



Institut für Telematik unter Betreuung der
Fraunhofer Management GmbH

Internet / Intranet

Preprint 00-02

ISSN 1433-8106

Dipl.-Inform. E.-G. Haffner

Dr. T. Engel

Prof. Dr. Ch. Meinel

Die Lock-Keeper-Architektur

Sicherer Schutz gegen Online-Attacken aus dem Internet
durch fortschrittliche Schleusentechnologie

Abstract.....	2
Sicherheit im Internet	2
Lock-Keeper	4
Praxis des Lock-Keepers	7
Zusammenfassung und Ausblick	8
Literaturverzeichnis.....	9

Abstract

Die Lock-Keeper Technologie stellt eine moderne Schleusenarchitektur dar, um sicheren Datenaustausch zwischen Computernetzwerken zu ermöglichen. Insbesondere dann, wenn die Sicherheitsbedürfnisse eines Unternehmens enorm hoch sind und ein passiver, zeitversetzter Informationsaustausch (z.B. Transfer sicherheitsrelevanter Dokumente, E-Mails u.a.) genügt, so empfiehlt sich der Einsatz des „Lock-Keepers“, der mit vergleichsweise geringem Konfigurationsaufwand höchste Sicherheitsvorgaben erfüllt.

Die Funktionsweise des Lock-Keepers entspricht dabei dem Passieren einer Schleuse: Zu keinem Zeitpunkt besteht eine direkte Verbindung zwischen den beiden Netzen, z.B. einem firmeneigenen Intranet und dem Internet, sondern, je nach Zustand der „Schleusentore“, findet der Informationsaustausch nur jeweils mit einem der Kommunikationspartner statt. Die fortschrittliche Architektur des Lock-Keepers erlaubt es, den Zeitversatz im Datenaustausch zu minimieren.

Sicherheit im Internet

Das „Internet“ ist ein Oberbegriff für den Zusammenschluß verschiedener Rechnernetzwerke, deren gemeinsames Protokoll TCP/IP¹ den Informationsaustausch an beliebigen Knotenpunkten ermöglicht. Ursprünglich als Wissenschaftsnetz konzipiert, hat sich das Internet durch die Einführung multimedialer Übertragungsprotokolle und –sprachen wie HTTP² und HTML³ inzwischen zu einem gigantischen Kommunikationsmedium entwickelt und längst haben kommerzielle Unternehmen, Dienstleister, Industrie und Handel die Möglichkeiten des neuen Mediums erkannt [ME97], [MEM97].

Allerdings wachsen mit den Chancen des Netzes auch seine Risiken. Nicht allein unberechtigte, räuberische Zugriffe auf das Firmennetz sind abzuwehren, auch unbeabsichtigte Preisgabe sensibler Daten, Kunden-, Personal- oder Unternehmensinformationen müssen geschützt werden und dürfen „von außen“ nicht einzusehen sein. Es gilt, neben Abhör- und Manipulationsschutz ebenfalls die Authentizität des Kommunikationspartners zu gewährleisten.

Neben derartigen kriminellen Attacken, gegen die sich Unternehmen schützen müssen, stellt sich ein weiteres Problem der Sicherheit im Datenaustausch. Programme, die Viren enthalten

¹ Transport Control Protocol/Internet Protocol

² Hypertext Transport Protocol

³ Hypertext Markup Language

und andere unerwünschte Software-Sendungen, insgesamt auch „Beastware“ genannt, sollten nicht in das innere Firmennetz eindringen.

Und ein weiterer Faktor kommt hinzu. Wenn berechtigter Datenaustausch zwischen zwei Netzen stattfindet, muss verhindert werden, dass im selben Moment ein unbefugter Zugriff auf weitere Daten erfolgt, insbesondere dann, wenn das Internet eines der beiden Netze darstellt. Solche Angriffe werden auch Online-Attacken genannt.

