Messaging Anti-Abuse Working Group

MAAWG Empfehlung - 10. November 2005

Port 25-Management im dynamischen IP-Netzbereich
Nutzen der Einführung - Risiken bei Untätigkeit

Einführung

Um eine wachsende Zahl von Computern zu kontrollieren benutzen Spammer und andere Kriminelle zunehmend Viren und Spyware. Die stete Zunahme von online Computern mit Verbindungen über Kabel, DSL oder Firmennetzwerke schafft immer mehr Ziele und bietet eine noch grössere Plattform, um schwer wiegenden Schaden im Internet anzurichten. Technische Anpassungen kombiniert mit einer intensivierten Benutzerinformation, wozu beispielsweise die Anregung zur Verwendung von Anti-Virus- und Firewall Software gehört, werden als zentrale Gegenmassnahmen betrachtet. Sie ermöglichen jedem Provider die verstärkte Unterbindung der missbräuchlichen Nutzung des Internet, welche aus der verseuchten Infrastruktur seiner Kunden hervorgeht. Durch das gezielte Management des Mailversands über infizierte Kunden-PC's können die Provider ihre Betriebskosten senken, die Kundenzufriedenheit verbessern und den Umfang des mit ihren Dienstleistungen verknüpften Internet-Missbrauchs reduzieren.

Bedrohungen und Missbrauch des Mailversands

Der wachsende vom E-Mail-Provider nicht geregelte oder überwachte Mailversand vom infizierten PC direkt auf externe Mail-Exchange Server (MX) bedeutet sowohl für den Provider als auch für den Kunden eine grosse Gefahr. PC's, welche unter der Kontrolle unbefugter und unerkannter Dritter stehen, gewähren diesen den anonymen Versand von Spam und Viren in grossen Mengen. Bis zu 80% aller Spam-Nachrichten laufen heute ohne Kenntnis oder Ermächtigung ihrer Besitzer über so genannte „Zombies".

Gefahren bei Untätigkeit

Die unliebsamen Auswirkungen auf die Besitzer der geschädigten Computer treten unverzüglich ein und sind schwerwiegend. Die Besitzer der Computer müssen oft erleben, dass ihr PC längere Zeit träge arbeitet, insbesondere dann, wenn versucht wird,

das Internet zu benutzen. Ohne dass die Kunden dies ahnen, kann ein Spammer ihre Bandbreite sättigen und sowohl den Down- als auch den Upload von Daten massgeblich einschränken oder verunmöglichen.

Dem Provider, an den der Computer angeschlossen ist, ist möglicherweise kaum bewusst, dass zusätzliche Bandbreite benutzt wird. Jedoch wird er üblicherweise ebenfalls negativ beeinflusst. Der betroffene Kunde verlangt allenfalls technische Unterstützung und diese kann den Provider rasch einen Monatsertrag und mehr kosten. Oder, gar noch schlimmer: der Kunde kommt ganz einfach zum Schluss, dass die Software, die Einwahl- oder die Breitbanddienste des Providers schlecht funktionieren und er kündigt den Dienst.

So lange der infizierte PC des Benutzers mit dem Netz verbunden bleibt, werden sich beim Provider Reklamationen von Empfängern anhäufen, die jenen Spam erhalten, der durch den entsprechenden Zombie hinausgepumpt wird. Auch wenn nur eine kleine Anzahl von verseuchten PC's am Werk ist, können die Kosten infolge von Reklamationen an den Kundendienst, an Missbrauchs- und Netzwerkbetriebsabteilungen in schmerzhafte Höhen klettern. Möglicherweise muss der Provider bald feststellen, dass sein ganzes Netzwerk wegen dem aus seinem Netz stammenden Missbrauchsmuster auf eine so genannte schwarze Liste (Blacklist) gesetzt wird, was in der Folge für den Kunden verunmöglicht, E-Mails an beliebige Empfänger mit fremden Maildomänen zu senden. Darüber bedeutet jede gesendete Spammail eine empfangene unerwünschte Nachricht mehr. Wenn man zulässt, dass diese Art von Missbrauch ungehemmt weiterläuft, dann hat das eine entsprechende globale, negative Auswirkung auf *alle* Internet-Benutzer und Zugangsprovider, indem es das Kundenvertrauen und damit die Bereitschaft der Kunden mindert, das Internet für die Kommunikation zu nutzen – sowohl geschäftlich, als auch privat.

„Best Practices" für den E-Mailversand

Eine Selbstregulierung durch die Branche ist die wirkungsvollste Massnahme, um dem Missbrauch von E-Mailversand zu begegnen. Das grosse Ausmass des Spamproblems erfordert sofortiges Handeln. Folgende Botschaft, welche von Regierungsbehörden der ganzen Welt laut wurde, ist unmissverständlich und wurde klar verstanden: wenn nicht sofort gehandelt und Resultate erbracht werden, dann wird sich die Branche in zunehmendem Mass der Überprüfung und Fremdregulierung ausgesetzt sehen. Darum empfiehlt die MAWWG die folgende Reihe von Arbeitsweisen für Internet- und E-Mail-Dienstprovider:

1. Bieten Sie E-Mailversand über Port 587 an, wie in RFC 2476 beschrieben wird.
2. Verlangen Sie für den E-Mailversand eine Authentisierung, wie in RFC 2554 beschrieben wird.
3. Stellen Sie Outbound Konnektivität über 587 sicher.
4. Konfigurieren Sie die E-Mail-Client-Software so, dass der Port 587 und Authentisierungen für den E-Mailversand benutzt wird.

