CENTRE FOR CYBERSECURITY BELGIUM

DDOS: VORBEUGUNG UND SCHUTZ

TECHNISCHE RICHTLINIE 2024

Belnet

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

.be

Stand: Februar 2024
Version: 2.1 Deutsch
Autor: Zentrum für Cybersicherheit Belgien (ZCB) in Zusammenarbeit mit Belnet

Das Zentrum für Cybersicherheit Belgien (ZCB) ist die nationale Behörde für Cybersicherheit in Belgien. Es wurde durch den königlichen Erlass vom 10. Oktober 2014 gegründet und ist dem Premierminister unterstellt.

Das ZCB hat den gesetzlichen Auftrag, Organisationen über den Schutz vor DDoS-Angriffen zu informieren und zu beraten. Angesichts der 2024 bevorstehenden Wahl in Belgien soll dieses Dokument als technische Richtlinie bei der Vorbeugung und Verhinderung von DDoS-Angriffen unterstützen und beraten.

ZUSAMMENFASSUNG

Im Kontext der 2024 in Belgien stattfindenden Wahl soll diese Richtlinie verschiedene DDoS-Schutzmaßnahmen erläutern. Auf föderaler Ebene sind unterschiedliche Gruppen an der Organisation und Durchführung der Wahl beteiligt. Ein wirkungsvoller Schutz vor DDoS-Angriffen erfordert eine Koordination dieser Gruppen.

Zunächst werden DDoS-Angriffe allgemein sowie ihre verschiedenen Ausprägungen, Wirkungen und Beweggründe charakterisiert. Kapitel 2 stellt proaktive Maßnahmen zur Vorbereitung auf DDoS-Angriffe vor und skizziert vorbeugende Lösungen. Kapitel 3 beschreibt mögliche Reaktionen auf einen DDoS-Angriff sowie technische Schutzvorkehrungen. Das letzte Kapitel enthält eine zweiteilige Checkliste. Der erste Teil ist eine Auflistung proaktiver Maßnahmen. Der zweite Teil fasst die in Kapitel drei beschriebenen Reaktionen in Listenform zusammen.

Die Richtlinie hat Hinweischarakter und ist als Beratung zu den Möglichkeiten der Vorbereitung und Reaktion auf eventuelle DDoS-Angriffe gedacht.

Das Dokument wurde in Zusammenarbeit mit Belnet erstellt.

Inhaltsverzeichnis

Glossar

ASN	autonome Systemnummer oder AS-Nummer
Botnet	verschiedene miteinander verbundene Geräte oft im Internet der Dinge (Internet of Things, IoT), die von Cyberkriminellen mit Schadsoftware infiziert und übernommen werden.
CDN	Content Delivery Network
CSIRT	Cyber Security Incident Response Team
C&C-Server	Command-and-Control-Server
DDoS	Distributed Denial of Service
DNS	Domain-Name-System
DoS	Denial of Service, Dienstblockade
Drupal	Content-Management-System
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
ISP	Internet Service Provider
NSM	Network Security Monitoring
OSI-Referenzmodell	Das Open Systems Interconnection-Modell definiert sieben Schichten, auf denen Computersysteme in einem Netzwerk kommunizieren.
SIP	Session Initiation Protocol (Sitzungs-Initiierungs-Protokoll)
SIEM	Security Information and Event Management (Management von Sicherheitsinformationen und -ereignissen)
SMTP	Simple Mail Transfer Protocol
SYN-Flood	Form eines Denial-of-Service-Angriffs (DDoS-Angriff), bei dem alle verfügbaren Serverkapazitäten belegt werden und der Server damit nicht mehr für den regulären Datenverkehr erreichbar ist.
TCP	Transmission Control Protocol
TTL	Time-to-Live
UDP	User Datagram Protocol
WAF	Web Application Firewall
ZCB	Zentrum für Cybersicherheit Belgien

1. Einleitung

1.1. ALLGEMEIN

Ein Denial of Service oder DoS ist ein Cyberangriff, der die Erreichbarkeit eines bestimmten Dienstes verhindern soll. Dazu werden nur ein Computer und eine Internet-Verbindung verwendet. Wird ein solcher Angriff mittels mehrerer Computer und ihrer Internet-Verbindungen parallel ausgeführt, spricht man von einem verteilten DoS oder Distributed Denial of Service (DDoS). Aber obwohl der Angriff verteilt erfolgt, haben alle daran beteiligten Computer ein gemeinsames Ziel und gehen koordiniert vor. Die Folge können schwerwiegende Auswirkungen auf den Betrieb von Organisationen und Unternehmen sein.

Die unterschiedlichen Arten von DDoS-Angriffen werden in Abschnitt 1.4. Arten von DDoS-Angriffen detailliert beschrieben.

