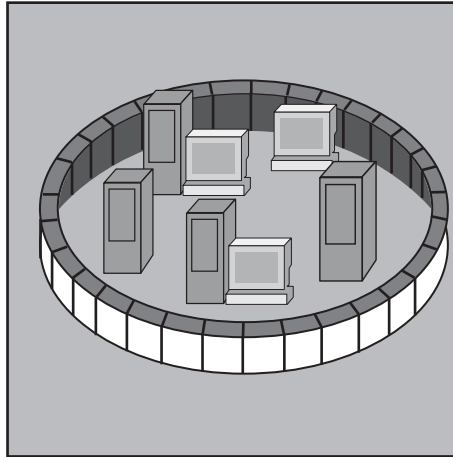


Schwerpunktthema

Sicherheitsanalyse des Cisco NAC Framework

von Dror-John Röcher, Michael Thumann

Das Cisco „Network Admission Framework“ hat zum Ziel, den Zugang zum Netzwerk basierend auf der Einhaltung einer „Policy“ zu reglementieren. Dazu werden Clients einer Prüfung unterzogen und basierend auf dieser Prüfung wird der Zugang in verschiedenen Stufen gewährt. Cisco NAC ist eine relativ junge Technologie, die langsam an Bedeutung für den Markt gewinnt. Neben Cisco gibt es noch etliche andere Hersteller mit eigenen „Admission-Control“-Lösungen, die aber in diesem Artikel nicht näher beschrieben oder analysiert werden. Im ersten Teil wird ein kurzer Überblick über die Funktionsweise und wichtigen Bestandteile



des Cisco NAC Frameworks gegeben, der zweite, aufbauende Teil, enthält eine Sicherheitsanalyse des Cisco NAC Framework. Abschließend werden Maßnahmen zur Erhöhung des Sicherheitsniveaus in Cisco NAC diskutiert.

weiter auf Seite 22

Zweitthema

Virtuelle Poststellen - sichere E-Mail für alle?

von Dipl.-Inform. Andreas Meder

In der heutigen Zeit, da einerseits das schnelle und zuverlässige Austauschen von Informationen für die Geschäftsprozesse der meisten Unternehmen - zumindest vom Mittelstand an aufwärts - essentiell ist (Stichwort: Informationsgesellschaft) und andererseits diese Informationen vermehrt nur noch in elektronischer Form vorliegen - zumindest während der Entwurfsphase - besteht mehr denn je die Anforderung nach

Möglichkeiten, diese Informationen, d.h. in aller Regel Dokumente respektive Daten, zwischen den eigenen Mitarbeitern und unternehmensfremden Anwendern auf sicherem Wege auszutauschen. Unter einem „sicheren Weg“ wird dabei allgemein eine Methode verstanden, die durch Einsatz kryptografischer Verfahren die Vertraulichkeit und Integrität der übermittelten Informationen hinreichend sicherstellt.

Zu den Nutzerkreisen eines solchen sicheren Dokumentenaustauschs gehören typischerweise neben Forschungs- und Entwicklungsgruppen insbesondere auch Anwender mit kaufmännischem oder juristischem Hintergrund.

weiter auf Seite 9

Top Veranstaltung

**ComConsult
SIP-
Forum 2007**

Geleit

**SOA ist, wenn 's
trotzdem läuft**

Report des Monats

**Voice-over-
IP-Lösungen
von Alcatel**

Zweitthema

Virtuelle Poststellen - sichere E-Mail für alle?

Fortsetzung von Seite 1



Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Man denke hier nur an den Erhalt eines erarbeiteten technologischen Vorsprungs während der gemeinsamen Entwicklungsarbeit über Standort- und mitunter sogar Unternehmensgrenzen hinweg oder an sensible Inhalte von Vertragstexten oder Angeboten. All dies soll verständlicherweise vor unbefugtem Zugriff möglichst sicher geschützt werden.

Derartige Informationen wurden früher in verschlossenem Umschlag der Post anvertraut - sofern man nicht aufgrund der besonderen Brisanz bestimmter Nachrichten auf Kuriere zurückgreifen musste. Die Rolle der Briefpost hat im Zeitalter des weltumspannenden Internets deren elektronisches Pendant übernommen. Allerdings bedarf es geeigneter Maßnahmen zum Schutz der Nachrichten während des Übermittlungsvorgangs: denn obwohl die Reisezeit elektronischer Post gegenüber der daher auch gern als „Snail Mail“ belächelten konventionellen Variante in aller Regel vernachlässigbar kurz ist, ist dennoch das Risiko eines Informationsabflusses an Unbefugte erheblich größer. Immerhin kennt die heute gebräuchliche E-Mail Technologie keinerlei informationstechnische Entsprechung des klassischen Briefumschlags, der konventionelle Briefpost vor neugierigen Blicken schützt und zumindest ein unbemerktes Lesen der Post erheblich erschwert; eine nicht durch Zusatzmaßnahmen geschützte E-Mail ist daher weit eher mit einer Postkarte vergleichbar, denn mit einem Brief. Und schlimmer noch: sogar Manipulationen am Inhalt der übermittelten Nachrichten sind prinzipiell mit Leichtigkeit möglich, ohne dass dieses dem Empfänger einer derart ihrer Integrität beraubten Botschaft unmittelbar auffallen kann.

Zum Glück lassen sich über zusätzliche Schutzmaßnahmen derartige Angrif-

fe auf die Vertraulichkeit und Integrität von E-Mails wirksam verhindern: Kryptografie wird schon seit dem Altertum eingesetzt, um übermittelte Botschaften abzusichern und steht spätestens seit Mitte der 90er Jahre des vorigen Jahrhunderts auch Unternehmen, Behörden und sogar Privatpersonen zur Verfügung. Bis zu diesem Zeitpunkt erforderten speziell Lösungen zur E-Mail-Verschlüsselung enorme Rechenkapazitäten, die in der Regel nur Geheimdiensten oder allenfalls Großkonzernen oder Universitätsrechenzentren zur Verfügung standen. Die Ursache hierfür lag in den aufwändigen mathematischen Algorithmen, die bei sicheren (genauer: derzeit als sicher angesehenen) asymmetrischen Verschlüsselungsverfahren zum Einsatz kommen: die Geheimhaltung des privaten Pendants zu einem öffentlichen Schlüssel basiert auf der Verwendung so genannter „Einwegfunktionen mit Hintertür“ auf Basis sehr großer Primzahlen. Klassische Vertreter im Umfeld von Public Key Infrastructures (PKI) sind RSA - benannt nach seinen Entwicklern Rivest, Shamir und Adleman -, Diffie-Hellman oder El-Gamal.

Erst die Veröffentlichung von PGP (Pretty Good Privacy) durch Phil Zimmerman ermöglichte es auch mit Ressourcen, wie sie ein damals üblicher Arbeitsplatzrechner zur Verfügung stellte, komfortabel und sicher E-Mails zu verschlüsseln und zu signieren. PGP verwendete erstmals ein so genanntes Hybrid-Verfahren, bei dem die rechenintensiven Algorithmen nur zur Chiffrierung eines symmetrischen Schlüssels verwendet werden, nicht jedoch zur Verschlüsselung der gesamten Nachricht. Letztere wird stattdessen unter Verwendung des symmetrischen Schlüssels erheblich schneller ver- und natürlich auch entschlüsselt.

