clavister WhitePaper

Clavister DoS- und DDoS-Protection

Wie man sich mit Clavister gegen DoS- und DDoS-Attacken schützen kann

Übersicht

Denials of Service (DoS, zu Deutsch: „blockierte Dienste“)-Attacken verfolgen, wie der Name bereits vermuten lässt, das Ziel, Services zu unterbrechen oder komplett zu blockieren. Viele Nutzer kennen die Abkürzung DoS oder DDoS hauptsächlich aus Artikeln, die von Überlastangriffen auf prominente Webseiten berichten – doch die Attacken sind viel umfangreicher. DoS- und DDoS-Angriffe treten in verschiedenen Formen auf und können ein ganzes Unternehmen bzw. dessen Geschäfte lahmlegen. Die negativen Folgen reichen von Produktivitätseinbußen bis hin zu enormen Umsatzeinbrüchen.

DoS- und DDoS-Attacken sind mittlerweile weit verbreitet, und die Anzahl betroffener Unternehmen steigt auf dramatische Weise an. Somit können diese Angriffe als Teil des täglichen IT-Lebens betrachtet werden, denn jeder Internetnutzer ist ein potenzielles Opfer.

Heutzutage gibt es spezielle „Off-the-Shelf“-Tools, mit denen die Attacken einfacher ausgeführt und noch bösartiger gestaltet werden können. Beispielsweise lassen sich so Funktionen zur Verwendung sogenannter Botnets integrieren, um die Angriffe noch zielgerichteter zu koordinieren (Distributed Denial of Services, DDoS). Auf diese Weise sind Attacken in der Regel schwerer zu bekämpfen und dadurch umso wirkungsvoller.

In diesem Whitepaper erklären wir die verschiedenen Konzepte und Technologien, die hinter diesen Attacken stecken. Zudem beleuchten wir, welche Sicherheitslücken und Schwachstellen am häufigsten von Hackern ausgenutzt werden und wie man sich wirksam vor solchen Bedrohungen schützen kann.

DoS und DDoS: ein exponentiell wachsendes Problem

Um zu verstehen, welchen Umfang DoS- und DDoS-Attacken mittlerweile erreicht haben, sollte man zwei wesentliche Faktoren betrachten: die Anzahl der Angriffe und deren Komplexität. Die Wahrscheinlichkeit, von einer solchen Attacke betroffen zu sein, ist höher denn je, und die Folgen sind schwerwiegender. Erhöhen sich diese Faktoren weiterhin in gleichem Maße, wächst auch das Problem exponentiell an und wahrscheinlich vielen Nutzern über den Kopf.

Hinzu kommt, dass auch die meisten Studien ein Wachstum in puncto Häufigkeit und Umfang aufzeigen. Ein bekanntes Serviceunternehmen, das sich mit der Verminderung von DoS-Attacken beschäftigt, veröffentlichte 2013 einen Report, der eine um 18 % gestiegene Anzahl der Angriffe im vierten Quartal verdeutlichter. Gleichzeitig nahm die Größe dieser Attacken um 84 % zu (d.h. die durchschnittliche Größe der Pakete, die während eines Angriffs in der Spitze pro Sekunde übermittelt werden).

Das derartig stark wachsende Problem von DoS- und DDoS-Attacken unterstreicht die Notwendigkeit einer gut durchdachten Strategie, wie man im Falle eines Angriffs reagieren und mit einer solchen Krisensituation umgehen sollte

Gelegenheit macht Diebe! Gilt das auch bei DoS-/DDoS-Attacken?

DoS- und DDoS-Angriffe gibt es schon fast so lange wie das Internet, doch sie flogen lange Zeit unter dem Radar, was daran liegt, dass vielen Hackern anfangs das Fachwissen für eine erfolgreiche Ausführung dieser IT-Attacken fehlte.

Ein Faktor, der zur dramatischen Vermehrung dieser Bedrohungen beitrug, sind spezielle Tools, mit denen DoS-Attacken kreiert werden können. Diese Werkzeuge waren und sind noch immer leicht zugänglich und sogar ohne Fachkenntnisse einfach anzuwenden.

Der Grund, warum sich auch die Anzahl von Paketen pro Sekunde während eines Angriffs vermehrt hat, beinhaltet viele Faktoren. Zum einen stehen immer mehr Web-, Internet- bzw. Computer-Ressourcen für eine Erstellung dieser Attacken bereit. Zum anderen, und das ist wahrscheinlich der wichtigste Grund, wurden die Tools zum Koordinieren der Angriffe noch leichter zugänglich. Im Rahmen dieser Attacken arbeiten mehrere Systeme immer besser zusammen. Diese Netzwerke an Maschinen, die bei DDoS-Angriffen genutzt werden, werden auch als Botnets bezeichnet und können heutzutage sogar zu niedrigen Konditionen angemietet werden.

Im Gegensatz zu vielen anderen Angriffsarten, die in der Regel von organisierten Kriminellen mit finanziellen Interessen durchgeführt werden, sind DoS- und DDoS-Attacken immer häufiger ein Ausdruck von Unzufriedenheit oder eine Form von Vergeltung seitens des Hackers gegenüber eines Unternehmens.

Organisierte Kriminalität mit finanziellem Interesse tritt in diesem Zusammenhang meist nur als Anbieter bzw. Vermieter einer Botnet-Infrastruktur in Erscheinung. Diese Kriminellen verfolgen lieber das Ziel, Tausende Computer auf einmal mit Trojanern zu infizieren. Die infizierten Maschinen, genannt Zombies, im Rahmen der gemieteten Infrastruktur können vom Mieter genutzt werden, um DDoS-Angriffe zu koordinieren bzw. durchzuführen.

Das organisierte Verbrechen hat ein finanzielles Interesse an großen Mengen infizierter Computer und ebenso daran, Angriffs-Tools noch besser, noch zugänglicher oder noch einfacher zu machen. Denn mehr Angriffe führen zu einem höheren Einkommen.

All das bedeutet, dass manche Menschen, die unzufrieden mit der Meinung oder dem Verhalten eines Unternehmens sind, leichter und aggressiver „Rache“ nehmen können.

Verschiedene Arten von DoS- und DDoS-Attacken

Um sich effektiv gegen diese Bedrohungen zu schützen, muss man verstehen, wie sie entwickelt wurden, welche Systeme normalerweise angegriffen werden und in welcher Art und Weise die Angriffe stattfinden. Man sollte auch hinterfragen, wie sehr DoS- und DDoS-Attacken Infrastrukturen schaden können, welche Netzwerkkomponenten Schwachstellen repräsentieren und wie einzelne Unternehmen via Domino-Effekt lahmgelegt werden können – z.B. nur durch den Angriff auf einen öffentlichen Web-Server.

DoS- und DDoS-Attacken lassen sich in der Regel in verschiedene Gruppen einteilen (siehe Liste „Die häufigsten Varianten von DoS- und DDoS-Attacken“).

