Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: INTERNET-DIENSTLEISTER

Anti-DDoS-Maßnahmen

Handlungsempfehlungen für Internet-Service-Provider (ISP)

Das vorliegende Dokument richtet sich an Internet-Dienstleister. Es ist Teil einer Dokumentenreihe, in der Empfehlungen zur sicheren Bereitstellung von verschiedenen Internet-Dienstleistungen gegeben werden.

Die Auswirkungen von DDoS-Angriffen können beträchtlich sein, für die betroffenen Institutionen einen großen wirtschaftlichen Schaden auslösen und auch einen Reputationsverlust nach sich ziehen.

Internet-Service-Provider tragen hier eine besondere Verantwortung und können durch ihr Handeln dazu beitragen, das Risiko erfolgreicher DDoS-Angriffe insgesamt zu verringern und deren Auswirkungen zu reduzieren.

Nachfolgend werden Maßnahmen für ISPs beschrieben, die zum einen durch interne Umsetzung und zum anderen in Zusammenarbeit mit den Kunden dazu beitragen können, DDoS-Angriffen und deren Auswirkungen entgegen zu wirken.

1 Interne Maßnahmen

1.1 Organisatorische Maßnahmen

Identifikation von bedrohten Zielen

Ziele von DDoS-Angriffen sind in der Regel aus dem Internet erreichbare Dienste. Insbesondere solche Systeme, deren Ausfall auf Kundenseite deutlich wahrgenommen wird, stehen im Fokus von Angreifern. In den meisten Fällen handelt es sich dabei um Webserver, Mailserver oder DNS-Server. ISPs sollten daher die potenziellen Ziele von DDoS-Angriffen im eigenen Netz, also Dienste und IT-Systeme, die eine wesentliche Rolle zur Gewährleistung eines störungsfreien Betriebs übernehmen, identifizieren und – abhängig von deren Schutzbedarf – ein geeignetes Vorgehen bei DDoS-Angriffen festlegen.

Austausch mit anderen Providern

Erkenntnisse über aktuelle Angriffsverfahren und -arten sowie passende Abwehrtechniken (z. B. Filterregeln) sollten providerübergreifend regelmäßig untereinander ausgetauscht werden.

Hierzu und um im Bedarfsfall eine schnelle Handlungsfähigkeit providerübergreifend sicherzustellen, empfiehlt es sich, Ansprechpartner, Erreichbarkeiten und Notfallnummern untereinander auszutauschen.

Die providerübergreifende Zusammenarbeit sollte durch regelmäßige Übungen optimiert werden.

Checklisten und Prozesse für den Angriffsfall definieren
Für die Abwehr und Analyse von DDoS-Angriffen sollten klare Prozesse definiert und Checklisten vorhanden sein, die es Mitarbeitern ermöglichen, bei Angriffen schnell und koordiniert handeln zu können.

Meldung von Vorfällen
Berichten Sie Vorfälle 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. Sie können Sicherheitsvorfälle auch anonymisiert melden – bspw. über die (anonyme) Meldestelle auf den Internetseiten der Allianz für Cyber-Sicherheit.

1.2 Technische Maßnahmen

Ertüchtigung der eigenen Infrastruktur
Im Fokus von DDoS-Angriffen stehende Systeme sollten in einem Maße überdimensioniert werden, dass ihre Funktionsfähigkeit auch bei einem mittelgroßen DDoS-Angriff ohne weitere Maßnahmen weiterhin gewährleistet ist.

Bereitstellung von Analysemitteln
Auf den Netzwerkkomponenten sollten Anwendungen zur Verkehrs- und Dienstanalyse bereitstehen, damit diese im Angriffsfall zur Analyse im Einklang mit §100 TKG direkt zur Verfügung stehen.

1.3 Leistungsgrenzen der Systeme bereits im Vorfeld identifizieren

Im Angriffsfall muss entschieden werden, ab welcher Last (z. B. Bandbreite, Anfrageanzahl pro Sekunde oder Paketrate) ein Angriff solche Einschränkungen oder Beeinträchtigungen hervorruft, dass eine gezielte Abwehrreaktion notwendig erscheint oder ob zunächst eine intensive Beobachtung des Angriffes vorteilhafter ist. Vor diesem Hintergrund ist es wichtig, die Leistungsgrenzen der Systeme zu kennen.

