IT-SERVICES

Institut für Telematik unter Betreuung der Fraunhofer-Gesellschaft

Security Solutions

Lock-Keeper™
Sicherheitsarchitektur

Lock-Keeper™

dt. Patent-Nr. 198 38 253.7-31

Die

Lock-Keeper™

Architektur

Authors	Dr. Ernst-Georg Haffner Dr. Thomas Engel Prof. Dr. sc. Christoph Meinel Gerhard Müllenheim Michael Noll Thomas Wagner

Printing	10/2001
Document status	Version 1.1

Inhalt

Die Bedrohungen aus dem Internet werden immer umfangreicher und sind noch lange nicht gebannt. Moderne Sicherheitssysteme sind so konzipiert, um die diversen Kommunikationsanforderungen von Unternehmen sowohl nach außen als auch untereinander vor Eindringlingen, sogenannten „Hackern", zu schützen. Dies geschieht durch verschiedene, Abwehrmaßnahmen, die die Unternehmensdaten und -systeme gegen unbefugten Missbrauch schützen sollen. Hierzu werden unterschiedliche Sicherheitsstufen (*Security Level)* mit den jeweilig erlaubten Anwendungen definiert und zum Einsatz gebracht. Auf den niedrigsten Sicherheitsebenen sind alle Protokolle erlaubt, während eine Erhöhung der Sicherheitsanforderungen zugleich eine Restriktion an möglichen Anwendungen nach sich zieht, die gewöhnlich durch *Firewalls* kontrolliert werden. Am oberen Ende der Sicherheitsskala sind die kommunizierenden Netze physikalisch getrennt und die zugelassenen Protokolle entsprechend eingeschränkt. Die *Lock-Keeper™ Architektur*[1] als eine Möglichkeit für hochsicheren Datenaustausch wird hier vorgestellt und ihre Integration in komplexe Sicherheitsstrukturen aufgezeichnet.

Integration der Schleusentechnologie Lock-Keeper™ in moderne Sicherheitsarchitekturen

Dr. Ernst-Georg Haffner
Dr. Thomas Engel
Prof. Dr. sc. Christoph Meinel
Gerhard Müllenheim
Michael Noll
Thomas Wagner

1. Einführung

Mit der weltweit wachsenden Vernetzungsdichte von Computern über das Internet und den sich daraus ergebenden Möglichkeiten zum Datentransfer zu den unterschiedlichsten Zwecken steigen auch die betrieblichen Anforderungen an die Rechnerkommunikation. Kaum ein Unternehmen kann es sich heutzutage leisten, ohne Zugriff auf den gigantischen Datenspeicher des Internets auszukommen und selbst der Datenaustausch zwischen Filialen eines Konzerns erfolgt nicht selten - zumeist verschlüsselt - über das Netz der Netze.

Dabei steigt ebenfalls der Anspruch an die Qualität der Datenformate. Moderne Medien verbessern jedoch nicht allein die Brauchbarkeit der dargestellten Informationen, sondern erfordern überdies Transferkanäle hoher Bandbreite.

Allerdings wachsen mit den vielen Chancen des heutigen Informationsaustausches ebenso die Risiken. Anbindungen von Institutionen, Behörden und Unternehmen an das Internet über Standleitungen generieren gefährliche Angriffsmöglichkeiten für Attacken. Die Integrität der unternehmenseigenen Daten zu schützen, die Authentizität der Kommunikationspartner zu gewährleisten und die Abhör- und Manipulationssicherheit während eines Datenaustausches zu garantieren wird in den sogenannten Security Policies geregelt. Je nach Sicherheitsbedürfnis der betroffenen Stellen sind unterschiedliche Maßregeln für den elektronischen Datenverkehr sowie Verhaltensvorschriften für die Mitarbeiter Bestandteil dieser Dokumente. Allerdings sind für große Konzerne keineswegs gleiche Anforderungen aller Abteilungen vorauszusetzen. Vielmehr sehen die Sicherheitsvorschriften komplexer Sicherheitsarchitekturen unterschiedliche Security Levels vor, wobei im Einzelnen zu klären ist, welche Kommunikationsziele - unter welchen Sicherheitsbedingungen - zu erreichen sind. Nicht selten müssen hier schwerwiegende Entscheidungen gefällt und Kompromisse eingegangen werden.

Als Werkzeuge zur Realisierung der angestrebten Ziele dienen im Bereich der Sicherheitsinfrastrukturen für den elektronischen Informationsaustausch zumeist Firewalls. Der Zweck dieser Systeme besteht in einer Art Filterfunktion: nur berechtigte Zugriffe für

[1] Das Patentverfahren der Lock-Keeper™-Architektur ist unter der Patentnummer 198 38 253.7-31 geführt.

authentifizierte Benutzer[2] mittels der erlaubten Protokolle dürfen zugelassen werden. In diesem Artikel werden wir darüber hinaus Einsatzmöglichkeiten der Schleusentechnik des Lock-Keeper™ vorstellen, einer Entwicklung des Instituts für Telematik, die mittels physikalischer Trennung der kommunizierenden Netzwerke in der Lage ist, höhere Sicherheitsanforderungen zu gewährleisten und bestimmte Attacken von Angreifern auszuschließen. Wir werden weiterhin aufzeigen, an welchen Stellen der Sicherheitsarchitekturen eine geeignete Analyse eingehender und ausgehender Daten erfolgen kann.

In den folgenden Abschnitten wollen wir zunächst die Gefährdungspotentiale von Angriffen gegen firmeneigene Netze aufzeigen und hier ebenfalls grundlegende Fragestellungen der Security Policies berücksichtigen (Abschnitt: „Angriffe gegen Datennetze"). In einem weiteren Abschnitt folgen dann diverse Ansätze zur Abwehr derartiger Angriffe, die zu komplexen Sicherheitsarchitekturen führen (Abschnitt: „Abwehrmaßnahmen gegen Angriffe"). Im Vordergrund wird dabei die Funktionsweise des Lock-Keeper™ stehen. Eine Zusammenfassung mit Ausblick auf künftige Aktivitäten beschließt die Ausführungen.