Da jede Angriffsart ein anderes Vorgehensmuster verfolgt, muss man auf verschiedenen Wegen einen angemessenen Schutz erzeugen, um die negativen Auswirkungen abzumildern.

Die häufigsten Varianten von DoS- und DDoS-Attacken sind:

Angriffe, die Services überlasten:

- Angriffe, die eine Überlastung der Internetverbindung erzeugen,
- Angriffe, die gezielt eine Überlastung von Computern oder Anwendungen/Services erzeugen.
- Angriffe, die gezielt eine Überlastung der Schwachstellen in einer Netzwerkinfrastruktur erzeugen.

Angriffe, die einen Service stören oder zum Absturz bringen, ohne ihn zu überlasten:

- Angriffe, die Sicherheitslücken in Anwendungen ausnutzen, um Services auszuschalten,
- Angriffe, die Konfigurationen verändern, um einen Service zu stören,
- Angriffe, die den herkömmlichen Datenverkehr stören, indem sie unerwünschte Nachrichten senden, die Verbindungen der Nutzer auflösen.

Die Internetverbindung überlasten

Angriffe, bei denen die Datenmenge die Kapazität der Internetverbindung des Opfers übersteigt, haben oftmals verheerende Folgen, z.B. weil Kunden und externe Nutzer nicht mehr auf die zahlreichen öffentlichen Services eines Unternehmens zugreifen können. Doch auch für die internen Nutzer entstehen Probleme, weil Systeme, die sich außerhalb ihres Netzwerks befinden, plötzlich nicht mehr zugänglich sind (z.B. Cloud-basierende Systeme wie Office365 oder Salesforce).

Um genügend Traffic und eine Überlastung der Internetverbindung zu erzeugen, müssen viele Computer an einem koordinierten Angriff teilnehmen. Abhängig von der Bandbreitenkapazität und Angriffsweise könnten ein paar Hundert, aber auch mehrere Tausend Computer beteiligt sein. Solche groß angelegten Angriffe sind nur sehr schwer zu stoppen und gleichzeitig einfach durchzuführen, wenn der Angreifer Zugang zu einem Botnet hat.

Auch wenn dieses Angriffsmuster womöglich nicht das am häufigsten auftretende ist: Die Schwere der Folgen ist ein guter Grund, über IT-Strategien zur Abmilderung nachzudenken. Darüber hinaus haben DDos-Angriffe nochmals neue Formen angenommen: Wo vorher noch Botnets mit großen Mengen von Nutzern bevorzugt wurden, geht der Trend nun zu kleineren Netzwerken mit leistungsstärkeren Hosts, die eine höhere Bandbreite besitzen. Fragt man die Hacker selbst, würden sie jederzeit einen leistungsstärkeren Rechner vorziehen, speziell bei komplizierteren Attacken.

Überlastete Schwachstellen in der Netzwerkinfrastruktur

Viele Organisationen verwenden aus praktischen und Sicherheitsgründen eine einzelne Schicht aus Firewalls, die sowohl die Public Services in der DMZ (Demilitarized Zone) als auch die privaten Services in diversen internen Netzwerken absichert. Zusätzlich könnte man die Firewall als Haupt-Router für die internen Netzwerke nutzen. Solche Architekturen sollten stetig auf potenzielle Schwachstellen überprüft werden. Man kann auf diese Weise nachvollziehen, wie sich eine DoS-Attacke gezielt an öffentliche Services richtet und nebenbei das gesamte Netzwerk und alle Nutzer lahmlegen kann.

Wenn eine unzureichend dimensionierte Firewall, ein Router oder ein anderes zentrales Netzwerkequipment von einer DDos-Attacke über das Internet überlastet wird, ist auch der Verkehr in den internen Netzwerken betroffen. Hier sind einige Beispiele, wie sich solche Angriffe in der Praxis bemerkbar machen:

- VPN-Verbindungen sind getrennt,
- VoIP-Calls haben schlechte Qualität oder sind nicht möglich,
- interner Datenaustausch läuft langsam oder ist nicht möglich,
- interne Anwendungen und Services laufen langsam oder sind blockiert,
- externe Services laufen langsam, oder es ist kein Zugriff über interne und externe Netzwerke möglich,
- der Zugriff auf E-Mails verlangsamt sich oder ist nicht möglich,
- Backup- und Protokolldaten, die zwischen verschiedenen Segmenten der Firewall gesendet werden, laufen langsam oder funktionieren nicht mehr

Firewalls werden fälschlicherweise häufig so dimensioniert, dass der Datenverkehr nur mit einem kleinen Teil der Sicherheitsfunktionen verwaltet werden kann. Nimmt das Unternehmen neue Services in Betrieb, werden mehr Funktionen aktiviert. Dies erhöht wiederum die Netzkapazität, die womöglich nicht in der Lage ist, die Last, die im Rahmen eines Angriffs erzeugt wird, zu tragen.

Sind UTM- und NGFW-Firewalls anfälliger für DoS-Attacken?

Viele Unternehmen entscheiden sich für ein Software-Upgrade und fügen UTM- und NGFW-Funktionen hinzu, z.B. Application Control, IPS und ähnliche Sicherheitsfunktionen. Diese zusätzlichen Features sollten jedoch kontrolliert und mit Bedacht hinzugefügt werden.

Je mehr Funktionen aktiviert sind, umso gestresster ist die Firewall. Man sollte daher sicherstellen, ob überhaupt genug Kapazitäten vorhanden sind, um auch den Traffic während eines DDoS-Angriffs in den Griff zu bekommen und darüber hinaus störungsfreie Services für das interne Netzwerk bereitzustellen.

Viele UTM- und NGFW-Produkte sind mit altmodischen Technologien ausgestattet, bei denen beispielsweise die Anwendungserkennung (samt mehreren Hunderttausend Signaturen) über eine einzige IPS-Engine erfolgt. Diese Technik führt nicht nur zu einer hohen Fehlerquote, sondern auch zu schweren Einbußen in puncto Leistung: Manche Anbieter leiden unter einer Leistungsminderung von bis zu 80 %. Ein Leistungsabfall von 80 % auf der Firewall kann Einfluss auf das gesamte Netzwerk haben, da nun wahrscheinlich alle Nutzer von einem Angriff betroffen sein werden.

Die Firewall ist in der Regel nicht der Hauptangriffspunkt, kann aber bei schlechter Netzwerkplanung ein Flaschenhals sein, der die Auswirkungen von Attacken zusätzlich verschlimmert.

Attacken auf spezifische Computer oder Applikationen

Anstatt Internetverbindungen zu überlasten, können Attacken auch auf spezielle Systeme und Services mit relativ geringem Traffic ausgerichtet werden.

Schwachstellen im System treten beispielsweise in Form eines Bug im Applikations-Code oder im Betriebssystem auf. Doch die Sicherheitslücke kann auch eine Webseite sein, die eine verhältnismäßig hohe Rechenleistung benötigt, um eine bestimmte Unterseite zu öffnen.

