Leistungsbeschreibung „aixGate – abgesichertes Internet“

der
ComNet Computer im Netzwerk Vertriebs GmbH
Carlo-Schmid-Str. 15
52146 Würselen
Tel.: +49 (0)2405 / 4888 - 0
eMail: info@comnet.de

Amtsgericht Aachen: HRB 4463
Geschäftsführer: Bernd Schmitz, Holger Schmitz

Stand 01.05.2018

Funktionsübersicht

Bei aixGate sorgt eine Vielzahl von Mechanismen für die Absicherung gegen Gefahren aus dem Internet (z.B. Proxy-Systeme, Firewalls, Viren-Scanner, Filter-Systeme usw.). aixGate ist ein Produkt zur abgesicherten Nutzung des Internets und wird permanent gewartet, gepflegt, administriert und weiterentwickelt. Das Sicherheitsrisiko durch Virenattacken und unbefugtes Eindringen in ein Kundennetzwerk kann mit aixGate auf ein Minimum reduziert werden. aixGate ist ein abgesicherter Internetzugang, bei dem der Auftraggeber eine Sicherheits-Netzübergangs-Einheit (aixGate-VPN-Gateway – siehe entspr. Beschreibung) von ComNet erhält, welches der Auftraggeber an einen normalen Internet-Anschluss anschließt. Dieses Gateway baut eine Punkt-zu-Punkt/VPN-Verbindung in das ComNet-Hochsicherheits-Rechenzentrum auf und leitet dann den gesamten Datenverkehr des Auftraggebers hierüber um.

Alle eingehenden E-Mails des Auftraggebers kommen erst im ComNet-Rechenzentrum an und werden dort von mindestens 5 verschiedenen, kaskadierten Virenscanner verschiedener Hersteller auf Viren gescannt. Zusätzlich werden potentiell gefährliche Anhänge geblockt und es werden diverse SPAM Abwehrmaßnahmen, wie z.B. Greylisting, Blacklisting, SPAM-Bewertung oder Reverse-DNS-Lookup durchgeführt. Wenn E-Mails die E-Mail-Security von aixGate durchlaufen haben, werden die E-Mails zum Kunden-System per SMTP übertragen. Auf der aixGate-Seite werden keine Postfächer verwaltet. E-Mails werden nur angenommen bzw. weitergeleitet, wenn die versendenden Mail-Server sich gemäß allgemein anerkannter Internet-Standards (sog. RFC) verhalten. Dadurch wird nicht nur SPAMs vorgebeugt, sondern auch die Identität der absendenden Systeme sichergestellt, sodass bei Unzustellbarkeit der eingehenden E-Mails in jedem Fall eine entsprechende Rückmeldung an den Absender erfolgen kann.

Funktionsbeschreibung

Sicherheit beim Surfen:

Der komplette Surf-Datenverkehr wird über das ComNet-Rechenzentrum mit leistungsfähigen, kontinuierlich administrierten Firewalls geleitet und dort auf Schadcode und Viren untersucht. Bei Aufruf von Internetseiten agieren bestimmte Instanzen im aixGate-System als Proxy-Server (Proxy = Stellvertreter), was bedeutet, dass im Internet nicht der einzelne Anwender von aixGate in Erscheinung tritt, sondern nur der Proxy-Server. Zugriffe über verschlüsselte Verbindungen (https) und verschlüsselte Dateien hingegen werden nicht überprüft. Hierfür sollte der Auftraggeber immer einen lokalen Viren-Scanner vorhalten, mit den neuesten Virendefinitionen.

E-Mail-Security:

Kaskadierter Viren-Check

Alle eingehenden E-Mails werden von mindestens 5, alle ausgehenden von mindestens einem Virenscanner untersucht und E-Mails mit identifizierten Schadcodes werden geblockt. Hier werden nicht nur die E-Mails geprüft, sondern auch die Anhänge.

