Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Prävention von DDoS-Angriffen

Diese BSI-Empfehlung behandelt Ansätze zur Vorbeugung gegen Distributed Denial-of-Service (DDoS) Angriffe. Neben technischen Möglichkeiten sind auch organisatorische Maßnahmen wesentliche Bestandteile eines effektiven Schutzes vor DDoS-Angriffen.

1 Organisatorische Maßnahmen

1.1 Identifizierung von bedrohten Zielen

Ziele von DDoS-Angriffen sind in der Regel aus dem Internet erreichbare Dienste. Insbesondere solche Systeme, welche eine deutliche Wahrnehmung für Kunden, andere Anwender oder die Öffentlichkeit aufweisen. In den meisten Fällen handelt es sich dabei um Webserver, Mailserver oder DNS-Server. Selbstverständlich können auch Systeme, wie z. B. VPN-Zugänge oder IT-Sicherheitskomponenten, wie die Firewall eines Unternehmens, einer Behörde oder einer Organisation, Ziel eines Angriffs sein. Eigene Dienste, die im Kundenauftrag von externen Anbietern erbracht werden, sollten als potenzielles Ziel von DDoS-Angriffen ebenso wie Middleware und Backends, z. B. in der Form von Web Services, als potenzielles Ziel berücksichtigt werden.

Häufig liegen besonders solche Dienste, die bei einem DDoS Auswirkungen auf eine hohe Anzahl von Nutzern haben, im Fokus von Angreifern.

1.2 Interne Verantwortlichkeiten für die identifizierten Systeme klären

Damit im Falle eines Angriffes die zur Koordination und zur Abwehr benötigten Verantwortlichen möglichst zügig eingebunden werden können, müssen diese bekannt sein. Die folgenden Personen oder Rollen sollten im Vorfeld identifiziert werden:

- ✔ Systemadministratoren zur Angriffsanalyse auf der betroffenen Serverplattform
- ✔ Netzwerkadministratoren zur Angriffsanalyse auf Komponenten, die sich im Netzwerk vor dem eigentlichen Angriffsziel befinden
- ✔ Administratoren oder Content-Manager, die bei Bedarf Änderungen an der Netzwerkkonfiguration oder an den Inhalten der Server vornehmen können
- ✔ Führungskräfte oder Techniker, die befugt sind, eine Entscheidung über Diensteinschränkungen, wie z. B. den eingeschränkten Weiterbetrieb oder die Abschaltung von betroffenen Diensten, zu treffen
- ✔ Mitarbeiter der PR-Abteilung sowie eine evtl. vorhandene Rechtsabteilung, die entscheiden, wann und in welchem Umfang Kunden informiert werden sollen

1.3 Kommunikation mit dem Provider (ISP) klären und evtl. Serviceangebote vereinbaren

Ab einer bestimmten Intensität eines DDoS-Angriffes 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 eigenen Internet-Anschlusses.

Um handlungsfähig zu sein, sollten bereits im Vorfeld die benötigten Ansprechpartner, Erreichbarkeiten und Notfallnummern aufseiten des ISP geklärt werden.

Einige Provider bieten auch individuelle oder Standard-Dienstleistungen im Bereich der DDoS-Erkennung und DDoS-Mitigation an. Auch hier gilt, dass die entsprechenden Dienstleistungen bereits im Vorfeld beauftragt oder abgestimmt sein müssen, um dem Provider ein entsprechendes Handeln im Angriffsfall zu ermöglichen.

1.4 Checklisten und Prozesse für den Angriffsfall definieren

Abwehr und Analyse von DDoS-Angriffen gehören für die meisten IT-Mitarbeiter nicht zu den täglichen Routinearbeiten. Darüber hinaus ist es nicht ungewöhnlich, wenn ein DDoS-Angriff außerhalb der regulären Arbeitszeit stattfindet. Dementsprechend ist u. U. zunächst mit Unsicherheit und Stress der Mitarbeiter zu rechnen.