Das PGP-Problem

Leider hat PGP - und mit ihm alle vergleichbaren E-Mail-Verschlüsselungslösungen - einen nicht zu unterschätzenden Nachteil: es handelt sich dabei typischerweise um Einzelplatzlösungen für den E-Mail-Client des jeweiligen Anwenders. Grundsätzlich erfüllen alle diese Lösungen zwar die typischerweise spezifizierten Sicherheitsanforderungen, sofern hinreichend starke kryptografische Verfahren, d.h. insbesondere solche mit ausreichender Schlüssellänge, genutzt werden. Als problematisch hat sich jedoch der Betrieb solcher Lösungen in größeren Netzwerkumgebungen erwiesen. Aufgrund des Einzelplatzcharakters ist grundsätzlich eine mehr oder minder aufwendige Administration der jeweiligen Client-Installation erforderlich. Auch die Bereitstellung der notwendigen öffentlichen Schlüssel für alle an der jeweiligen Kommunikation Beteiligten generiert einen nicht zu unterschätzenden Overhead. Schließlich ist auch ein gewisses Augenmerk auf die Nutzer derartiger Lösungen zu richten: da heute der Einsatz von Verschlüsselung im Zusammenhang mit dem Austausch von E-Mails noch immer eher die Ausnahme als die Regel darstellt, stellt sich mangels regelmäßiger Nutzung bei vielen Anwendern die ansonsten hilfreiche Routine nicht oder stets nur phasenweise ein. Die Folge ist ein intensiver Betreuungsbedarf bei den meisten Nutzern hinsichtlich der Bedienung der jeweiligen Software.

Auch ist festzuhalten, dass insbesondere PGP zwar vor allem im Consumerbereich einen hohen Verbreitungsgrad erlangt hat, aber nicht den einzigen relevanten Standard für verschlüsselte E-Mail-Kommunikation darstellt. Insbesondere im Bereich des professionellen E-Mail-Einsatzes kommt häufig S/MIME (Secure Multip-

Virtuelle Poststellen - sichere E-Mail für alle?

urpose Internet Mail Extensions) zur Anwendung. Die Inkompatibilität der beiden Standards führt dazu, dass ggfs. einer der beiden Kommunikationspartner ein zusätzliches Produkt neben seiner etablierten Standardlösung einsetzen muss. Auch dadurch steigt der Administrations- und Betreuungsaufwand - wenn auch in der Regel nicht auf beiden Seiten der Kommunikationsbeziehung.

Deutlich besser geeignet wäre hier eine Lösung mit zentralistischem Ansatz. Bei diesem Prinzip wird ein spezieller Server eingesetzt, der aus- und eingehende Mails bei Bedarf zentral einer Ver- bzw. Entschlüsselung unterwirft.

Basierend auf den mit gängigen Stand-alone-Lösungen gemachten meist eher negativen Erfahrungen sowie unter Berücksichtigung genereller Erwägungen - insbesondere hinsichtlich Sicherheit und Handhabbarkeit - lassen sich folgende grundsätzlichen Anforderungen an eine derartige Lösung formulieren:

- Die Lösung muss eine Verschlüsselung und Signatur nach dem aktuellen Stand der Technik bieten.
- Die Lösung muss zumindest zu den beiden am weitesten verbreiteten Standards für sicheren E-Mail-Verkehr, OpenPGP und S-MIME, kompatibel sein.
- Die Lösung sollte Optionen für den kontrollierten automatisierten Import von unterstützten Zertifikaten aus vorhandenen Client-Installationen bzw. empfangenen E-Mails bieten.
- Die Lösung muss ohne einen speziellen Client bzw. spezielle Client-Erweiterungen (Plug-Ins o.ä.) auskommen.
- Die Lösung sollte zur Vermeidung von Bedienfehlern weitestgehend automatisiert arbeiten, d.h. ohne bewusstes Zutun des jeweiligen Anwenders alle E-Mails, die als vertraulich eingestuft sind, der Verschlüsselung unterwerfen. Im Idealfall stellt sich die Lösung für den Anwender somit völlig transparent dar.
- Die Lösung sollte nach Möglichkeit auch für Umgebungen mit hoher Fluktuationsrate geeignet sein, da „vertrauliche Kommunikationsbeziehungen“ auch wechseln können und in solchen Fällen auch für neue Kommunikationsbeziehungen meist die Forderung nach schneller Verfügbarkeit der Verschlüsselungsoption gestellt werden wird.

Die Lösung: Virtuelle Poststellen

Einen besonders eleganten Weg zur Lösung der skizzierten Aufgabe bieten so genannte virtuelle Poststellen, die ein Mail-Gateway mit einem per Web-Browser nutzbaren Ablageserver nach folgendem Prinzip kombinieren:

- Das Mail-Gateway der virtuellen Poststelle untersucht jede ausgehende E-Mail dahingehend, ob diese zu verschlüsseln und/oder zu signieren ist. Falls nicht, wird die E-Mail unverändert weitergeleitet. Die Anweisung, ggfs. zu verschlüsseln bzw. zu signieren, kann sich dabei u.a. aus einer zentral einzurichtenden Richtlinie (z.B.: „Alle Nachrichten an Empfänger name@maildomain.de sind zu verschlüsseln!“) oder auch aus dem Inhalt der Nachricht, etwa der Betreffzeile, ergeben (z.B. gibt es Lösungen, die E-Mails verschlüsseln, wenn der Betreff mit einem bestimmten Schlüsselwort beginnt).
- Muss Verschlüsselung eingesetzt werden, prüft das Gateway, ob es im Besitz der notwendigen Schlüsselinformationen für den Empfänger ist. Falls ja, kann das Gateway die Mail geeignet verschlüsseln und der Empfänger die verschlüsselte Mail offensichtlich verarbeiten. Letzteres impliziert insbesondere das Vorhandensein eines entsprechenden Clients.
- Ist keine Schlüsselinformation vorhanden - sei es, weil der Empfänger kei-

ne E-Mail-Verschlüsselung einsetzt und daher verständlicherweise auch nicht im Besitz eines kompatiblen öffentlichen Schlüssels ist, oder weil mit diesem Empfänger bis dato noch keine Kommunikation stattgefunden hat - , so wird die Mail in ein Postfach eines zur Lösung gehörenden Web-Mailers umgeleitet; der Empfänger erhält eine entsprechende Benachrichtigung, dass in diesem Postfach eine Mail für ihn eingegangen ist.

- Der Zugriff auf das Web-Mail-Postfach erfolgt mittels Browser via HTTPS. Die Mail kann jetzt gelesen bzw. bei Bedarf auch auf den eigenen E-Mail-Client heruntergeladen werden.
- Über den Web-Mail-Zugang kann der Empfänger auch auf die empfangene Mail antworten bzw. aktiv Mails versenden.
- Umgekehrt werden alle ankommenden verschlüsselten E-Mails entschlüsselt und die Signaturen aller ankommenden signierten E-Mails auf Korrektheit überprüft.

Dieser Ansatz erfüllt die meisten der oben formulierten Anforderungen. Insbesondere ist die geforderte Transparenz für die Anwender gewährleistet. Auch sind alle auf diesem Wege ausgetauschten E-Mails auf dem gesamten Übertragungsweg geschützt.

Seminar

Zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs

27.08. - 31.08.07 in Aachen



Dieses einmalige Seminar vermittelt intensiv innerhalb von 5 Tagen den praktischen Umgang mit Firewalls, VPNs, Windows-Sicherheit und WLAN-Sicherheit. Im Rahmen von praktischen Live-Übungen werden typische Konfigurationen analysiert und vermittelt.

Referenten: Dipl.-Inform. Andreas Meder, Sven Ossendorf
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com

Virtuelle Poststellen - sichere E-Mail für alle?

Einzig verbleibendes Risiko ist die Möglichkeit, dass ein externer Kommunikationspartner vertrauliche E-Mails unverschlüsselt über den „normalen“ E-Mail-Weg sendet. Dies lässt sich auf technischem Wege kaum zuverlässig verhindern und muss daher anderweitig unterbunden werden, z.B. über entsprechende vertragliche Regelungen.

Der Markt in diesem Segment ist vergleichsweise überschaubar, zumindest in Deutschland: eine projektbezogene Recherche lieferte im Jahre 2006 folgende Anbieter kommerzieller Produkte:

- ICC: Julia Mail Office
- Utimaco: Secure E-Mail Gateway
- PGP: PGP Universal 500
- Zertificon: Secure Mail Gateway

Der grundlegende Funktionsumfang ist übrigens mittlerweile bei allen Produkten vergleichbar:

- Unterstützung von PGP zur E-Mail-Verschlüsselung
- Unterstützung von S/MIME zur E-Mail-Verschlüsselung
- Integrierter bzw. zurüstbarer Web-Mailer als Fallback-Option für Empfänger, die weder PGP noch S/MIME unterstützen

Insofern sollten alle benannten Lösungen grundsätzlich für eine konkrete Realisierung infrage kommen. Unterschiede sind freilich in Details der Handhabung und der Administration auszumachen. Diese fallen zwar in aller Regel nicht gravierend aus und sind häufig lediglich geeignet, einen von mehreren kostentechnisch vergleichbaren Kandidaten zu präferieren. Dennoch oder gerade deshalb sollte diesem Aspekt bei einer etwaigen Produktentscheidung die notwendige Aufmerksamkeit zuteil werden.