Bei der klassischen Form eines Angriffs auf eine spezifische Anwendung werden http-Anfragen auf einer bestimmten Webseite, die große Bilder und Dateien enthält, erzeugt. Ein paar Megabyte-Anfragen von Clients führen dazu, dass der Webserver mit mehreren Gigabyte antwortet. Dies kann sowohl den Betrieb des Webservers stören als auch Probleme mit der Internetverbindung hervorrufen.

Ausnutzen von Schwachstellen in Anwendungen

Das Ausnutzen von Bugs in Anwendungen kann verheerende Auswirkungen haben, verlangt aber in der Regel fortgeschrittene Fähigkeiten vom Angreifer. Werden Applikationen z.B. von IPS-Systemen geschützt, muss der Angreifer individuelle, speziell auf unbekannte Schwachstellen ausgerichtete Attacken starten. Mit 08/15-„Off-the-Shelf"-Angriffstools kommt man hier nicht weit.

Diese spezielle Vorgehensweise der Angreifer nimmt jedoch viel Zeit in Anspruch und kann nur von versierten Hackern durchgeführt werden. Hat man allerdings Erfolg mit einer solchen Attacke, kann die gesamte IT-Umgebung kompromittiert werden, inklusive des Ausfalls aller Services sowie Datenverlusten.

Zusätzlich zu den materiellen Folgen eines solchen Angriffs wird die spätere Wiederherstellung aller Services sehr kompliziert und zeitaufwendig.

Ausnutzen von Features und Unterseiten

Doch es gibt im Vergleich zu zielgerichteten Angriffen auf Schwachstellen noch eine einfachere Vorgehensweise. Die Theorie ist ebenso simpel: Zuerst sollten die Applikationen oder Webseiten analysiert werden, um Features oder Unterseiten zu finden, die länger zum Laden bzw. mehr Rechenleistung benötigen. Sobald Schwachstellen gefunden werden, kann die Attacke gezielt eine Überlastung dieses Features oder dieser Unterseite herbeiführen.

Die meistgefährdeten Unterseiten oder Funktionen sind die, die große Bilder enthalten oder komplexe SQL-Ausdrücke nutzen.

Diese Art des Angreifens ist beliebt, weil sie so einfach umzusetzen ist und kein großes Botnet benötigt. Ein simples Tool, das die Reaktionszeiten und Größen aller Seiten einer Website analysiert, kann bereits einen Service stören.

Um sich gegen diese Angriffe zu schützen, ist es notwendig, sowohl einen sogenannten verhaltensbasierenden Schutz einzurichten als auch aktuelle Applikationen so zu konfigurieren, dass sie nicht so einfach für Angriffe genutzt werden können. Z.B. sollte eine Webseite, die einen Telefonbuch-Service bietet, folgende Sicherheitsmerkmale einführen:

- Die Antwort auf jede Anfrage sollte nicht mit mehr als 100 Einträgen pro Seite zurückkehren,
- der Suchbegriff sollte mindestens fünf Zeichen betragen,
- die Suchbegriffe sollten auf Unregelmäßigkeiten geprüft werden (z.B. alphanumerische Werte),
- wenn es mehr als eine Suchanfrage pro Sekunde auf der gleichen IP-Adresse gibt, sollten Captcha-Abfragen eingegeben werden.

Andere Schwachstellen in Anwendungen lassen sich oft in den Features finden, die zur Kompensierung gestörter Verbindungen integriert wurden. Beispielsweise werden FTP-Anwendungen so gestaltet, dass bei der einmaligen Nutzung mehrere Arten von Signalisierungspaketen erzeugt werden, die in bestimmten Reihenfolgen gesendet werden müssen. Wird dieser Vorgang unterbrochen, erscheinen plötzlich Pakete, die nichts mit der aktuellen Nutzung der Anwendung zu tun haben. Daher sollte die Anwendung diese Pakete dringend ignorieren. Leider sind manche Anwendungen so entwickelt, dass sie störende Verbindungen auf dem Client immer kompensieren wollen. Wenn ein Paket, das nicht mit einer aktuellen Anwendungssitzung übereinstimmt, ankommt, gibt es Features, die das Paket wieder an eine bereits aufgelöste Sitzung anpassen und diese wiederherstellen. Diese großartige Funktion ist jedoch manchmal einfach auszutricksen, z.B. indem „illegale" Pakete an eine Applikation gesendet werden. Die Anwendung wird jetzt eine Menge Informationen und hohe CPU- und Speicherressourcen benötigen, um die illegalen und irrelevanten Daten zu verarbeiten. Dies führt sehr schnell zu einer Überlastung.

„Reflection“-Angriffe

Reflection-Attacken nutzen eine Technik, mit der sich Opfer indirekt angreifen lassen, und zwar durch einen Mittelsmann (Vermittler). Das Prinzip hinter diesen Attacken ist, dass der Täter eine gefälschte Anfrage an den Mittelsmann sendet und dieser sie an das Opfer weiterleitet. Diese Technik erschwert die Bemühungen, dem Täter auf die Schliche zu kommen.

Ein klassisches Beispiel für eine Reflection-Attacke: Der Täter sendet eine „Record“-Anfrage, um einen DNS (Domain Name Server) zu legitimieren. Die gefälschte Anforderung sieht so aus, als ob sie vom Opfer selbst und nicht vom Angreifer sei. Dieser Verkehr wird häufig als „Backscatter“ (Rückstreuung) bezeichnet.

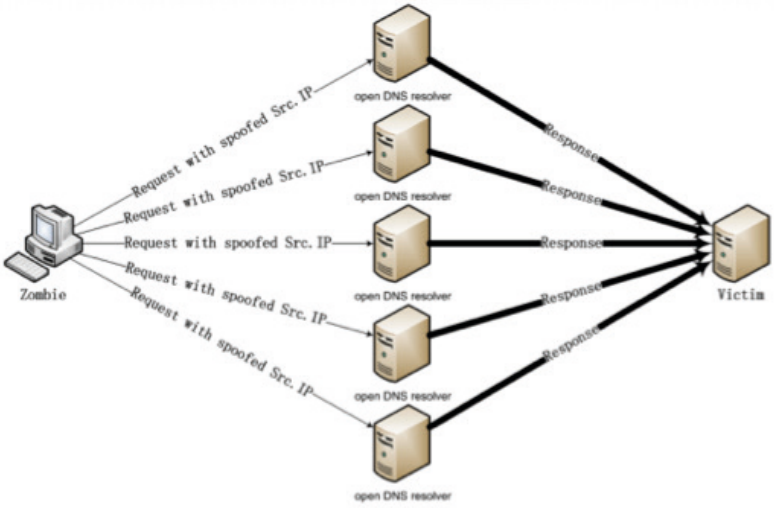

Abbildung 2: „Reflection“-Angriff

Reflection-Attacken sind am erfolgreichsten, wenn sie mit Techniken wie „Amplification“ (Verstärkung) kombiniert werden. Eine kombinierte Reflection- und Amplification-Attacke verursacht, dass das Opfer über Vermittler attackiert wird und die Antwortnachrichten länger als die Anfragen sind, die der Angreifer an den Vermittler weitergibt. Bei DNS-Reflection- und Amplification-Attacken stammen die DNS-Anfragen aus gefälschten IP-Quelladressen, die der Server für TXT-Datensätze benötigt.

