Base Solution

Schützen Sie Ihren guten Namen

Einleitung:

Alle von Message Solution eingesetzten E-Mail-Security-Instanzen basieren auf einem speziell entwickelten Betriebssystem (M/OS, Message Operation System), das ausschließlich für die sichere Nachrichtenübermittlung entworfen wurde. Herkömmliche E-Mail-Lösungen steuern etwa 200 gleichzeitige ein- und ausgehende Nachrichtenverbindungen mit einer einzigen Nachrichtenwarteschlange für die gesamte Lösung. Eine Message Solution Instanz steuert in derselben Zeit etwa 10.000 gleichzeitige ein- und ausgehende Nachrichtenverbindungen mit, für jeden Empfänger eigenen Nachrichtenwarteschlangen. Nicht verfügbare Nachrichtenempfänger bzw. Domains haben deshalb keinen Einfluss auf die Geschwindigkeit einer Message Solution Instanz. Die wesentlich höhere Leistungsfähigkeit von Message Solution Instanzen ist ein Garant für die sichere und zuverlässige Nachrichtenübermittlung sowie eine permanente Verfügbarkeit.

M/OS	Herkömmliche Email- Lösungen
10.000 gleichzeitige ein- und ausgehende Verbindungen	200 gleichzeitige ein- und ausgehende Verbindungen
Hohe Performance, garantierte Zustellung	Niedrige Performance, Denial of Service Attacks
Per-Destination Warteschlangen	Single Warteschlange für alle Destinationen
Fehlertolerant und individuelle Kontrolle	Bei Problemen mit der Warteschlange sind alle Nachrichten betroffen

Base Solution, M/OS Vergleich

Message Solution stellt für jede Domain eine eigene E-Mail-Pipeline zur Verfügung, in der die weitere Nachrichtenübermittlung individuell definiert werden kann. Durch diese Technologie kann sichergestellt werden dass, ein- und ausgehende Nachrichten wirklich alle gewünschten Sicherheitsüberprüfungen passieren müssen.

Benefits / Philosophie:

Schützen Sie Ihr Unternehmen vor Überlastungs- Attacken

Message Solution bietet ein speziell für die Nachrichtenübermittlung entwickeltes Betriebssystem (M/OS), das bis zu 10.000 gleichzeitige Verbindungen bei hoher Performance gewährleistet. Das ist das 50fache von dem was herkömmliche E-Mail-Lösungen bieten.

Schützen Sie Ihren guten Namen

Durch die von Message Solution eingesetzten Technologien können Dritte Ihre Identität nicht fälschen und Ihre Reputation nicht nachhaltig beeinträchtigen.

Schützen Sie Ihre Informationen

Das Message Solution Nachrichtenbetriebssystem M/OS gewährt nur eindeutig authentifizierten Anfragen Zugriff auf weitere Nachrichtendienste.

Wirtschaftlichkeit

Message Solution bietet die Möglichkeit eine direkte Integration mit Ihren unternehmensweiten Verzeichnisdiensten (LDAP) vorzunehmen. Dadurch entstehen keine weiteren Administrationskosten zur Anwenderpflege.

