Wenn die Cloud angreift...

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Sicherheitsbedenken gegenüber Cloud-Computing-Angeboten drehen sich in der Regel um die Absicherung eigener ausgelagerter Daten, die einerseits vor Fremdzugriff geschützt werden müssen und andererseits jederzeit verfügbar sein sollen. Doch was ist, wenn die Cloud selbst zum Angreifer wird?

Anlass für derlei Sorge bietet etwa eine Meldung, die US-amerikanische Medien im August veröffentlichten: Ausgehend von virtuellen Servern des Cloud-Computing-Anbieters Amazon erfolgte eine Denial-of-Service-Attacke (DoS) gegen das Netzwerk eines Unternehmens, das so vom Internet abgeschnitten wurde. Bekannt für Angriffe dieser Art waren bislang die Betreiber bzw. Kunden sogenannter „Botnetze“, die damit beispielsweise unliebsame Konkurrenten schädigen oder vielleicht sogar erpressen wollen. Das auch ein legaler Service Ausgangspunkt für solche Attacken sein kann, ist neu und weckt einige Bedenken.

Zunächst sollte jedoch klar sein, welche Gefahren sich hinter DoS-Angriffen und Botnetzen verbergen: Unter einer Denial-of-Service-Attacke, so erklärt das Bundesministerium des Innern (BMI) in der Vorabfassung des Verfassungschutzberichts 2009, versteht man „einen Angriff durch eine hohe Anzahl von Anfragen an einen Server, einen Rechner oder an sonstige Netzkomponenten in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen.“ Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt vor solchen Angriffen, die von Programmen ausgeführt werden, die etwa Bugs und Schwachstellen von Programmen oder Betriebssystemen oder Fehlimplementierungen von Protokollen ausnutzen. „Andere Angriffe“, so das BSI, „überlasten ein System schlicht mit zu vielen Anfragen.“

Besonders effektiv sind solche DoS-Angriffe, die nicht von einem einzelnen, sondern koordiniert und gleichzeitig von einer Vielzahl unterschiedlicher Systeme ausgeführt werden. Häufig führen Cyberkrimelle solche Angriffe, die ihrer Verteilung wegen auch als „Distributed-Denial-of-Service-Attacken“ (DDoS) bezeichnet werden, über die bereits erwähnten Botnetze aus. Harald Philipp, Geschäftsführer des Sicherheitsanbieters Bitdefender GmbH, beschreibt sie folgendermaßen: „Die größte Bedrohung für Unternehmensnetzwerke durch Botnetze sind sogenannte DDoS-Attacken auf die Server einer Unternehmung. Durch diese Art von Angriffen wird die Netzwerkinfrastruktur, beispielsweise Web- oder Mailserver, vollständig überlastet.“

Angriff per Fernsteuerung

Dass dies insbesondere für E-Commerce-Anbieter kritisch ist, deren Geschäft von der Verfügbarkeit der eigenen Webshops abhängt, liegt auf der Hand. Darüber hinaus „stellt eine DoS-Attacke für jedes Unternehmen, das Geld mit dem Internet verdient oder Internetauftritte pflegt, eine große Gefahr dar“, ergänzt Stefan Ortloff, Virusanalyst beim russischen

Sicherheitsspezialisten Kaspersky Lab. Eindringlicher noch beschreibt es Harald Philipp: „DDos-Attacken bedrohen jede Form von Geschäftsmodell, das auf der digitalen Kommunikation mit Kunden basiert. Als Ziele kommen sowohl Banken, Videoplattformen, Bloggingportale oder sogar Hersteller von Antivirensoftware in Frage. Denkbar sind auch Angriffe auf große Softwareunternehmen, um beispielsweise einen Produktlaunch zu sabotieren oder Erpressungsversuche zu starten."

