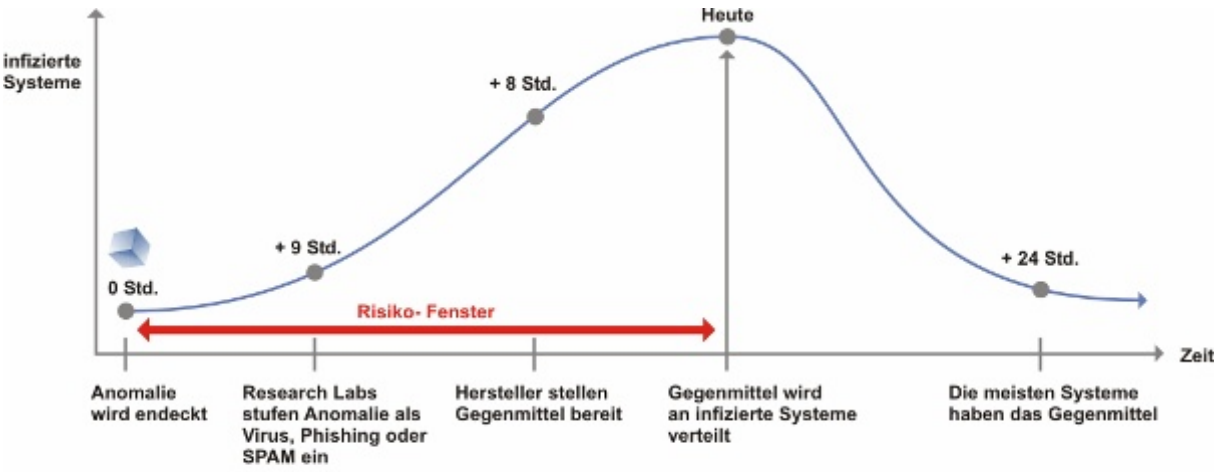
Pre-Detection Solution

Schutz vor noch unbekannten Bedrohungen

Einleitung

Herkömmliche E-Mail-Lösungen müssen eine Nachricht in Ihrer Gesamtheit annehmen, zerlegen, analysieren und zuordnen um zu entscheiden, ob eine eingehende Nachricht grundsätzlich von einem Absender erwünscht oder unerwünscht ist. Diese traditionelle Vorgehensweise führt erhebliche Nachteile mit sich. Die zusätzliche Belastung der Anti-Spam Filter und der Antiviren-Scanner kann zu einer totalen Überlastung führen und damit zum gesamten Systemausfall. Die einzige Ausnahme stellen so genannte Blacklisten dar. Eine Blackliste ist eine Liste, die Informationen über vermeintliche Spammer oder unerwünschte E-Mail-Versender führt. Herkömmliche E-Mail-Lösungen replizieren solche Blacklisten permanent von frei verfügbaren oder kommerziell betriebenen Quellen und unterbinden die gesamte Nachrichtenzustellung, falls sich ein Nachrichtensender auf einer solchen Liste befindet. Diese Verfahrensweise ist sehr statisch und das Mailgateway kann ausschließlich zwischen Zulassen oder Ablehnen der Kommunikationsverbindung entscheiden. Viele Firmen geraten jeden Tag unverschuldet auf solche Blacklisten. Für die betroffenen Firmen bedeutet das in jedem Fall eine Nachrichtensperre für mindestens 24 Stunden, bis die verantwortlichen Administratoren, dem Blacklisten Anbieter nachweisen können, dass sie zu unrecht auf einer solchen Liste stehen.



Pre-Detection, Vorsprung bei neuen unbekannten Gefahren

Die Pre-Detection Technologie von Message Solution verhindert solche Szenarien, die durch den Einsatz herkömmlicher E-Mail-Lösungen zwangsläufig entstehen. Pre-Detection schützt unsere Kunden vor noch unbekannten Gefahren und schickt entdeckte Nachrichtenanomalien, in der Frühphase einer Spam- / Viren- Attacke, in eine isolierte Vorsorge- Quarantäne. Damit ist Pre-Detection die erste Verteidigungsinstanz für die Message Solution Infrastruktur und bietet einen äußerst wirksamen Schutz vor unbekannten Bedrohungen.

Benefits / Philosophie:

Schützen Sie Ihr Unternehmen vor noch unbekannten Bedrohungen

Message Solution erkennt bisher unbekannte Gefahren in Echtzeit, durch die Überwachung des weltweiten Nachrichtenverkehrs, viele Stunden bevor die von reaktiven AntiSpam- /AntiVirus -Lösungen verwendeten Signaturen aktualisiert werden.

Stelle Sie Ihre Kommunikation sicher

Durch die von Message Solution eingesetzte Technologie der dynamischen Bonitäts- Ermittlung, werden seriöse Kommunikationspartner, trotz Blacklisten Einstufung weiter Nachrichten eingeschränkt senden und empfangen können ohne direkt geblockt zu werden.