Leistungsmerkmale

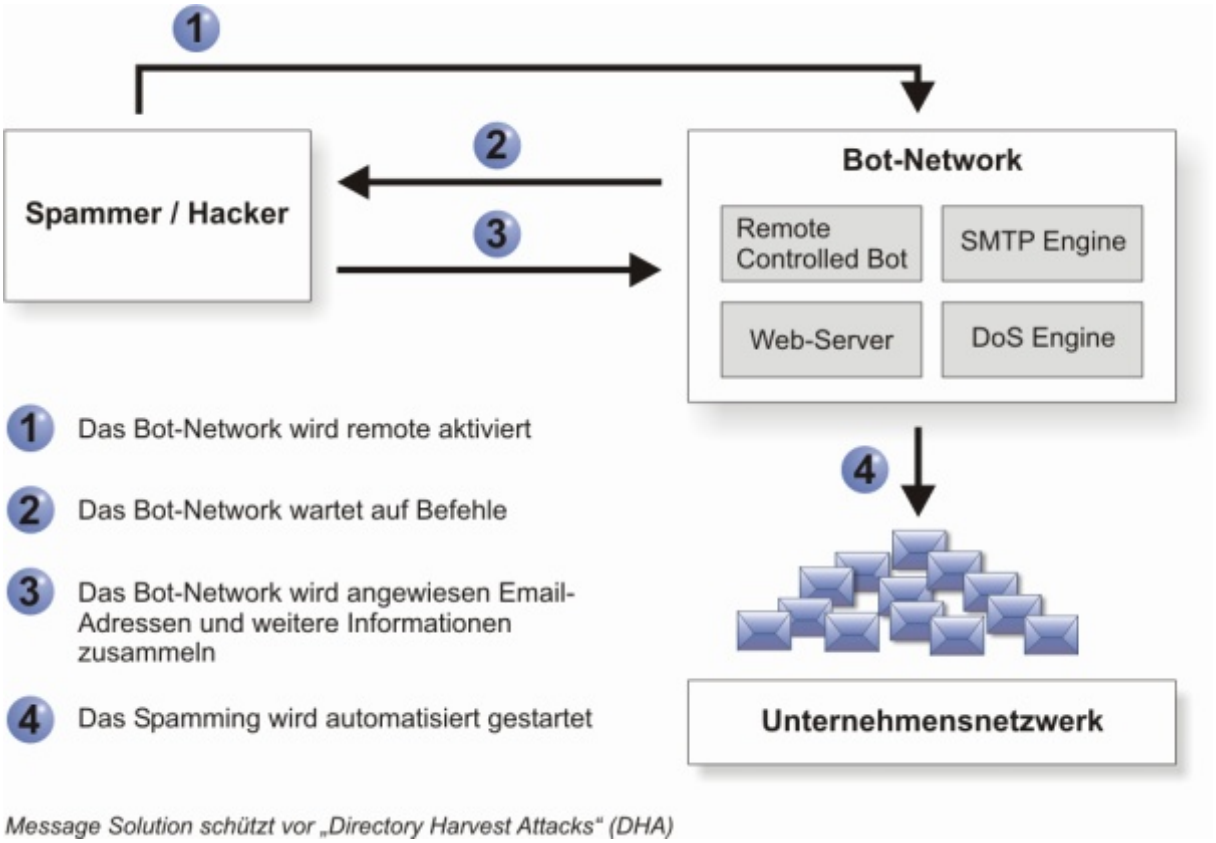
- Ausschließlich für die Nachrichtenübermittlung speziell entwickeltes Betriebssystem
- Mehr als 10.000 gleichzeitige Nachrichtenverbindungen (140 Stck. / Sek. oder 500.000 Stck. / Std.)
- Die Basis Security-Instanzen sind Teil des Betriebssystems
- Identitäts- und Integritäts- Prüfung durch Domain-Key Technologie
- Schutz vor nicht autorisierten Zugriffen (HAT-, RAT-, Exception- Table)
- Direkte Kommunikation mit unternehmensweiten Verzeichnisdiensten (LDAP)
- Definition eigener E-Mail-Pipelines pro Domain
- Message Solution passt sich dynamisch und schnell an die jeweils geforderten Unternehmensprozesse an
- Message Solution ist eine hochverfügbare, skalierbare und robuste Unternehmenslösung

Technik:

Das von Message Solution eingesetzte Nachrichtenbetriebssystem (M/OS) enthält neben den Basis Security-Instanzen, ein sehr leistungsfähiges Datei- und I/O- System, das speziell für die asynchronen Eigenschaften der Nachrichtenübermittlung optimiert wurde.

Schutz vor „Directory Harvest Attacks“ (DHA)