Möglich werden die verteilten Angriffe durch Botnetze, die gemäß den Erklärungen von Yuri Namestnikov, Virenanalyst bei Kaspersky Lab, aus dem Zusammenschluss tausender, unter Umständen sogar Millionen von Rechnern bestehen, die alle mit einem Schadprogramm infiziert sind. Das Programm ermöglicht Cyberkriminellen, die befallenen Computer aus der Ferne zu steuern, weshalb diese auch als „Zombie-Rechner" bezeichnet werden. Zu Zombie-Rechnern werden sowohl die Computer von Privatanwendern als auch Unternehmensrechner, wenn diese sich mit einem entsprechenden Schadprogramm infizieren. Als Infektionsquelle dienen dabei zum Beispiel Spam-Mails mit Malware-Anhang oder verseuchten Links, die auch in Foren oder sozialen Netzwerken veröffentlicht werden. Auch kann sich ein Bot-Programm auf dem PC des Besuchers einer infizierten Webseite per „Drive-by-Download" installieren, wobei Sicherheitslücken des verwendeten Browsers ausgenutzt werden. Nicht zuletzt verfügt Bot-Malware wie auch andere Viren und Würmer in der Regel über eine Selbstverbreitungsfunktion, wodurch beispielsweise ein befallener Rechner im Unternehmensnetzwerk auch alle anderen Computer des Netzes infiziert, sofern diese nicht entsprechend geschützt sind.

Wollte man dieser Art von Schadprogrammen menschliche Eigenschaften zuschreiben, müsste man sie geradezu als hinterhältig bezeichnen, denn ohne weiteres stellt ein Anwender nicht einmal fest, dass sein Rechner einem oder gleich mehreren Bots als Heimstatt dient. Luis Corrons, Technical Director der Pandalabs des Antivirusspezialisten Panda Security, verrät: „Zwischen einem PC mit etlichen Bots oder einem ohne erkennt man als User leider keinerlei Unterschied. Sie nisten sich unbemerkt ein, je länger, desto besser. Oftmals tarnen Sie sich als reguläre Anwendung oder ändern ihren Speicherplatz, damit sie nicht erkennbar sind."

Spurensuche und Gegenmaßnahmen

Um eine Bot-Infektion festzustellen und zu beseitigen, eignet sich laut Stefan Ortloff eine aktuelle Antiviruslösung. Auch Harald Philipp weiß: „Die meisten Bots werden normalerweise von Antimalwareprodukten aufgespürt und unschädlich gemacht." Es gebe aber auch Bots, die Schutzmechanismen durch spezielle Techniken aushebelten und PCs bzw. Netzwerke infizierten. „Sobald sie in ein System eingedrungen sind", erklärt er, „verraten sie sich jedoch meist durch folgende Aktivitäten: Erhöhtes Aufkommen von Traffic im Netzwerk, wenn der Bot mit seinem Command-and-Control-Center kommuniziert, verstärkte Anfragen an andere Webseiten oder ein Anstieg von E-Mails, die über das Netzwerk gesendet werden." Spezielle Software sei aber auch in diesem Fall dazu in

der Lage, ein befallenes Netzwerk zu desinfizieren. Entsprechende Lösungen liefen simultan auf allen Arbeitsplatzrechnern und verhinderten so die Neuinfektion bereits gesäuberter Endpoints durch immer noch kontaminierte Rechner.

Das eigene Netzwerk gegen Bot-Befall zu präparieren, empfiehlt sich aus verschiedenen Gründen, die Stefan Ortloff zusammenfasst: „Unmittelbare Gefahren liegen zum Beispiel im Abgreifen von kritischen Zugangsdaten auf Firmenrechnern, wodurch weitere Zugangsmöglichkeiten für Cyberkriminelle entstehen. Weiterhin drohen der Diebstahl sensibler Unternehmensdaten und die missbräuchliche Verwendung der Firmen-IP-Adresse. Letzteres dient etwa zum Versand von Spam durch das Botnet – dadurch entsteht auch die Gefahr, in Spam-Blacklisten zu erscheinen – , um als Teil eines DDoS-Angriffs eingesetzt zu werden oder als Proxy für kriminelle Handlungen zu dienen, bei denen Kriminelle ihre wahre Identität verschleiern."

Gemäß den Angaben der befragten Sicherheitsanbieter ist es nicht besonders schwer, Botnetze im Internet zu mieten oder entsprechende Schadsoftware von Cyberkriminellen zu kaufen. Es gebe eine Reihe von „Untergrundforen", die für die Umsetzung von DDoS-Attacken werben und Preislisten für solche Angriffe enthielten. Dort träfen sich Botmaster, präsentierten ihre „Produkte" und tätigten Geschäfte. „Generell sind diese Foren ganz leicht bei Google über die entsprechenden Suchbegriffe zu finden", sagt Luis Corrons. Die meisten dieser Foren seien öffentlich und für jeden zugänglich. „Einige dieser Treffpunkte", ergänzt Harald Philipp, „sind jedoch vergleichbar mit geschlossen Clubs: Neulinge erhalten nur dann Zugang, wenn sich ein bewährtes Mitglied für sie verbürgt."