2. Angriffe gegen Datennetze

Klassifikation von Attacken

Um Technologien gegen Angreifer auf Datennetze geeignet beurteilen und bewerten zu können, werden wir zunächst die wesentlichen Aspekte moderner Sicherheitskonzepte aufzeigen.

Wir unterscheiden hierbei zwischen einem inneren Computer-Netzwerk (inner network, "IN") und einem äußeren (outer network, "ON"). Das IN beinhaltet jedwede Art vertraulicher und zu schützender Information eines Unternehmens, einer Behörde oder sonstigen Institution. Das ON ist ein Netzwerk oder ein Verbund von Netzen, über das Datenaustausch mit Kommunikationspartnern erfolgen soll. Ein prominentes Beispiel eines ON ist das Internet. Firmeneigene Intranets bzw. LANs stellen INs dar. Allerdings können die Netzwerkstrukturen auch komplexer sein. Innerhalb größerer Unternehmen und Konzerne kann auch der Datenaustausch untereinander mittels INs und ONs modelliert werden.

Ein wesentlicher, allerdings nicht der einzige Sicherheitsaspekt konzentriert sich hierbei auf die Frage, wie der Datenaustausch zwischen IN und ON gegen mögliche Angriffe von außen (aus dem ON) geschützt werden kann. Allerdings darf hierbei nicht vergessen werden, dass de facto die meisten Attacken gegen Netze aus den INs selbst erfolgen [1].

Mögliche Risiken im Datenaustausch sind nicht-gewährleistete Authentizität von Sender und Empfänger, Abhör- und Manipulationsmöglichkeiten seitens Dritter und das unbefugte Eindringen in das IN, während gerade ein Datentransfer zwischen den Netzen erfolgt. Auch die Daten selbst können das Computernetzwerk gefährden. „Viren", „Würmer" und andere sogenannte „Beastware" ([7], [8], [9]) stellen eine Bedrohung des INs dar.

Aufgrund dieser komplexen und umfangreichen Gefährdungspotentiale sollte ein Unternehmen zunächst eine Security-Policy [2] aufstellen, die im Detail die wichtigsten Sicherheitsfragen beantworten muss. Wie bereits in der Einleitung erwähnt, geht das größte Sicherheitsrisiko im Umgang mit elektronischem Datentransfer mit dem höchsten Quality of Service (QoS) einher. Wenn alle Arten von Programmen und Protokollen zu Verfügung stehen, wächst die Begeisterung des Anwenders mit dem Missfallen der Sicherheitsexperten. Typische moderne Internet-Protokolle und -Anwendungen wie http, ftp, telnet, rlogin [3], smtp und sendmail [4] stellen ebenfalls enorme Risiken dar[3].

---

[2] Zumeist wird anstatt der Überprüfung der Authentizität des Benutzers auch eine solche des Quellrechner-Systems als statthaft empfunden.

[3] Zu generellen Sicherheitsrisiken von UNIX siehe [5].

Die Bedeutung der Security Policy

Zum Erstellen einer spezifischen Security-Policy, die als Grundlage zur Absicherung gegen Angriffe von innen oder außen dient, ist es erforderlich, die möglichen Arten von Attacken zu klassifizieren und dabei festzuhalten, welche Abwehrmaßnahmen geeignet sind, den Bedürfnissen des jeweiligen Unternehmens bzw. der entsprechenden Abteilungen zu genügen.

Generell lassen sich Angriffe auf ein Computernetzwerk in zwei verschiedene Kategorien untergliedern:

Beim „Online-Angriff" handelt es sich um eine sehr gefährliche Angriffsmethode, bei der sich der Angreifer interaktiv über das Netz auf die Systeme im inneren Netz Zugang verschafft, und so die Möglichkeit hat, über einen direkten Kanal sensible Daten zu kopieren und Passworte auszuspionieren.
Die meisten PC's bieten dem Administrator gewisse Dienste (wie zum Beispiel *telnet* oder *ftp*) an, die eine Interaktion über das Internet zulassen. Für den Administrator ist es dann zwar sehr bequem sich zum Beispiel von seinem PC auf einen anderen im Internet stehenden PC einzuloggen, jedoch bietet dieser Dienst einem potenziellen Hacker auch die Möglichkeit, sich als Administrator auszugeben und das System so zu beeinträchtigen.
Angreifer benutzen meist sog. Session-Logger um fremde Passwörter auszuspionieren oder verschaffen sich durch Beobachtung des sozialen Umfelds einer Person Hinweise auf deren Passwort, um es dann mit meist nur wenigen Versuchen erraten zu können. Eine andere Gegebenheit, die sich Hacker zu Nutze machen, sind sog. Sicherheitslöcher („Security Holes" oder „Security Bugs") der eingesetzten Applikationen und Betriebssysteme. Je komplexer ein Programmcode ist, desto höher ist auch die Gefahr der „Hintertürchen" und Sicherheitslöcher. Beim Software Release ist meist noch unbekannt, welche Löcher die Software noch beinhaltet, da es unmöglich ist, alle potentiellen Angriffspunkte einer neuen Software vorauszusehen.