5. Sperren Sie den Zugang **zum** Port 25 **von** allen Hosts in Ihrem Netzwerk, mit Ausnahme von denjenigen, die Sie ausdrücklich zur Ausübung von SMTP-Relaisfunktionen ermächtigen. Dies werden zum einen Ihre eigenen Mailserver sein. Allenfalls gehören auch die legitimen Mailserver Ihrer verantwortlichen Kunden dazu.
6. Sperren Sie über Port 25 eingehenden Verkehr zu Ihrem Netzwerk. Dadurch verhindern Sie Missbrauch durch Spammer, die asymmetrisches Routing und spoofing IP-Adressen in Ihrem Netzwerk benutzen.

Diese Massnahmen wurden von Providern aller Grössen, vieler der weltweit beliebtesten Dienstprovider und von vielen MAAWG-Mitgliedern ohne nennenswerten Rückgang des Kundenstamms eingeführt.

Nutzen der Einführung

Die Anforderung einer Authentisierung und die Bündelung des E-Mailversands durch SMTP-Relais bringen einem ISP viele wertvolle Vorteile. Diese Massnahmen ermöglichen dem ISP:

- Die für die versendete Nachricht verantwortliche Person zu identifizieren.
- Belastungen durch Spam, Viren und andere missbräuchliche Nachrichten zu reduzieren.
- Die Übertragungsraten pro Kunde und/oder gesamthaft zu überwachen und zu beschränken.
- Für die Versendung von E-Mails annehmbare Benutzungsrichtlinien und Dienstbedingungen durchzusetzen.

Zudem gewinnt der ISP die folgenden Wettbewerbsvorteile:

- Verbesserte Lieferbarkeit für legitime E-Mails aufgrund verminderten Risikos, von empfangenden Internet- und E-Mail-Providern auf die schwarze Liste gesetzt zu werden.
- Reduzierte Kosten für Abuse-Desk, den Kundendienst und die Netzwerk-Betriebszentren.
- Fähigkeit, jenen Kunden Premium-Dienststufen anzubieten, die ein legitimes Bedürfnis nach einem Betrieb von E-Mail-Servern mit direktem Zugang zum Port 25 haben.
- Reduzierte Infrastrukturkosten infolge Verminderungen der Port-Benutzung und des Bandbreitenverbrauchs.
- Wichtige Beteiligung resp. sinkender Anteil pro Kunde an der Reduktion des globalen Spam Volumens.

Sobald diese Massnahmen greifen, verlieren die Spammer vorerst die schützende Anonymität. Geschädigte Computer können rasch erkannt und unter Quarantäne gestellt werden, bis sich der Besitzer des Problems bewusst wird und es behebt. Bei

diesem Vorgang werden die Kunden über Sicherheitsbedrohungen unterrichtet und angeregt, sich besser zu schützen. Diese Anpassungen und Optimierungen erhöhen die Sicherheit und den Schutz *aller* Endverbraucher.

Kundeninformation

Die MAAWG erachtet es als enorm wichtig, mit den Kunden zu kommunizieren. Die Internet- und E-Mail-Dienstprovider müssen ihre Kunden darüber ins Bild setzen, was sie tun und warum sie es tun. Sind diese ausreichend über die Bedrohungen sowie entsprechende Gegenmassnahmen informiert, so können sie diese eher nachvollziehen und verstehen. Auch werden sie begreifen, welche wichtige Rolle sie selbst zum Beispiel bei der Umstellung auf eine neue Methode des Mailversands spielen. Alle Mitglieder der Messaging Industrie werden nachdrücklich aufgefordert, diese technischen Vorgehensweisen einzuführen, ihre Kunden laufend und so rasch als möglich zu informieren, um dadurch die Kontrolle über den Port 25 zu erlangen und Messaging Dienste vor Missbrauch zu schützen.

Weiterführende Informationen

„SMTP Service Extension for Authentication“, J. Meyers, March 1999:
http://www.ietf.org/rfc/rfc2554.txt

„Message Submission“, R. Gellens and J. Klensin, December 1998:
http://www.ietf.org/rfc/rfc2476.txt

„Operation Spam Zombies”, Federal Trade Commission, May 2005:
http://www.ftc.gov/bcp/conline/edcams/spam/zombie/

“Anti Spam Technical Alliance Technology and Policy Proposal”, Anti Spam Technical Alliance, June 11, 2004: http://www.postmaster.aol.com/asta/proposal_html.html

“Stopping Spam – Creating a stronger, safer Internet”, Industry Canada, April 2005:
http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/gv00329e.html