Somit führt eine einfache Anfrage durch den Mittelsmann zu einer größeren Antwortnachricht, und das Opfer hat es schwer, den Angriff zurückzuverfolgen.

Wie baut man ein robustes Netzwerk auf, um sich gegen DoS- und DDoS-Attacken zu schützen?

Es gibt keine Patentlösung für den Schutz vor DoS- und DDoS-Attacken. Da es mehrere verschiedene Arten von Angriffen, verschiedene Angriffsmöglichkeiten gibt, gibt es auch verschiedene Wege, sich zu schützen. Eine effiziente Absicherung kann man definitiv erreichen, sie erfordert jedoch eine durchdachte Planung, bei der man diverse Faktoren kombinieren sollte, z.B. ein robustes und widerstandsfähiges Netzwerk, gehärtete Anwendungen und Firewalls mit speziellen Funktionen.

Seitdem DoS- und DDoS-Angriffe in so vielen Variationen auftreten, erfordert das eine Kombination aus verschiedenen Features für guten Schutz. Die folgende Tabelle gibt einen Überblick über die Techniken, die für jede Angriffskategorie geeignet sind.

	IPS	AC	Übertragungs-begrenzung	Traffic Shaping	SLB	RLB	Cloud und CDN	Kapazitäts-planung	Multi Layer FW
Überlastete Internetverbindung						**X**	**X**		
Geblockter oder gestörter Zugriff für externe Nutzer auf interne Systeme				**X**					
Geblockter oder limitierter Zugriff auf den ein- und ausgehenden Traffic für Mitarbeiter und Nutzer				**X**		**X**			
Überlastung von Netzwerkinfrastruktur-equipment									

	IPS	AC	Übertragungs-begrenzung	Traffic Shaping	SLB	RLB	Cloud und CDN	Kapazitäts-planung	Multi Layer FW
Verursacht durch hohes Traffic-Aufkommen			X	X				X	X
Verursacht durch viele gleichzeitige Netzwerknutzer			X		X			X	X
Service-spezifische Attacken									
Überlastung verursacht durch …									
… das Herunterladen großer Dateien		X	X	X	X		X		
… die Nutzung von Ressourcen und Funktionen, die viel RAM- und CPU benötigen		X	X	X	X		X		
… viel „valid Traffic“			X	X	X		X		
… häufige Nutzung von verschlüsselten SSL-Zertifikaten		X	X		X				
Abstürze oder Störungen durch ausgenutzte Schwachstellen, unabhängig vom Netzwerkverkehr	X	X							
Reflection-Attacken (DNS)		X	X	X	X		X		

Netzwerkdesign

Eine zentrale Firewall korrekt einbinden

Es ist unerlässlich, eine passende Firewall zu besitzen; vor allem, wenn die Firewall sowohl die internen als auch die öffentlichen Netzwerke schützen soll. Eine korrekte Dimensionierung von Firewalls und anderem Equipment muss daher unter der Berücksichtigung durchgeführt werden, dass genügend Kapazität für alle angebundenen Netzwerke vorhanden ist. Die gesamte Kapazität des Netzwerkverkehrs muss in beide Richtungen von der Firewall abgesichert werden. Es ist also sinnvoll, seine Firewall genauer zu analysieren und zu beurteilen, wie sie in einem normalen und in einem Worst-Case-Szenario reagiert.

Darüber hinaus sollte bei der Dimensionierung der Firewalls gecheckt werden, ob deren Kapazität alle Funktionen unterstützt. Funktionen, die häufig eine hohe CPU-Kapazität benötigen, erfordern noch detailliertere Analysen oder eine Ver- bzw. Entschlüsselung. Beispiele für solche Funktionalitäten sind:

- das Einrichten von SSL-Zertifikaten mit langen Verschlüsselungs-Keys;
- die Inspektion von SSL-Datenverkehr, der sowohl Entschlüsselung als auch Wiederverschlüsselung beinhaltet;
- Application Control;
- Antivirus;
- IPS;
- VPNs mit vielen Verschlüsselungsmöglichkeiten und/oder vielen „Tunnel“-Einrichtungen.

Viele Hersteller von Netzwerkgeräten geben lediglich Kapazitätszahlen für sogenannten Klartextverkehr an und bieten dabei grundlegende Firewall-Funktionen an. Diese weichen oftmals stark von den Konfigurationen ab, die im wirklichen IT-Altag benötigt werden. Es ist wichtig zu untersuchen, wie die Geräte der Hersteller beeinträchtigt werden können, wenn man Funktionen von Services wie UTM- und NGFW integrieren möchte. Denn die Leistung mancher Produkte kann sich um 80 % verschlechtern, wenn UTM- und NGFW-Funktionen genutzt werden. Das bedeutet, dass selbst eine relativ kleine Menge des Verkehrs während eines DoS- und DDoS-Angriffs die Geräte überlasten könnte. Das Überlasten einer zentralen Einheit führt zu schlechten bzw. langsamen Antwortzeiten im Netzwerk und kann sogar alle Services im gesamten Netzwerk außer Kraft setzen.

In puncto Bandbreite muss sichergestellt werden, dass Firewalls und andere Geräte eine große Anzahl neuer Verbindungen pro Sekunde, viele Datenpakete pro Sekunde und gleichzeitige Verbindungen unterstützen können.

Im Gegensatz zu Clavister sind die meisten Firewalls so konzipiert, dass beim Erreichen der maximalen Anzahl von Verbindungen alle neuen Verbindungen blockiert werden, solange bis die „alten“ ihr Time-Out erreicht haben. Diese Schwäche haben die meisten Firewalls auf dem Markt. Dies führt zu Service-Ausfällen für einige Minuten oder im schlimmsten Fall für einige Stunden, bevor neuer Verkehr die Firewall passieren darf.

Unterteilte Netzwerke mit separaten Firewalls für öffentliche und interne Services

Durch eine Aufteilung des Netzwerks und eine Abspaltung der öffentlichen und internen Systeme können die Folgen von DoS- und DDoS-Attacken beherrscht und Störungen abgemildert werden.

Wird zum Beispiel ein Angriff auf öffentliche Systeme gerichtet, können die internen Systeme währenddessen komplett abgeschottet werden.

Speziell in IT-Umgebungen, in denen TCP- und IP-basierende Lösungen für Speicherzwecke genutzt werden (z.B. NFS), ist es wichtig, das Netzwerk so zu trennen, dass ein Überlastungsangriff auf den Webserver nicht die zentralen Datenspeicher des Unternehmens erreicht.

