-Sharing, Dateifreigabe, Audiokonferenzen).

Der OTMS kann mit einem oder mehreren OXEs vernetzt werden. Er bietet auch Sprachnachrichtendienste an.

Datenschutz

Der Datenschutz wird durch ein Regelwerk sichergestellt, das den Zugang zu Informationen einschränkt.

Zugriffssteuerung

Passive Beschränkung des Zugangs zu Ressourcen

Dies betrifft Daten, die Datenverarbeitung, die Protokolle und die Verwaltung. Ports werden standardmäßig für den Zugriff geschlossen und während der OTMS-Implementierung für den Zugriff durch den Administrator geöffnet, idealerweise gemäß ALE-Empfehlungen.

Aktive Beschränkung des Zugangs

Authentifizierung für den Zugriff auf Daten, die Datenverarbeitung, Protokolle und die Verwaltung.

Basis-Anmeldemodus (Benutzername und Passwort)

- Der OTMS-Server authentifiziert Benutzer anhand ihres Logins/Passworts.

Interne/externe Authentifizierung

- Die Authentifizierung kann über das interne LDAP des OTMS erfolgen.
- Die Authentifizierung kann extern erfolgen, entweder auf der Basis eines LDAP-Servers des Unternehmens oder über einen RADIUS-Server, sodass die zentralisierte und eindeutige Authentifizierungsrichtlinie des Unternehmens übernommen werden kann.

Single Sign-on auf MS Windows-Plattform

- Für OTMS-Software-Clients, die auf der Plattform Microsoft Windows laufen, kann ein Single Sign-on (SSO) mit Kerberos-Protokoll verwendet werden. In diesem Fall verwendet der OTMS-Server die Authentifizierung der Windows-Sitzung, um den Endnutzer im Hintergrund zu authentifizieren.

Passwort-Richtlinie

- Eine Passwort-Richtlinie kann durch das OTMS oder durch ein externes Authentifizierungsverfahren (z. B. MS Active Directory) verwaltet werden

Zugang zu Telefonkonferenzen

- Der Nutzer benötigt für den Zugriff auf Telefonkonferenzen eine zusätzliche Authentifizierung.
- Zugangscode zur Identifizierung der Konferenz und eventuell zusätzliches Passwort.

Überwachung

- Es ist möglich, den Zugriff auf die OTMS zu protokollieren und zu überwachen.

Verschlüsselung

- Die Datenkommunikation wird mit HTTPS verschlüsselt.
- Die Passwörter werden systematisch mit Hilfe von Authentifizierungssystemen Dritter, wie z.B. MS Active Directory, verschlüsselt.

Integrität

Server-Integrität

Die OTMS-Server unterstützen verkettete Zertifikate. Dies ermöglicht es den Clients, den OTMS-Server zu authentifizieren. Der Kunde kann sein eigenes Zertifikat auf dem OTMS einsetzen.

Software-Integrität

Alle Komponenten, die zu den OTMS-Desktop-Anwendungen gehören, werden mit einem digitalen SHA-256-Zertifikat signiert, das DigiCert Inc. an Alcatel-Lucent Enterprise ausgibt.

Wir empfehlen, auf Desktops und Servern für OTMS-Clients einen Virenschutz einzusetzen.

Eingabesteuerung

- Alle auf OTMS-Daten bezogenen Aktivitäten wie das Lesen, Ändern und Löschen werden protokolliert und können überwacht werden.

Mit der OmniVista 8770 NMS Audit-Anwendung kann der für die Sicherheit zuständige Administrator Audits durchführen und die folgenden Prozesse nachverfolgen, um die Sicherheit zu gewährleisten und seiner Verantwortung nachzukommen:

- Alle Verwaltungsschritte wie das Erstellen, Ändern und Löschen von Daten, die in OTMS von Administratoren durchgeführt werden – unabhängig davon, welche Verwaltungsclients verwendet werden (WBM, 8770 oder öffentliche WebServices API, wenn API offiziell unterstützt wird). Diese Operationen werden über die CMS-Verwaltungs-API veröffentlicht.
- Alle Administrator-Anmeldesitzungen, die in den OTMS geöffnet wurden, einschließlich des Authentifizierungsstatus.
- Alle in den OTMS durchgeführten SSH-Sitzungen (Öffnen/Schließen), einschließlich des Authentifizierungsstatus.

Verfügbarkeit

Sicherstellung der Verfügbarkeit durch den Aufbau

- Das OTMS verfügt über Redundanzfähigkeiten und Backup-Funktionen.