Das Standardverfahren zum Schutz der eigenen Daten gegen unberechtigten Zugriff aus dem Internet sieht als Vermittlungsstelle zwischen Intranet und Internet eine sogenannte „Firewall“ vor: Aufgabe dieses Systems ist das Filtern von IP-Paketen durch Überprüfung von Quellen- und Zieladressen, TCP-Ports und den angeforderten Diensten (Details über Firewalls finden sich in [CB95]). Die Rechnersysteme im Intranet werden so „unsichtbar“ für den Beobachter von Seiten des Internets. (vgl. Abbildung 1)

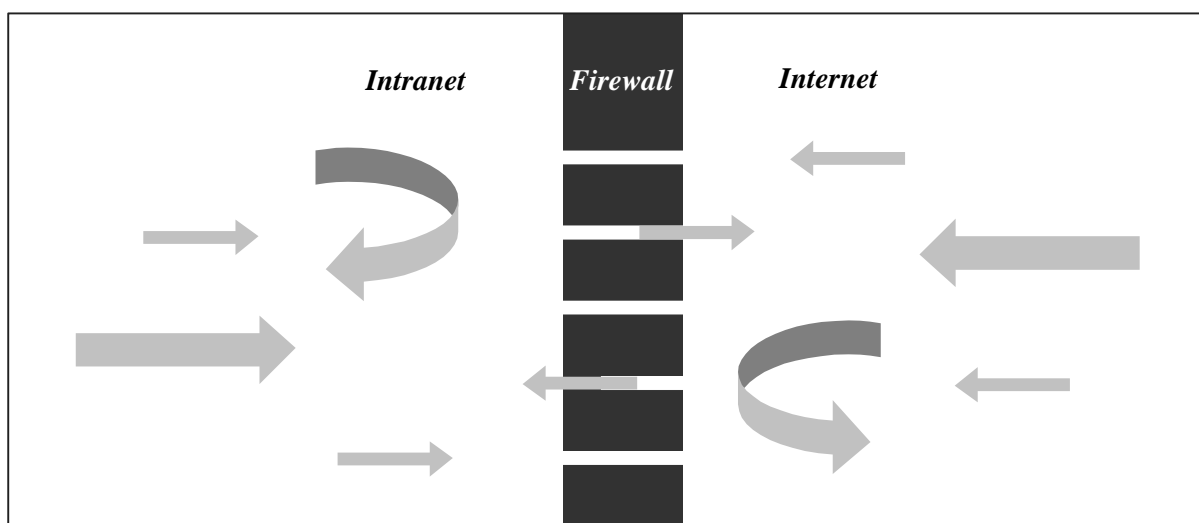


Abbildung 1: Funktionsweise einer Firewall

Eine derartige „Software-Lösung“ genügt jedoch den Sicherheitsexperten einiger Firmen nicht. Sie beunruhigt neben dem hohen Konfigurationsaufwand und einem nicht unerheblichen Kostenfaktor die Kreativität und kriminelle Energie unberechtigter Eindringlinge. Simulation zugriffsberechtigter IP-Nummern, „Schnüffeln“ von TCP/IP-Paketen und die mißbräuchliche Nutzung bestimmter TCP-Dienste machen in regelmäßigen Abständen negative Schlagzeilen und führen zur Verunsicherung der Unternehmensführung. Immer wieder zeigen sich neue Schwachpunkte von Firewalls, Beispiele sind etwa in [PP98] und [LA94] zu finden.

Immer wieder zeigt sich, dass Kommunikationsabläufe, die „eigentlich“ als sicher eingestuft wurden, durch raffinierte Tricks der „Hacker“ zu unberechtigtem Eindringen in das firmeneigene Netz geführt haben.

Natürlich werden enorme Anstrengungen unternommen, den Datentransfer im Internet sicherer zu machen [RA97]. Beispielsweise kann die Einführung des SSL⁴ zum Verschlüsseln der IP-Pakete als ein wichtiger Schritt in diesem Bestreben angesehen werden. Allein das Un-

⁴ Secure Socket Layer

behagen bleibt. Wie kann die Kontrolle über den Datenfluss aus dem Internet auf klare und einfache Weise beim Unternehmen verbleiben?