Zu den Fragestellungen, die in diesem Zusammenhang möglicherweise zu klären sein werden, gehören u.a. die nachfolgend aufgeführten:

Art und Schutz administrativer Zugriffe

Da auch die fortschrittlichste Virtuelle Poststelle bei aller Transparenz für den Anwender eines kontinuierlichen Managements durch einen Administrator bedarf, lohnt es sich, einen Blick auf die entsprechende Schnittstelle, sprich das Graphical User Interface, kurz GUI, zu werfen - sofern vorhanden und nicht stattdessen ein spartanisches Command Line Interface (CLI) herangezogen werden muss.

Von großem Vorteil ist es, wenn der administrative Zugriff via Web-Browser erfolgen kann: der landläufige Administrator sollte mit dieser Client-Software umgehen können und eine Installation ist nicht notwendig, so dass prinzipiell eine Administration von jedem beliebigen Büroarbeitsplatzrechner aus erfolgen kann. Diese Zugriffe müssen natürlich ausreichend gegen Mitlesen und/oder Manipulation geschützt sein; hierzu bietet sich z.B. die Nutzung von HTTPS an.

Schutz der Nachrichten auf dem Web-Mailer

Basis des Web-Mailers ist grundsätzlich eine Web-Server-Applikation, auf die von jedermann mindestens mittels HTTPS zugegriffen werden kann. Aufgrund dieser Konstellation und vor dem Hintergrund der Erfahrungen mit der Sicherheit von Web-Server-Implementierungen muss von einem nicht vernachlässigbaren Restrisiko ausgegangen werden, dass im Zuge eines Angriffs auf diese Web-Server-Applikation ein Datenzugriff durch Unbefugte möglich ist.

Insofern in jedem einzelnen Fall zu prüfen, ob erweiterte Anforderungen an die Absicherung der Postfachinhalte des Web-Mailers zu stellen sind. Ein denkbarer Ansatz könnte z.B. eine Verschlüsselung der Nachrichten sein. Zu beachten ist dabei, dass eine Verschlüsselung auf Betriebssystemebene oder darunter vermutlich keinen akzeptablen Schutz bietet, da unbefugte Zugriffe der beschriebenen Art möglicherweise unter Missbrauch der Identität berechtigter User bzw. Applikationen erfolgen.

Verhindern ungewollter Klartextkommunikation

Einige Lösungen (Beispiel: PGP) bieten beim erstmaligen Zugriff auf den Web-Mailer einen Auswahldialog, der es dem externen Mail-Empfänger ermöglicht, das zukünftige Verhalten des Mail Gateways zu beeinflussen. Steht als Option dabei u.a. auch der zukünftige Empfang von Klartext-Mails zur Verfügung, so ist zu prüfen, ob diese Option durch Setzen serverseitiger Parameter abschaltbar ist. Andernfalls könnte ein Empfänger versehentlich die Verschlüsselungsfunktion des Gateways für an ihn gerichtete Nachrichten außer Kraft setzen.

Kontrolle der Nutzerlizenzierung

Die oben erwähnten Produkte werden allesamt User-basiert lizenziert. Dabei ist nicht per se klar, welche internen User der

Lizenzierung zugrunde zu legen sind. In der Regel dürfte es sich zwar um „aktive“ User handeln, d.h. solche, die die Funktion der virtuellen Poststelle nutzen, aber es sollte dennoch geprüft werden, wer durch das Gateway (bzw. den Anbieter) als „aktiver“ User angesehen wird. Es bestehen hier durchaus verschiedene Möglichkeiten:

- User, die als Sender verschlüsseln und/oder signieren
- User, an die eine empfangene verschlüsselte und/oder signierte E-Mail weitergeleitet wird
- User, die Mails mit externen Adressaten austauschen
- User, die prinzipiell die Möglichkeit haben, zu den bisher genannten zu gehören
- Beliebige Kombinationen davon

Um nicht plötzlich ungewollt gegen die Lizenzbedingungen zu verstoßen, sollte zusätzlich untersucht werden, ob und auf welche Weise die Lösung ein Controlling der Lizenzen unterstützt. Dabei sollte nicht vergessen werden, dass häufig aufgrund interner Fristen für Beschaffungen und Budgetplanung ein sich anbahnendes Überschreiten der Lizenz bereits sehr frühzeitig erkennbar sein muss; eine bloße Warnung (oder gar Einstellung der Funktion) im Moment der Lizenzüberschreitung wird daher in aller Regel nicht ausreichen.

Sicherheit der Implementierung

Die Implementierung der Virtuellen Poststelle sollte natürlich ausreichend sicher sein. Die Anforderungen an die diesbezügliche Robustheit des Systems entsprechen mindestens denen an andere öffentlich zugängliche Server in einer DMZ der Perimeter-Firewall am Übergang zum Internet.

Insofern müssen sowohl die eingesetzte Software der Virtuellen Poststelle selbst als auch das Basissystem gegen Angriffsversuche aus dem Internet hinreichend „gehärtet“ sein. Je nach Produkt sind dabei unterschiedliche Rahmenbedingungen zu berücksichtigen:

- Handelt es sich um eine reine Software-Lösung, die auf einem unterstützten Serverbetriebssystem installiert wird, so liegt die Vorbereitung/Härtung des Serverbetriebssystems in der Verantwortung des Installateurs. Bei Basisbetriebssystemen, für die intern kein oder nur unzureichendes Know-how vorhan-

Virtuelle Poststellen - sichere E-Mail für alle?

den ist, empfiehlt es sich, die Installation einschließlich Systemhärtung als Dienstleistung im Zuge der Beschaffung einzukaufen.

- Handelt es sich um eine „Soft-Appliance“, d.h. eine Lösung, die auf einer unterstützten Hardware sowohl ein entsprechend zugeschnittenes Betriebssystem als auch die Software der Virtuellen Poststelle selbst mit einer einzigen Setup-Routine installiert, so muss die Systemhärtung vom Anbieter bei der Erstellung des Setup-Datenträgers vorgenommen werden. Eine manuelle „Nachhärtung“ ist zwar meistens theoretisch möglich – zumindest wenn es sich um Systeme auf Linux-Basis handelt –, aber aufgrund der unkalkulierbaren Auswirkungen auf die Funktion des Gesamtsystems nicht unbedingt zu empfehlen. Ggfs. sollte im Zuge der Beschaffung ein Sicherheitsscan des installierten Systems durchgeführt werden, um eine ausreichende Systemrobustheit sicherzustellen.
- Handelt es sich um eine Appliance, d.h. eine Komplettlösung, bei der der Anbieter von der Hardware, über die ggfs. proprietäre Firmware bis zur Software alle Komponenten des Gesamtsystems in betriebsbereitem Zustand ausliefert, so ist eine manuelle Nachhärtung in den meisten Fällen ausgeschlossen. Umso mehr ist darauf zu achten, dass das Gesamtsystem ausreichend robust ist. Auch in diesem Falle sollte daher ein Sicherheitsscan der Appliance im Rahmen des Beschaffungsvorgangs erwogen werden.

Ausfallsicherheit

Es muss bei der Planung einer Virtuellen Poststelle natürlich auch darüber nachgedacht und letztendlich entschieden werden, ob und in welchem Rahmen Störungen der E-Mail-Kommunikation toleriert werden können. Da E-Mail kein online-Medium ist, sind vorübergehende Ausfälle des Systems häufig akzeptabel, solange die jeweilige Ausfallzeit „überschaubar“ bleibt. Muss eine permanente Funktionsfähigkeit gewährleistet sein, kommt man um den Einsatz von Hochverfügbarkeitslösungen (Cluster o.ä.) nicht herum.

