



20 Massnahmen gegen Spam und Malware

Um die Sicherheit in einem Unternehmen garantieren zu können, müssen verschiedene Aufgaben zusammenspielen: organisatorische Regeln, physische Systeme und die Informatiksicherheit. **VON CHRISTOPH BAUMGARTNER ***

Der Empfang unerwünschter Werbung ist nicht nur ärgerlich, sondern beeinflusst auch die Produktivität der Betroffenen massgeblich. Digitales Ungeziefer wie Viren, Würmer und Trojaner bedroht die Verfügbarkeit und die Integrität der IT-Infrastruktur. Spyware und Remote Administration Trojaner unterwandern die Vertraulichkeit, indem sie Benutzeraktivitäten ausspionieren, Systeme gezielt nach relevanten Informationen absuchen und die gesammelten Daten in irgendeiner Form an den Autor des Trojaners weiterleiten oder gar die Remotekontrolle des infizierten Systems er-

möglichen. Besonders beunruhigend ist der Trend, dass professionelle Spammer Hand in Hand mit Malwareautoren arbeiten um an neue Versandplattformen für Massenmails zu kommen. Dank dieser unheiligen Allianz können Unternehmen und Private plötzlich zu Spammern werden, weil ihre Internetinfrastruktur ohne ihr Wissen zweckentfremdet wird. Gerade die Verantwortlichen in Unternehmen geraten spätestens dann in Erklärungsnöte, wenn die Firmendomain als offizielle Spamdomain erfasst wird (was die E-Mail-Kommunikation via der betroffenen Domain über längere

Zeit nahezu verunmöglicht) oder wenn der Internet Service Provider mit der Deaktivierung der Internetanbindung droht. Leider gibt es kein Universalrezept gegen Spam und Malware. Sicherheitsbewusstes Handeln kombiniert mit geeigneten organisatorischen und technischen Massnahmen schützt aber vor allzu bösen Überraschungen. Folgende Massnahmen dämmen die Spamflut ein und helfen im Kampf gegen Malware.

* Christoph Baumgartner ist CEO/Senior Consultant bei der Sicherheitsberaterin Oneconsult, Thalwil, www.oneconsult.com.

Nr.	Bedrohung	Massnahme	
		Name	Beschreibung
1	E-Mail-Adressen-Harvesting	Nur generische E-Mail-Adressen veröffentlichen	Bei der Domain-Registrierung und auf Webservern sollten nur generische E-Mail-Adressen (z.B. webmaster@firma.ch oder info@firma.ch) veröffentlicht werden, weil Spammer mittels automatisierten Tools systematisch das Internet nach gültigen E-Mail-Adressen abgrasen.
2		Rein geschäftliche Nutzung der Mitarbeiter-E-Mailadresse	Persönliche Mitarbeiter-E-Mail-Adressen dürfen nur geschäftlich genutzt werden, weil diese E-Mail-Adressen für Spammer besonders interessant sind.

Nr.	Bedrohung	Massnahme	
3	E-Mail-Adressen-Harvesting	Free-Mail-Adressen für Beiträge in Newsgroups	Für Beiträge in Newsgroups und Mailinglisten sollten kostenlose E-Mail-Accounts verwendet werden, weil Newsgroup-Beiträge selbst nach Jahren noch im Internet gelistet sind.
4		Empfangsbestätigung deaktivieren	Die automatische Empfangsbestätigung sollte deaktiviert oder auf Modus «Benutzer fragen» geschaltet werden, weil sie oftmals von dem E-Mail-Account aus beantwortet wird, an den die E-Mail weitergeleitet wurde (generische Adresse -> Mitarbeiteradresse).
5		Auf Spam nie reagieren	Grundsätzlich darf nie die Zustellungs-Abmeldemöglichkeit in Spammails benutzt oder irgendeinem Link in der Spam-Mail gefolgt werden, da dies den Spammern die gültige direkte Mitarbeiteradresse verschafft.
6	Belästigung / Produktivitätssenkung durch Spam	Spamfilter	Spamfilter kennzeichnen und/oder löschen, bei Spamverdacht die betroffene E-Mail.
7		SPF Sender Policy Framework	Mittels Koppelung von DNS-Einträgen und zugehörigen Mailservern kann der empfangende Mailserver mittels DNS-Abfrage prüfen, ob der sendende Mailserver mit der in der E-Mail bezeichneten Absenderdomain übereinstimmt (Spammer verwenden oft gekaperte Mailserver und gefälschte Absenderadressen).
8		Zertifikatsbasierte Verschlüsselung und/oder Signierung	Für geschlossene Benutzergruppen kann der Mailserver so konfiguriert werden, dass er nur mittels digitalen Zertifikaten (nach X.509 oder PGP) signierte und/oder verschlüsselte E-Mail weiterleitet.
9	Missbrauch durch Spammer	Mailrelaying nur für eigene Organisation	Der Mailserver sollte so konfiguriert werden, dass nur Berechtigte seine Dienste in Anspruch nehmen können.
10	Infektion mit Malware	Firewall	Soft- und Hardwarefirewalls schützen Systeme generell vor Malware, welche sich mittels Direktverbindung verbreitet. Ausserdem kann der Zugriff auf als gefährlich geltende Websites mittels Black List gesperrt werden.
11		Anti-Viren-Lösung	Anti-Viren-Lösungen schützen vor der Infektion mit bekannter Malware bzw. erkennen und löschen bereits «installierte» Malware.
12	Infektion mit Malware / Missbrauch durch Unberechtigte	Systemhärtung	Deaktivierung/Deinstallation nicht benötigter Dienste und regelmässiges Einspielen von Security Updates und Firmware Upgrades helfen gegen Malware und schützen vor Missbrauch durch Unberechtigte.
13	Infektion mit Malware / Informationsdiebstahl Informationsdiebstahl durch Malware	Contentfilter	Contentfilter überwachen den Netzwerkverkehr und können verdächtige Aktivitäten im Netzwerk erkennen und unterbinden.
14	Informationsdiebstahl durch Malware	Spywaredetektor	Spywaredetektoren helfen bei der Erkennung von bereits «installierter» Spyware (Trojaner).
15		IDS/IPS	Intrusion Detection- bzw. Intrusion-Prevention-Systeme erkennen bei richtiger Konfiguration verdächtige Kommunikationsaktivitäten im Netzwerk.
16		Network Sniffer	Network Sniffer helfen bei der Erkennung von Systemen, welche mit durch ein Rootkit geschützte Spyware infiziert wurden. Die Erkennung erfolgt mittels der Auswertung des von einem verdächtigen System ausgehenden Netzwerkverkehrs.
17		Port Scan	Ein Port Scan hilft bei der Erkennung von (verdächtigen) Diensten. Manche Malware kann nur mit einem so genannten Ack-Scan (Port Scan mit aktiviertem Ack Flag) erkannt werden.
18		Suche nach verdächtigen Einträgen	Malware, welche sich dauerhaft auf einem System niederlässt, hinterlässt üblicherweise Spuren in Form von neuen Dateien im Filesystem und/oder Einträgen in der Windows Registry.
19	Generelle Bedrohungen	Security Awareness	Die Förderung von sicherheitsbewusstem Handeln der Mitarbeiter und entsprechend verantwortungsvollem Umgang mit Informatikmitteln ist eine nachhaltige, technologieunabhängige Massnahme.
20		Audit	In regelmässigen Abständen sollten Prozesse und Systeme mittels Audits auf Schwachstellen hin untersucht werden, damit pro-aktives Risk Management betrieben werden kann.