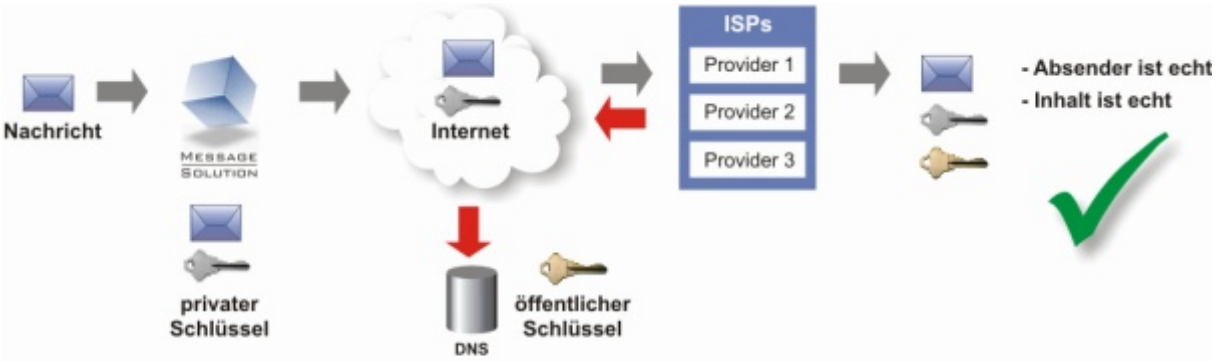
Das Message Solution Betriebssystem M/OS verhindert, dass potentielle Spammer E-Mail-Directories nach Adressen durchsuchen können. M/OS übermittelt keine Informationen, während des Verbindungsaufbaus zur Nachrichtenübermittlung, für gefälschte oder erfundene E-Mail-Adressen. Diese Adressattacken werden in der Regel von so genannten Zombie-Netzwerken oder BOT-Netzwerken (infizierte Computer, die ohne das Wissen des Nutzers Spam-Nachrichten verbreiten) durchgeführt. Dabei testet jeder Zombie-Rechner eine andere E-Mail-Adresse. Das Message Operating System erkennt solche Angriffe automatisch und verhindert sie erfolgreich.



Message Solution schützt vor „Directory Harvest Attacks“ (DHA)

Identitäts- und Integritäts- Prüfung durch Domain-Keys

Um die eindeutige Identität eines Nachrichten-Absenders und die Integrität einer Nachricht feststellen zu können, wurde die Domain-Key Technologie, als integraler Bestandteil, in das Message Operating System fest implementiert. Dabei wird jedem E-Mail-Header automatisch eine digitale Signatur hinzugefügt, welche die Absender-Domain und den Inhalt der Nachricht gegen Fälschungen und Veränderungen absichert. Der Nachrichten-Empfänger kann diese digitale Signatur auswerten und so eindeutig die Identität des Nachrichten-Senders und die Integrität des Nachrichten-Inhaltes überprüfen. Spammer, die mit gefälschten Absender-Adressen arbeiten, um so mit falscher Identität an persönliche Daten zu gelangen, werden sofort entlarvt und vom Message Operation System abgewiesen. Nur verifizierte Nachrichten von tatsächlich existierenden Absendern werden weiterverarbeitet.



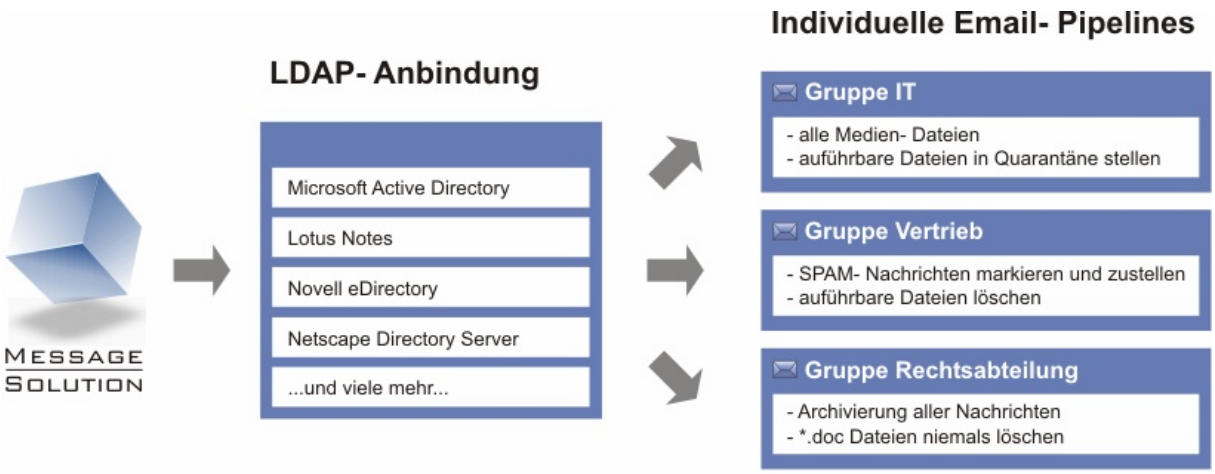
Identitäts- und Integritäts- Prüfung durch Domain-Keys

Schutz vor nicht autorisierten Zugriffen (HAT-, RAT-, Exception- Table)

M/OS regelt zusätzlich den Systemzugriff über so genannte Host Access- und Recipient Access-Tables (HAT, RAT). Diese System-Tabellen enthalten die autorisierten Host-Rechner und E-Mail-Empfänger. Nur eindeutig authentifizierten Anfragen gewährt M/OS Zugriff auf weitere Nachrichtendienste. Nicht autorisierte Anfragen werden von M/OS über die so genannte Exception Table (EXT) beantwortet. Die von M/OS gesendeten Antworten sind, über die Exception Table, für jede Domain und jede E-Mail-Adresse individuell konfigurierbar.