Die normale Systemlast sollte daher im Vorfeld bestimmt werden (Baselining), um Abweichungen schnell erkennen zu können. Das Baselining sollte sowohl für Systeme der eigenen Infrastruktur als auch für Kundenanbindungen durchgeführt werden.

2 Kundenseitige Maßnahmen

2.1 Gemeinsame Identifizierung von bedrohten Zielen beim Kunden

Ziele von DDoS-Angriffen sind häufig aus dem Internet erreichbare Dienste von Unternehmen oder Behörden. Insbesondere solche Systeme, deren Ausfall von den Kunden solcher Institutionen deutlich wahrgenommen wird, stehen im Fokus von Angreifern. In den meisten Fällen handelt es sich dabei um Webserver, Mailserver oder DNS-Server. ISPs sollten daher die potenziellen Ziele von DDoS-Angriffen, also Dienste und IT-Systeme, die sie für Kunden betreiben, identifizieren und – abhängig von deren Schutzbedarf – ein geeignetes Vorgehen bei DDoS-Angriffen in Abstimmung mit den Kunden festlegen.

Bei der Bereitstellung von Internetzugängen für entsprechende Systeme sollten die betreffenden Kunden über die Gefahren aufgeklärt und in Abstimmung mit dem Kunden eine Risikoanalyse durchgeführt werden.

2.2 Aufklärung / Sensibilisierung des Kunden / Kommunikation mit dem Kunden

Ab einer bestimmten Intensität eines DDoS-Angriffes auf Kundensysteme kann eine effektive Abmilderung nur mit Unterstützung des Internet Service Providers (ISP) erreicht werden. Die Mitwirkung des ISP ist für gewöhnlich spätestens dann erforderlich, wenn die Angriffsbandbreite höher ist, als die Bandbreite des Kundenanschlusses.

Um im Bedarfsfall eine schnelle Handlungsfähigkeit sicherzustellen, sollten die gegenseitigen Ansprechpartner, Erreichbarkeiten und Notfallnummern bereits im Vorfeld zwischen ISP und Kunden ausgetauscht werden.

Das BSI hat sowohl zur Prävention von DDoS-Angriffen[1] als auch zur Abwehr von DDoS-Angriffen[2] Empfehlungen für Unternehmen veröffentlicht, auf die gerne verwiesen werden kann.

2.3 Angebot von Schutzprodukten an Kunden

Dem Kunden sollten die verschiedenen Möglichkeiten zur DDoS-Abwehr und entsprechende Angebote über individuelle oder Standard-Dienstleistungen im Bereich der DDoS-Erkennung und DDoS-Mitigation aufgezeigt werden.

3 Weiterführende Informationen

Handlungsempfehlungen, die zur Bekämpfung von Malware und somit zur Reduktion von Botnetzen als häufige Quelle von DDoS-Angriffen beitragen, finden Sie im Dokument „Malware-Schutz: Handlungsempfehlungen für Internet-Service-Provider“[3].

Maßnahmen zur Reduzierung der Verbreitung von Malware über Webseiten werden im Dokument „Sicheres Webhosting“[4] beschrieben.

Im Zusammenhang mit DDoS-Angriffen werden zunehmend DNS-Server als Verstärker missbraucht. Beachten Sie in diesem Zusammenhang die Empfehlungen zur sicheren Bereitstellung von DNS-Diensten[5].

Diese BSI-Empfehlung ist unter Mitwirkung der als Partner der Allianz für Cyber-Sicherheit registrierten Internet-Service-Provider 1&1 Internet AG, Deutsche Telekom, STRATO AG und Vodafone entstanden.

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.

1 https://www.allianz-fuer-cybersicherheit.de/dok/6643788
2 https://www.allianz-fuer-cybersicherheit.de/dok/6643790
3 https://www.allianz-fuer-cybersicherheit.de/dok/6621316
4 https://www.allianz-fuer-cybersicherheit.de/dok/6621318
5 https://www.allianz-fuer-cybersicherheit.de/dok/6621324