Zu den Mechanismen der „Offline-Angriffe", bei denen man mittels kleiner Programmfragmente, die in das System eingeschleust werden und dort selbständig agieren, sich selbst reproduzieren, Daten nach außen schicken oder das System außer Funktion setzen. Formen solcher eigenständigen Programme oder ausführbaren Codefragmente sind z.B. Computerviren, (Internet-)Würmer oder Trojanische Pferde, die man unter dem Begriff „Beastware" zusammenfasst. In den letzten Jahren sind immer neuere Viren oder Virenmutationen aufgetaucht, die mit der Zeit intelligenter und schadhafter wurden.
Inzwischen existieren zwar eine Reihe von Werkzeugen und Analysetools, welche einen gewissen Anteil wohlbekannter Beastware erkennen und eliminieren können (Virenscanner, Mail-Analyser etc.), allerdings sollte dies nicht darüber hinwegtäuschen, dass ein Sicherheitsrisiko grundsätzlich für jeden ausführbaren Code bestehen bleibt.
Es handelt sich jedoch informationstheoretisch de facto um ein unentscheidbares Problem, dass ein Programm prinzipiell nicht herausfinden kann, welche Aktionen eine bestimmte Software ausführen kann. Und dies gilt nicht nur für eine automatische Analyse der Beastware: wie sollte ein menschlicher Administrator alle Wirkungen eines Programms mit den verschiedensten Eingabewerten ermitteln (z.B. wenn eine unendliche Testmenge erforderlich ist)?
Deshalb sind es durchaus berechtigte Sorgen, die Sicherheitsexperten von Unternehmen dazu veranlassen, keine unbekannte Software von außen in das firmeneigene Netz aufzunehmen und sehr restriktive Maßnahmen anstrengen, damit nicht durch diverse Kompilations-, Umwandlungs- oder Dekodierprozesse aus einfachem ASCII-Text ein Stück selbstlaufender Software wird. Im Rahmen einer klar definierten Security-Policy lassen sich derartige Restriktionen und Maßnahmen für gewöhnlich, insbesondere in Hochsicherheitsbereichen, als völlig legitim vertreten.

Die nachfolgende Tabelle 1 gibt einen kurzen Überblick über die möglichen Klassen von Attacken und zeigt, ob es sich hierbei um einen „Online-Angriff" handelt, bei dem der Angreifer interaktiv über das Netz auf die Systeme im IN gelangt (vgl. [2]).
Diese Klassifikation zeigt auf, dass zahlreiche Möglichkeiten für den Angriff gegen ein IN existieren. Rein zahlenmäßig gehören die Offline-Angriffe mittels Beastware inzwischen zu den meistverbreiteten Angriffstypen, jedoch gelten die Online-Angriffe als die gefährlichsten, da die gesamte Integrität des inneren Netzwerks potentiell in Frage gestellt wird.

Klasse	Beschreibung der Quelle	On-line
Passwort-Diebstahl	Passwörter befinden sich in Klartext-Dateien oder werden abgehört auf IP-Ebene. Dictionary-Attacks raten Passwörter systematisch.	✓
„Social engineering"	Passwörter werden durch menschliche Interaktion bewusst oder unbewusst übermittelt (z.B. telefonisch).	✓
Bugs und Hintertüren	Fehlverhalten von Software; bewusste Abweichung von der Programmspezifikation durch den Programmierer; oder Viren und Würmer schaffen neue „Hintertüren".	✓
Authentifi-kationsfehler	Programme zeigen Einwahlmasken im IN und senden die Passwörter ins ON.	✓
Fehler auf Protokollebene	Sicherheitslücken im TCP-Protokoll, etwa „TCP sequence number attack"; Tunneling; „message encapsulating"; „tiny fragment attack"; „overlapping fragment attack" [6].	✓
Offline-Angriff (meist „Denial-of-service")	Würmer, Trojanische Pferde und Viren („Beastware") können das IN in seiner Funktion beeinträchtigen oder gar zerstören. Daten des IN können ins ON gelangen.	--

Tabelle 1: Klassifizierung von Angriffsmöglichkeiten gegen Computernetze

Psychologische Faktoren

Interessanterweise spielen für den Einsatz von Sicherheitswerkzeugen neben der technischen Relevanz auch psychologische Faktoren eine wichtige Rolle. Das „Gefühl der Sicherheit" ist kein bloßer Zusatz oder gar ein Nebeneffekt in der informations- und kommunikationsbetonten Arbeitswelt. Ein aus sicherheitstechnischer Sicht objektiv überzeugendes System kann – wenn die Security-Policy in dieser Frage noch Lücken aufweist – durchaus verunsichernd auf die betroffenen Personen wirken. Eine zentrale Rolle spielt hierbei die Klarheit und Überschaubarkeit des Sicherheitskonzepts, die sich in der Security Policy offenbart.

3. Abwehrmaßnahmen gegen Angriffe

Firewalls

Als ein sehr wichtiges Werkzeug zur Gewährleistung von Netzwerksicherheit hat sich in den vergangenen Jahren die bereits erwähnte Firewall etabliert. Eine Firewall ist eine Sammlung von Komponenten zwischen zwei Netzwerken, die zusammen folgende Eigenschaften erfüllen.

- Der Datenverkehr zwischen den beiden Netzen muss in beiden Richtungen die Firewall passieren.
- Nur autorisierter Datenverkehr - gemäß der jeweiligen Security-Policy - darf die Firewall passieren.
- Die Firewall selbst kann nicht angegriffen werden. (vgl. [2])

Prinzip und Funktionsweise

Fast alle Firewalls basieren auf dem Prinzip der Paket-Filterung. Sie analysieren TCP/IP[4]-Pakete, indem sie Sender und Empfänger gemäß der IP-Adresse verifizieren; sie kontrollieren den TCP-Port um sicherzustellen, dass der gewählte Dienst auch in Anspruch genommen werden darf. Allerdings gibt es zahlreiche Methoden, mit denen die Analysemechanismen einer Firewall hintergangen werden können. Mängel und Sicherheitslücken in der Konstruktion einer Firewall versuchen die Hersteller schnellstmöglich zu schließen. Jedoch bietet neben der eigentlichen Firewall z.B. auch das zugrundeliegende Betriebssystem Angriffsmöglichkeiten zur Kompromittierung des Systems.