Mit einem auf mehrere Layer (Schichten) aufgeteilten Netzwerk wird es einfacher, alle Netzwerkelemente so zu dimensionieren, dass „Überkapazitäten" verhindert werden und wichtige Faktoren des Netzwerks keine Angriffspunkte bieten.

Dieses Verfahren empfiehlt sich vor allem für größere und komplexere Netzwerke, in denen sich viele Faktoren gegenseitig beeinflussen. Dort können die Folgen eines Angriffs schwerwiegender sein.

Der Kosten- und Verwaltungsaufwand sind Nachteile dieser Lösung, da Investitionen in die Verwaltung von mehreren Firewall-Layern und anderen Netzwerkgeräten erforderlich sind. Doch diese Nachteile können begrenzt werden, da die Kapazität für Internetverbindungen und öffentliche Systeme in der Regel relativ niedrig ist und demnach kein ähnlich kostenintensives Equipment wie das interne Netzwerk benötigt wird.

Man kann das jeweilige Netzwerk näher an das Leistungslimit bringen und Überkapazitäten minimieren, die bei einer einzigen zentralen Firewall-Schicht im Netzwerk auftreten würden. Abhängig von der Größe des Netzwerks kann die Methode mit mehreren kleineren Firewalls tatsächlich billiger sein, vor allem in Bezug auf die Kosten pro Mbps, die oft in horrendem Maße für zentrale High-End-Firewalls zu zahlen sind.

Unterteilte Netzwerke und Cloud-Services

Cloud-Services und so genannte Content-Deliver-Netzwerke können verwendet werden, um die verschiedenen geschäftskritischen Systeme auf mehrere Bereiche zu verteilen und dadurch Attacken zu vermeiden, die durch das Ausnutzen einer einzigen Schwachstelle ganze Services lahmlegen.

Cloud-Services haben zudem den Vorteil, dass sie sehr skalierbar sind und vorübergehend die Kapazität für kritische Services erhöhen können. Dadurch sind sie in der Lage, die Erhöhung des Verkehrs im Rahmen eines DoS- und DDoS-Angriffs zu kompensieren.

Clavister bietet virtuelle Firewalls an, die es ermöglichen, die gleiche Art von Firewall-Technologie in vielen IT-Umgebungen bereitzustellen: im physischen Inhouse-Netzwerk, im internen virtualisierten Rechenzentrum oder in einer gehosteten Cloud-Umgebung. Alle Clavister-Plattformen (physisch und virtuell) basieren auf den gleichen ausgereiften und bewährten Kernfunktionalitäten und können mit dem gleichen zentralen Administrations-Tool verwaltet werden. Daher sind Nutzer in der Lage, bisherige Erfahrungen mit Clavister-Produkten schnell in die neuen Lösungen zu überführen bzw. zu nutzen.

Funktionen, die D(D)oS-Attacken verhindern oder währenddessen helfen

Die Anzahl der Verbindungen einschränken

Threshold Rules – Rate Limiting (Grenzwert-Regeln – Ratenbeschränkung) ist eine Funktion der Clavister-Produkte, die es ermöglicht zu definieren, was normales oder unnormales Traffic-Verhalten ist. Durch die Kontrolle über die Anzahl neu eingerichteter Verbindungen, entweder innerhalb eines spezifischen Zeitintervalls oder als Gesamtsumme eines einzelnen Users oder Netzwerks, wird es Hackern signifikant erschwert, die geschützten Systeme zu überlasten. Da diese Form des Schutzes nicht auf Signaturen bekannter Angriffe vertraut und stattdessen auf Basis bekannter Verhaltensmuster operiert, greift sie sowohl bei bekannten als auch unbekannten Attacken.

Das ist einer der effektivsten Wege, um Angriffe abzuwehren oder zu blockieren, die auf der Anzahl von Verbindungen basieren, die innerhalb kurzer Zeit erstellt werden und jegliche Schwachstellen ausnutzen. Der Angriffsvektor hierbei ist die Einrichtung neuer Verbindungen.

Intrusion Prevention System (IPS)

Das Intrusion Prevention System in den Clavister-Produkten kann sowohl bekannte als auch unbekannte Attacken identifizieren, indem es verschiedene Techniken kombiniert, u.a. Signaturen. Die Clavister IPS-Funktion sucht nach bekannten und unbekannten Angriffen, die versuchen, Schwachstellen auszunutzen. Wird eine Attacke erkannt, können Sie entscheiden, ob die Verbindung gestoppt, der Traffic nur geloggt oder sogar auf eine Blacklist gesetzt werden soll, geltend für die Hosts, die als Auslöser identifiziert wurden.

Bandbreiten-Management

Traffic oder Bandbreiten-Shaping ist eine Funktion, die normalerweise dazu benutzt wird, verschiedenen Nutzern oder Anwendungen Bandbreite zuzuteilen. Korrekt angewendet ist dieses Feature auch hocheffektiv, um Überlastungsangriffe

zu bekämpfen. Die Funktion kann entsprechend konfiguriert werden, um entweder einen einzelnen User davon abzuhalten, die geschützten Systeme zu überlasten, oder um die Totallast einzuschränken, die allen Usern für eine spezifische Serverressource erlaubt ist. Das bedeutet, dass die Bedrohung an der Firewall gestoppt wird, bevor die geschützten Services zusammenbrechen oder hängenbleiben.

Mit Clavister-Lösungen lässt sich außerdem Traffic Shaping mit dem Intrusion Prevention System (IPS) und/oder Application Control kombinieren. Dies ermöglicht die Beschränkung von Bandbreite für spezifische Nutzer, deren Verhalten als abweichend von der Norm identifiziert wird. Dadurch ist es einfacher, Kunden guten Service zu bieten und gefährlichen Traffic einzuschränken. Oftmals ist es effektiver, den Täter in die Irre zu führen und es erscheinen zu lassen, als ob die Attacke funktioniert, und dem Traffic weniger Bandbreite bereitzustellen als ihn komplett zu blockieren.

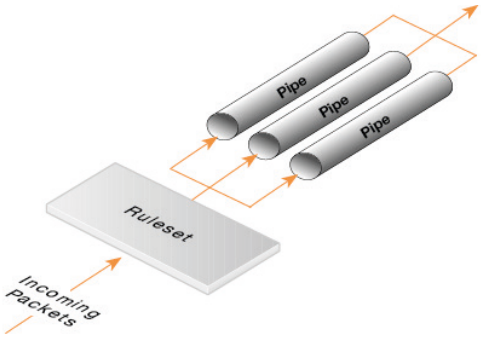

Abbildung 2: Bandbreiten-Management

Load Balancing und Server Farming (SLB)

Wie die Bezeichnung bereits besagt, verteilt dieses Feature die Auslastung oder den Traffic auf mehrerer Server. Durch die Nutzung dieser Funktion ist es möglich, die Gesamtkapazität zu erhöhen, indem die Last auf ein Cluster von Servern verteilt wird, die dieselben Service-Arten bieten (eine Serverfarm). Zusätzlich zu erhöhter und skalierbarer Kapazität optimiert das Feature auch die Belastbarkeit und Fehlertoleranz, was wiederum das Netzwerk robuster macht. Als angenehmer Nebeneffekt wird die tägliche Wartungsarbeit wie z.B. Server und Patch Management vereinfacht. Anstatt Downtime einplanen zu müssen, um auf einem Server als Single Point of Failure ein Software-Upgrade durchführen zu können, ist es möglich, Wartungsarbeiten auf einem Server zu erledigen, während kontinuierlicher Service mit reduzierter Kapazität angeboten wird.