Allumfassender Schutz für Ihr Unternehmen

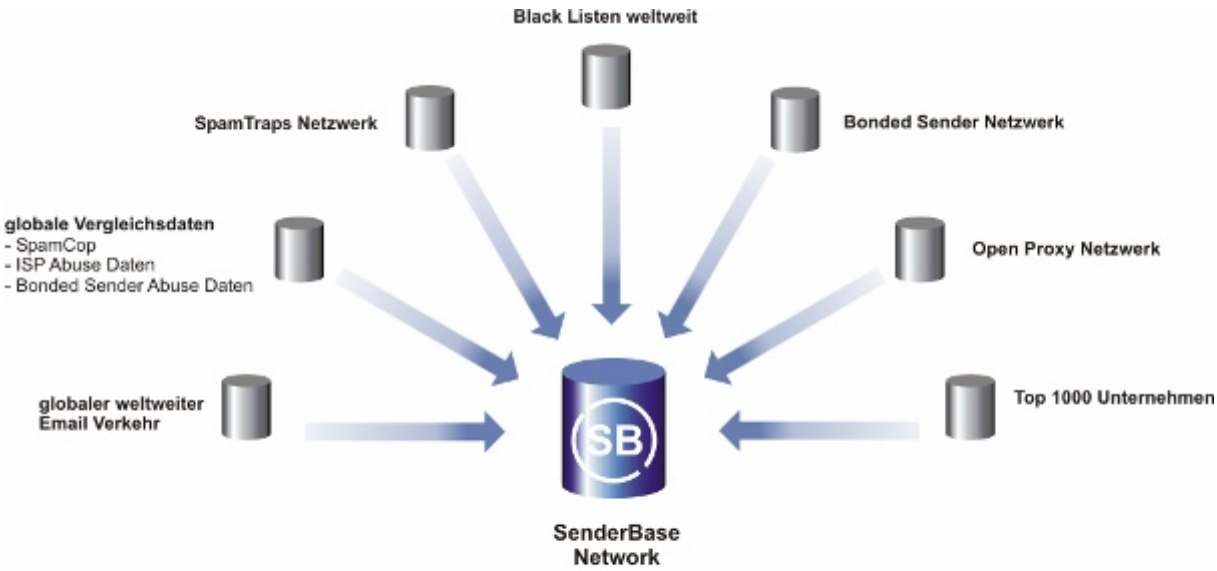
Message Solution bietet durch den Einsatz der Pre-Detection Technologie (präventiver Schutz), sowie weiterer AntiSpam- / AntiVirus- Technologien (reaktiver Schutz) in Kombination erstmalig einen allumfassenden Schutz unternehmensweiter Nachrichtensysteme.

Leistungsmerkmale

- Präventiver Schutz vor noch unbekannten Gefahren durch ständige Überwachung des weltweiten Nachrichtenverkehrs
- Absender Identitäten können eindeutig festgestellt werden
- Nachrichten müssen nicht, in Ihrer Gesamtheit, angenommen werden um zu entscheiden ob Sie erwünscht oder unerwünscht sind
- Keine statischen Positiv- / Negativ- Endscheidungen durch Blacklisten bei seriösen Kommunikationspartnern. Nachrichten von seriösen Kommunikationspartnern werden immer zugestellt.
- Dynamischer Schutz unternehmensweiter Nachrichtensysteme
- Pre-Detection Solution passt sich dynamisch und schnell an die jeweils geforderten Unternehmensprozesse an.
- Message Solution ist eine hochverfügbare, skalierbare und robuste Unternehmenslösung.

Die Technik

Die von Message Solution eingesetzte Technologie namens Pre-Detection- Solution umgeht alle Nachteile herkömmlicher E-Mail- Lösungen bei gleichzeitiger Steigerung der Leistung und Effizienz. Die Bonitätsprüfungs- Technologie basiert auf dem SenderBase® Netzwerk. Das SenderBase® Netzwerk ist das größte Datenbankbasierende Netzwerk zur Beobachtung des weltweiten E-Mailverkehrs. Mehr als 5 Mrd. Nachrichten am Tag werden von SenderBase® verarbeitet (das sind über 35% des gesamten E-Mailverkehrs weltweit, mit steigender Tendenz) und bieten einen Blick in Echtzeit auf alle Informationen des globalen Nachrichtenvolumens. Dabei werden automatisch eine Vielzahl von Parametern überprüft, ausgewertet und korreliert wie z. B., ob es sich bei den betroffenen IP-Adressen um offene Proxies handelt, ob sich Adressaten über Spam bestimmter Sender beschweren, ob die DNS Konfiguration von Versende- Domänen ordnungsgemäß aufgeschlüsselte Rücksendungen annimmt, ob das Herkunftsland zur IP-Adresse oder zur Domäne passt, u.s.w.…