Doch auch eine konzeptionell bedingte „Schwachstelle" einer Firewall ermöglicht es Unbefugten, sich trotz der Absicherung durch eine Firewall Zugang aus dem ON in das IN verschaffen. Die Ursache hierfür liegt in der prinzipiellen Aufgabenstellung dieser Sicherheitsmaßnahme: eine Firewall muss erlaubte Anfragen von nicht-autorisierten unterscheiden und hierbei erstere ermöglichen, während letztere abzuwehren sind. Angriffe mit hoher krimineller Energie basieren in der Regel darauf, dass die Kriterien für den berechtigten Zugriff durch den unberechtigten Angreifer gefälscht werden, und somit die Firewall ungehindert passiert werden kann. Es besteht hier demnach durch die prinzipielle Funktionsweise dieses Systems ein inhärentes Sicherheitsrisiko.

[4] **T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol

4. Die Lock-Keeper™ Architektur

Idee

Bei vielen Unternehmen wie z.B. Banken ist die Anforderung an die Sicherheit so hoch, dass Standardmittel der IT-Sicherheit diesen Anforderungen nicht mehr gerecht werden. In solchen Fällen stellt der Lock-Keeper™ als eine Hochsicherheitslösung zum Datenaustausch zwischen zwei Netzwerken eine echte Ergänzung oder gar Alternative zu klassischen Firewall-Lösungen dar.

Das Lock-Keeper™ Prinzip ist aus der Frage entstanden, auf welche Weise Daten zwischen einem internen, hochsicheren Netzwerk und einem externen, weniger sicheren Netz wie z.B. dem Internet ausgetauscht werden können, ohne dabei eine - wenn auch nur kurzfristig bestehende – direkte Verbindung aufbauen zu müssen. In Anlehnung an den eher trivialen Mechanismus, die Daten zwischen den beiden Netzwerken per Diskette zu transferieren, entstand die Idee, eine Lösung zu entwickeln, die diesen „Austausch per Diskette" automatisiert durchführen kann.

Der Lock-Keeper™ basiert hierbei auf einem altbekannten und an sich simplen Mechanismus: der Schleuse. Wie bei einer Schiffsschleuse werden beim Lock-Keeper™ die Daten so durchgeleitet, dass zu keinem Zeitpunkt eine direkte Verbindung zwischen im inneren und dem äußeren Netzwerk besteht.

Abb. 1: Topologie der Schleusentechnologie des Lock-Keeper™

Wie funktioniert der Datenaustausch zwischen den Netzen ?

Der Lock-Keeper™ an sich besteht intern aus drei aktiven Komponenten auf PC Basis, wobei der innere dieser Lock-Keeper™ PC's mit dem internen Hochsicherheitsnetz des Unternehmens verbunden wird. Der äußere PC wird an das weniger gesicherte Netz wie zum Beispiel das Internet angeschlossen. Der dritte Lock-Keeper™ PC, die eigentliche Schleuse, bietet die Möglichkeit zur ausführlichen Analyse des durchgehenden Verkehrs. Weitere Komponenten können hier modular an den Lock-Keeper™ angedockt werden.[5]
Die Lock-Keeper™ internen Komponenten sind an einer patentierten* Schaltplatine angeschlossen, und zwar so, dass maximal zwei der LK-PC's gleichzeitig miteinander kommunizieren können. Dies gewähren sog. Schaltrelais (elektronische Schalter) auf der Platine, die die Verbindung auf physikalischer Ebene umschalten, d.h. die Stromkreise der Datenleitungen unterbrechen.

[5] s. Abschnitt "Kombinierte Sicherheitsarchitekturen", Anwendungsbeispiele

Der Schaltmechanismus hat somit zwei definierte Zustände:

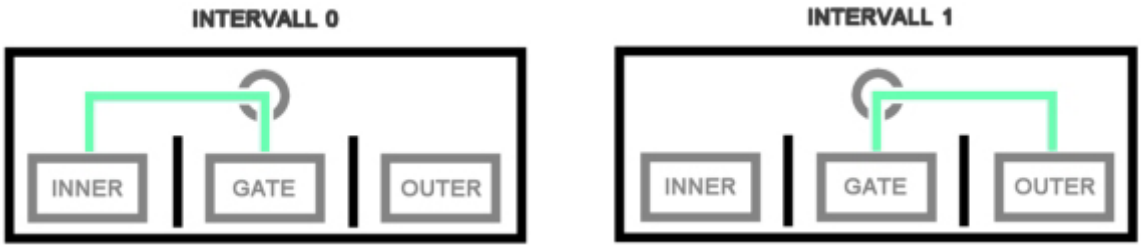

Abb. 2: Schaltzustände des Lock-Keepers™, wobei „Inner" den nach innen zeigende, „Outer" den nach außen zeigende und „Gate" den mittleren internen Lock-Keeper™-Rechner darstellt.

Die Steuerung der Schleuse bzw. der Schaltrelais ist autonom und kann auch durch einen Zugriff auf das Restsystem nicht geändert oder ausser Kraft gesetzt werden. Daher können weder externe Hacker-Angriffe noch geschulte Insider die physikalische Trennung der Netzwerke aufheben oder umgehen.

Anhand des Beispiels „Benutzer A schickt eine Mail ins Internet" lässt sich der Datentransfer über den Lock-Keeper™ recht anschaulich erläutern (vgl. Abb. 3, unten):

Fallbeispiel: Mailversand

Der Benutzer A, ein Mitarbeiter des Unternehmens, welches den Lock-Keeper™ einsetzt, schickt eine Mail aus dem gesicherten Firmennetz in das Internet.

