Grafik: akindo / iStock.com

Dossier
DDoS-Attacken

In Kooperation mit **Aspectra**

Ein Schutzschild gegen DDoS-Attacken

osc. Wenn massenhafte Anfragen aus dem Internet Server und die auf ihnen gehosteten Websites und Dienstleistungen in die Knie zwingen, steckt nicht selten eine Distributed-Denial-of-Service-Attacke (DDoS) dahinter. Cyberkriminelle nutzen diese Angriffe, um bestimmte Websites möglichst lange lahmzulegen und den dahinterstehenden Unternehmen und Organisationen Schaden zuzufügen. Wie Analysten in letzter Zeit herausgefunden haben, ermöglichen kurze DDoS-Attacken aber auch, Hackerangriffe unbemerkt durchzuführen. Die Eindringlinge gehen dann im Rauschen der Attacke quasi unter.
Welche Gefahren durch DDoS-Angriffe sonst noch drohen, wie sich Unternehmen dagegen rüsten können und wie man «guten» von «schlechtem» Netzwerk-Traffic unterscheidet, erklärt Kaspar Geiser, Geschäftsführer von Aspectra, auf den folgenden Seiten.

Cyberangriffe vor den Front-Routern abwehren

Cyberattacken sind gemäss Nachrichtendienst des Bundes neben Terrorismus die Hauptgefahr für die Schweiz. Der Schutz vor Cyberattacken bedingt Abwehrszenarien «im Grossen» wie «im Kleinen». Wirksamen Schutz bieten im Rechenzentrum betriebene Boxen, die den Internetverkehr analysieren und einen Angriff vor den sogenannten Front-Routern abwehren.

DER AUTOR

Kaspar Geiser
Geschäftsführer,
Aspectra

Distributed-Denial-of-Service-Attacken, kurz DDoS-Attacken, sind gefürchtet. Die Überlastungsangriffe legen Websites, Onlinedienste und Server lahm, indem sie ein Internetangebot so lange aufrufen, bis es zusammenbricht. DDoS-Attacken kommen von tausenden Systemen irgendwo im Internet. Sie sind deshalb nur schwer vom normalen Datenverkehr im Internet zu unterscheiden. Woher DDoS-Attacken kommen und wie sie orchestriert werden, ist selten eruierbar. Die Angreifer verteilen sich über die ganze Welt und werden gezielt für die Angriffe ausgewählt. Würde ein Angriff auf ein Schweizer Finanzinstitut beispielsweise nur aus Kenia stattfinden, wäre das a) offensichtlich und b) mit einem einfachen Geoblocking mitigierbar.

Gefährlich sind DDoS-Attacken, weil es schwierig ist, sie überhaupt als solche zu erkennen. Die Medien berichteten in den letzten Jahren vor allem über die grossen und lange anhaltenden Angriffe. Neuere Attacken zielen aber häufig auf E-Mail- oder DNS-Server und nicht mehr unbedingt auf eine eigentliche Website. Bei betroffenen Unternehmen werden dann etwa Bestellungen nicht mehr automatisch via E-Mail bestätigt oder E-Banking-Log-in-Seiten sind im Browser nicht mehr auffindbar. Es folgen «Phishing E-Mails», in denen sich das Unternehmen für den Teilausfall entschuldigt und die Kunden bittet, ihre Angaben nochmals einzugeben – dann allerdings auf einer Seite des Angreifers.

Die Überlastungsangriffe legen Websites, Onlinedienste und Server lahm, indem sie ein Internetangebot so lange aufrufen, bis es zusammenbricht.

Sicherheitsarchitektur

Die Angriffsszenarien sind vielseitig und erfordern deshalb ausgeklügelte Sicherheitsarchitekturen. Kritische Anwendungen aus dem eigenen Rechenzentrum auszulagern, bietet besseren Schutz, da Serviceprovider oder Public Clouds über entsprechende Dienste verfügen. Mit dem Auslagern sind aber Schwierigkeiten verbunden, etwa was den Standort der Datenhaltung anbelangt oder den Weg, der eine Anfrage zwischen Kunde und Anbieter zurücklegt. Schützt man sich über einen vorgelagerten Proxy, etwa einer Web Application Firewall eines Content Distribution Networks, gibt man einen Teil des Steuers aus der Hand. So steht mindestens der DNS, meist aber auch die TLS/SSL-Terminierung ausserhalb des bekannten Perimeters und ist nicht selten über die ganze Welt verteilt.