Spionagethriller oder Hirngespinst?

Dass es kriminelle Vereinigungen gibt, die Millionen von Computern mit Viren infizieren, um geldwerte Informationen ihrer Besitzer zu erhalten sowie deren Rechenkapazitäten für illegale Angriffe gegen Netzwerke und Organisationen durchzuführen, mag nach Stoff für einen billigen Spionagethriller klingen. Tatsächlich handelt es sich aber keineswegs um Hirngespinste oder Übertreibungen, wie Veröffentlichungen über länderübergreifende gemeinsame Aktivitäten von Polizei- und Geheimdienstbehörden belegen. Über solche Fälle berichten zum Beispiel Vertreter der Antivirusindustrie wie Panda Security, die gemeinsam mit einer kanadischen IT-Sicherheitsfirma die Botnetz-Software Mariposa analysierten und gemäß eigenen Angaben dem amerikanischen FBI dazu verhalfen, den spanischen Betreiber des gleichnamigen Netzes in Slowenien festzunehmen. Bevor dessen Botnetz, das bislang größte bekannt gewordene seiner Art, lahmgelegt wurde, hatte es bereits 12,7 Mio. Rechner weltweit infiziert und somit fernsteuerbar gemacht.

Auch Oberstleutnant Volker Kozok, Referent beim Bundesministerium der Verteidigung, erklärt auf Sicherheitskonferenzen wie der diesjährigen IT-Defense in Köln, welche Anstrengungen die Behörden unternehmen, um

der Gefahr aus dem Internet Herr zu werden. Sein besonderes Augenmerk gilt dabei dem sogenannten „Bullet Proof Hosting“, bei dem legale Internet Service Provider sichere Dienste für die organisierte Kriminalität anbieten. Sie dienen etwa als Hoster für Botnetze und andere Malware und schützen sie vor dem Zugriff von Ermittlungsbehörden – Spionagethriller ja also, Hirngespinst nein.

Warum es so schwierig ist, auf Gesetzesebene gegen öffentlich zugängliche Treffpunkte von Cyberkriminellen und Umschlagplätze von Schadsoftware vorzugehen, erklärt Luis Corrons: „Diese Seiten zu schließen ist so schwierig, weil solche Aktivitäten nicht in allen Ländern als illegal eingestuft werden. Online-Kriminelle kennen oft die landestypischen Gesetze und können ihre Seiten dementsprechend konzipieren.“

Botnetze bald überflüssig?

Nun ist es an der Zeit, das eingangs angeführte besorgniserregende Fallbeispiel wieder aufzugreifen, bei dem die Amazon-Cloud zum Ausgangspunkt einer DoS-Attacke gegen ein Unternehmen aus dem Mittelstand wurde. Zunächst sei klargestellt, dass es sich bei Amazon ganz sicher nicht um einen kriminellen Service Provider handelt. Auch war die DoS-Attacke kein Angriff kreativer Cyberkrimineller, die gerade keinen Zugriff auf ein geeignetes Botnet hatten. Tatsächlich handelte es sich den Berichten zufolge lediglich um zwei Sicherheitsberater, die von einem Unternehmen damit beauftragt wurden, dessen Konnektivität zu prüfen. Um ihren Auftrag zu erfüllen, mieteten die beiden mittels Kreditkarte und E-Mail-Adresse einige virtuelle Server in Amazons EC2-Cloud (Elastic Compute Cloud), und führten von dort aus ein selbstgeschriebenes Programm aus, mit dem sie die besagte DoS-Attacke gegen die Server ihres Auftraggebers ausführten und ihn so vom Netz trennten. Der Kostenaufwand soll sich dabei im Übrigen auf ganze sechs Dollar belaufen haben.

Vor dem Hintergrund dieses Falls und angesichts der enormen Rechenkapazitäten eines Cloud-Computing-Anbieters wie Amazon darf man berechtigterweise die Frage stellen, ob dessen Ressourcen für illegale Zwecke missbraucht werden können bzw. wie genau das verhindert werden kann. Denn wer braucht noch Botnetze, wenn große Rechenkapazitäten mit Angeboten wie den Amazon Web Services (AWS) bei relativ geringem Aufwand und zu relativ geringen Kosten bedarfsgerecht angemietet werden können?