Anti-Viren-Software reagiert unterschiedlich schnell auf neue Virengefahren: Hier liegen bei aktuellen Virenbedrohungen nicht nur Stunden oder Tage, sondern manchmal auch Wochen und Monate bis einzelne Virenscanner die neuen Virengefahren erkennen. Dies liegt zum Teil an der unterschiedlichen Herangehensweise der Sicherheitsfirmen, die diese Anti-Viren-Software bereitstellen. Manche Virenscanner erkennen Viren an gewissen Bitfolgen der Schadprogramme, andere an der Bauform, da Viren-Bedrohungen zum Teil Baukastenartig mutieren. Da Virenscanner aber nur bekannte Viren

erkennen und eliminieren können, ist es wichtig möglichst zeitnah beim Aus-bruch einer neuen Virus-Epidemie, Scanner im Einsatz zu haben, die diese neuen Viren auch erkennen. Dies ist der Grund, warum im aixGate-System jede E-Mail mindestens 5 verschiedene Scanner verschiedener Hersteller durchläuft. Die Virendefinitionen werden von ComNet dabei stündlich upgedatet und das rund um die Uhr. Erst die hohe Anzahl an Virenscannern und die hohe Frequenz an Updates bieten den größtmöglichen Schutz.

Bei Erkennung eines gefährdenden Objekts in einer eingehenden E-Mail wird die E-Mail auf Providerseite durch aixGate sofort in eine Quarantäne verschoben und der aixGate-Kunde informiert.

Sicherheitshinweis 1: Wenn verschlüsselte E-Mails empfangen oder versendet werden oder E-Mails mit verschlüsselten Anhängen übertragen werden, versagt dieser kaskadierte Virus-Check von E-Mails. Hier können absenderseitig Viren „mitverschlüsselt" werden, die erst bei der Entschlüsselung auf der Anwenderseite wieder „frei werden" und dort ihr Unheil nun anrichten können. Hier hilft dann ggfs. nur noch der lokale Virenscanner …. der aber ggfs. zu alt ist und den aktuellen Virus (noch) nicht erkennt.

Sicherheitshinweis 2: Nutzt ein Anwender des durch aixGate eigentlich geschützten Systems private E-Mail-Zugänge (z.B. von Googlemail, T-Online, GMX, WEB.DE usw.) und überträgt dann Dateien auf die Server, wird die aixGate-Sicherheits-Architektur umgangen. Die Nutzung von privaten E-Mail-Zugängen in geschützten Umgebungen sollten den Anwendern untersagt werden.

E-Mail-Attachment-Blocking

Unter Attachment - Blocking versteht man, dass bestimmte Dateien als Anhänge in E-Mails generell verboten sind und nicht übertragen werden. Betroffen sind Datei-Anhänge, die ein hohes Gefährdungs-Potential haben. Hierzu gehören unter anderem Dateianhänge mit den Endungen .exe, .com und .cmd. Aber auch ca. 100 weitere Dateitypen werden bei aixGate als E-Mail-Anhang nicht durchgelassen. Um das Risiko der noch nicht bekannten Viren (siehe Virenscan) zu vermindern, werden diese Attachments im Vorfeld bereits geblockt bevor sie beim Empfänger ankommen. Diese E-Mails werden in Quarantäne verschoben und können auf Wunsch des Kunden nachträglich freigegeben werden. Möchte man solche Anhänge trotzdem durchlassen, kann der Absender diese z.B. in eine ZIP-Datei verpacken oder die Datei-Endung verändern. Bei akuten Bedrohungslagen behält sich ComNet das Recht vor, auch schon einmal Dateien wie .doc oder .xls vorübergehend global zu sperren.