Grafik: Neyro / Fotolia.com

Ein anderer Architekturansatz implementiert den kritischen Internetverkehr über ein zentrales Element mit einem Partner vor Ort, der diesen Dienst in und aus der Schweiz bewerkstelligt.

Der Schutz vor den Front-Routern

Doch auch ein zentraler Schutz hat Grenzen: Sind die Ressourcen an Bandbreite ausgeschöpft, kann auch dieser ungenügend sein. Ein solch zentraler Schutz kennt typischerweise mehrere Zustände: a) kein Angriff, b) ein Angriff, der mit lokalen Ressourcen mitigiert wird, c) ein Angriff, der mit lokalen Ressourcen nicht mitigiert werden kann.

A) Kein Angriff

Genau genommen wird man permanent angegriffen. Es stellt sich eher die Frage, ob man den Angriff feststellt und ob dieser Schaden

Grafik: Choo Studio / shutterstock.com

anrichtet oder zu viele Ressourcen bindet. Denn Cyberschutz besteht nicht nur aus Abwehr von Attacken, sondern auch aus dem minutiösen Aufzeichnen des Verhaltens aller Verbindungen. Die Auswertungen bestimmen die Trigger, die gesetzt werden, wie zum Beispiel das Sperren einer Quelle. Serviceprovider bieten ihren Kunden idealerweise Zugang zu diesem Monitoring. So arbeiten sie nicht nur transparent, sondern sensibilisieren ihre Kunden auch für mögliche Gefahren.

B) Angriffe, die mit lokalen Ressourcen mitigiert werden

Serviceprovider verfügen immer über mehrere Internetleitungen. Jede einzelne Leitung schützen sie separat, idealerweise noch vor den sogenannten Front-Routern. Dabei wird der Verkehr nach verschiedenen Kriterien analysiert und im Bedarfsfall abgewehrt. Der Vorteil: Der Internetverkehr zwischen Kunden und Unternehmen nimmt immer den gleichen Weg und wird nicht umgeleitet über externe Systeme, die unter Umständen im Ausland verteilt sind. Der Nachteil: Ein solcher Schutz ist abhängig von den Ressourcen des Serviceproviders bei seinen Internetlieferanten.

C) Angriffe, die mit lokalen Ressourcen nicht mitigiert werden können

Jede Internetanbindung ist limitiert. Sind bei einem Angriff alle Internetlinks ausgelastet, muss die Mitigation des Angriffs im Internet selbst stattfinden. Das betroffene IP-Netzwerk (mindestens 255 IP-Adressen) wird dann nicht mehr vom Serviceprovider im Internet angepriesen, sondern von einem CDN (Content Delivery Network), etwa Akamai. CDN-Provider verfügen im Verhältnis zum Serviceprovider über beinahe unendliche, global verteilte Ressourcen, weshalb ein Angriff für einen CDN-Provider einfacher zu bewältigen ist. Im CDN werden offensichtliche Angriffspakete, wie Angriffe auf Ports oder Protokolle zurückgehalten. Zwischen CDN und Serviceprovider besteht eine gesicherte und isolierte direkte Verbindung. Über diese Leitung gelangen dann die «guten» Anfragen zum Serviceprovider. Dieser «White Traffic» wird beim Serviceprovider erneut geprüft und danach von der Anwendung beantwortet. Bei diesem Verfahren wird der Internetverkehr in keinem Fall im Ausland oder im CDN aufgebrochen oder terminiert. So bleiben auch DNS und Zertifikate voll und ganz in der Hand des lokalen Serviceproviders.

Um sich vor massiven Attacken zuverlässig zu schützen, sind mehrstufige Konzepte notwendig.

Cyberattacken finden dauernd statt

Keine Organisation und keine Website ist vor Angriffen gefeit. Um sich vor massiven Attacken zuverlässig zu schützen, sind mehrstufige Konzepte notwendig. Für maximale Handlungs- und Analysemöglichkeiten empfiehlt sich ein zentraler, lokaler Schutz, der DDoS-Attacken mitigiert und den «guten» Verkehr an die zu schützende Anwendung weiterleitet. Idealerweise werden der lokale Schutz und die Anwendung beim selben Serviceprovider betrieben. Alternativ verfügt der Serviceprovider über entsprechend gesicherte Verbindungen zur Anwendung, wodurch die Anwendung auch in einer Public Cloud betrieben werden kann.