Einfacher (und in der Regel deutlich preiswerter) lässt sich ein derartiges System realisieren, wenn auf die Hochverfügbarkeit verzichtet werden kann. Es sollte in diesem Fall jedoch dafür Sorge getragen werden, dass vor allem zwei wesentliche Bedingungen erfüllt sind:

- Es muss sichergestellt sein, dass Hardware-Fehler innerhalb der zulässigen Ausfallzeit behoben werden können.

Dies kann durch einen Wartungsvertrag mit entsprechenden Service Level Parametern erreicht werden. Dies ist ein Ansatz, der sich vor allem bei Verwendung von (Hard) Appliances empfiehlt.

Alternativ kann ein zweites System bevorratet werden (Cold Standby). Dieser Ansatz hat den Vorteil, dass die Ausfallzeit in der Regel erheblich verkürzt werden kann, macht aber aufgrund der ansonsten zu erwartenden hohen Systemkosten nur bei Software-basierten Lösungen Sinn. In diesem Fall beschränken sich die Kosten auf die Bereitstellung der Basishardware, ggfs. inklusive Betriebssystem.

- Es muss sichergestellt sein, dass die vollständige Konfiguration innerhalb der Zeitspanne wiederhergestellt werden kann, die nach Wiederverfügbarkeit des Systems noch bis zur maximal tolerierbaren Ausfallzeit verbleibt.

Hierzu bedarf es eines geeigneten Backup- und Restore-Konzepts. Dabei ist zu beachten, dass ggfs. auch alle E-Mail-Daten auf dem Webmailer wiederherstellbar sein müssen; insofern sind nur Konzepte tauglich, die eine sofortige Sicherung jeder Änderung am Datenbestand vorsehen.

Im Zuge der Produktauswahl und –beschaffung sollte daher sorgfältig geprüft werden, inwieweit entsprechende Funktionen zur Datensicherung bzw. deren Unterstützung vorhanden sind.

Sprachen des Web-Mailers

Es sollte sorgfältig geprüft werden, welche Sprachen der Web-Mailer unterstützt. Sinnvollerweise sollten zumindest Deutsch als auch Englisch im Angebot sein; je nach erwarteter Klientel kann es aber sehr sinnvoll sein, wenn auch andere Sprachen verfügbar sind, insbesondere Spanisch, Französisch, etc.

Benachrichtigungstexte

Die Virtuelle Poststelle versendet bei Einsatz des Web-Mailers Benachrichtigungen: zumindest an den Empfänger der Mitteilung – immerhin muss dieser ja davon in Kenntnis gesetzt werden, dass er auf diesem Wege eine E-Mail erhalten hat –, aber ggfs. auch an den Absender. Im Einzelnen sollten die im Zuge der Nutzung des Web-Mailers erforderlichen Benachrichtigungen mindestens folgende Nachrichten bzw. Texte enthalten:

- Nachricht an den externen Empfänger, dass an ihn eine Mail per Web-Mailer ausgeliefert wurde – diese sollte aus den unterstützten Sprachen frei wählbar sein, nach Möglichkeit abhängig vom Empfänger.

Seminar



Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit 18.06. - 22.06.07 in Bonn

Bedrohungen der IT-Sicherheit bestehen für praktisch alle Elemente einer vernetzten IT-Infrastruktur. Die Quelle der Bedrohung kann sowohl von außen auf das Netz wirken als auch von innen stammen. Sicherheit entsteht erst, wenn alle signifikanten Gefahrenbereiche systematisch verriegelt werden. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Dabei wird jeder einzelne Baustein detailliert erklärt und anhand typischer Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Referenten: Dipl.-Inform. Oliver Flüs, Dipl.-Inform. Andreas Meder, Sven Ossendorf
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com

Virtuelle Poststellen - sichere E-Mail für alle?

- Nachricht an den internen Absender, dass seine Mail per Web-Mailer ausgeliefert wurde - dies ist essentiell, wenn er beim Erstzugriff des externen Empfängers auf sein Web-Mailer-Postfach mitwirken muss.
- Zusatzinformation in Mails an den internen Empfänger, dass diese über den Web-Mailer versandt wurden - dies ist interessant, damit der Empfänger auf einen Blick erkennen kann, ob sich sein Kommunikationspartner beim Versand der Botschaft des sicheren Weges bedient hat oder nicht.

Die jeweiligen Nachrichten bzw. Zusatzinformationen sollten hinsichtlich des textlichen Inhalts frei durch den Administrator konfigurierbar sein, nach Möglichkeit abhängig vom Empfänger - dadurch können insbesondere notwendige Erläuterungen und Hilfestellungen optimal auf die jeweiligen Bedürfnisse der Anwender zugeschnitten werden. Soweit durch das Produkt vorgegebene Texte zum Einsatz kommen, sollte die jeweilige Sprache im Rahmen der unterstützten Sprachen frei wählbar sein, nach Möglichkeit abhängig vom Empfänger. Die Texte sollten Informationen zum Ablauf der Nutzung beinhalten, um Support-Anfragen - insbesondere bei erstmaliger Nutzung - zu minimieren.

Kennwortübermittlung

Erhält ein externer Empfänger erstmals eine E-Mail über den Web-Mailer, so muss er nicht nur darüber und über die Verfahrensweise unterrichtet werden; ihm müssen auch auf akzeptable sichere Art und Weise die Anmeldeinformationen für sein persönliches Postfach auf diesem Web-Mailer mitgeteilt werden.

Hierzu existieren im Detail unterschiedliche Verfahren in den verschiedenen Produkten; klar ist jedoch, dass eine Übermittlung in der Benachrichtigungs-Mail nicht in Frage kommt. In der Regel geht man den Weg, das Kennwort über den internen Anwender, der die zu schützende Nachricht gesendet hat, übergeben zu lassen. Demzufolge enthält die Benachrichtigung an den externen Empfänger z.B. den Hinweis, dass er sein Kennwort vom Absender der auslösenden E-Mail erhält - dabei wird, durchaus nicht zu Unrecht, unterstellt, dass letzterer dem Empfänger meist bekannt ist.

Zum weitergehenden Schutz wird die Login-Information noch geteilt übermittelt: z.B. ist der Login-Name in der Benachrichtigung enthalten, so dass er dem internen Absender nicht bekannt ist. Teilweise wird

auch eine Hälfte des Kennworts per Mail und die andere Hälfte per Telefon vom internen Absender übergeben. Hier sollten die jeweiligen Konzepte geprüft und auf Akzeptabilität und Praktikabilität hin evaluiert werden.

Architekturen

Die Auswahl eines geeigneten Produktes ist eine Sache, die Implementierung und dabei insbesondere die Integration in die ja in den allermeisten Fällen bereits vorhandene E-Mail-Architektur eine andere. Nach Möglichkeit sollte der Einsatz einer virtuellen Poststelle keine einschneidenden Änderungen am grundlegenden E-Mail-Konzept erforderlich machen. Da kommt es gelegentlich, dass zumindest alle hier angesprochenen Produkte nach dem Prinzip des E-Mail-Relays arbeiten; sie lassen sich daher normalerweise sehr leicht als weiteres Element in die vorhandene Relay-Kette integrieren - lediglich das Mail-Forwarding ist ggfs. entsprechend anzupassen, damit alle Nachrichten an das jeweils korrekte Relay-System weitergegeben werden und sichergestellt ist, dass die virtuelle Poststelle dabei zwingend durchlaufen wird.

Im globalen Kontext ist dabei die Frage nicht uninteressant, ob die Verarbeitung von E-Mails einem zentralen oder einem dezentralen Ansatz folgt. Existieren (viele) dezentrale Mail-Systeme, die Botschaften von und zu externen Adressaten unmittelbar empfangen bzw. versenden, so steigt die Komplexität einer virtuellen Poststelle deutlich an: es muss mehrere Instanzen geben - eine je möglichem Mail-Pfad - und diese müssen sich untereinander hinsichtlich ihrer Konfiguration und ihres Datenbestands (insbesondere bezüglich der bekannten öffentlichen Schlüssel) abgleichen.