Abb. 3: Funktionsweise des Lock-Keepers™

Im ersten Schritt landen die Datenpakete (die Email) des Benutzers auf dem inneren Mailserver, der sie an den Lock-Keeper™ weiterleitet. Im Lock-Keeper™ werden die Daten auf dem zum inneren Netz zeigenden Rechner gespeichert. Dieser prüft, ob eine Verbindung zum mittleren Rechner besteht und wartet - bei nichtvorhandener Verbindung - bis die Platinensteuerung die Leitungen umschaltet. Nun wird die Mail an den

eigentlichen Schleusenrechner (Mitte) weitergeleitet, wo sie nach Bedarf und je nach Sicherheitsanforderung analysiert wird, bevor sie ihren Weg ins Internet fortsetzen darf. Ist die Sicherheitsüberprüfung geglückt (z.B. Virusscan) ermittelt nun der mittlere Rechner, ob eine Verbindung zum äußeren, an das Internet angeschlossenen Rechner besteht. Wenn ja, wird die Mail dorthin weitergeleitet und kann über das Internet zum Empfänger geschickt werden.
Bei dem kompletten eben geschilderten Prozess besteht zu keinem Zeitpunkt des Transfers eine direkte physikalische Verbindung vom Internet zum Intranet, da beim Lock-Keeper™ der Datentransfer nicht nur auf Applikations- oder Protokollebene getrennt wird, wie es bei Firewalls üblich ist, sondern tatsächlich die Stromkreise der Leitungen unterbrochen werden.

Eine Schleusentechnologie wie die des Lock-Keeper™ bleibt somit für die möglichen Online-Angriffe immun (vgl. 2.2), da das zugehörige Sicherheitskonzept nicht etwa berechtigte von nicht-erlaubten Anfragen trennt (wie bei einer Firewall, 3.1), sondern grundsätzlich – unabhängig von einer optionalen Analyse – jedweden Datenverkehr zwischen IN und ON zwischenspeichert und hierdurch alle direkten Angriffsmöglichkeiten unterbindet. In der Umkehrung bedeutet dies natürlich ebenfalls, dass bestimmte Dienste, die eine direkte und unmittelbare Verbindung zwischen den Computer-Netzwerken erfordern, durch den Lock-Keeper™ nicht oder nur sehr schwer bereitgestellt werden können. Im Ausblick wird auf künftige Entwicklungen und bestehende Lösungen in diesem Bereich hingewiesen.

5. Firewall und Lock-Keeper™

Stärken einer Firewall

Wie oben bereits angesprochen stellen Firewalls das derzeitige Standardmittel der IT-Sicherheit dar. Die Vorteile der Firewall-Technologien liegen hauptsächlich im Bereich der Komfortabilität bei einer immer noch recht hohen Sicherheit. Die Firewall bietet mittlerweile ein sehr großes Spektrum an unterstützter Funktionalität bzw. Protokolle und somit auch ein hohes Maß an „Quality of Service".

Je höher das Sicherheitsniveau sein soll, desto weniger Protokolle und Anwendungen dürfen zugelassen werden. Was aber immer und bei jeder Firewall bestehen bleibt, ist die tatsächliche Verbindung auf den untersten Netzwerkschichten, nämlich dem „Physical Layer" und dem „Data Link Layer"[6].

Angriffspunkte

Der Komfort, den die große Funktionalität der Firewall mit sich bringt, geht natürlich zu Lasten der Sicherheit, da Firewalls, auch wenn sie das Standardmittel der IT-Sicherheit sind, auch eine große Anzahl von Sicherheitslücken und damit Risiken aufweisen:

i) Risiko Mensch

Eine zentrale Komponente zum Betrieb einer Firewall ist die Security Policy. Sie stellt die Grundlage dar, anhand derer die Firewall aufgesetzt, konfiguriert und betrieben wird. Häufig leidet die Durchsetzung der Policy auch unter fehlendem und/oder unzureichend ausgebildetem Personal. Das regelmäßige Warten und Aufspielen von Security Patches sind ebenso wichtig wie das Aufsetzen der Policy selbst und sollte nur von geschultem Fachpersonal durchgeführt werden.

[6] vgl. OSI-Reference Model

ii) Risiko Technik

Technische Schwachstellen kann man nur schwer im Voraus erkennen. Aus je mehr Zeilen Programmcode eine Software (Firewall) besteht, desto mehr Fehler, seien es nun logische oder Programmierfehler an sich, können sich potentiell im Programm verbergen. Diese Fehler oder „Bugs" können einem Hacker zu einem erfolgreichen Einbruch verhelfen. Doch nicht nur Bugs in der Firewallsoftware selbst, sondern auch Fehler im zugrundeliegenden Betriebssystem können solche „Security Holes" darstellen.

Eine weitere Schwachstelle der softwarebasierten Sicherheitslösungen sind undefinierte Zustände nach einem Ausfall. Hat beispielsweise ein Stromausfall einen Neustart der Software verursacht, kann das System in einen undefinierten Zustand geraten, der u.U. zwar die Funktionalität, aber nicht mehr die Sicherheit gewährleistet.

Stärken des Lock-Keepers™

Beim Lock-Keeper™ Schleusenmechanismus werden, wie bereits erwähnt, die Netzwerke physikalisch voneinander getrennt, sodass kein Zustand „online" mehr existiert.

Es ist nunmehr auch Insidern unmöglich, die Sicherheitsbarriere der hardwareseitigen Trennung von Netzwerken aufzuheben oder zu umgehen. Sowohl Software-Fehler als auch versehentliche oder absichtliche Misskonfigurationen des Systems gestatten aufgrund des Aufbaus keine direkte Verbindung der Netze durch die Schleuse.

Eine fehlerhafte Software-Komponente oder eine falsche oder unzureichende Konfiguration kann im schlimmsten Falle nur dazu führen, dass der Datenaustausch beeinträchtigt wird, allerdings wird die Integrität der Daten des internen Netzes dabei nicht gefährdet.

Durch das Schleusenkonzept kann ein Ausfall oder gar ein Angriff keinen Zustand erzeugen, der die beiden Netze direkt miteinander verbindet, da selbst bei einem Ausfall die Relais immer in einem definierten Zustand (entweder Verbindung nach innen oder Verbindung nach außen) bleiben.