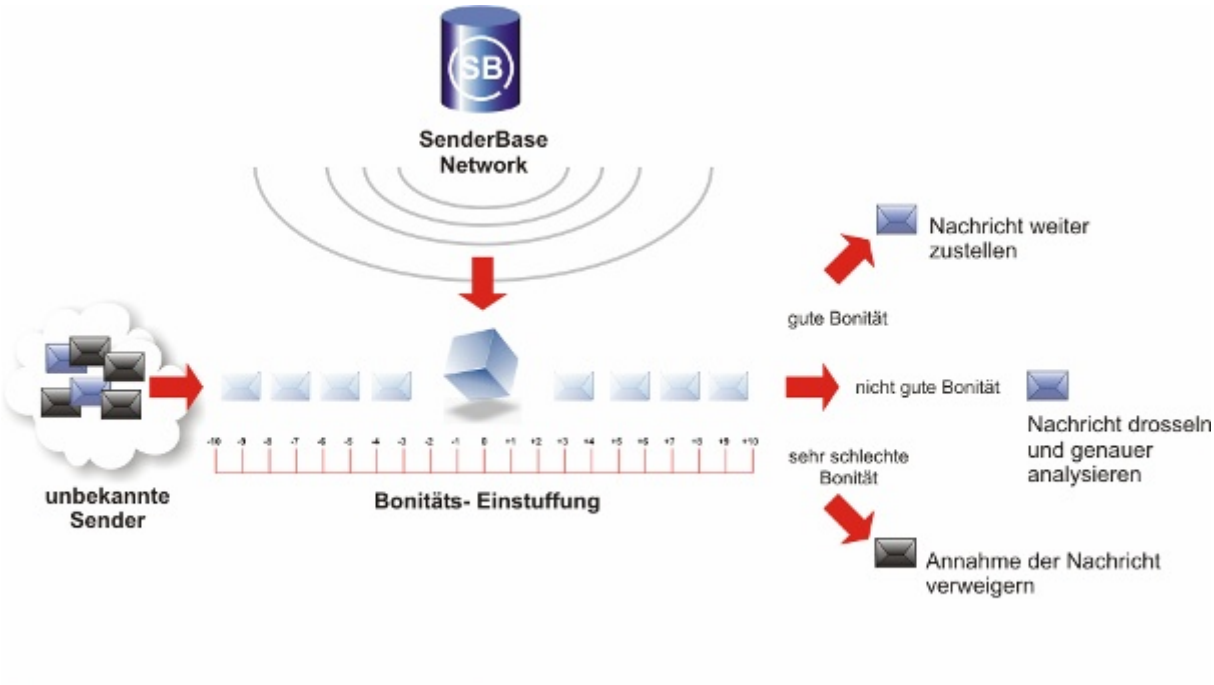


SenderBase® Network

Dynamische Bonitäts- Ermittlung

Message Solution repliziert permanent Daten und definierte Reputationen aus dem SenderBase® Netzwerk und bildet daraus eine Bonität für Nachrichtensender und Nachrichtenempfänger mit einer Bonitätsskala von 20 Stufen. Anhand der dynamischen Einstufung (Bonität) einer Nachricht kann Message Solution unterschiedliche Richtlinien (Policies) aktivieren die die weitere Vermittlung einer Nachricht regeln. Richtlinien können von Message Solution beliebig definiert werden.

Eine Richtlinie könnte besagen, dass seriöse Unternehmenskunden trotz Blacklisten Einstufung weiter Nachrichten eingeschränkt senden können ohne direkt geblockt zu werden. Als ein weiteres Beispiel könnten Versender mit immer schlechter werdender Bonität nur noch wenige E-Mails pro Stunde an eine Kunden-Domain versenden, bis die Bonität wiederhergestellt wurde.



Pre-Detection, dynamische Bonitäts- Ermittlung

Erkennung von neuen unbekannten Gefahren in Echtzeit

Neue und bisher unbekannte Gefahren werden in Echtzeit, viele Stunden bevor die von reaktiven AntiSpam- /AntiVirus -Lösungen verwendeten Signaturen aktualisiert werden, erkannt. Die Erkennung erfolgt über die in der Pre-Detection Technologie verwendeten Informationen aus dem SenderBase® Netzwerk. In Echtzeit werden die Daten von Message Solution verarbeitet und mit den schon vorhandenen Basisdaten verglichen. Anomalien, die auf erprobte Weise das Auftreten neuer Spam- / Viren-Attacken vorhersagen, werden somit sofort erkannt. Das Threat-Operations-Center (TOC) überprüft die Daten in Echtzeit und erstellt einen neuen Threat-Score. Message Solution setzt die vom TOC erstellten Scores in dynamische Nachrichten Richtlinien um. Wenn ein Score erhöht ist, wird die Nachricht automatisch gefiltert und in Vorsorge- Quarantäne geschickt. Diese Dynamik bietet Schutz vor neuen unbekannten Gefahren, bis Message Solution aktualisierte AntiSpam- / AntiViren Signaturen vorliegen.

