Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

SOFORTMAßNAHME

Abwehr von DDoS-Angriffen

Diese BSI-Empfehlung behandelt Maßnahmen zur Reaktion bei akuten Distributed Denial-of-Service (DDoS) Angriffen. Durch diese Maßnahmen besteht die Möglichkeit, die Folgen eines DDoS-Angriffes auch dann noch abzumildern, wenn keine präventiven Vorkehrungen getroffen wurden oder sich diese als ineffektiv erwiesen haben.

1 Checkliste zum Vorgehen bei DDoS-Angriffen

- ✔ Bilden Sie ein Krisenreaktionsteam aus erfahrenen Mitarbeitern des IT-Betriebs, des IT-Sicherheitsteams, dem IT-Sicherheitsbeauftragten / CSO sowie der Presse- und Öffentlichkeitsarbeit, um schnellstmöglich die unten beschriebenen technischen Maßnahmen einzuleiten und begleitende Maßnahmen zu koordinieren.
- ✔ Berichten Sie den Vorfall, entsprechend Ihrer internen Richtlinien, zur Eskalation an das Management.
- ✔ Binden Sie den eigenen Internet-Service-Provider (ISP) bzw. Hosting-Provider frühzeitig ein.
- ✔ Sie sollten ihr Justiziariat oder ihren Anwalt einschalten und Strafanzeige bei der örtlichen Polizei stellen.
- ✔ Für die Presse- und Öffentlichkeitsarbeit müssen Informationen zum Vorfall aufbereitet werden, um bei möglichen Presseanfragen auskunftsfähig zu sein.
- ✔ Vertragspartner und/oder Kunden sollten über die möglichen Einschränkungen der Verfügbarkeit informiert werden.
- ✔ Berichten Sie den Vorfall an das BSI: Das BSI ist als zentrale IT-Sicherheitsbehörde bei größeren DDoS-Angriffen an Berichten der Betroffenen interessiert, um die aktuelle IT-Bedrohungslage in Deutschland analysieren zu können. Diese Berichte erfolgen auf freiwilliger Basis und werden vertraulich behandelt.

2 Maßnahmen zur Abwehr von DDoS-Angriffen

2.1 Server härten

Für Webserver-Produkte, z.B. Apache, gibt es in der Regel diverse Module oder Funktionen, die die Erreichbarkeit im Falle eines DDoS-Angriffes verbessern. Beispielsweise lässt sich die Anzahl der IP-Verbindungen pro IP-Adresse beschränken oder Anfragen verzögert beantworten. Sollte der DDoS-Angriff darauf abzielen, die halboffenen Verbindungen des Servers auszulasten, sollten TCP-SYN-Cookies aktiviert werden.

Die Konfiguration des Servers sollte so geändert werden, dass der Server möglichst wenig Angriffsfläche bietet. Zum Beispiel sollte ein Webserver nur TCP-Pakete auf Port 80 und 443 (für TLS/SSL) annehmen und den Rest aus dem Internet verwerfen. Dies kann auch bereits per Filterung an der Firewall geschehen.

2.2 Filterung nach Quelladressen (Blackholing)

IP-Pakete, deren Quelladresse im Bereich der angreifenden IP-Adressen liegt, können am Router verworfen werden („Blackholing"). Dies kann auch auf ganze GEO-IP-Regionen ausgeweitet werden. Damit werden zwar auch legitime Nutzer dieser Regionen ausgesperrt, für User aus anderen Regionen bleibt die Webseite aber eventuell erreichbar.

2.3 Filterung nach Zieladressen (Sinkholing)

Ein anderer Ansatz zur Abwehr ist, das Ziel des Angriffes temporär nicht erreichbar zu machen. Falls beispielsweise nur eine spezielle IP-Adresse oder URL angegriffen wird, können IP-Pakete, deren Zieladresse mit dem Angriffsziel übereinstimmt, am Router verworfen werden („Sinkholing“). Dadurch erreicht zwar der Angreifer sein Ziel, die Adresse nicht erreichbar zu machen, aber es werden Kollateralschäden auf anderen Webpräsenzen unter Umständen vermieden.

2.4 Filterung nach verschiedenen Kriterien

Nach einer Analyse des Angriffsverkehrs kann versucht werden, diesen anhand geeigneter Filterkriterien am Router oder an einer Firewall zu filtern. Die Filterkriterien hängen von der Art des Angriffes ab.

Bei Angriffen auf der HTTP-Ebene können oftmals bestimmte Felder im Header eines HTTP-Paketes als Filterkriterien herangezogen werden, da viele Tools zur Durchführung von DDoS-Angriffen hier Eigenheiten aufweisen, die eine Unterscheidung von legitimem Verkehr ermöglichen.

Bei Angriffen mit politischem Hintergrund werden oft auch im Zusammenhang stehende Wörter, wie z. B. „Anonymous“, in die Pakete eingebaut.

Achtung: Eine zustandsbasierte Firewall vor einer Webseite kann selbst zum Flaschenhals werden und die Auswirkungen eines DDoS-Angriffes verschlimmern.

2.5 DDoS-Mitigation Appliances oder DDoS-Mitigation-Services bei Providern nutzen

DDoS-Mitigation-Appliances bieten in der Regel eine Vielzahl an vorbereiteten DDoS-Mitigation-Maßnahmen. Die meisten Angriffe können mit diesen Appliances abgewehrt werden, solange die Leitungskapazität zur Appliance nicht durch den DDoS-Angriff komplett ausgelastet wird. Der Verkehr sollte mit diesen Appliances so früh wie möglich, am besten direkt beim Provider, gefiltert werden.

ISP und Hoster bieten zunehmend auch DDoS-Mitigation-Services als zusätzlich beauftragbaren Dienst an.

3 Unterstützende Maßnahmen

3.1 Analyse des Netzwerkverkehrs

Die Analyse des eingehenden Netzwerkverkehrs ermöglicht es, die Angriffsmethode zu bestimmen und bildet damit im konkreten Fall die Grundlage für die Gegenmaßnahmen.

3.2 Protokollierung

Die IP-Adressen der angreifenden Systeme sollten protokolliert und mit einer Abuse-Meldung an die zuständigen Provider gemeldet werden. Folgende Informationen sind zu übermitteln:

- Angreifende IP-Adresse
- Genauer Zeitstempel, inkl. Zeitzonenangabe
- IP-Adresse des Opfers

Die Meldung sollte zeitnah erfolgen, da in der Regel bei Providern nur Logdaten der letzten sieben Tage vorgehalten werden. Vorschriften und Regelungen des Datenschutzes sind in jedem Fall einzuhalten!

Weiterführende Maßnahmen zur Bewältigung von IT-Krisen finden Sie im BSI-Standard 100-4 „Notfallmanagement“ und im Baustein „DER.4 Notfallmanagement“ des IT-Grundschutz-Kompendiums.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.