Sicherheit gegen Komfort

Die Tatsache, dass der Lock-Keeper™ durch die physikalische Trennung der Netze keinen Online-Status besitzt, wurde bereits angesprochen. Somit können natürlich auch keine gewollten Protokolle direkt über den Lock-Keeper™ gefahren werden, die auf einer Onlineverbindung bestehen.
Eine von uns durchgeführten Studie zeigt jedoch, dass sich die meisten Szenarien trotzdem und ohne großen Komforteinbüßungen mit dem Lock-Keeper™ realisieren lassen.
So ist es zum Beispiel nicht nur möglich Mails oder Dateien über den Lock-Keeper™ zu transferieren, sondern auch die interne Firmendatenbank galvanisch vom Netz zu trennen, mit deren Daten z.B. die Webseite versorgt wird.. Ebenso lässt sich auch eine verschlüsselte Verbindung (z.B. VPN) mit dem Lock-Keeper™ realisierten, indem die jeweils nach außen zeigenden Lock-Keeper™-Rechner als Tunnelendpunkte fungieren. (s. Anwendungsbeispiele)

Dienste, die auf eine permanente Onlineverbindung bestehen, können nicht oder nur schwer durch den Lock-Keeper™ geschützt werden. Es ist zum Beispiel von Fall zu Fall zu entscheiden, ob sinnvolles Surfen im Internet über den Lock-Keeper™ zu realisieren ist, da hierbei die Antwort um mindestens zwei Schaltintervalle verzögert beim Benutzer ankommt (über Cache-Proxies). Andererseits stellt sich hier die Frage, ob „Surf-PC's" überhaupt in einem Hochsicherheitsnetz positioniert werden sollten.

Der Preis für eine sichere Abwehr von Online-Attacken muss also durch Einbußen im Quality of Service gezahlt werden. Einen Ausweg aus diesem Dilemma bieten hier mehrschichtige Sicherheitsarchitekturen. So kann ein Unternehmen das eigene Netz in mehrere Subnetze aufteilen, wobei – je nach Sicherheitslevel – diese Netze untereinander mittels einer Firewall oder eines Lock-Keeper™ gesichert sind. Selbstverständlich können Firewall und Lock-Keeper™ auch kombiniert eingesetzt werden.

Kombinierte Sicherheitsarchitekturen

Typischerweise beinhalten die IT-Architekturen von Unternehmen mit Internet-Standleitungszugängen neben der Absicherung durch eine Firewall ebenfalls Virenscanner und Mail-Analysetools.

Da der Lock-Keeper™ intern aus drei Rechnern besteht, kann praktisch jede Applikation installiert werden, die momentan auf dem Markt existiert und auf dem zugrundeliegenden Betriebssystem installiert werden kann. Es gibt mehrere Produkte (wie z.B. Virenscanner), die bereits ausgiebig auf dem Lock-Keeper™ getestet wurden.
Der Lock-Keeper™ an sich gewährleistet also durch die physikalische Trennung der Netze einen hundertprozentigen Schutz vor Online-Attacken. Darüber hinaus besteht zusätzlich noch die Möglichkeit, Offline-Attacken abzuwehren, da die Daten auf dem Weg durch den Lock-Keeper™ auf Viren, Würmer und Trojaner je nach Bedarf und Intensität untersucht werden können.

6. Anwendungsbeispiele

Im Folgenden sind einige Anwendungsbeispiele des Lock-Keepers™ aufgeführt. Grundsätzlich ist nahezu jeder Dienst über den Lock-Keeper™ transparent nutzbar, welcher sich auf dem „Store and Forward"-Prinzip realisieren lässt.

Mail Transfer via Lock-Keeper™

Der im Internet am meisten genutzte Dienst ist die elektronische Post, was gleichzeitig auch das klassischen Anwendungsbeispiel des Lock-Keepers™ darstellt. Der Mailaustausch kann hier in beide Richtungen praktisch transparent durchgeführt werden, indem man wie bei einem Proxy die Mails über den Lock-Keeper™ transferiert. Auch hier spielt der Zeitversatz praktisch keine Rolle, da es in den meisten Fällen irrelevant ist, ob eine Mail bspw. zwei Minuten später ankommt.

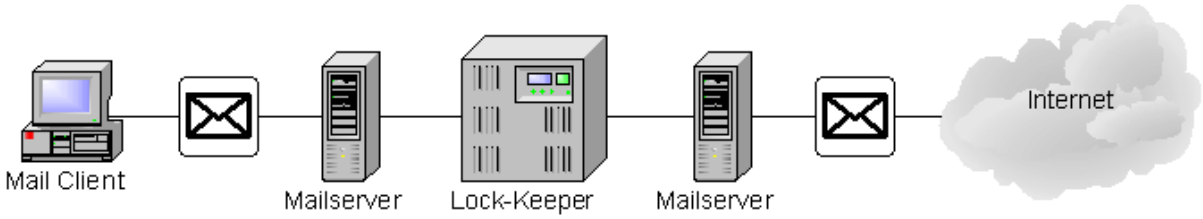

Abb. 4: Anwendungsbeispiel Mailtransfer

Dateitransfer via Lock-Keeper™

Ähnlich wie bei dem Transfer von Emails können auch Dateien automatisiert über den Lock-Keeper™ offline transportiert werden. Hierbei werden die Dateien z.B. in ein oder mehrere dafür vorgesehenen Ordner kopiert, von wo aus sie über den Lock-Keeper™ transferiert werden.