Sicherstellung der Verfügbarkeit durch Prozesse

- Ob ein Business Continuity Plan (BCP) und Disaster Recovery Plan (DRP) vorhanden sind, und wie effektiv diese sind, hängt von den Verfahren der Kunden/Partner ab.
- Das entsprechende OTMS-Tool bietet eine einheitliche Funktion zur Sicherung/Wiederherstellung.

OmniVista 8770 NMS

Beim NMS = Netzwerkmanagementsystem OmniVista 8770 handelt es sich um eine Reihe von Anwendungen, die eine zentralisierte Verwaltung von Netzwerkknoten wie OmniPCX Enterprise und OpenTouch-Knoten ermöglicht. Nur Administratoren von Sprachdiensten haben Zugang zu dieser Plattform.

Datenschutz

Zugriffssteuerung

Passive Zugangskontrolle

Passive Beschränkung des Zugangs zu Ressourcen: Daten, Verarbeitung, Protokolle, Verwaltung – Ports standardmäßig geschlossen

Kontrolle aktiver Zugriffe

Aktive Beschränkung des Zugangs: Authentifizierung für den Zugriff auf Daten, die Verarbeitung, die Protokolle, die Verwaltung etc.

Die Authentifizierung von Administrator und Benutzer ist erforderlich und basiert auf dem Login/Passwort-Prinzip. Die einzige Ausnahme ist die Webverzeichnis-Anwendung, auf der sich Firmenbenutzer ohne Authentifizierung verbinden können. Diese Anwendung ermöglicht den Benutzern den Zugriff auf das Firmenverzeichnis und die persönlichen Adressbücher. Die Authentifizierung wird erzwungen, indem eine strikte Konformität mit den Sicherheitsrichtlinien auf Grundlage der Standards ermöglicht wird.

Interne/externe Authentifizierung

Die Authentifizierung kann intern oder über externe Mechanismen erfolgen, sodass die zentralisierte und einzigartige Authentifizierungsrichtlinie des Unternehmens übernommen werden kann.

Berechtigungskonzept

- **Rollenbasierte Verwaltung:** Sie können für jeden Nutzer benutzerdefinierte Zugriffsebenen definieren. Die Administratoren mit der passenden Berechtigungsstufe können für jeden Benutzer eine andere Zugriffsstufe gewähren. Diese Zugriffsebene kann für jede Anwendung unterschiedlich sein. Ein und derselbe Nutzer hat beispielsweise einen Lesezugriff auf die Warnmeldungen und keinen Zugriff auf die Konfiguration, während er Berichte ändern darf.
- **Zugriffsgruppen:** Das OmniVista 8770 NMS definiert mehrere Zugriffsgruppen, von denen jede mit Zugriffsrechten für Anwendungen verbunden ist. Standardmäßig sind alle Gruppen leer. Diese Gruppen können nur Mitglieder der Kategorien „Administrator“ und „Sicherheitsmanager“ einsehen.
- **Gruppe mit Zugriffsrechten von Administratoren:** Mitglieder dieser Gruppe haben uneingeschränkten Zugriff auf alle Anwendungen des OmniVista 8770 NMS. Die Mitglieder dieser Gruppe haben als Einzige Zugriff auf die Administrationsanwendung. Sie können daher alle Kontenrechte verwalten – mit Ausnahme der Rechte des AdminNMC-Kontos.

Überwachung

Es ist möglich, die Zugriffe auf das OmniVista 8770 NMS zu protokollieren und zu überwachen.

Verschlüsselung

Alle Benutzerzugriffe auf das OmniVista 8770 NMS werden mit HTTPS, LLDAPS und IPsec verschlüsselt.

Integrität

Systemintegrität

Sie können bei OmniVista 8770 NMS über verschiedene Funktionen die Daten- und Konfigurationskonsistenz des Systems sicherstellen. Diese Funktionen sind direkt als Administrationsdienste eingebettet, oder sie werden von ALE Applikationspartner bereitgestellt. Sie gewährleisten die Verifizierungsintegrität der auf Servern installierten Software-Releases. Sie protokollieren den Zugriff auf und die Änderung von Datenbanken und ermöglichen es Ihnen, die Konsistenz der Systemkonfiguration zu überprüfen.

Eingabesteuerung

Alle auf Daten des OmniVista 8770 NMS bezogenen Aktivitäten wie das Lesen, Ändern und Löschen werden protokolliert und können überwacht werden.

Für OmniVista 8770 NMS-Anwendungen (Server und Client) empfehlen wir Ihnen, eine Antiviren-Strategie zu implementieren.