Typischerweise wird der E-Mail-Verkehr über eine Relay-Kette, bestehend aus dem (in-

ternen) Mail-Server, Content Security Systemen (Anti Spam, Anti Virus) - meist in einer DMZ der Firewall realisiert - sowie einem (externen) Mail-Relay abgewickelt. Davon ausgehend ergibt sich die in Abbildung 1 dargestellte Architektur für eine Relay-Kette mit integrierter Virtueller Poststelle. Damit die Content Security Systeme (in Abbildung 1 ist ein Filter mit kombinierter Anti-Spam- und Virenschutzfunktion dargestellt - bei weiteren und/oder dedizierten Systemen verlängert sich die Relay-Kette entsprechend) auch von der Virtuellen Poststelle verschlüsselte E-Mails untersuchen können, muss die Virtuelle Poststelle in der Kette weiter „außen“ angesiedelt sein. Es bietet sich an, die Virtuelle Poststelle gleichzeitig als Mail-Relay zu verwenden - vorausgesetzt, die notwendige Systemrobustheit (s.o.) ist gewährleistet.

Ist letzteres nicht der Fall, kann natürlich jederzeit auch ein separates vorgelagertes Mail-Relay eingesetzt werden (s. Abbildung 2). Hierdurch wird das Risiko für die Virtuelle Poststelle reduziert, da ein direkter SMTP-Zugriff von außen auf die Virtuelle Poststelle nicht mehr erforderlich ist. Außerdem bietet ein dediziertes Mail-Relay verbesserte Flexibilität für zukünftige Anpassungen der E-Mail-Architektur: etwaige Änderungen an Spezialsystemen haben keine externen Auswirkungen mehr, da die externe SMTP-Schnittstelle stets konstant bleibt.

Übrigens empfiehlt es sich grundsätzlich, zumindest die Web-Mailer-Komponente der Virtuellen Poststelle auf einer separaten Plattform zu implementieren. Dies wird allgemein auch von den Herstellern der angebotenen Produkte so gesehen; bei Produkten auf Appliance-Basis gibt es demzufolge dann je ein System für die eigentliche Virtuelle Poststelle und eines für den Webmailer. Zusätzlich kann erwogen werden, das Web-Mailer-System in einer separaten DMZ zu positionieren.

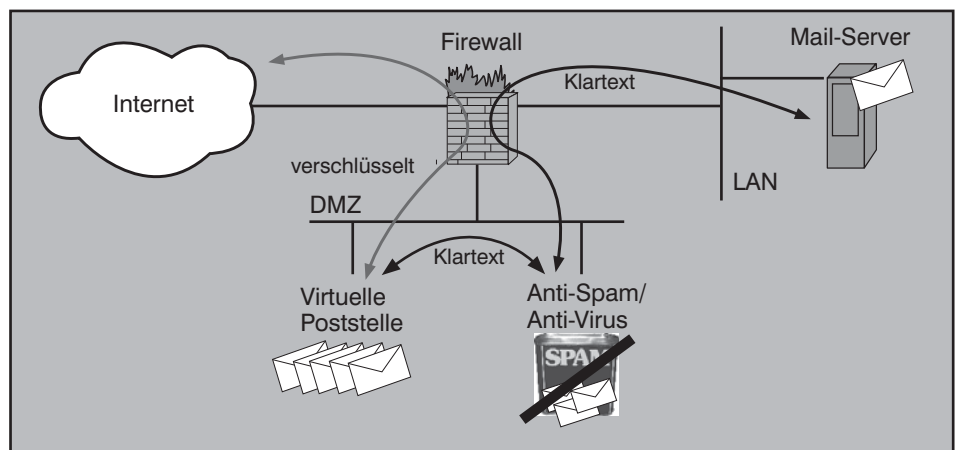


Abbildung 1: Typische Mail-Architektur mit virtueller Poststelle

Virtuelle Poststellen - sichere E-Mail für alle?

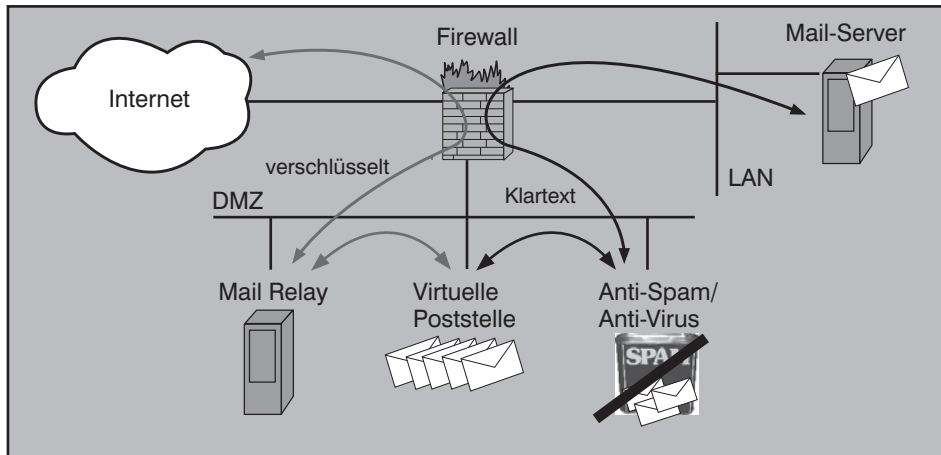


Abbildung 2: Variante mit vorgelagertem Mail-Relay

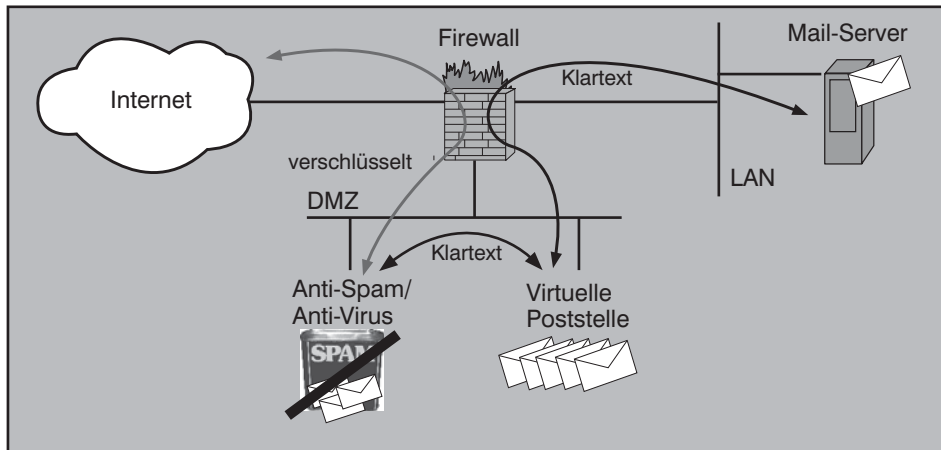


Abbildung 3: Alternative zur Nutzung spezieller Anti-Spam-Features

Allerdings verfügen manche Spam-Filter über spezielle Funktionen (z.B. Herabsetzung der „Annahmerate“ von E-Mails, die von offenkundig als Spam-verseucht anzusehenden Mail-Servern versendet werden), die nur dann genutzt werden können, wenn der Spam-Filter das äußerste Glied der Relay-Kette ist (s. Abbildung 1). Eine entsprechende Positionierung bedeutet dann aber zwangsläufig, dass eine weitergehende Content-Security durch den Spam-Filter für verschlüsselte Mails nicht geleistet werden kann. Doch keine Panik: unter Berücksichtigung der erweiterten Vertrauensstellung, die Kommunikationspartner genießen, mit denen verschlüsselt kommuniziert wird, kann diese Einschränkung der Schutzwirkung des Spam-Filters meist in Kauf genommen werden. Dies gilt insbesondere, wenn der interne Mail-Server über einen zusätzlichen eigenen Virenschutz verfügt.

