Cybercrime: Shops kontra DDoS

VON GERALD FIEBIG

Quelle: Fotolia © V. Yakobchuk

Schlagzeilen machen Angriffe zum Blockieren von Webseiten meist bei politischen Protestaktionen. Aber auch im schmutzigen Tagesgeschäft der Internetkriminalität werden immer wieder Shopbetreiber mit Blockaden erpresst: Ein Erfahrungsbericht einer Shop-DDoS-Attacke.

Michael Büchel_
Kriminaloberkommissar (Kriminalfachdezernat 2, Nürnberg).

Johannes Klinger_
Vorstandsvorsitzender beim E-Commerce-Dienstleister Websale.

Websale betreibt für rund 300 Versandhändler etwa 550 verschiedene Onlineshops, stellt dabei die Software und hostet diese auch für die Shops ihrer Kunden. Im September 2010 wurden Websale-Shops Opfer eines Distributed Denial of Service (DDoS). Bei dieser „verteilten Dienstblokkade“ nutzen Cyberkriminelle so genannte Botnetze, die per Fernsteuerung Zehntausende und mehr Anfragen pro Sekunde an einen Webserver schicken, bis dieser unter der abnormen Rechenlast zusammenbricht. Botnetze sind Verbünde aus Hunderten, Tausenden oder mehr Rechnern, die meist mittels Virensoftware ohne Wissen der Besitzer zu einem Netz zusammengeschlossen wurden. Kriminelle können solche Angriffs-Netze sogar von zwielichtigen Anbietern für ihre Zwecke mieten. Der Angriff auf einige der Websale-Shops im September 2010 begann am Wochenende. Das Technikteam wurde vom automatischen Warnsystem sofort alarmiert und konnte nach einigen Arbeitsstunden mit hauseigenen Mitteln die Stärke des Angriffs so weit abschwächen, dass die Shops wieder erreichbar waren. Im Laufe der nächsten Tage wurde der Angriff schwächer und dann eingestellt. Zur Tagesordnung übergehen wollte man bei Websale nach dieser Heimsuchung jedoch nicht. „Wir haben nicht nur unsere Kunden, die Versandhäuser, informiert, sondern sofort auch die Polizei eingeschaltet“, berichtet Johannes Klinger, Vorstandsvorsitzender von Websale. „Unklar war jedoch das Ziel des Angreifers, da mehrere Shops betroffen waren, von deren Betreibern aber keiner ein Erpresserschreiben erhalten hatte. Und damit verbunden war die Frage: Wird sich die Attacke wiederholen?“

Im Gespräch mit dem zuständigen Dezernat der Polizei wurde deutlich, dass sich ein ähnlicher Angriff im Zusammenhang mit einer Erpressung von Shopbetreibern jederzeit wiederholen könnte. Die Erpressung von Onlinehändlern „läuft immer wieder“, sagt Kriminaloberkommissar Michael Büchel, der als Cybercrime-Experte beim Kriminalfachdezernat 2 in Nürnberg die Ermittlungen übernahm. DDoS-Attacken dieser Art kämen zwar „nicht täglich“ vor, seien aber „durchaus gängig“. Büchel vermutet, dass viele betroffene Händler aus Angst vor Imageverlusten nicht über DDoS-Angriffe und Erpressungen sprächen.

> ONLINESHOPS IN GEFAHR

Vom Gang zur Polizei sollte diese Erwägung aber niemanden abhalten, beruhigt Büchel. Da die Anzeigen diskret behandelt werden, sei kein Imageschaden zu befürchten. „Onlineshops sind beliebte Ziele. In den seltensten Fällen verfügen die Betreiber selbst über genügend technisches Know-how, um Shops und Server individuell zu konfigurieren, regelmäßig upzudaten oder mit Abwehrtechnik zu schützen“, warnt Büchel. „Zusätzliche Gefahren zur DDoS-Anfälligkeit drohen, weil Shops oft mit veralteten Versionen betrieben werden. Wenn es sich um eine verbreitete Software mit ihren bekannten Schwachstellen handelt, haben Angreifer leider leichtes Spiel, weil sie diese Lücken ohne weiteres immer wieder ausnutzen können.“

Die Analyse des Angriffs zeigte, dass nicht das Ziel war, in die Shops einzudringen, sondern – typisch für einen DDoS-Angriff – sie lahmzulegen. Der Angriff war in diesem Fall abgewehrt, doch in Sicherheit wiegen wollte sich Websale als Softwarehersteller und Shop-Hoster trotzdem nicht, so Johannes Klinger. „Das hätte für uns geheißen, den Kopf in den Sand zu stecken. Deshalb ist es zumindest für uns keine Option, einen angegriffenen Shop einfach nur abzuschalten, um die anderen zu schützen, wie es in der Praxis fast immer gemacht wird."