Um in dieser Situation Fehlern vorzubeugen, ist es empfehlenswert, im Vorfeld klare Prozesse zu entwickeln und Checklisten bereitzustellen, anhand derer sich die IT-Mitarbeiter, die Mitarbeiter der IT-Rufbereitschaft oder andere Prozessbeteiligte orientieren können.

Als erste Basis zur Erstellung dieser Leitlinien kann das Dokument „Abwehr von DDoS-Angriffen“ (BSI-Empfehlungen zur Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de/dok/6643790) dienen.

1.5 Schulung der verantwortlichen Mitarbeiter

Zur Vorbereitung auf DDoS-Angriffe gehört auch die Schulung der verantwortlichen Mitarbeiter. Es sollte darauf geachtet werden, dass folgende Kerninhalte thematisch berücksichtigt werden:

- Performance-Einstellungen und Abwehrmöglichkeiten für den jeweiligen Dienst oder das jeweilige System
- Performance-Einstellungen und Abwehrmöglichkeiten auf Ebene von Netzwerkkomponenten
- Überblick über aktuelle DDoS-Angriffstechniken und Härtungsmaßnahmen
- Möglichkeiten der Analyse
- Prozesse und Kommunikation im Angriffsfall

2 Technische Präventions-Maßnahmen

2.1 Bereitstellung von Analysemitteln

Sofern es aus Sicherheitsgründen vertretbar ist, sollten bereits im Vorfeld Anwendungen zur Verkehrs- und Dienstanalyse auf den Servern bereitgestellt werden, damit diese im Angriffsfall direkt zur Verfügung stehen und nicht erst nachinstalliert werden müssen. Gleiches gilt auf den betroffenen Netzwerkkomponenten.

Weiterhin ist zu empfehlen, die für externe Nutzer angebotenen Dienste über ein von Extern zugreifendes Monitoring zu überwachen. So ist im Angriffsfall nachweisbar, ob der Dienst noch verfügbar ist.

2.2 Netzwerksegmentierung nach Art und Nutzung der Dienste

Ein erfolgreicher Angriff auf einen Dienst, wie z. B. einen Webserver, legt in vielen Fällen nicht nur diesen Server lahm, sondern oft auch das ganze Netzsegment, in welchem sich der betroffene Server befindet. Durch eine Aufteilung unterschiedlicher Dienste auf mehrere Netzsegmente können die Auswirkungen auf die Gesamt-IT abgemildert werden. Es empfiehlt sich, die nach außen angebotenen Dienste auf mehrere DMZ aufzuteilen. Hierbei sollte vor allem nach der Nutzung und der Art der Dienste unterschieden werden. Eine Beispielsegmentierung könnte wie folgt aussehen:

Segment 1 – Webserver mit ausschließlich extern angebotenen Diensten
Segment 2 – Webproxy der Mitarbeiter, E-Mail-Server
Segment 3 – Webserver mit sowohl interner als auch externer Nutzung

2.3 Absicherung der Netzwerkinfrastruktur

Auch auf der Netzwerkebene können vorbeugende Maßnahmen für den DDoS-Fall getroffen werden.

✔ Einsatz von Proxys und Loadbalancern, um eine höhere Last auf Dienstebene zu verarbeiten

✔ Schutz von Netzsegmenten, die bei einem Angriff indirekt betroffen wären: Einführung von Kapazitätsgrenzen (z. B. mithilfe von Traffic-Shaping innerhalb eines gewissen Spielraums)

Es sollte berücksichtigt werden, dass sich u. U. auch die Netzwerkkomponenten selbst im Angriffsfall in eine Überlastsituation geraten oder sogar selbst zum Ziel werden können.

2.4 Leistungsgrenzen der Systeme bereits im Vorfeld identifizieren

Im Angriffsfall muss entschieden werden, ab welcher Last (normalerweise ab welcher Bandbreite, ab welcher Anfrageanzahl pro Sekunde oder ab welcher 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.