Hinzu kommt eine weitere, prekäre Anforderung bezüglich der Kommunikation aus dem Intranet in die „weite Welt“. Wie können Mitarbeiter davor geschützt werden, freiwillig oder unfreiwillig sensible Daten ins „Netz der Netze“ zu senden? Im allgemeinen wird der Datenaustausch in dieser Richtung weniger stark als Bedrohung thematisiert, doch was nützen Sicherheitsvorkehrungen wie das Entfernen lokaler Diskettenlaufwerke und die ausschließliche Verwendung von Fileserver-Speichermedien, wenn Mitarbeiter unerlaubt und unbeobachtet sensible Daten ins Internet versenden?

Das Konzept der *Firewalls* wurde im Laufe der letzten Jahre stark verbessert und verfeinert, doch mit dem Anspruch der interaktiven Kommunikation zwischen Intranet und Internet lassen sich Restrisiken nicht vermeiden.

Lock-Keeper

Hier setzt das Prinzip des *Lock-Keepers* an: Der Lock-Keeper setzt (mindestens) 2 voneinander unabhängige Rechnersysteme voraus, einen „Intranet-Server“ (*INS*) und einen „Lock-Keeper-Server“ (*LKS*). Zwischen *INS* und *LKS* befindet sich das „innere Schleusentor“ (*inner gate, IG*) und zwischen *LKS* und dem Internet das „äußere Schleusentor“ (*outer gate, OG*). (vgl. Abbildung 2)

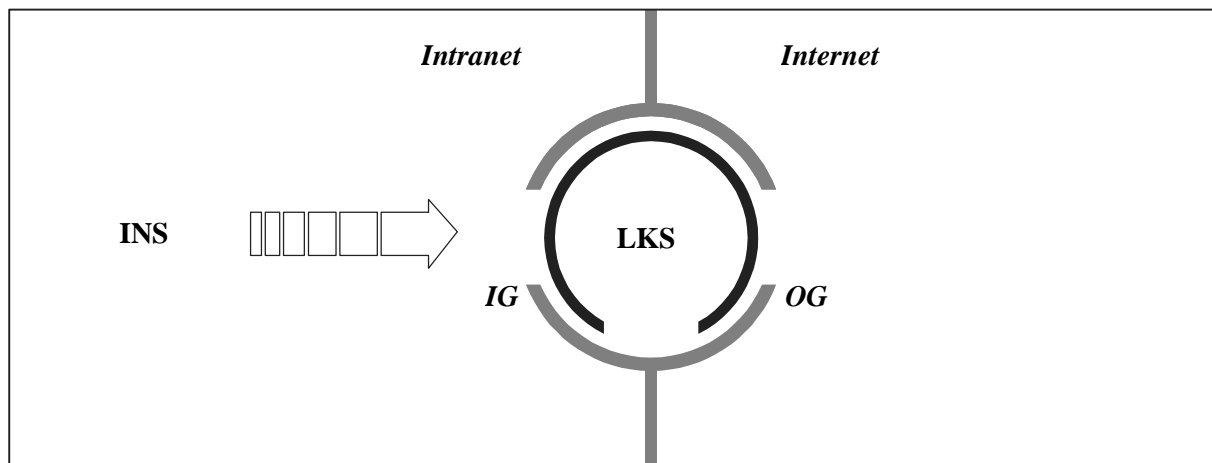


Abbildung 2: Aufbau der Lock-Keeper-Komponenten

Von höchster Bedeutung ist hierbei, dass zu keinem Zeitpunkt beide Schleusentore, *IG* und *OG*, gleichzeitig geöffnet sind. Darüber hinaus muss diese Aussage *physikalisch erzwungen* sein, d.h. selbst bei fehlerhafter Software oder erfolgreichem Angriff auf eine der Komponenten darf die Topologie der Gesamtarchitektur hierdurch nicht korrumpiert werden. Dies gilt auch für berechtigte Zugreifer. Aufgrund der physikalischen Gegebenheiten können auch Systemadministratoren keine Möglichkeit entwickeln, die Schleusentore gleichzeitig zu öffnen, um beispielsweise eine schnellere Durchlaufzeit von Daten zu erzielen. Somit kann zu keinem Zeitpunkt eine *durchgängige* Verbindung zwischen Intranet und Internet bestehen.