Amazon selbst mag sich mit solchen Fragen scheinbar nicht beschäftigen – zumindest nicht in aller Öffentlichkeit. Auf eine Anfrage von IT-MITTELSTAND nach einem sachkundigen Ansprechpartner, der sich zu Sicherheitsaspekten der angebotenen Services äußern könnte, reagierte der Cloud-Spezialist sofort. Binnen weniger Stunden stellte Amazon-Sprecherin Kay Kinton über zwanzig Seiten an Hintergrundmaterial zu den AWS zur Verfügung. Auf die explizite Nachfrage, wie der Anbieter den Missbrauch seiner Services für illegale Zwecke wie DoS-Attacken gegenüber Unternehmen verhindern wolle, reagierte die Sprecherin

allerdings nicht einmal mehr mit einem Standardschreiben...

Es soll an dieser Stelle nicht erörtert werden, ob es klug ist, unangenehmen Pressefragen mit der Vogel-Strauß-Taktik zu begegnen. Stattdessen muss zugestanden werden, dass die Kontrollmöglichkeiten der Service Provider gegenüber Inhalten auf von ihnen vermieteten Servern beschränkt sind. Rechtsanwältin Dr. Selina Karvani, Partnerin der Rechtsanwälte Wienke & Becker in Köln, erklärt: „Ein Zugriff des Anbieters auf die von Nutzern hinterlegten nicht öffentlichen Daten dürfte – ausgehend von deutschem Rechtsverständnis – nicht zulässig sein.“ Entsprechende Ermächtigungsgrundlagen sehe das deutsche Recht unter bestimmten Voraussetzungen zwar für öffentliche Behörden wie Staatsanwaltschaft oder Polizei, grundsätzlich aber nicht für sonstige Personen vor.“

Darüber hinaus gibt Dr. Karvani zu bedenken, dass im Bereich des Cloud Computing noch viele komplexe Rechtsfragen, unter anderem zur IT-Sicherheit und zum Datenschutz, ungeklärt sind. Dennoch werde ein Cloud-Computing-Anbieter im Rahmen von Verkehrssicherungspflichten die Aufgabe haben, „zumutbare“ Maßnahmen zu treffen, die Angriffe auf Server verhindern können. Inwiefern Amazon dem nachkommt, bleibt zunächst ungeklärt.

Andere Cloud-Computing-Anbieter zeigen dem unangenehmen Thema gegenüber weniger Berührungsängste. Google bietet beispielsweise ebenfalls einen Service für das Cloud Computing an, die Google App Engine, die Entwicklern und Unternehmen die Möglichkeit gibt, insbesondere I/O-lastige Applikationen kurzfristig auszulagern und auf den Servern von Google zu betreiben. Im Gegensatz zu den Amazon Web Services werden dabei jedoch keine virtuellen Server zur Verfügung gestellt, die einen Zugriff auf die Betriebssystemebene zulassen, was die Möglichkeiten des Missbrauchs stark einschränkt. Zudem unterstützt die Plattform ausschließlich Applikationen auf Basis der Programmiersprachen Java und Python, was laut Experten ebenfalls weniger Spielraum bei der Zweckentfremdung des Services lässt, wenn es etwa um Tools geht, die DoS-Attacken ausführen sollen.

Auf die Frage nach Maßnahmen zur Verhinderung des Missbrauchs der Google App Engine antwortet Kai Gutzeit, Head of Google Enterprise für die DACH-Region und den Bereich Nordics, freimütig: „Jede Applikation, die auf der App-Engine-Infrastruktur läuft, muss vorab mit einem per SMS versandten Code aktiviert werden. Dies vereinfacht die spätere Zuordnung der Applikationen zu „realen Personen" und soll potentielle Entwickler schädlicher Software abschrecken. Durch die Limitierung der Ressourcen auf 500 MB und die bei einer Benutzung jenseits dieser Quotas entstehenden Kosten kann die Gefährdung durch Hacker zudem weitgehend ausgeschlossen werden.“ – Das beruhigt.

itmittelstand.de 29.09.10