Bei der Untersuchung ist zu beachten, dass nicht alleine die Parameter des identifizierten möglichen Angriffszieles (z. B. Webserver) entscheidend sind. Bei der Identifikation der Leistungsgrenzen sind insbesondere auch die Netzwerkkomponenten mit einzubeziehen, die sich auf den wahrscheinlichen Angriffswegen befinden (Paketfilter, Switche, Router, etc.). Oftmals stellt sich bei einer genauen Analyse heraus, dass die Verarbeitungskapazitäten der vorgelagerten Netzwerkkomponenten mit den im Lauf der Betriebsjahre durchgeführten Performanceverbesserungen bei den Diensten nicht schrittgehalten haben. Hier gilt es, gezielt Abhilfe zu schaffen und diese Komponenten in die aktuelle und zukünftige Kapazitätsbetrachtung mit einzubeziehen.

2.5 Härtung und Konfiguration der Systeme auf Dienst- und Serverebene

Viele Internetdienste verfügen über Möglichkeiten, Angriffs- und Lastsituationen abzumildern oder zu vermeiden. Bereits bei der Einrichtung der Dienste sollten diese Optionen berücksichtigt werden.

- ✔ Abweichend von den üblichen Werten in den Voreinstellungen: Konfiguration einer höheren Anzahl an zugelassenen Verbindungen auf der jeweiligen Hardware als per Default vorgegeben, sodass die Performance-Möglichkeiten der Hardware auch real zur Verfügung stehen
- ✔ Verwendung von Proxyservern

Um Überlastzustände auf den betroffenen Servern zu vermeiden, sind aber auch organisatorische Entscheidungen in der Dienstnutzung zielführend.

- ✔ Zusätzlich zu einem Webserver mit dynamischen Inhalten ist das Einbinden eines weiteren Servers in den Dienst zu empfehlen. Dieser hält lediglich ein Basisset an statischen Webseiten vor und kann auch bereits im Regelbetrieb mit deutlich höherer Last umgehen.
- ✔ Außerdem sollte beim Patch- und Sicherheitsmanagement Wert darauf gelegt werden, bekannte DoS-Schwachstellen zu identifizieren und zu schließen. Dazu wird das Beobachten entsprechender Security Advisories empfohlen.

2.6 Einsatz gezielter DDoS-Abwehrsysteme

Am Markt sind einige Softwarelösungen und Appliances erhältlich, welche gezielt eine Abwehr oder eine Minderung (Mitigation) des durch den DDoS-Angriff verursachten Verkehrs ermöglichen. Die Abschwächung wird zumeist durch das Erzwingen von Protokollkonformität, Shaping des Gesamtverkehrs anhand unterschiedlicher Kriterien oder durch das Unterdrücken von Dienstanfragen erreicht. Die Systeme orientieren sich u. a. am vom regulären Netzverkehr abweichenden Verhalten oder unterdrücken Angriffsverkehr von bestimmten Quellen.

Hierbei ist zu beachten, dass durch die Eingriffe eine Beeinträchtigung des legitimen Verkehrs wahrscheinlich ist. Die Mitarbeiter müssen im Umgang mit solchen Systemen daher entsprechend geschult werden.

3 Optionale Maßnahmen

3.1 Verlagerung besonders bedrohter Systeme zu Drittanbietern

Gerade bei Webservern, die zu den häufigsten Zielen von DDoS-Angriffen gehören, kann es bei besonders exponierten Systemen vorteilhaft sein, wenn diese zu Drittanbietern ausgelagert werden, die in der Lage sind, DDoS-Abwehrmaßnahmen in ihren Netzen bereitzustellen. Aufgrund der vollständigen Verlagerung zu einem Dienstleister ist das eigene Netz bei einem Angriff nicht mehr betroffen.

Es ist jedoch zu beachten, dass eine Remote-Analyse des Angriffsverkehrs an anderen Standorten und in anderen Netzen oft schwieriger oder eingeschränkt möglich ist. Bei Bedarf sollte geprüft werden, ob die Verkehrsanalyse ebenfalls vom Drittanbieter durchgeführt werden kann.

Außerdem wird empfohlen, auch die verlagerten Systeme in die Konzepte zur DDoS-Reaktion einzubeziehen.

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.