SPAM-Abwehr durch Greylisting

Dies ist nach dem Stand der heutigen Technik die effektivste Abwehr von SPAMs. Die Greylisting-Methode geht von der praktischen Erfahrung aus, dass SPAM-Versender (zumeist ja durch Viren oder Trojaner gekaperte Server und PCs, aber auch Router und seit Neuestem auch ungeschützte, programmierbare elektronische Geräte aus dem „Internet-of-Things", wie programmierbare Waschmaschinen oder Heizungssteuerungen aus dem SmartHome-Bereich usw.) aufgrund der unglaublichen Masse an E-Mails, die Sie versenden wollen, jede Zustellung nur ein einziges Mal probieren und Algorithmen des Internet-Protokolls nicht einhalten. So funktioniert das Greylisting-Verfahren: Eine eingehende E-Mail besteht aus 3 signifikanten Werten: der Absenderadresse, der Empfängeradresse und der IP des absendenden Mailservers. Wenn im aixGate-System dieses Triplet nicht bekannt ist - also beim ersten Mail-Eingang - wird eine künstliche Fehlermeldung erzeugt, die besagt, dass der ComNet-Mailserver gerade ein technisches Problem hat und das der sendende Mailserver es doch bitte mit der Mail-Zustellung noch einmal probieren möge. Für 5 Minuten wird dann eine Mail-Zustellung von diesem Absender blockiert. Wenn der Absender dann nach diesen 5 Minuten oder ggfs. später, je nachdem wie er konfiguriert ist, die E-Mail noch einmal zustellt (was ein regulärer und RFC-konform konfigurierter SMTP-Mail-Server auf jeden Fall tun sollte), wird die E-Mail ohne

weitere Verzögerung akzeptiert und an die nachfolgende E-Mail-Waschstraße weitergeleitet. Erfolgen dann weitere E-Mail-Zustellungen vom gleichen Absender, werden diese sofort durchgelassen. Man erhöht zwar durch die erstmalige Ablehnung einen etwas höheren Mail-Traffic, wehrt hierdurch aber schon rund 80% des SPAM-Aufkommens ab. Wenn man überlegt, dass heute fast 90% des gesamten Mail-Traffics im Internet aus Viren, Phishing-Mails und SPAMs besteht, ist dies ein sehr effizientes Abwehr-Verfahren.

Einzelne Probleme mit wechselnden Serveradressen: Manche größere Mail-Server-Betreiber verteilen das Versenden der E-Mails ihrer Anwender auf mehrere Server, mit unterschiedlichen IP-Adressen, um so die Last der zu versendenden E-Mails zu verteilen. Je nach Konfiguration dieser Mail-Absender-Serverfarm kann es dann bei Wiederholung der Mail-Zustellungsversuche zu unterschiedlichen IP-Absender-Adressen kommen, so dass auf aixGate-Seite dies als neuer Mail-Zustellungsversuch interpretiert wird. Dies führt ggfs. zu längeren Mail-Zustellungszeiten und ComNet hat eine Reihe von bekannten Mail-Zustellern die so arbeiten vom Greylisting ausgenommen.

SPAM-Bewertung

Es gibt in Deutschland die Postzustellungsverpflichtung, die auch für E-Mails gilt. Danach muss Werbepost zugestellt werden, auch wenn die hohe Vermutung besteht, dass sie auf Empfängerseite ungewünscht ist. Ein Postzusteller oder Provider darf nicht entscheiden, welche Post er zustellt und welche nicht - hier wird gerne die E-Mail mit dem Viagra-Angebot als Beispiel herangezogen. ComNet als Provider darf nur die Annahme und Weiterleitung von E-Mails ablehnen, die klar als Schadmail mit gefahrbringenden Viren erkannt wurde (siehe kaskadierter Virus-Check) oder die technischen Konventionen des Internets nicht berücksichtigen (siehe SPAM-Abwehr durch Greylisting). Da dann aber den Anwendern zu viele SPAMs zugeleitet würden, setzt ComNet ein „SpamAssassin"-System ein, ein ausgezeichnetes Filtersystem, mit dem unerwünschte E-Mails (Spam) automatisch gekennzeichnet werden. Verdächtige E-Mails bekommen einen Eintrag in den sogenannten E-Mail-Header (verdeckte Kopfzeile) und auf Benutzerseite kann man solche gekennzeichneten Mails z.B. mit Regeln in Outlook in ein SPAM- oder Junk-Mail-Verzeichnis verschieben und in Zeitabständen löschen. Dieses „SpamAssassin"-Programm bewertet den Inhalt von E-Mails, dessen Betreff und einige andere Kriterien und vergibt Punkte für einzelne vorgefundene Umstände. Zum Schluss der Bewertung werden alle Punkte addiert und die erreichte Punktzahl wird in den E-Mail-Header geschrieben und wenn eine bestimmte Punktzahl erreicht wurde, wird ein sogenanntes SPAM-Flag (Markierung) gesetzt, das diese Mail als möglichen Spam ausweist. Im Gegensatz zu Viren, die eine eindeutige Bedrohung darstellen, ist eine SPAM selbst keine Bedrohung, sondern nur lästig. Ob es sich bei einer E-Mail um SPAM handelt liegt hierbei im Auge des Betrachters, manche Anwender finden Werbe-Mails von Internet-Versendern schon als SPAMs, an deren WEB-Shops man sich einmal angemeldet hatte. Aus diesem Grund finden auf den aixGate-Servern zwar Bewertungen statt, aber keine Löschungen.