1.2. BEWEGGRÜNDE FÜR DDOS-ANGRIFFE

Ein böswilliger DDoS-Angriff kann verschiedene Gründe haben: Erpressung durch Kapern des Netzwerks, Ideologie oder Hass, Wettbewerb, Politik, elektronischer Protest, Verschleierung, Auskundschaften, Experiment, Hacktivismus, Prestige/Aufgabe oder Erpressung durch Datendiebstahl. Hacktivisten richten ihre DDoS-Angriffe zum Beispiel auf Webseiten im Zusammenhang mit der Wahl, indem sie riesige Mengen an Datenverkehr an die Server senden. Dadurch sind die Seiten für andere Nutzer nicht mehr erreichbar. Diese Angriffsform ist oft politisch motiviert und zielt auf eine Störung des demokratischen Prozesses oder auf Unordnung ab oder ist gegen politische Entscheidungen gerichtet.

Die Hauptbedrohung im DDoS-Bereich geht aktuell von dem Anfang 2022 gestarteten Projekt DDoSia aus. Dahinter steht eine russisch-nationalistische Hackergruppierung, die bevorzugt der Ukraine und der NATO nahestehende Länder und Dienste angreift.

1.3. AUSGANGSPUNKTE VON DDOS-ANGRIFFEN

Die meisten DDoS-Angriffe erfolgen über ein Botnet.

Ähnlich wie bei „DDoS-as-a-Service“ wird ein Botnet dazu für mehrere Stunden „gemietet“. Dabei sind die Botnet-Eigentümer allerdings meistens nicht die Angreifer. Ein Botnet besteht aus zahlreichen Computern, die alle mit einer Schadsoftware infiziert wurden. Eine Agentenkomponente der Schadsoftware führt dann den eigentlichen Angriff durch, wobei die DDoS-Funktion zumeist nur eine der schädlichen Eigenschaften darstellt. Der Agent auf der befallenen Maschine erhält seine Anweisungen von einem C&C-Server, der alle beteiligten Agenten kontrolliert und steuert. Von der Infektion ihrer Maschinen und ihrer Beteiligung an einem DDoS-Angriff wissen die Besitzer in der Regel nichts. Bedeutsam ist, dass nahezu jeder Mensch einen DDoS-Angriff starten kann.

Dafür stehen zahlreiche Tools und Ressourcen (Botnets) zur Verfügung. Wer nur über begrenztes Wissen, aber ausreichend Entschlossenheit verfügt (oder Geld, obwohl Botnets nicht sonderlich teuer sind), kann einen DDoS-Angriff durchführen.

1.4. ARTEN VON DDOS-ANGRIFFEN

Die häufigsten DDoS-Angriffe lassen sich generell drei Kategorien zuordnen:

1. **Volumetrisch**: Volumetrische DDoS-Angriffe dienen dazu, normale Anfragen oder den legitimen Datenverkehr zu unterbrechen, indem sie die Netzwerkschicht eines Diensts mit gefälschten Anfragen aus zahlreichen Quellen fluten. Der Dienst ist auch für berechtigte Anwender dann kaum oder gar nicht mehr erreichbar. Das wird oft als Schicht-3-Angriff bezeichnet. Dazu gehören beispielsweise Reflection-/Amplifikations-Angriffe (UDP-Flood) oder ICMP-Floods auf das Internet Control Message Protocol.

2. **Protokoll**: DDoS-Protokollangriffe zielen auf Schwachstellen in Internet-Kommunikationsprotokollen. Hierfür eignen sich verschiedene Protokolle wie TCP oder ICMP. Typische DDoS-Protokollangriffe initiieren zahlreiche Verbindungen, jedoch ohne sie richtig zu starten (Beispiel: SYN-Flood). Dadurch soll die maximale Anzahl an Serververbindungen erschöpft werden. Da es sich beim Hauptvektor dieser Angriffe um die SYN-Flood (TCP) handelt, werden sie oft auch als Schicht-4-DDoS-Angriffe bezeichnet.

3. **Anwendungsschicht**: Angriffe auf der Anwendungsebene sind als Schicht-7-DDoS-Angriffe klassifiziert. Das Verfahren zielt auf die Anwendungsschicht des Netzwerk-Stacks ab, also auf die Schicht, auf der bestimmte Protokolle wie HTTP, SMTP oder DNS ausgeführt werden. Für Angriffe auf die Anwendungsschicht sind generell die meisten Kenntnisse über die Infrastruktur des Opfers erforderlich. Sofern sie korrekt durchgeführt werden, benötigen sie auf Seiten des Angreifers zugleich die wenigsten Ressourcen. Bei typischen Schicht-7-DDoS-Angriffen wird die Datenbank durch wahllos in die Suchmaske einer Webseite eingetragene Daten überlastet. Alternativ können auch nicht existente Subdomains beim DNS-Server angefragt werden. Ein Beispiel für Angriffe auf der Anwendungsebene sind Slowloris-HTTP-Angriffe, bei denen der Angreifer Daten absichtlich sehr langsam versendet. Dadurch werden geöffnete Verbindungen lange gehalten und die Ressourcen des Servers allmählich erschöpft.