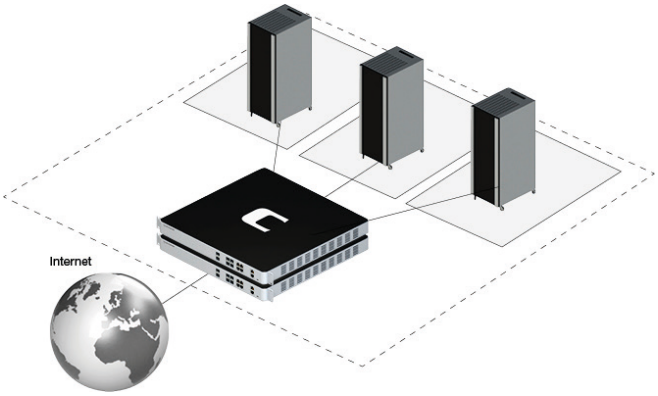

Abbildung 3: Load Balancing und Server Farming (SLB)

Load Balancing – redundante Internetverbindugen

Durch die Nutzung mehrerer Internetanbindungen, die durch die Route Load Balancing-Funktion von Clavister koordiniert werden, ist es möglich, sicherzustellen, dass interne User Zugang zum Internet und zu Services außerhalb der Organisation haben, selbst während einer laufenden Attacke, bei der die primäre Internetverbindung geflutet wird.

Anstelle einer gelähmten Organisation dürften kritische Services immer noch erreichbar sein, und Administratoren können daran arbeiten, den Angriff abzumildern – unter weniger Druck und Risiko menschlichen Versagens.

Clavisters Funktionalität, den Traffic über mehrere parallele Anbindungen zu verteilen, kann auf verschiedene Weisen konfiguriert werden, um sie der aktuellen Situation anzupassen. Der Traffic kann über eine zweite Konnektivität verteilt werden,

entweder entsprechend einer Verteilungsrichtlinie für normale Operationen oder als passives Failover, bei dem der komplette Traffic nur dann über eine zweite Anbindung geleitet wird, wenn der erste nicht verfügbar ist oder Anzeichen schlechter Reaktionszeit zu erkennen sind.

Aktive Redundanz – Load Balancing
Dies bedeutet, dass der Traffic über alle Internetverbindungen verteilt wird, auch im normalen Betrieb, was zu erhöhter Kapazität und verbesserten Antwortzeiten führt. Es ist eine gute Lösung, wenn die Subscription für die sekundären Verbindungen unbegrenzten Datentransfer über eine Flatrate/einen Fixbetrag erlaubt.

Passive Redundanz – Failover
Hierunter ist zu verstehen, dass der Traffic nur dann über den sekundären Link geleitet wird, sofern ein Problem mit der primären Verbindung besteht. Das ist wünschenswert, wenn die sekundären Verbindungen in der Gesamtdatenmenge pro Monat (Eg 3G/4G-LTE-Subscription) beschränkt sind.

Verbindungs-Monitoring
Zusätzlich zu den Lastverteilungskapazitäten sind Clavister-Lösungen in der Lage, jede einzelne Anbindung zu monitoren. Die Antworten des integrierten „Link Monitoring"-Features werden evaluiert und die Verteilung entsprechend den vorkonfigurierten Richtlinien dynamisch angepasst. Das Clavister Link Monitoring (Route Monitor)-Subsystem kann Latenz, Ping-Antworten und sogar die Antworten von Anwendungsanfragen messen. Dadurch wird die Evaluierung des Status und der Performance der Verbindungen vereinfacht und nicht nur erkannt, ob die Verbindung funktioniert oder down ist.

Mit dem Clavister Route Load Balancing und Link Monitoring-Feature kann auf einfache Weise ein robustes und effizientes Netzwerk errichtet werden, das in der Lage ist, DDoS-Angriffe zu handhaben, und gleichzeitig Vorteile während des normalen Betriebs bietet.

Application Control

Application Control ist eine Funktion von Clavister-Lösungen, die Traffic auf Basis der verwendeten Anwendung erkennt und kontrolliert, unabhängig vom eingesetzten Port oder Service.

Mit Application Control können Sie die Hacker daran hindern, bösartigen Traffic, der als legitimer Traffic getarnt ist, an interne Systeme zu senden. Herkömmliche Firewalls ohne dieses Feature würden diesem verseuchten Traffic den Weg durchs Gateway einfach erlauben.

Application Control kann auch dazu genutzt werden, um Richtlinien durchzusetzen, z.B. welcher Browser genutzt werden darf, welche Websites aufgerufen werden dürfen und Ähnliches. Dies sorgt für erhöhten Schutz und kann verhindern, dass Standard-Angriffs-Tools benutzt werden. Natürlich lassen sich diese Werkzeuge von denjenigen anpassen, die das nötige Wissen haben, aber es senkt die Anfälligkeit und reduziert das Risiko von Attacken durch Cyber-Vandalen, denen das Know-how fehlt.

Abbildung 5: Clavister Web Management

Protokollvalidierung und Konsistenzprüfung

Die Protokollvalidierung wird genutzt, um sicherzustellen, dass der von der Firewall erlaubte Traffic den definierten Standards folgt, die für jedes Protokoll gelten. Typische Checks, die mittels Protokollvalidierung erfolgen, prüfen z.B. die richtige Sequenznummer, die auf Paketen genutzt wird, ob die korrekten Flaggen gesetzt sind und dass die Sessions korrekt aufgesetzt sind. Da viele Angriffs-Tools auf aufgezeichnetem Traffic beruhen, in dem beispielsweise Sequenznummern und andere

Werte nicht korrekt sind, lassen sich diese Attacken einfach mittels Protokollvalidierung und Konsistenzprüfungen blocken, die Teil der grundlegenden Firewall-Funktionalität sind. Auch diese Dinge können von jemandem mit genügend Wissen angepasst werden, aber sie erschweren es weniger fähigen Hackern, die den Angriff mit Standardtools versuchen.

Auch für diejenigen, die das entsprechende Wissen mitbringen, sind die Funktionen effektiv, denn sie erfordern eine weitaus kompliziertere Prozedur sowie mehr Kapazitäten und Power vom Host, der das Netzwerk angreift.