E-Mail-Überprüfung: DNS-Reverse-Lookup

Das DNS-System im Internet ist dafür zuständig, Namen in IP-Adressen bzw. IP-Adressen in Namen zu übersetzen. Das Domain-Name-System (DNS) ist einer der wichtigsten Dienste in IP-basierten Netzwerken und die Hauptaufgabe besteht darin, die Beantwortung von Anfragen zur Namensauflösung vorzunehmen. Ein Reverse-Lookup ist nun eine Rückwärtsauflösung. Das DNS-Reverse-Lookup ist ein anerkanntes Verfahren um E-Mails auszufiltern, die von gekaperten Computern verschickt werden, die als Mailserver missbraucht werden, d.h. bei denen die Namensauflösung nicht stimmt. Dieses Verfahren wird u.a. auch von GMX, WEB.DE, 1&1, AOL usw. genutzt, kann aber bei manchen Absendern ggs. dazu führen, das richtige Mails zur Weiterleitung abgelehnt werden.

E-Mail-Überprüfung: Blackhole–Listing

Es gibt im Internet sogenannte Realtime-Blackhole-List-Server (RBL-Server) die Listen bzw. Datenbanken mit bekannten SPAM-Versendern führen. Diese Listen bestehen aus den IP-Adressen und Domainnamen der Server die dadurch aufgefallen sind, dass diese Server in hohem Maße SPAMs verbreiten. aixGate nutzt diese Funktion und beim Eingang einer E-Mail erfolgt in Echtzeit die Auswertung und bei positivem Ergebnis wird der E-Mail-Empfang abgelehnt.

Die größten SPAM-Versender haben weltweit hunderttausende von privaten aber auch öffentlichen Computern gekapert und verschicken darüber Ihre SPAM-Fluten. Diese gekaperten Computer nennt man Bot-Netze oder auch Zombie-Hosts. Eben genau diese „entführten" Computer bilden die größte Gefahr in Bezug auf SPAMs. Aus diesem Grund sind diese Systeme dann auch meistens innerhalb von kürzester Zeit auf diesen Blackhole-Lists und werden dann erfolgreich abgewehrt. Dies kann aber auch zur Folge haben, dass ComNet oder aixGate-Anwender auf diesen Listen vermerkt werden können, denn z.B. kann eine falsch konfigurierte Abwesenheits-Benachrichtigung in Outlook zu Ping-Pong-Mails führen und diese dann zu einem Eintrag auf diesen RBL-Servern. Dies kann dann ggfs. dazu führen, dass man für Stunden vom E-Mail-Verkehr ausgeschlossen wird und man erst umständlich für die Löschung eines solchen (Fehl-) Eintrages auf diesen Blackhole-List-Servern sorgen muss.