Alle Daten aus dem Intranet werden zum INS gesendet und hier eingehend analysiert (Phase 1). Erst bei geöffnetem IG gelangen die „bereinigten Informationen“ in die „entmilitarisierte Zone“, den LKS (Phase 2). Anschließend wird das innere Schleusentor geschlossen und die auszutauschenden Daten befinden sich auf dem LKS (Phase 3). Hier finden allerdings, aus Gründen, die weiter unten erläutert werden, keine weiteren Analyseprozesse statt. Die Verweildauer der Informationen richtet sich nach den Anforderungen des Unternehmens und der Dringlichkeit der Inhalte. Sobald das OG geöffnet ist, werden die Daten ins Internet gesendet (Phase 4). Zugleich können berechtigte oder gegebenenfalls auch unberechtigte Zugriffe von außen an den LKS erfolgen. In diesem Moment ist die Sicherheit des LKS nicht höher als die einer herkömmlichen Firewall, dennoch bleibt das Intranet des Unternehmens unangetastet, da *keine physikalische Verbindung* hierzu aufgebaut werden kann, solange der Kontakt zum Internet aufrecht erhalten bleibt!

Das OG wird nach Austausch der Daten mit dem Internet-POP⁵ wieder geschlossen und die Daten verbleiben auf dem LKS (Phase 5). An dieser Stelle wird klar, warum der LKS die transferierten Informationen nicht analysieren darf. Durch den direkten Kontakt mit dem Internet könnte der Analysemechanismus selbst durch unberechtigte Eindringlinge manipuliert worden sein.

Wenn im letzten Schritt das IG erneut geöffnet wird und die Daten vom LKS zum INS gelangen (Phase 6), können zwar „infizierte“ Dateien im IFS abgelegt werden; dennoch besteht hier ein qualitativer Unterschied zur Funktionsweise von Firewalls. Anstatt „online“ alle Analyseprozesse durchzuführen, kann der INS ohne Bedrohung durch interaktive Manipulationen die „passiven“ Daten, die der LKS aus dem Internet erhalten hat, je nach gewünschter, skalierbarer Analysetiefe untersuchen und gegebenenfalls vernichten (Phase 7). Der Schwerpunkt dieser Untersuchungen richtet sich auf das Eindringen sogenannter „Trojanischer Pferde“, Daten, die selbst wiederum Prozesse ausführen und beispielsweise als Makroviren Schaden anrichten können⁶.

Interessant scheint auch die Perspektive zur semantischen Analyse von Texten. Dürfen bestimmte Inhalte das unternehmensweite LAN/WAN verlassen? Oftmals können derartige Entscheidungen nur durch menschliche Experten gefällt werden. Auch diese Option steht durch den Lock-Keeper-Mechanismus zur Verfügung, weil die Analysezeiträume flexibel zu gestalten sind. Im Falle des Mail-Austausches lassen sich deren Typen (*Content-Type*), die Kodierungsarten (*Content-Transfer-Encoding*) und die Größen analysieren und entsprechend kann hierauf reagiert werden.

Tabelle 1 verdeutlicht den Zusammenhang zwischen den geschilderten Phasen und dem jeweiligen Zustand der beiden Schleusentore. Der Tabelle ist zu entnehmen, dass sich aufgrund eines identischen Schleusenzustands (Stati α , β oder γ) sowohl die Phasen 1, 3, 5 und 7 als auch die Phasen 2 und 3 gleichzeitig durchführen lassen. Die Phase 4 beinhaltet als Teilphasen die Datenausgabe ins Internet sowie deren Aufnahme.