« Die Attacken werden kürzer und gezielter »

Cybergefahren kommen nicht nur in Form von Viren, Würmern oder Ransomware daher. Auch die Überlastung von Datennetzen mittels DDoS-Attacken stellt eine Bedrohung dar. Im Interview erklärt Kaspar Geiser, Geschäftsführer von Aspectra, wie sich Unternehmen dagegen wappnen können. Interview: Oliver Schneider

Wie funktionieren die von Ihnen erwähnten Boxen, die DDoS-Attacken schon vor dem Router abfangen sollen?
Kaspar Geiser: Diese Boxen erkennen eine Vielzahl von bekannten Mustern wie «TCP/UDP/ICMP Flood Attacks», «Malformed Packets», «Smurf Attacks» oder aber auch «SSDP und DNS Amplification». Mit der Abwehr dieser Attacken werden die Router und dahinterstehenden Ressourcen geschont und diese können so auch unter Attacke «normal» arbeiten. Auch heuristische Analysen werden angewendet, um Layer-1- bis -4-Attacken abzuwehren.

« Bekannte Fälle waren politischer Natur und betrafen die Schweiz und Österreich vor und während Besuchen von ranghohen Regierungsvertretern in oder aus Asien. »

Kaspar Geiser, Geschäftsführer, Aspectra

Kaspar Geiser, Geschäftsführer, Aspectra

Wie haben sich DDoS-Attacken Ihrer Erfahrung nach in den letzten Jahren verändert?
Die Attacken werden kürzer und gezielter. Wo früher ein manuelles Eingreifen ausreichte, muss heute mit Automatismen der Schutz sofort aktiv werden.

Wer steckt hinter den DDoS-Angriffen?
Es gibt nur wenige Fälle, die von Melani und anderen Stellen kommentiert werden. Bekannte Fälle waren politischer Natur und betrafen die Schweiz und Österreich vor und während Besuchen von ranghohen Regierungsvertretern in oder aus Asien.

Welche Art von Firmen sind besonders anfällig für DDoS-Attacken?
Leider alle. Grossfirmen und reine Internetfirmen haben die Gefahr teilweise bereits erkannt und schützen sich. KMUs oder Vereine sind sich der Gefahr zwar bewusst, können aber die Tragweite selten abschätzen. Neben DDoS-Attacken gibt es eine Vielzahl an weiteren Angriffs- und Manipulationsmöglichkeiten. Hier lauern noch viele Gefahren für Firmen.

Was raten Sie KMUs, um ihre IT-Systeme vor DDoS-Attacken zu schützen?
DDoS-Attacken sind eine reelle Gefahr. Um einen umfassenden und auf die verschiedenen Gefahren abgestimmten IT-Schutz eines Unternehmens zu erlangen, empfehlen wir die Zusammenarbeit mit Managed-Service-Providern. Eine Auslagerung oder mindestens Aufteilung der IT in «interne» und «externe» IT-Infrastruktur ist ebenfalls ratsam, um die Risiken und Schutzmassnahmen zu verteilen, beziehungsweise gezielt zu implementieren.

Wie merkt ein Hoster, ob eine DDoS-Attacke stattfindet oder einfach nur viel Traffic im Netzwerk herrscht?
Dies bedingt die Korrelation verschiedener Parameter des Netzwerks: über das Betriebssystem bis hin zur Anwendung und die damit involvierten Schutzstufen wie Firewall und WAF. Bei einer DDoS-Attacke weisen diese Parameter Anomalien auf, da eine DDoS-Attacke nie perfekt ist. So steigt beispielsweise die Anzahl Anfragen von einer Quell-IP-Adresse bei Attacken überproportional an, was ein Indiz sein kann. Um Attacken zu erkennen, sind Hoster auf umfangreiche Security-Information-and-Event-Management-Lösungen, kurz SIEM, angewiesen. Diese Systeme dienen der Analyse oder der automatischen Auslösung von Massnahmen.