E-Mail-Überprüfung: Sender Policy Framework (SPF)

Auf das SPF-Verfahren haben sich eine Reihe von Providern geeinigt (u.a. nutzen dieses Verfahren heute neben ComNet auch Strato, GMX, WEB.de, 1&1, Host-Europe, Microsoft mit Hotmail und Outlook.com, Arcor, AOL, Gmail, Yahoo usw. – andererseits machen aber leider andere große Provider wie z.B. T-Onine hier nicht mit) und ist ein Verfahren, das das Fälschen der Absenderadresse einer E-Mail verhindern soll. Mit SPF (Sender Policy Framework) ist es auf Empfängerseite relativ einfach eine Prüfung durchzuführen, ob möglicherweise der Absender gefälscht wurde.

Voraussetzungen für den Betrieb

Um den Dienst nutzen zu können, sind folgende Voraussetzungen zu erfüllen:

- Einen aixGate-Vertrag oder einen ComNet -Server-Housing-, IAAS-, ASP-Vertrag, bei dem aixGate Vertragsbestandteil ist
- Ein installiertes aixGate-VPN-Gateway - das Gateway wird zentral von ComNet verwaltet und überwacht, Aktualisierungen der Konfiguration werden zentral durch ComNet durchgeführt, hierzu erfolgt ein Remote-Zugriff auf das aixGate-VPN-Gateway durch ComNet
- Einen Internetzugang
- Einen zweiten Internetzugang aus Redundanzgründen (optional)
- Werden in einem Kunden-Netzwerk weitere, nicht mit aixGate abgesicherte, Internetzugänge betrieben (z.B. für VoIP, SIP-Gateways, WLAN-Router usw.), können erhebliche Risiken entstehen, da hierdurch die aixGate-Schutzmechanismen umgangen werden. Der Kunde muss dieses Risiko durch geeignete lokale Maßnahmen minimieren, wie z.B. durch getrennte Internet-Verbindungen.

Verfügbarkeit

Die redundanten VPN-Einwahlserver im ComNet-RZ stehen rund um die Uhr zur Verfügung. Für aixGate- bzw. ComNet-Server-Housing-, IaaS- oder ASP-Verträge bestehen jedoch Service-Level-Agreement-Vereinbarungen mit verschiedenen Wartungsfenstern, in denen keine Einwahl möglich ist.

Treten neue Gefährdungen auf, die über aixGate noch nicht abgewendet werden können, werden die gefährdeten Dienste so lange gestoppt, bis durch geeignete Maßnahmen seitens ComNet die Sicherheit von aixGate wiederhergestellt worden ist.

ComNet hat auf Kundenseite nur wenige Ports freigeschaltet. ComNet kann kostenpflichtig individuelle Freischaltungen einzelner Ports durchführen. Voraussetzung ist eine Überprüfung des Einzelfalls unter Sicherheits-Aspekten durch ComNet. Nach einer individuellen Port-/Firewall-Freischaltung kann ComNet keine Sicherheit mehr für das Kunden-Netzwerk gewährleisten, da der betreffende Port nicht von aixGate-Mechanismen überwacht werden kann. Angriffe auf/über diesen Port können von aixGate nicht überwacht werden.

Die Performance von aixGate wird insgesamt durch eine Vielzahl von Faktoren beeinflusst, deswegen können keine festen Aussagen über Durchsatzraten getroffen werden.

ComNet weist hier darauf hin, dass Anwender durch den ordnungsgemäßen Einsatz von aixGate die Gefahren aus dem Internet minimieren können – eine 100%ige Sicherheit kann hier nicht gewährleistet werden, z.B. können die eingesetzten Viren-Scanner nur Viren erkennen, die bekannt sind, dies kann aber bei einem neuen Viren-Angriffs-Szenario Stunden oder Tage dauern.

ComNet appelliert auch an alle Nutzer nur Anhänge in Mails zu öffnen bzw. Links in Mails zu bestätigen, wenn diese Mails erwartet wurden und man die Absenderangaben überprüft hat.