Dargestellt sind die Schleusenzustände für den einfachsten Fall des Lock-Keeper Einsatzes. Im folgenden Kapitel werden darüber hinausgehende Möglichkeiten gezeigt, um den Durchsatz von Informationen mittels der dargestellten Zustände noch weiter zu beschleunigen.

⁵ **Point of Presence**. Nicht zu verwechseln mit dem Post-Office-Protocol zum Empfangen von Mails!

⁶ Unlängst ist es zwei Schülern gelungen, mittels eines solchen „Trojanisches Pferds“ unberechtigt in das Netz des Providers „T-Online“ einzudringen

Phase	Beschreibung	IG	OG	Status
1	Analyse ausgehender Daten durch INS	geschlossen	geschlossen	α
2	Datentransfer vom INS zum LKS	offen	geschlossen	β
3	Warten des LKS auf Öffnung OG	geschlossen	geschlossen	α
4	Datentransfer vom LKS ins Internet und in der Gegenrichtung	geschlossen	offen	γ
5	Warten des LKS auf Öffnung IG	geschlossen	geschlossen	α
6	Datentransfer vom LKS zum INS	offen	geschlossen	β
7	Analyse eingehender Daten durch INS	geschlossen	geschlossen	α

Tabelle 1: Phasen des Austauschmechanismus und Zustände des Lock-Keepers

Die folgende Abbildung 3 verdeutlicht noch einmal die Funktionsweise des Lock-Keepers. Zur besseren Übersicht werden allerdings nur die Phasen 2 bis 4 dargestellt.

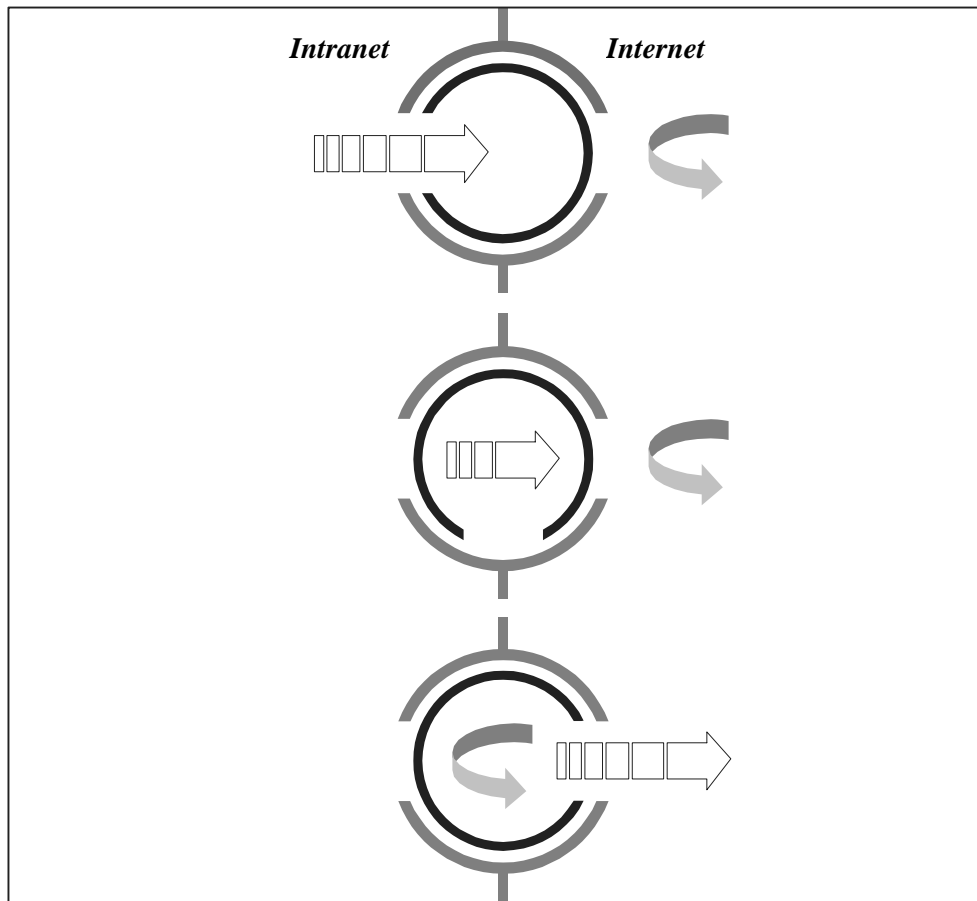


Abbildung 3: Funktionsweise des Lock-Keeper Mechanismus
 Unternehmensinformationen gelangen durch den Lock-Keeper ins Internet