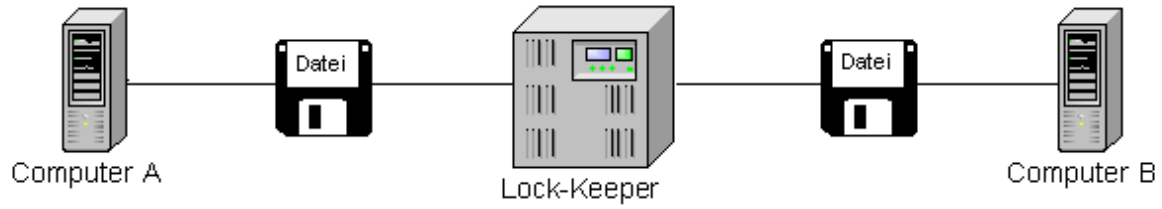

Abb. 5: Anwendungsbeispiel Dateitransfer

Datenbankabgleich über den Lock-Keeper™

Hierbei steht der Lock-Keeper™ zwischen dem eigentlichen Datenbankserver des Unternehmens, auf dem sämtliche relevanten (und u.U. auch äußerst sensiblen) Daten gespeichert sind. Mit dem Lock-Keeper™ bietet sich nun die Möglichkeit, z.B. einen Webserver mit Daten aus dem Hauptdatenbankserver (A) zu versorgen. Dies geschieht durch eine zweiten, mit dem Webserver auf online-Ebene verbundenen Datenbank (B), die ihre Daten offline über den Lock-Keeper™ vom Hauptserver A bekommt. Somit stehen bei einem Webseitenaufruf die relevanten Daten sofort und ohne Verzögerung zur Verfügung, wohingegen die Web-Datenbank B ihre Daten in bestimmten Zeitintervallen mit der Hauptdatenbank A abgleicht.

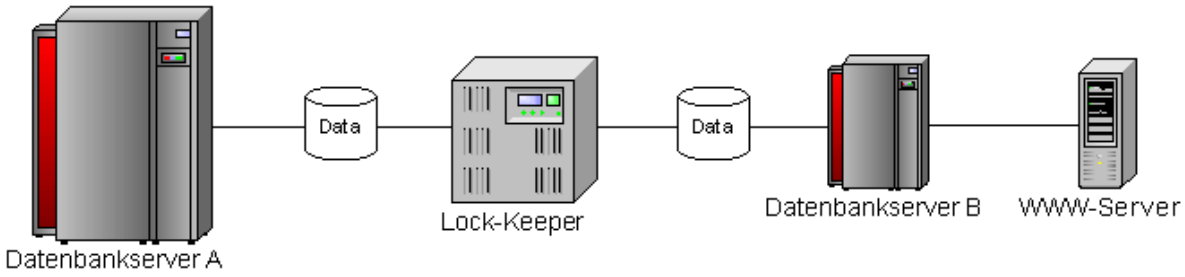

Abb. 6: Anwendungsbeispiel Datenbankabgleich

Sichere Verbindung zweier Unternehmen

Da bei der Verbindung zweier Unternehmen über das Internet praktisch eine neue Tür in ein offenes Netz geöffnet wird, entstehen dadurch natürlich ebenso die gleichen Risiken, wie bei der Anbindung an das Internet selbst. Neben der Tatsache, dass die dort ausgetauschten Daten u.U. äußerst sensibel sein können und von Dritten nicht „mitgehört" werden sollen, kann man auch nicht ausschließen, dass ein potentieller Angreifer die Verbindung zum eigentlich vertrauenswürdigen Partnerunternehmen ausnutzt und über diese Leitung Zugang zum internen Firmennetz erlangt.
Ersteres Problem kann mittels einer verschlüsselten Verbindung (z.B. VPN) der beiden Unternehmen gelöst werden. Jedoch stellt sich auch hier das Problem, immer noch eine direkte Onlineverbindung zwischen beiden Unternehmen zu haben, die – wenn auch verschlüsselt - ein Risiko darstellt.

Durch die Kombination beider Lösungen kann sowohl die Vorteile der verschlüsselten Verbindung als auch die physikalische Trennung der Netze gewährleistet werden.