Verfügbarkeit

Sicherstellung der Verfügbarkeit durch Prozesse (Backup)

Das Dienstprogramm „Backup Restore“ sichert täglich und automatisch Konfigurations- und Anwendungsdaten – auf Anfrage auch auf einem Live-Produktionssystem. Das Tool wird auch zur Wiederherstellung von Daten verwendet, wobei der Wiederherstellungsvorgang eine Unterbrechung des Dienstes verursacht.

Ob ein Business Continuity Plan (BCP) und Disaster Recovery Plan (DRP) vorhanden sind, und wie effektiv diese sind, hängt von den Verfahren des Kunden/Partners ab.

4. Zusätzliche allgemeine organisatorische Maßnahmen

Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 S. 1 lit. d DSGVO, Art. 25 S. 1 DSGVO)

A. Datenschutz – Verwaltung

Die folgenden Richtlinien, Verfahren oder Anweisungen zur Datensicherheit sind im ALE-ISMS dokumentiert. Hierzu gehören die folgenden Punkte:

- Verpflichtung aller Mitarbeiter zur Geheimhaltung (Datengeheimnis)
- Maßnahmen zur Sensibilisierung der Mitarbeiter
- ALE-Sicherheitscharta
- ALE-Sicherheitsrichtlinien
- ALE-Sicherheitspolitik
- ALE-Datenschutzrichtlinie
- Datenschutz-Grundverordnung (DSGVO) von ALE
- Richtlinien zum Krisenmanagement und zugehörige Verfahren
- Regelungen der Datenschutzrichtlinien
- Informationsverwaltungssystem

- Audits durch den Datenschutzbeauftragten
- Audits durch externe Prüfer
- Dokumentation der Aktivitäten zur Datenverarbeitung
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen
- Sorgfältige Auswahl der Serviceanbieter (siehe auch Vertragsmanagement)

B. Datenschutzbeauftragter

Louis-Philippe Ollier

E-Mail: dataprivacy@al-enterprise.com

Telefon: +331 5566 3147

C. Incident-Response-Management

Richtlinien zum Krisenmanagement

Etablierte und dokumentierte Prozesse zur Behandlung von Vorfällen.

- Verantwortungsbereiche
- Definierte Berichtskanäle
- Verfahren bei Verstößen gegen den Datenschutz

D. Datenschutz durch Aufbau

Grundsätzlich dürfen ALE-Produkte nur so eingesetzt werden, dass nur die Daten erhoben und verarbeitet werden können, die für geschäftliche Zwecke geeignet und notwendig sind. Die Verfahren zur automatisierten Datenerhebung und -verarbeitung sind so konzipiert, dass nur die notwendigen Daten erhoben werden.

E. Vertragsmanagement

Wenn Unterauftragnehmer für die Datenverarbeitung eingesetzt werden, gelten bestimmte Anforderungen. Dazu gehört, dass die technischen und organisatorischen Massnahmen der Unterlieferanten Art. 28 DSGVO sowie Art. 32 Abs. 1 DSGVO entsprechen.

Die folgenden Anforderungen gelten für Vertragsverhältnisse mit Unterauftragnehmern:

- Laut Art. 28 Abs. 3 DSGVO sind ausführliche Informationen zu Art, Zweck und Umfang der Auftragsbearbeitung und Nutzung von personenbezogenen Daten des Auftraggebers bereitzustellen. Die entsprechenden Details sind vertraglich festgelegt.
- Deutsche/EU-Dienstleister müssen, wie gesetzlich vorgeschrieben, einen betrieblichen Datenschutzbeauftragten benennen und durch die Datenschutzorganisation sicherstellen, dass dieser effektiv in die jeweiligen betrieblichen Abläufe eingebunden ist.
- Mündliche Aufträge sind schriftlich zu bestätigen und dokumentieren.
- Einzelne Aufträge werden nur durch namentlich genannte Kontakte vergeben.
- Für die betroffenen technischen Umgebungen werden nur eingeschränkte Zugriffsberechtigungen gewährt. Im Falle eines externen Zugriffs auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.
- Für die Übermittlung personenbezogener Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsdatenverarbeitung zur Verfügung, die entsprechende Kontrollregelungen enthält.
- Alcatel-Lucent Enterprise hat wo notwendig entsprechend der Anweisungen in Art. 28 DSGVO Datenschutzvereinbarungen mit allen beteiligten Parteien abgeschlossen.

Alcatel·Lucent Enterprise