Es zeigt sich, dass der physikalischen Trennung der beiden Schleusentore IG und OG eine zentrale Rolle zukommt. Würde hier eine Software-Lösung anvisiert, könnte die Sicherheit des Gesamtsystems kaum höher als die herkömmlicher Firewalls eingestuft werden.

Praxis des Lock-Keepers

Das oben beschriebene Verfahren wurde durch das *Institut für Telematik* konkret auf das Mailaustausch-Verfahren einer bedeutenden Bank angewendet.

Ziel dieses Projektes war der sichere Datenaustausch zwischen der Bank und dem Internet. Die auszutauschenden Informationen beschränkten sich hierbei auf elektronische Post. Es mußte gewährleistet werden, dass sowohl die Nachrichtenübermittlung der Mitarbeiter ins Internet als auch die Analyse der eingehenden Daten aus dem Internet auf höchstem Sicherheitsniveau stattfinden sollte. Selbstverständlich haben diese E-Mails nicht den Status einer „privaten“ Post, die nur vom Empfänger dekodiert werden sollte (vgl. [LU98], [WE97]). Wir entschieden uns für ISDN-PPP-Connections als Schleusentore, um einen schnellen Verbindungsaufbau zu gewährleisten und einen ansehnlichen Datendurchsatz zu erzielen. Die beiden Server LKS und INS wurden durch Linux-PC's bereitgestellt.

Unser Lock-Keeper-Konzept bestach durch das einfache Grundprinzip und seine offensichtlichen Sicherheitscharakteristika. Das Problem der physikalischen Trennung der Schleusen konnte von uns gelöst werden, indem wir beide Server, INS und LKS, an **denselben** ISDN-NTBA anschlossen. Dieses Endgerät gestattet maximal 2 Amtsverbindungen pro Zeitpunkt. Wenn INS zu LKS eine Verbindung aufbaute, wurden beide Kanäle hierfür beansprucht: einer für die Auswahl, einer für die Einwahl. Eine gleichzeitige Verbindung von LKS ins Internet war so per se ausgeschlossen. Wenn dagegen bereits eine Verbindung zwischen dem POP-Server im Internet und LKS bestand, konnte INS nur den einen verbleibenden Kanal für die Wahl nach außen einsetzen, während die Verbindung zum LKS nicht mehr möglich war. Zusätzlich konnte die Initiierung des Wahlvorganges nur „von innen nach außen“ erfolgen, d.h. INS kontaktiert LKS und dieser den Internet-POP, nicht etwa umgekehrt.

Eigene Mailanalyse-Programme führten eine Vorsortierung der Information in „kritische“ und „unkritische“ aus. Erstere wurden zur weiteren Behandlung an einen menschlichen Experten weitergeleitet, während letztere sofort zugestellt werden konnten.

Sowohl bei ausgehenden als auch bei eingehenden Sendungen wurde der Mitarbeiter, der Empfänger bzw. Sender der kritischen Information gewesen ist, automatisch informiert.

Diese Architektur, die mittels der Schleusentechnologie des Lock-Keepers höchste Sicherheitsanforderungen bei gleichzeitiger klarer, überschaubarer Prozesshaftigkeit gewährleistete, zeitigte rasch die erhofften Ergebnisse.

Für den Email-Verkehr ist jedoch mit einer gewissen Verzögerungszeit zu rechnen, da die Zustellung jeweilig über 2 Stationen, innerhalb von zwei *Zyklen* erfolgen musste. Eine unmittelbare Zustellung von elektronischer Post ist nicht möglich.