Bedenken, dass womöglich infolge einer allgemeinen Veröffentlichung des öffentlichen Unternehmens-Schlüssels durch die Virtuelle Poststelle vermehrt verseuchte Mails unter dem Schutz der Verschlüsse-

lung eindringen könnten, erscheinen dabei kaum gerechtfertigt, da eine derartige Veröffentlichung standardmäßig **nicht** stattfindet. Auch steht zu erwarten, dass insbesondere absichtliche Versender unerwünschter Mails aufgrund der jeweiligen Gesamtvolumina je Sendung von performancemindernden Verschlüsselungsopere-

rationen in aller Regel Abstand nehmen werden, zumal der Einsatz von Verschlüsselung bereits auf entsprechende Sicherheitsmaßnahmen hinweist, die es nahe legen, eher andere, leichtere Opfer zu be-helligen.

Soll trotz des insgesamt eher niedrig an-zusehenden Risikos auch für verschlüsselte E-Mails ein erster Virenscan bereits innerhalb der DMZ erfolgen, so muss ent-weder ein kombiniertes Anti-Virus/Anti-Spam-System zweifach durchlaufen werden (siehe Abbildung 3) oder - falls eine derartige Konstellation aufgrund eventuell unzureichender Parametrierungsoptionen zu einem Loop führt - ein Einsatz dedizierter Systeme erfolgen, wobei dann die Anti-Virus-Funktion zwischen Virtueller Poststelle und internem Mail-Server installiert wird (siehe Abbildung 5).

Je nach Rahmenbedingungen können freilich auch noch andere Architekturen sinnvoll sein.

Für den Fall, dass eine für den Einsatz in der DMZ hinreichende Systemrobustheit nicht gegeben ist, - oder weil man generell ein System mit derart vergleichsweise sensibler Aufgabe nicht exponieren will - kann z.B. die Virtuelle Poststelle aus dem öffentlich zugänglichen in einen weniger exponierten Netzbereich verlagert werden; dieser kann u.U. auch das interne LAN sein. Bei diesem Ansatz muss jedoch der Web-Mailer auf ein separates System ausgelagert werden, da dieser in jedem Fall öffentlich zugänglich bleiben muss. Dieser bliebe dann zwar eine Schwachstelle im Gesamtsystem; bei einem angenommenen Ausfall infolge eines Angriffs von außen bliebe jedoch die eigentliche Virtuelle Poststelle, d.h. das Mail-Gateway, weiter einsatzfähig.

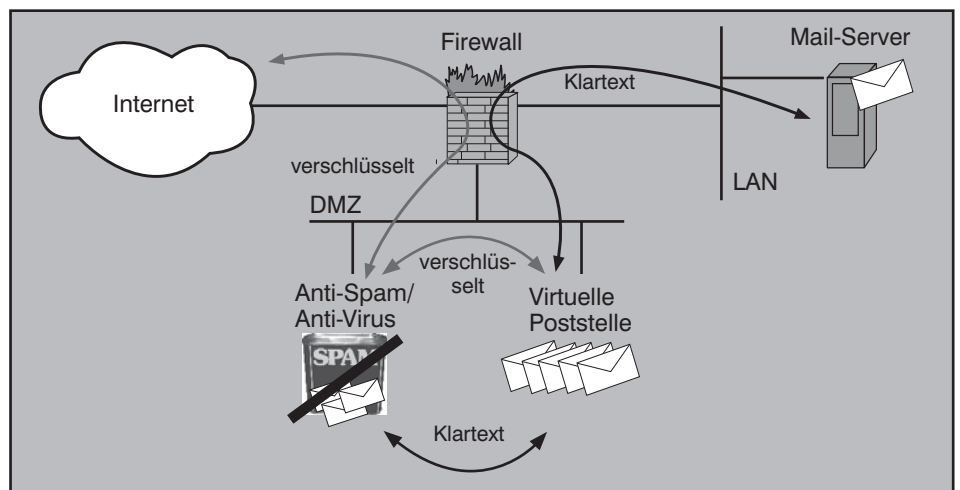


Abbildung 4: Zweifacher Durchlauf des Content Security Gateways

Virtuelle Poststellen - sichere E-Mail für alle?

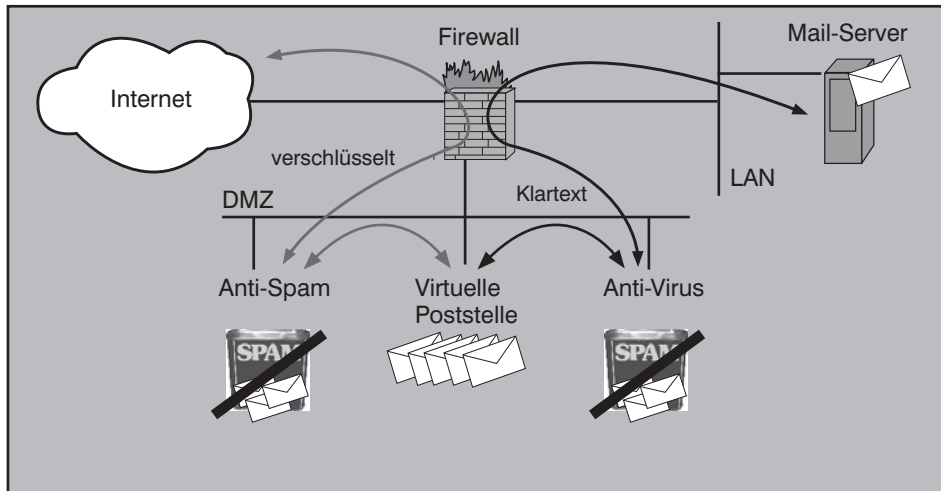


Abbildung 5: Zwei Content Security Gateways

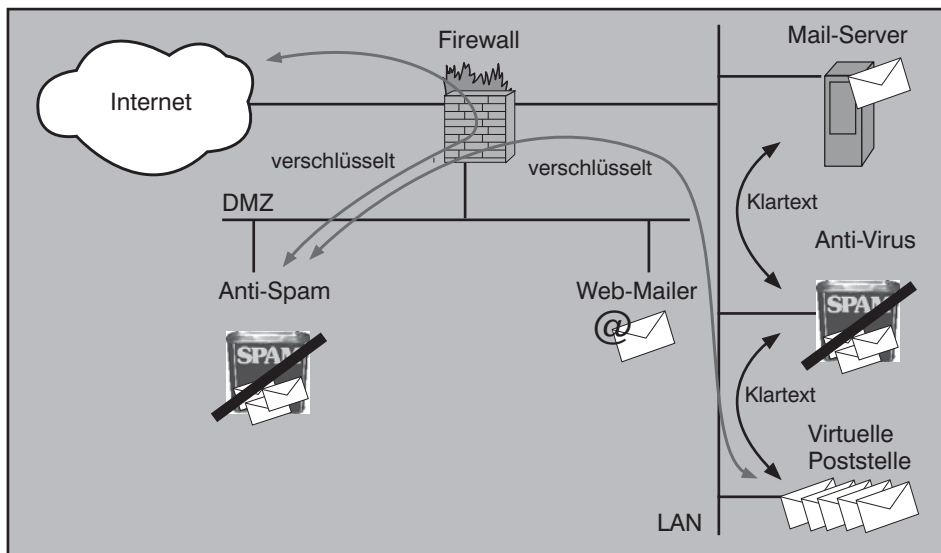


Abbildung 6: Virtuelle Poststelle im nichtöffentlichen Netzbereich

Nutzt man bei diesem Ansatz das Security Gateway als Mail-Relay, sollte jedoch auf den mehrfachen Durchlauf des Security Gateways (vgl. Abbildung 4) verzichtet und stattdessen in jedem Fall ein dediziertes zweites Gerät für den Virenskan eingesetzt werden (Abbildung 6). Steht ein dediziertes Mail-Relay ohne spezielle Content Security Funktion am vorderen Ende der Mail-Relay-Kette, kann hingegen wieder ein kombiniertes System zur Abwehr von Spam und Viren eingesetzt werden.

Migration

Neben der Integration der Virtuellen Poststelle in den E-Mail-Pfad müssen bei der Einführung einer solchen Lösung auch noch weitere Aspekte berücksichtigt werden. Dies gilt insbesondere dann, wenn in der Vergangenheit bereits Einzelplatzinstallationen von E-Mail-Verschlüsselungssoftware im Einsatz war.