Virus	Datum	Virus Threat Level verfügbar	Erste AntiVirus Signatur verfügbar	Vorsprung
Bagle.BX	27.02.05	10:39	04:22 am übernächsten Tag	+ 41:43 Stunden
MyDoom.BB	15.02.05	18:08	21:57 am nächsten Tag	+ 27:00 Stunden
Sober.J	30.01.05	23:01	09:21 am nächsten Tag	+ 10:00 Stunden
Bagel.AI	30.08.04	17:38	22:26	+ 04:48 Stunden
Bagel.Z	26.04.04	06:15	11:50	+ 05:30 Stunden
MyDoom.O	26.07.04	00:15	08:30	+ 08:15 Stunden

Pre-Detection, Vorsprung bei neuen Virenausbrüchen

Präventiver und Reaktiver Schutz ist allumfassend

Als präventiver Schutz ergänzt Pre-Detection die AntiVirus- und AntiSpam- Systeme von Message Solution. Pre-Detection erkennt neue unbekannte Bedrohungen in Echtzeit und leitet sie weiter, über dynamische Richtlinien, in eine isolierte Vorsorge- Quarantäne. Als reaktiver Schutz, in der weiteren E-Mail-Pipeline, überprüfen AntiVirus- und AntiSpam- Solution die, in Vorsorge- Quarantäne gestellten Nachrichten auf mögliche Bedrohungen anhand aktueller Signaturen. Damit bilden Pre-Detection-, AntiVirus- und AntiSpam- Solution in Kombination erstmalig einen allumfassenden Schutz unternehmensweiter Nachrichtensysteme.

Frequenty asked question:

Wie stellt Pre-Detection Absender Identitäten eindeutig fest?

- Absender Identitäten werden durch verschiedene Technologien geprüft. Zum Beispiel können Nachrichtenversender über den Domain-Name-Service geprüft werden. Dabei wird validiert, ob sich die Absender Adresse ordnungsgemäß aufschlüsseln lässt und auch Rücksendungen annimmt. Oder es wird das Domain-Key verfahren eingesetzt, das anhand von Zertifikaten prüft, ob der Absender authentisch ist.

Wie kann Pre-Detection dynamischen Schutz gewährleisten?

- Durch die ständige Überwachung des weltweiten Nachrichtenverkehrs erkennt Pre-Detection noch unbekannte Bedrohungen innerhalb von wenigen Minuten und stellt solche Nachrichtenanomalien anhand dynamischer Richtlinien in Vorsorge- Quarantäne.

Was ist ein Risiko Fenster?

- Als Risiko Fenster wird der Zeitabschnitt zwischen dem tatsächlichen Ausbruch einer Virus- / Spam- Attacke und der Erkennung durch ein Anti -Viren / -Spam Research Lab, sowie die Bereitstellung von Gegenmitteln, bezeichnet.

Was sind Quarantäne Systeme?

- Quarantäne Systeme sind physisch eigene Bereiche in Message Solution, in denen verhaltensauffällige oder virulente Nachrichten isoliert werden.

Wie schützt Pre-Detection vor PHISHING Angriffen?

- Bei Phising Attacken wird häufig versucht, Zugangsdaten und Passworte des Opfers zu erlangen, in dem man diesen auf „nachempfunde“ Webseiten lockt und diese durch bekannte Abfrageroutinen erfragt. Durch die Überwachung des weltweiten Nachrichtenverkehrs werden von Pre-Detection URL-Muster (inkl. der gesamten Web-Server Pfade) in allen Nachrichten korreliert. Diese Daten werden in Echtzeit ausgewertet und bilden die Basis für eine dynamische Bonitäts- Ermittlung von HTTP Verlinkungen in eingehenden Nachrichten.

Was ist unter dem Begriff dynamische Bonitäts- Ermittlung zu verstehen?

- Unter dem Begriff dynamische Bonitäts- Ermittlung versteht man die Einstufung eines Versenders, anhand der Echtzeitdaten aus der Überwachung des weltweiten Nachrichtenverkehrs, auf Vertraulichkeit und Seriosität.

Was ist eine E-Mail-Pipeline?

- Eine Email-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 sind dynamische Richtlinien in Bezug auf Pre-Detection?

- Richtlinien sind unumgängliche System Regeln (Security-Policies) die von Pre-Detection dynamisch angewendet werden um den Nachrichtenverkehr sicher und effizient zu kontrollieren.

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