Eine fortgeschrittene Lösung dieser Schwierigkeit bietet sich durch eine Verdopplung der LKS-Stufe an: INS kann somit stets entweder LKS1 oder LKS2 kontaktieren. Die beiden Lock-Keeper Systeme sind untereinander unverbunden! Beide können jedoch, allerdings nur dann, wenn gerade keine Verbindung zum INS besteht, zum Internet-POP eine PPP-Connection erzeugen. Hierdurch verringert sich die Wartezeit von ausgehender Email auf den LKS-Systemen, während sich ein kompletter Zyklus auf INS verkürzt. Post wird hier unmittelbar zu einem der beiden LKS-Systeme zugestellt.

Zusammenfassung und Ausblick

Das Lock-Keeper-Konzept bietet eine sehr hohe Sicherheit beim Informationsaustausch zwischen firmeneigenen Intranets und dem Internet. Die Einfachheit des Konzepts und die freie Skalierbarkeit der Analysetiefe sind die großen Stärken dieser Lösung. Das Verfahren ist dazu geeignet, das Vertrauen der Sicherheitsexperten großer Unternehmen bezüglich der Kontrolle des Informationsflusses zu genießen.

Alle Online-Attacken auf ein internes Netz lassen sich durch die physikalische Basis der Schleusentoren mit höchstem Sicherheitsniveau ausschließen. Allerdings auch andere Arten von räuberischem oder kriminellen Zugriff auf Firmendaten können innerhalb der Lock-Keeper-Architektur adäquat bekämpft werden. Die vorgestellten Mechanismen lassen sich zur Steigerung von Performance und Durchsatz, bzw. zur Reduktion von Durchlaufzyklen erweitern.

Das Konzept lässt sich ferner dahingehend erweitern, dass weitere Lock-Keeper, dem Intranet-Server nachgeschaltet, die unterschiedlichen Sicherheitsanforderungen verschiedener Abteilungen und Mitarbeiter noch adäquater abbilden.

Literaturverzeichnis

- [BO97] Greg Bossert et al.: Request for Comments: 2084, Considerations for Web Transaction Security, January 1997
- [CB95] William R. Cheswick, Steven M. Bellovin: Firewalls and Internet Security, Addison-Wesley, 5th printing April, 1995
- [CO84] F. Cohen: Computer Viruses: Theory and Experiments”, proceedings of the 7th National Computer Security Conference, Gaithersburg 1984, 240-263
- [DO91] Douglas E. Comer: Internetworking with TCP/IP: Principles, Protocols and Architecture, Vol. 1, Prentice-Hall, second edition, 1991
- [ED97] M. Edwards, Security gets easier, cheaper, Communication News, November 1997, S. 82-83
- [ME97] Ch. Meinel, Wie funktioniert das Internet?, ITWM-Preprint 97-01, 1997
- [MEM97] S. Müller, T. Engel, Ch. Meinel, Das Internet – Neues Medium für kommerzielle Aktivitäten, Studie erstellt am ITWM-Trier, 1997
- [LA84] C. E. Landwehr: The Best Available Technologies for Computer Security, Advances in Computer Security, vol. 2, Artech House, 1984, 108-122
- [LA94] M. Laubach, Request for Comments: 1577, Classical IP and ARP over ATM, 1994
- [LU98] N. Luckhardt, Kryptokampagne, c't 6/98, S. 32-33, 16.03.98
- [PE94] Heribert Peuckert: Datenschutz und Datensicherheit aus technischer Sicht, Sichere Daten, sichere Kommunikation, Springer-Verlag, 1994, 13-26
- [PP98] I. Pakhomenko, E. Pless, Sicherheitsprobleme in IP-über-ATM-Netzen, iX 3/98, S. 118-121, März 98
- [RA97] M. J. Ranum, Network security: safety is next, Data Communication, 21.10.97, S. 128-132
- [WE97] T. E. Weber, Should only the paranoid get E-mail protection?, Wall Street Journal, 25.09.97