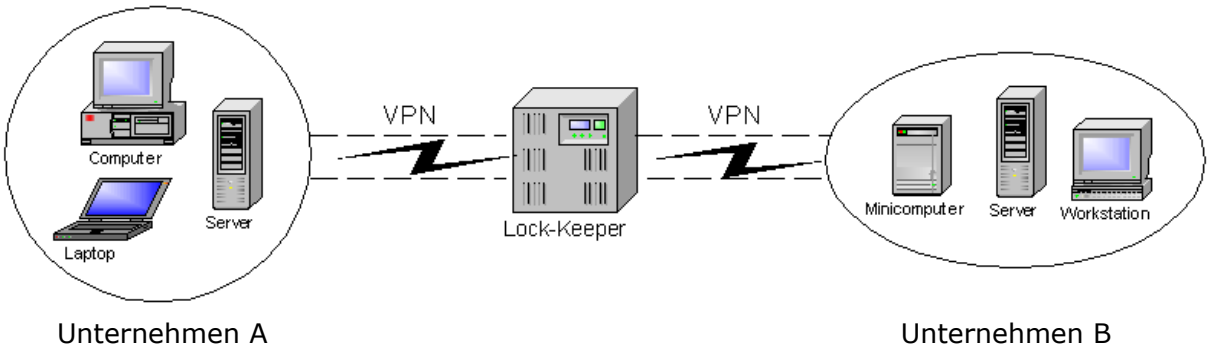

Abb. 7: Unternehmensanbindung mit VPN

Zusammenfassung und Ausblick

Moderne Sicherheitsarchitekturen müssen sich am wandelnden und wachsenden Bedarf an elektronischem Datenaustausch orientieren. Vielfältiger und multimedialer Transfer von Informationen zieht jedoch ebenso vielfältig ausgeprägte Angriffsmöglichkeiten nach sich. Durch unterschiedliche Sicherheitslevel lassen sich Anforderungen an den Quality-of-Service mit den jeweiligen Sicherheitsbedürfnissen in Einklang bringen. Hierzu ist eine möglichst breit angelegte Palette einsetzbarer Sicherheitskomponenten zu berücksichtigen. Neben und in Erweiterung zu klassischen Firewalls stellen so auch Lock-Keeper™ Infrastrukturen bereit, die sicheren Datenaustausch ermöglichen.
Neben der prinzipiellen Funktionsweise dieser Systeme wurde in der vorliegenden Arbeit zudem die Integration in komplexe Sicherheitsarchitekturen gezeigt. Zur Überwindung von zeitlichen Engpässen oder Beschränkungen von Diensten wurden darüber hinaus komplexe Erweiterungsmöglichkeiten skizziert.
Für künftige Ausbaustufen der Schleusentechnologie wird derzeit daran gearbeitet, zeitverzögert auch solche Dienste bereitzustellen, die für gewöhnlich eine unmittelbare Verbindung zwischen den datenaustauschenden Netzen erfordern. Die Einschränkungen im Bereich des Quality-of-Service könnten damit vermindert werden.

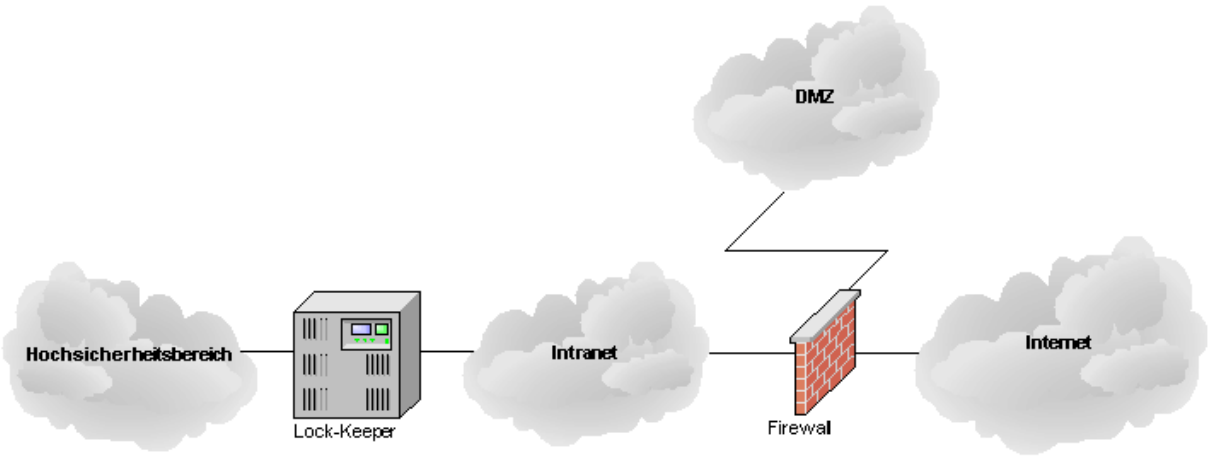

Abb. 8: Einsatz des Lock-Keepers™ mit einer Firewall zum Absichern eines Hochsicherheitsbereiches und eines Intranets.

Anhang A: Technische Spezifikationen des Lock-Keepers™

Beschreibung	Spezifikationen
Abmessungen (H x B x T)	86 x 482 x 573 mm (19" 4 HE)
Eingangsspannung Strom Frequenz Leistung	230 V AC ± 5 % 0.5 A 50 Hz 350 W Netzteil
Umgebungstemperatur (Betriebszustand) Umgebungstemperatur (Ruhezustand)	10-30° C 0-40° C

System Lock-Keeper™

Beschreibung	Spezifikationen
Interne Rechnerkarten Lock-Keeper™	 3 x CPU SBC PC Industriesteckkarten 3 x IBM IC35L040AVER07 7300 rpm UDMA TI-LK Steuerplatine v1.4
Hardwarespezifikationen pro PC-Karte	Intel Pentium LowPower 266 Mhz 64 MB SDRAM
Anschlüsse (je Karte)	RJ45 FE PS/2 Tastatur Monitor, 15 polig (3x5) Seriell, 9 polig (Konsole)
Betriebssystem	SuSE Linux v. 7.2
max. interner Datendurchsatz	115.200 bps, seriell (Lock-Keeper™ Basic) 100 Mbps, FE (Lock-Keeper™ Advanced)

Anhang B: Literatur

[1] Morrie Gasser: Building a secure Computer System, Van Nostrand Reinhold, 1988

[2] William R. Cheswick, Steven M. Bellovin: Firewalls and Internet Security, Addison-Wesley, 5th printing April, 1995

[3] P. Gulbins, UNIX Version 7, bis System V.3, Springer-Verlag, 1988

[4] B. Costales, E. Allmann: sendmail, O'Reilley and Associates, 2nd edition, 1997

[5] David A. Curry: UNIX System Security: A Guide for Users and System Administrators, Addison-Wesley, 1992

[6] G. Paul Ziemba et al.: Request for Comments: 1858, Security Considerations – IP Fragment Filtering, October 1996

[7] Klaus Brunnstein: Beastware (Viren, Würmer, trojanische Pferde) Paradigmen Systemischer Unsicherheit, Sichere Daten, sichere Kommunikation, Springer-Verlag, 1994, 44-60

[8] F. Cohen: Computer Viruses: Theory and Experiments", proceedings of the 7th National Computer Security Conference, Gaithersburg 1984, 240-263

[9] P. A. Karger: Limiting the Potential Damage of Discretionary Trojan Horses, Proceedings of the 1987 Symposium on Security and Privacy, IEEE Computer Society, 1987, 32-37

Kontakt

IT-Services s.à.r.l.
25C, boulevard Royal
L-2449 Luxembourg

Tel: +352 46 13 3 13 – 01
Fax: +352 46 13 3 13 – 09

Web: http://www.it-services.lu/

General Information:
info@it-services.lu

Join our team:
jobs@it-services.lu