Monitoring und Alarme

Eine vorbildliche Vorgehensweise im Bereich Monitoring zu Security-Zwecken ist es, das komplette Equipment und alle Services im Netzwerk zu überwachen. Der Grund für ein solch umfangreiches Monitoring ist, dass Sie ein gutes und ausführliches Verständnis für den normalen Systemstatus erlangen sollten, um es dadurch einfacher zu machen, Anomalien zu erkennen. Verschiedene Tools lassen sich einsetzen, um Abnormitäten zu visualisieren oder Alarme abzusetzen, wenn Abweichungen auftreten. Manche Abläufe können automatisiert werden, während andere auf manuellem Wege besser gehandhabt werden können. Es gibt zahlreiche unterschiedliche Lösungen für das Monitoring von Netzwerk-Equipment. Für das Monitoring und Alarmmanagement mit Clavister-Lösungen empfehlen wir die folgenden Tools:

- **Clavister InControl**

  Zentrales Management für Clavister- Lösungen. Enthält Funktionen für das Management, das Monitoring und die Log-Analyse. Clavister InControl kann gleichzeitig hunderte Firewalls und Administratoren verwalten, außerdem ist es in den Wartungsvertrag für Firewall-Produkte inkludiert; ohne zusätzliche Lizenzgebühren.
- **Multi Router Traffic Grapher - MRTG**

  MRTG ist ein kostenloses und bekanntes Tool für das Monitoring von Status und Traffic vieler Netzwerkgeräte, die SNMP einsetzen. Es bietet einen exzellenten Überblick darüber, wie Traffic durch das ganze Netzwerk fließt, was die Entdeckung von Problemen vereinfacht und anzeigt, wo genau im Netzwerk Schwierigkeiten auftreten (könnten).
- **OSsec**

  OSsec ist ein kostenfreies, bekanntes Tool, das verwendet werden kann, um Log-Daten verschiedener Quellen zu analysieren. Dazu zählen Log-Daten von Firewalls, VPN-Geräten, Betriebssystemen, Anwendungen und mehr. OSsec lässt sich nutzen, um potentielle Lecks zu identifizieren, indem es Log-Daten verschiedener Systeme korreliert und Alarme auslöst, sobald spezifische Verhaltensmuster erkannt werden.
- **SIEM-Tools (Splunk und andere)**

  Während einer Attacke ist es eher die Regel statt die Ausnahme, dass verschiedene Geräte in irgendeiner Weise davon betroffen sind. Es kann sich als schwierige und umständliche Aufgabe erweisen, einen Angriff zu identifizieren und zu verstehen, wenn dazu die Daten eines jeden Geräts angeschaut werden, weil das bedeuten könnte, Hunderttausende – wenn nicht gar Millionen – von Log-Aufzeichnungen durchsehen zu müssen. Um die Nadel im Heuhaufen zu finden, können automatisierte und Richtlinien-basierte Log Correlations verwendet werden. Diese sind zentrale Schlüsselbestandteile in Security Information und Event Management (SIEM)-Tools. Diese Lösungen können auch eingerichtet werden, um Alarme auszulösen, die mehrere verschiedene Vorfälle auf mehreren Geräten erfordern, wodurch das IT-Personal von einer Alarmierung in der Anfangsphase eines Angriffs profitiert.

Vorbereitungsplan und Durchführung

Keine Security-Lösung ist 100 % perfekt, und selbst wenn es eine solche Lösung gäbe, könnte die Internetverbindung dennoch überlastet werden.

Um eine Attacke schnell und effektiv zu stoppen und den Schaden gering zu halten, ist es ausschlaggebend, einen Notfallplan zu haben. Ein guter Plan sollte enthalten, wer für die Arbeit verantwortlich ist, wie die Attacke, der man ausgesetzt ist, identifiziert werden soll, eine Beschreibung, wie sich die Attacke auf die Organisation auswirkt und wie sich kurz-, mittel- und langfristig verhalten werden soll, um den Angriff abzumildern.

Ein effektiver Plan sollte außerdem detaillierte Beschreibungen liefern, wie sich verhalten werden soll, und er sollte mindestens alle drei Monate aktualisiert werden, um die aktuelle Umgebung abzubilden.

Viele Administratoren vermeiden Übungen und praktizieren diese Pläne in einer Demo-Umgebung, was nachvollziehbar ist, wenn man die potenzielle Unterbrechung bedenkt, die für das Geschäft auftreten kann. Allerdings kann die beschränkte Unterbrechung, ausgelöst durch eine Übung im Produktionsnetzwerk, zukünftige Desaster vermeiden.

Es wird dringend empfohlen, einen Spezialisten zu kontaktieren, der bei der Erstellung einer Untersuchung hilft und Ratschläge erteilt, ob es irgendwelche Verzögerungen oder einen Grund gibt anzunehmen, dass Lücken und Löcher existieren, die ein reibungsloses und kontinuierliches Weiterarbeiten im Ernstfall gefährden.

Empfehlungen

DoS- und DDoS-Attacken zählen zu einem breit angelegten Konzept, das viele verschiedene Angriffstechniken und damit verbundene Risiken umfasst. Es ist schwierig, kurze und einfache Ratschläge zu geben, ohne zu verallgemeinern. Ein guter Schutz vor DoS- und DDoS-Attacken muss maßgeschneidert sein, um zu jeder individuellen Organisation und jedem individuellen Netzwerk optimal zu passen, aber es gibt ein paar generelle Prinzipien, die helfen, unabhängig von der betroffenen Umgebung und Situation.

- **Analyse und Netzwerkabbildung**

  Analysieren Sie Ihr Netzwerk und kartieren Sie, welche Systeme öffentlich und intern sind und wie die Abhängigkeiten zwischen all diesen Geräten aussehen. Prüfen Sie die Konsequenzen und Auswirkungen auf andere Systeme, wenn eines ausfällt, inklusive Netzwerk-Equipment wie z.B. Router und Firewalls.
- **Planung**

  Führen Sie einen praktischen „Hands-on"-Handlungsplan ein, aus dem klar hervorgeht, wer für was verantwortlich ist und wer die Entscheidungen in einer Krisensituation trifft.
- **Dokumentierung**

  Stellen Sie sicher, dass die Systemdokumentierung auf dem neuesten Stand ist und dass jeder weiß, wo die Dokumentation abgespeichert ist. Achten Sie besonders auf die Dokumentation, wie Backups gespeichert werden und wie komplette Server wiederhergestellt werden können.
- **Monitoring**

  Monitoren Sie alle Services und richten Sie besonderes Augenmerk auf alle Services, die öffentlich sind und als Ziel für User, Kunden oder andere Gruppen mit bösartigen Absichten dienen können.
- **Redundanz**

  Ein robustes Netzwerk mit Redundanz hilft im Falle eines Angriffs, aber trägt auch zu einem effizienteren Netzwerk bei normalem Betrieb bei. Dies gilt insbesondere für redundante Internetverbindungen und Serverfarmen.
- **Virtualisierung und virtuelle Firewalls**