Insbesondere müssen die betroffenen Mitarbeiter umfassend von den Möglichkeiten und Erfordernissen der neuen Lösung in Kenntnis gesetzt werden. Zwar erfolgt die Ver- und Entschlüsselung ebenso wie die Signatur bzw. deren Prüfung transparent und somit ohne unmittelbares Zutun der Nutzer. Immerhin müssen letztere aber auch sinnvoll mitwirken, damit die Virtuelle Poststelle ihre Arbeit sinnvoll tun kann. Zu dieser Mitwirkung gehört neben der schon angesprochenen Übermittlung des initialen Kennwortes des Web-Mail-Postfaches an betroffene externe Mail-Empfänger vor allem auch die Mithilfe bei der Definition der Richtlinie, nach der die Verschlüsselung gesteuert wird: damit ausgehende E-Mails bei Bedarf automatisch muss z.B. festgelegt werden, welche Adressaten ausschließlich (oder ggfs. bevorzugt) verschlüsselte Mails erhalten sollen. Sofern dies nicht unternehmensweit festgelegt ist, ist der Administrator der Virtuellen Poststelle hier auf Informationen durch die internen Mail-Nutzer angewiesen. Es empfiehlt sich im Übrigen, hierzu wie auch für einen eventuell notwendigen Nutzungsantrag standardisierte Formulare zu entwerfen und einzusetzen. Alle (potenziell) betroffenen Nutzer sollten darauf hingewiesen werden, dass ohne entsprechenden Antrag und Freigabe durch den zuständigen Vorgesetzten keine Nutzung der Virtuellen Poststelle möglich sein wird. Analog gilt, dass bei fehlerhaften oder unvollständigen Angaben im Formular eine korrekte Funktionalität aus Sicht des betroffenen Nutzers nicht gewährleistet ist.

Besondere Aufmerksamkeit ist denjenigen Mitarbeitern zu widmen, die in der Vergangenheit bereits Desktop-Lösung zur sicheren E-Mail-Kommunikation eingesetzt haben und nun sukzessive auf die Nut-

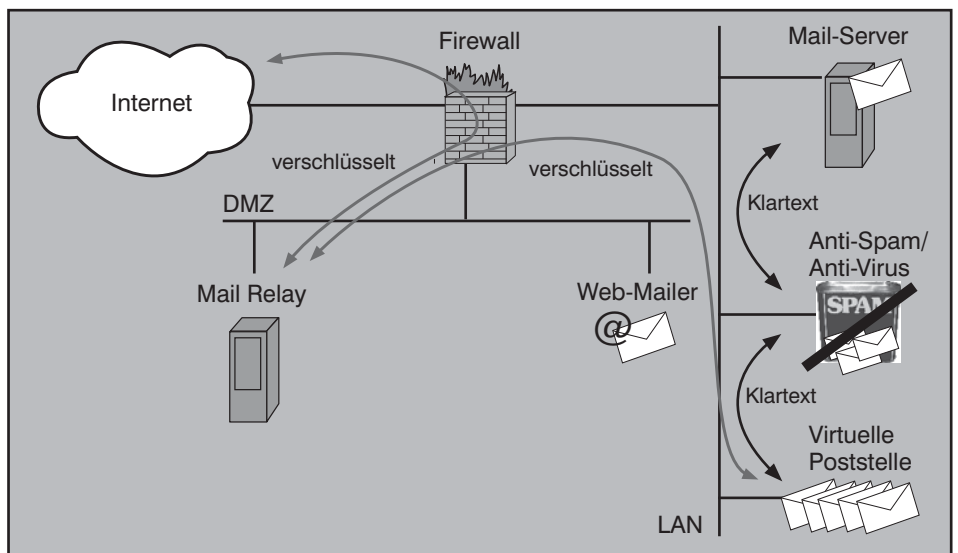


Abbildung 7: Virtuelle Poststelle im nichtöffentlichen Netzbereich mit separatem Mail-Relay

Virtuelle Poststellen - sichere E-Mail für alle?

zung der Virtuellen Poststelle umzustellen sind. Eine Weiternutzung der bisherigen Lösung sollte dabei zumindest mittelfristig nur in begründeten Einzelfällen vorgesehen werden. Eine solche Begründung könnte etwa das Vorliegen entsprechender vertraglicher Regelungen sein, die explizit die bisherige Lösung zur Verwendung vorschreiben.

Daneben sollten auch Nutzungsbedingungen für den Web-Mailer formuliert und den externen Nutzern bekannt gegeben werden (z.B. über einen in der ersten Benachrichtigung enthaltenen Link auf die eigene Website oder über einen entsprechenden Text in der Benachrichtigung). In der Regel sollte mindestens auf folgende Punkte eingegangen werden:

- Weisen Sie darauf hin, dass das Postfach als Übergangslösung bis zum Aufbau einer zur Virtuellen Poststelle kompatiblen E-Mail-Verschlüsselungslösung beim externen Nutzer dient, nicht für eine dauerhafte Nutzung ausgelegt ist und daher keine Alternative zum Aufbau einer eigenen Lösung darstellt.
- Das Postfach ist typischerweise auch nicht als Ersatz oder Ergänzung für das eigene Postfach des externen Nutzers vorgesehen. Weisen Sie ihn daher sicherheitshalber darauf hin, dass demzufolge keinerlei Anspruch auf dauerhafte Vorhaltung oder garantierte Wiederherstellbarkeit von Nachrichten besteht, die in Postfächern des Web-Messengers abgelegt sind.
- Behalten Sie sich ausdrücklich vor, E-Mails nach einer bestimmten Verweildauer (z.B. von mehr als 3 Monaten) ohne Vorwarnung aus den Postfächern zu löschen.
- Das bei der Einrichtung eines neuen Postfachs vom System vergebene Benutzerkennwort sollte umgehend vom Nutzer durch ein anderes, nur ihm bekanntes ersetzt werden.
- Benutzerkennwörter müssen selbstverständlich geheim gehalten werden, d.h. sie sind sicher aufzubewahren und dürfen anderen Personen nicht zugänglich gemacht werden.

Neben diesen eher technischen bzw. organisatorischen Aspekten der Nutzung darf auch nicht vergessen werden, den externen Nutzer hinsichtlich seiner ggfs. sogar vertraglich fixierten Pflichten ins Gebot zu nehmen – meist wird dies Aufgabe des zugeordneten internen Nutzers sein. Auch eine Virtuelle Poststelle näm-

lich kann nicht sicherstellen, dass ein externer Absender ebenfalls einen sicheren Versandweg wählt - sei es seine lokale E-Mail-Verschlüsselungslösung oder den Web-Mailer. Zwar könnte die Virtuelle Poststelle unverschlüsselte E-Mails bestimmter Absender zurückweisen - zu diesem Zeitpunkt ist der potenzielle Schaden aber bereits angerichtet. Hier muss also durch entsprechende Aufklärung darauf hingearbeitet werden, dass keine Fehler vorkommen; dies gilt insbesondere für Nutzer des Web-Mailers, denen mangels lokaler Verschlüsselungsoption meist die Nutzung der sicheren Variante noch nicht in Fleisch und Blut übergegangen sein dürfte.

Zur Vermeidung von Fehlern in der Bedienung sowie im organisatorischen Ablauf – diesmal auf der internen Seite – ist übrigens generell ein vorgeschalteter Pilotbetrieb unbedingt zu empfehlen. In diesem Rahmen lassen sich eventuelle Defizite noch mit geringem bis vertretbarem Aufwand korrigieren. Für den Pilotbetrieb sollten tunlichst „problemresistente“ Anwender ausgesucht werden, da insbesondere zu Beginn noch mit technischen und organisatorischen Anlaufschwierigkeiten zu rechnen sein wird. Ein Produktiveinsatz in dieser Phase erscheint risikobehaftet und sollte nur in dringenden Fällen erwogen werden; betroffene Anwender sollten entsprechend intensiv betreut werden.