> WIE MAN SICH WEHREN KANN

Herkömmliche Firewalls sind gegen DDoS-Angriffe kein wirksamer Schutz, weil sie für andere Aufgaben entwickelt werden und nur bestimmte Arten von schädlichen Datenanfragen an einen Server analysieren und wegfiltern können, sodass die Angriffe trotz Firewall auf das Zielsystem durchschlagen und es blockieren. Außerdem „verstopft" die enorme Menge der Zugriffe bei einem DDoS-Angriff häufig die Filter – die Firewall ist blockiert, und damit wird das Zielsystem ebenso blockiert. „Aufgrund dieser Sachlage haben wir uns intensiv nach DDoS-Abwehrmöglichkeiten umgesehen, die auf dem Markt verfügbar sind", berichtet Klinger. Dabei fanden sich einmal Online-Anbieter wie etwa www.blockdos.net oder www.verisigninc.com, zu denen ein angegriffener Shopbetreiber mit entsprechenden technischen Kenntnissen seinen Traffic umleiten kann, um ihn filtern zu lassen. Klinger zufolge reichen die Kosten dabei je nach Datenaufkommen von einigen Hundert bis zu etlichen Tausend Euro pro Monat. Für Websale erschien dies wegen der schwer kalkulierbaren Kosten unbefriedigend, denn ein starker Angriff kann auch beim kleinsten Shop riesige Datenmengen und damit hohe Kosten produzieren. Außerdem wäre damit gerade mal ein Shop geschützt. DDoS-Schutzsysteme werden auch als Kauflösungen in einer Kombination aus Hardware und Software angeboten. Bei Recherchen zu dem Thema findet man viele Hersteller, die mehr oder weniger effektive Systeme anpreisen. „Wir haben eine Kauflösung in Erwägung gezogen, standen aber vor dem Problem, dass wir nur Prospektwerte und Vertriebsaussagen hatten. Die effektive Wirksamkeit während eines echten Angriffs in unserer Systemumgebung war unklar", erinnert sich Klinger. „Wie also soll die tatsächliche Wirksamkeit so eines Systems, bei dem die Einstands- und Updatekosten für die bei uns zu schützende Bandbreite exorbitant hoch sind, aussagekräftig in einer Produktivumgebung getestet werden?"

WAS SIND EIGENTLICH...?

Als Denial of Service
(kurz DoS, englisch für: Dienstverweigerung oder -ablehnung) wird in der digitalen Datenverarbeitung die Folge einer Überlastung von Infrastruktursystemen bezeichnet. Dies kann durch unbeabsichtigte Überlastungen verursacht werden oder durch einen mutwilligen Angriff auf einen Host (Server), einen Rechner oder sonstige Komponenten in einem Datennetz. Wird der DoS mutwillig herbeigeführt, geschieht dies in der Regel mit der Absicht, einen oder mehrere bereitgestellte Dienste arbeitsunfähig zu machen. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von verteilter Dienstblockade oder englisch Distributed Denial of Service (DDoS). Die wohl prominentesten DDoS-Attacken der jüngsten Vergangenheit fanden vom 6. bis 8. Dezember 2010 statt, als als Reaktion auf Sperrungen von WikiLeaks-Konten bei der PostFinance wie auch bei den Zahlungsdiensten MasterCard, Visa, PayPal und Amazon deren Webseiten angegriffen und zeitweise in die Knie gezwungen wurden. (Quelle: Wikipedia)

Am 13. November 2010 zeigte sich, dass Websale mit seiner Vorabauswahl die Zeichen der Zeit richtig gedeutet hatte: Mitten im Vorweihnachtsgeschäft wurde erneut ein Server angegriffen. Schnell wurde klar, dass diesmal die Erpressung eines Shopbetreibers vorlag. Ein Websale-Kunde hatte kurz vor dem Angriff eine E-Mail mit eindeutigem Inhalt erhalten, die er zunächst für einen schlechten Scherz hielt. Darin wurde er aufgefordert, 500 Euro zu zahlen. Andernfalls werde sein Shop lahmgelegt – zunächst stundenweise, dann länger, bis zum kompletten Ausfall. Solche gering anmutenden Erpressungssummen sind nicht unüblich, weiß Cybercrime-Experte Büchel. Bei solchen Summen beißen Erpressungsopfer eher in den sauren Apfel und bezahlen den geforderten Preis – in der Hoffnung, dann Ruhe zu haben. Das jedoch sei ein Fehler, meint Büchel. Wenn der Täter sieht, dass das Opfer sich erpressen lässt, sei die Wahrscheinlichkeit groß, dass die Erpressung immer wieder stattfindet. Da der Angriff eine enorme Stärke erreichte, trat eine massive Systembeeinträchtigung auf und der Shop war offline, wie angekündigt zunächst für die Dauer einer Stunde. Der Ernstfall war wieder eingetreten. Kurzentschlossen orderte Websale das als am besten geeignet ausgewählte Gerät per Eilfracht aus den USA. Die Angriffe setzten sich mit steigender Häufigkeit fort, und die Abwehrmaßnahmen mit vorhandenen Mitteln konnten nur Teilerfolge erzielen. Kurz nachdem das Gerät eingetroffen und installiert war, ging der Angriff in eine besonders heiße, drei Tage dauernde Phase. Der gewünschte Abwehreffekt, den Schadtraffic so massiv abzuschwächen, dass normales Bedienen und Bestellen im Shop möglich war, konnte dennoch während der ganzen Zeit voll erreicht werden. Somit konnte sowohl der Betrieb des betroffenen Shops als auch des ganzen Rechenzentrums reibungslos weiterlaufen. Knapp drei Tage nach der Inbetriebnahme des Schutzsystems gab der Angreifer auf. „Die Ergebnisse", so Klinger, „waren so hervorragend, dass wir uns entschlossen haben, vorsorglich sämtliche bei uns gehosteten Shops unter diesen DDoS-Schutzschirm zu nehmen und so die Gefahr der Erpressbarkeit der Websale-Versandhändler zu bannen. Die Investition für Anschaffung, Installation, Updating und Betrieb dieses Systems liegt pro Jahr im sechsstelligen Bereich. Der betroffene Shopbetreiber hätte das vermutlich nicht stemmen können – ebenso wie viele andere mittelständischen Versandhändler", sagt Klinger. „Seit Dezember konnten wir alle Händler, die an einem schnellen Schutz interessiert waren, schützen. Und seit dem 1. Februar genießt jeder der Shopbetreiber bei uns diesen Schutz vor Cyberkriminalität." ■

> ***Kennziffer: ecm21852***