  Entlasten und vereinfachen Sie die Konfiguration der zentralen Firewall durch die Nutzung einer virtuellen Firewall für die komplexeren und ressourcenintensiven Funktionen (UTM/NGFW), die verwendet werden, um die virtuelle Umgebung abzusichern. Beobachten Sie, wie sich die dynamische Ressourcenzuordnung auf Ihre virtuellen Maschinen auswirkt. Konfigurieren Sie stets sowohl die minimale als auch die maximale Ressourcenkapazität für kritische Funktionen, die im virtuellen Datacenter betrieben werden, insbesondere die virtuellen Security-Produkte.
- **Kapazitätsplanung**

  Ein gutes Grundprinzip ist es, einen Kapazitätsüberschuss zu kalkulieren, wenn Services und Server zentralisiert sind, als dass sie getrennt und isoliert sind. Wenn Sie einen Layer an Firewalls nutzen, um sowohl interne als auch öffentliche Netzwerke zu managen, sollten Sie deren Kapazität überprüfen, wenn alle Funktionen aktiviert sind, und mit der aggregierten Kapazität aller Netzwerke in einem Worst-Case-Szenario vergleichen. Wenn Sie bereits in eine zentrale Firewall investiert haben und die Sicherheit mit UTM- und NGFW-Funktionalitäten erweitern möchten, sollten Sie besonders umsichtig vorgehen und das Upgrade auf größere Hardware in Betracht ziehen oder die Aufteilung der öffentlichen und internen Netzwerke mit der Bestückung einer weiteren Firewall-Ebene erwägen.
- **Reports und Analysen**

  Nutzen Sie sogenannte SIEM(Security Information and Event Management)-Tools, um Informationen von mehreren Anwendungen und Systemen zu analysieren. Durch die Korrelierung von Informationen verschiedener Systeme kann ein Angriff in einem früheren Stadium erkannt werden. SIEM-Tools unterstützen außerdem beim Wiederaufbau und dem Verständnis, wie die Attacke stattgefunden hat und was genau passiert ist. Das ist sehr wichtig, um dieselben Probleme zukünftig verhindern zu können.
- **Prioritäten setzen**

  Sehen Sie ein klares Gesamtbild und priorisieren Sie, was für Ihre Organisation kritisch ist. Konzentrieren Sie sich darauf, dass priorisierte Funktionen und Services ordnungsgemäß abgesichert sind, bevor Sie versuchen, alle Funktionen abzusichern, und sich in zu vielen Details verlieren. Vielleicht ist es akzeptabel, dass die Website während eines Angriffs eine schlechte Reaktionszeit aufweist, aber ist es geschäftsentscheidend, dass das Personal weiterarbeiten sowie E-Mails, CRM, Office Tools in der Cloud etc. weiter nutzen kann. Für andere Kunden mag es genau die umgekehrte Situation sein, bei der die Mitarbeiter betroffen sein könnten, aber das E-Commerce-Portal unbedingt funktionieren muss.

Zusammenfassung

Da die IT ein Business-Bestandteil ist, bedeutet jegliche Störung finanzielle Verluste.

DoS- und DDoS-Attacken mehren sich, und die Folgen eines Angriffs können verheerend sein.

Unzureichender Schutz, unzulängliches Monitoring und ungenügende Notfallpläne können den Unterschied machen zwischen kleineren Störungen und einem kompletten Stopp der Produktion, verärgerten Mitarbeitern, Umsatzverlusten und potenziell verlorenen Kunden.

Es gibt keinen absoluten Schutz, aber einfache Dinge wie eine korrekt dimensionierte und konfigurierte Firewall, Notfallpläne und kostengünstige Redundanzfähigkeiten können die meisten Attacken abfangen, insbesondere solche, die von Personen ohne Spezialwissen womöglich im Affekt gestartet werden.

Die Lösungen von Clavister besitzen umfangreiche Schutzmaßnahmen gegen DoS- und DDoS-Attacken. Sie können entweder als zentraler Schutz oder nachträglich als separater Layer in ein bestehendes Netzwerk (Retrofitting) eingebaut werden. Entgegen kostspieliger Nischenprodukte bietet Clavister einen guten Schutz, ohne die Administration und die Kosten signifikant zu erhöhen.

Die Cloud, Content Delivery Networks und Virtualisierungen sind wirksame Wege, um Risiken zu verringern und eine robustere und tolerante Umgebung zu errichten. Die Sicherheit dieser Umgebungen sollte nicht außer Acht gelassen und der Schutz äquivalent zu einem physikalischen Netzwerk ohne Kompromisse angewendet werden. Clavister VSG ist eine virtuelle Firewall mit denselben Funktionalitäten wie die Hardware-basierte Version und kann sowohl in der Cloud als auch im virtuellen Netzwerk eingesetzt werden, um diese Umgebungen vor DoS-/DDoS-Attacken und anderen Security-Problemen zu schützen.

Ein guter Rat ist es, überhaupt mit der Thematik zu starten und die Security-Lösung in kleinen Schritten zu verbessern.

Es wird dringend dazu geraten, Managed Services in Erwägung zu ziehen oder Hilfe von spezialisierten Beratern anzufordern, falls die Fähigkeiten und Erfahrungen in-house nicht ausreichend zur Verfügung stehen.

Abwarten ist eine oft angewandte Strategie, die aber in größeren und irreparablen Schäden enden kann. Handeln, bevor es zu spät ist, mag nach einem Klischee klingen, aber es ist sehr real und auf jede Netzwerksicherheitsstrategie anwendbar.

Kontaktieren Sie Clavister

Besuchen Sie www.clavister.com für weitere Informationen oder kontaktieren Sie uns oder einen unserer zertifizierten Partner für eine Beratung.

Über Clavister
Clavister ist ein führender Security-Anbieter für feste, mobile und virtuelle Netzwerkumgebungen. Die preisgekrönten Lösungen ermöglichen Unternehmen, Cloud Service-Providern und Telekom-Netzbetreibern den höchsten Schutz gegen aktuelle und neue Bedrohungen mit unübertroffener Zuverlässigkeit. Die Leistung Clavisters im Security-Sektor wurde mit dem 2012 Product Quality Leadership Award von Frost & Sullivan anerkannt. Das Unternehmen wurde 1997 in Schweden gegründet. Die Lösungen sind weltweit über das Netzwerk von Channel-Partnern erhältlich. Weitere Informationen unter www.clavister.com.

Wo kaufen?
www.clavister.com/partners

Kontakt:
www.clavister.com/contact

clavister®
WE ARE NETWORK SECURITY

Clavister DACH, Paul-Dessau-Str. 8 D-22761 Hamburg, Germany
■ **Phone:** +49 40 411259-0 ■ **Fax:** +49 40 411259-299 ■ **Web:** www.clavister.com