Zur Verifikation der grundlegenden Funktionalitäten sowie der korrekten Implementierung empfiehlt sich darüber hinaus ein

intensiver Test im Vorfeld der Pilotphase. Hier können insbesondere auch Erkenntnisse gewonnen werden, die bei der Vervollständigung und Optimierung der für den Pilot- und späteren Regelbetrieb notwendigen Dokumente (Antragsformular, Benutzerinformation, Betriebshandbuch, etc.) nützlich sein können.

Um sicherzustellen, dass durch die Migration und insbesondere die ggfs. notwendige Deinstallation bereits vorhandener Desktop-basierter E-Mail-Verschlüsselungslösungen keine Beeinträchtigung der Kommunikationsfähigkeit bzw. des Datenbestands erfolgt, ist ein ausreichend dimensionierter Übergangszeitraum vorzusehen, innerhalb dessen eine Weiternutzung der Altlösung im Bedarfsfalle möglich ist.

Dieser Übergangszeitraum ist insbesondere auch zu nutzen, um – soweit möglich - weiterhin erforderliche Schlüssel und Zertifikate der Altlösung in die Virtuelle Poststelle zu importieren. Das genaue Prozedere des Imports ist dabei im Rahmen des oben empfohlenen Tests zu klären. Dazu sollte das gewählte Produkt nach Möglichkeit entsprechende Importfunktionen, z.B. für PGP-Keyring-Dateien, bieten. Für den Fall, dass vorhandene Schlüssel-Dateien importiert werden können, sollten diese jedoch durch die Anwender frühzeitig geeignet bereitgestellt werden. Eine praktikabel erscheinende Möglichkeit ist z.B. die Einrichtung eines speziellen Postfachs, an das die entsprechenden Dateien vom Anwender gesendet werden. Für

Kongress



IT-Sicherheits-Forum 2007 07.05. - 10.05.07 in Königswinter

Das Programm besteht aus Seminaren, Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und interaktiver Erarbeitung von Schutzszenarien. Das Forum verbindet damit in idealer Weise die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Als Schwerpunktthemen sind in diesem Jahr vorgesehen:

- Welche neuen Bedrohungen erwarten uns in 2007?
- Windows Vista unter Sicherheitsaspekten
- Content-Security: Umgang mit gefährlichen Inhalten
- Sicherheit in Automatisierungs- und Prozesskontrollsystemen

Fachliche Leitung: Dipl.-Inform. Detlef Weidenhammer

Preis: € 2.190,- zzgl. MwSt. mit Tutorium - € 1.790,- zzgl. MwSt. ohne Tutorium



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com

Virtuelle Poststellen - sichere E-Mail für alle?

den Anwender sollte sinnvollerweise eine entsprechende Anleitung verfasst werden, die ihm das Auffinden der entsprechenden lokalen Dateien erleichtert.

Besonders wichtig ist der Übergangszeitraum mit Blick auf die in der Vergangenheit verschlüsselt ausgetauschten Nachrichten. Diese liegen im Mail-System stets nur in verschlüsselter Form vor. Nach einer vollständigen Deinstallation der bisherigen Verschlüsselungslösung ist eine Entschlüsselung derart geschützter Nachrichten in der Regel nicht mehr möglich! Daher müssen vor Entfernen der lokalen Installationen derartige Nachrichten - soweit nicht in der Vergangenheit bereits geschehen - in entschlüsselter Form gespeichert werden, sofern ein Bedarf an dauerhafter Zugriffsmöglichkeit besteht.

Um für den Fall, dass eine wichtige Nachricht tatsächlich nicht in entschlüsselter Form gespeichert worden sein sollte, auch in Zukunft eine Entschlüsselung sicherzustellen, kann erwogen werden, durch Sichern der privaten Schlüsselinformationen und der notwendigen Zugriffsinformationen (Passphrase oder ähnliches) eine Rekonstruktionsmöglichkeit für Notfälle zu schaffen; aufgrund des damit verbundenen Risikos und Aufwands erscheint jedoch die oben beschriebene Vorgehensweise grundsätzlich empfehlenswerter. Darüber hinaus birgt das Speichern der oben genannten sensiblen Informationen ein erhebliches Missbrauchspotenzial - insbesondere, wenn diese Keys womöglich auch zum Signieren und damit als Identitätsnachweis verwendet werden können.

Basierend auf den in zuvor diskutierten Aspekten bietet sich insgesamt beispielsweise folgender Migrationsablauf an:

1. Funktionaler Test der Lösung und Optimierung der Betriebsdokumente, insbesondere Antrag und Benutzerinformation
2. Festlegung der Pilotanwender, Information/Unterweisung, Ausfüllen der jeweiligen Anträge, Schlüssel-/Zertifikatsexport
3. Parametrierung der Virtuellen Poststelle auf Basis der Pilotanträge, Schlüssel-/Zertifikatsimport
4. Nutzung der Virtuellen Poststelle durch die Pilotanwender
5. Abschließende Optimierung der Betriebsdokumente

6. Information aller Anwender über die Umstellung, Verfügbarmachung der entsprechenden Dokumente
7. Beginn des vorläufigen Regelbetriebs
8. Festlegung Ende des Übergangszeitraums bis zur Deinstallation der Altlösung
9. Optimierung des Betriebs und Deinstallation Altlösung

Fazit

Grundsätzlich sind Virtuelle Poststellen

eine sehr interessante Lösung zur Bereitstellung sicherer E-Mail-Kommunikation vor allem in umfangreichen Umgebungen. Zwar erfordert ihr Einsatz gewisse konzeptionelle und planerische Vorüberlegungen und eine sorgfältige Realisierung, insbesondere wenn eine Migration von bestehenden Desktop-Lösungen ansteht, das Resultat lässt aber diese Mühen hoffentlich vergessen. Immerhin gehören anschließend per elektronischer Postkarte jedermann unfreiwillig zugänglich gemachte Unternehmensgeheimnisse der Vergangenheit an - oder genießen zumindest Seltenheitswert...

Seminar



Erarbeitung und Umsetzung von Sicherheitskonzepten 25.06. - 29.06.07 in Berlin

Auflagen zum Risikomanagement (Sarbanes-Oxley Act, Basel II oder FDA-Forderungen) und zum Datenschutz schließen eine „gelebte“ IT-Sicherheit als zwingenden Bestandteil ein. Die konsequente Einhaltung solcher Anforderungen kann zudem signifikante Wettbewerbsvorteile schaffen.

Sicherheitskonzepte müssen also mehr sein als Papier. Ihre erfolgreiche Umsetzung erfordert: eine umsichtige Planung und Beschaffung der Sicherheitsinfrastruktur, eine effektive Integration in Prozesse und Organisation, konzeptkonforme Einbindung externer Leistungen (Lieferung, Implementierung, Wartung und Betriebsleistungen). Bei der notwendigen Erfolgskontrolle helfen Standards wie BS7799, ISO 27001 und die IT-Grundschutz-Standards und -Kataloge des BSI. Eine entsprechende Zertifizierung des erreichten Sicherheitsniveaus ist möglich, aber auch eine Verwendung solcher Standards als internes Hilfsmittel.

Anhand konkreter Projektbeispiele zeigt dieses Seminar auf, wie diese Aufgabenstellung von der Konzipierung über Ausschreibung, Abnahme und Betrieb bis hin zur Außerbetriebnahme der entsprechenden Systeme erfolgreich und wirtschaftlich bewältigt wird.

In diesem Seminar lernen Sie

- wie Sicherheitsstandards auf Ihre Bedürfnisse zugeschnitten angewendet werden können
- wie bedarfsgerechte Sicherheitsleitlinien und -konzepte entwickelt werden
- wie man Qualitäts- und Risikomanagement mit der IT-Sicherheit (ggf. sogar revisionsfest) verknüpft
- wie Sie in der Praxis Sicherheitslösungen konzipieren, planen, ausschreiben und betreiben

Referenten: Dipl.-Inform. Oliver Flüs, Dr. Simon Hoff, Sven Ossendorf,
Dipl.-Inform. Andreas Meder
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite www.comconsult-akademie.com