Direkte Kommunikation mit unternehmensweiten Verzeichnisdiensten (LDAP)

Durch den, in M/OS integrierten, LDAP-Service wird die direkte Kommunikation mit unternehmensweiten Verzeichnisdiensten erst möglich. Dabei werden Eigenschaften wie LDAP-basiertes Domain Routing, Alias-Tabellen und LDAP-Gruppen direkt unterstützt. Der LDAP-Service arbeitet mit allen führenden Directory-Servern zusammen (Microsoft Active Directory, Lotus Notes, Novell eDirectory, Netscape Directory Server, etc.). Durch den Einsatz von LDAP ist M/OS in der Lage, E-Mail-Empfänger in unternehmensweiten Verzeichnisdiensten zu suchen und zu authentifizieren. Eingehende Nachrichten werden erst dann angenommen, wenn M/OS eine erfolgreiche LDAP-Autorisierung vornehmen konnte. Darüber hinaus unterstützt M/OS die Domain-Maskierung für alle ausgehenden Nachrichten. Mit dieser Technologie werden automatisch alle internen Details vom unternehmensweiten Netzwerk und den Verzeichnisdiensten verborgen.



Kommunikation mit unternehmensweiten Verzeichnisdiensten

Frequenty asked question:

Was verbirgt sich hinter dem Begriff M/OS?

- M/OS heißt Message Operating System. M/OS ist ein, von Message Solution eingesetztes Betriebssystem, das speziell für die Nachrichtenübermittlung entwickelt wurde. Das Datei- und I/O- System von M/OS hat besondere asynchrone Eigenschaften und wurde ebenfalls speziell für die Nachrichtenübermittlung entwickelt.

Was ist eine E-Mail-Pipeline?

- Eine E-Mail-Pipeline ist ein, in Message Solution, definierter Nachrichtenweg. Eine E-Mail-Pipeline zwingt Nachrichten bestimmte Wege über frei definierbare Message Solution Instanzen zu nehmen.

Was bedeutet DHA?

- DHA ist die Abkürung für „Directory Harvest Attacks“. Unter DHA versteht man das Ausspionieren von E-Mail-Adressen in einem zentralen Adressbuch.

Was ist die Domain Key Technologie?

- Die Domain Key Technologie beschreibt ein spezielles Verfahren, bei dem E-Mail-Header ausgehender Nachrichten digital signiert werden. Die digitale Signatur gestattet es dem Nachrichten Empfänger System die Identität des E-Mail-Versenders eindeutig festzustellen und zu prüfen, ob die eingehende Nachricht digital verändert wurde (Integritäts- Test).

Was verbirgt sich hinter dem Begriff LDAP?

- LDAP steht für Lightweight Directory Access Protocol. LDAP ist ein Netzwerkprotokoll, das die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes (eine im Netzwerk verteilte hierarchische Datenbank) erlaubt.

Was bedeutet HAT?

- HAT ist die Abkürzung für „Host Access Table“. HAT ist eine System-Tabelle in M/OS, die Zugriffe von Host-Systemen auf Dienste in Message Solution überwacht und autorisiert.

Was bedeutet RAT?

- RAT ist die Abkürzung für „Recipient Access Table“. RAT ist eine System-Tabelle in M/OS, die Zugriffe auf E-Mail-Empfänger in Message Solution überwacht und autorisiert.

Was ist ein Exception Table?

- Exception Table oder EXT steht für Ausnahme-Tabelle. EXT ist eine System-Tabelle in M/OS, die Ausnahme-Fälle mit vorher definierten Antworten behandelt.

Kontakt

Für Fragen, Anmerkungen und weitere Informationen stehen wir Ihnen auch gerne persönlich zur Verfügung:

Message Solution
Biegenstr. 20
D-35037 Marburg
Tel.: +49 (0) 6421 / 175 17 60
Fax: +49 (0) 6421 / 175 17 69
E-Mail: sales@message-solution.com
Web: http://www.message-solution.com