2. Proaktive Maßnahmen

Dieses Kapitel stellt einige proaktive Maßnahmen technischer und nicht technischer Art vor, mit denen sich die Auswirkungen möglicher DDoS-Angriffe begrenzen lassen.

2.1. KENNE DEIN NETZWERK

Das eigene Netzwerk zu kennen, ist von großer Bedeutung. Welche öffentlichen Netzwerke und Netzwerkdienste sind vorhanden? Welche Dienste sind ausgelagert (zum Beispiel Cloud-Dienste)? Kein Zugriff ohne Internetverbindung!

Der gesamte Bestand an Netzwerktypologien, externen und internen IP-Adressen usw. sollte inventarisiert werden. Bei einem Angriff kann eine solche Bestandsliste entscheidend sein. Bei einem Cyberangriff sollte darauf auch offline zugegriffen werden können.

Ein nicht ins Netzwerk eingebundener Netzwerkscanner hilft bei der Erfassung der öffentlich zugänglichen und im Internet sichtbaren Geräte und Dienste. Hilfreich ist eine Liste der Diensteigentümer und der für die sichtbaren (technischen und nicht technischen) Positionen verantwortlichen Personen.

2.2. KENNE DEINE ANWENDUNGEN

Kenntnisse über die eigenen Anwendungen und entsprechend angepasste Schutzvorkehrungen sind von großer Bedeutung. Zur Belastung gleich mehrerer Systeme greifen DDoS-Angriffe oftmals ganz bestimmte Anwendungsteile an. Die entsprechenden Schwachstellen zu kennen, hilft bei der Entwicklung spezieller Schutzvorkehrungen.

Einige Seiten eines Webportals (zum Beispiel Suchmasken) können die Datenbankkapazitäten stark belasten und werden gerne angegriffen, um die Datenbank unerreichbar zu machen. Außerdem lassen sie sich oft auch nicht wirksam cachen. Zur Minimierung der DDoS-Wirkungen sollten sie erfasst und im Falle eines Angriffs gezielt deaktivierbar sein. Auch eine statische Kopie der Site kann sich als vorläufiger Ersatz für den Ernstfall als nützlich erweisen.

2.3. REAKTION AUF VORFÄLLE

Die Reaktionen auf Vorfälle sollten möglichst geplant und fortlaufend aktualisiert werden, denn ein DDoS-Angriff erfordert eine möglichst umgehende und wirkungsvolle Reaktion.

Die entsprechende Verfahrensanweisung beschreibt das Verhalten bei einem Cyberangriff und gibt die einzelnen Schritte der Reaktionsmaßnahmen vor:

- Ermitteln der Systeme und Geräte des Unternehmens
- Erstellen eines Business-Continuity-Plans (Geschäftskontinuitätsplans)/Notfallplans
- Zuweisen von Prioritäten bei der Wiederherstellung
- Aktuelle Funktionsweise von Systemen dokumentieren
- Zuweisen von Verantwortlichkeiten und Rollen an Personen mit den erforderlichen Fähigkeiten
- Vorhalten eines separaten Kommunikationskanals („Out-of-Band“)
- Erstellen einer Liste der Kontaktpersonen
- Einbinden von Experten für Cybereereignisse
- Erstellen einer Kommunikationsstrategie – weitere Hinweise: https://atwork.safeonweb.be/de/recent-news-tips-and-warning/krisenkommunikation-im-falle-eines-cyberangriffs

Besonders bei DDoS-Angriffen sind folgende Punkte unbedingt zu beachten:

- Besprechung mit dem Internet Service Provider (ISP): Wie sorgt der ISP gegen DDoS-Angriffe vor und welchen Schutz bietet er im Falle eines Angriffs? Beispiele wären Geoblocking, Änderung der öffentlichen IP-Adresse, Paket-Normalisierung usw.

- Service Level Agreements (SLAs) mit dem ISP speziell für DDoS-Ereignisse allgemein und auf allen Netzwerkebenen.

- Überprüfung und ggf. Überarbeitung der Verträge mit dem ISP und Cloud- und Hosting-Anbietern im

Hinblick auf den DDoS-Schutz.

- Engmaschige Überwachung der zentralen Infrastruktur zur schnellen Erkennung verstärkt verwendeter/erschöpfter Ressourcen und umgehenden Reaktion. Festlegen von entsprechenden Verantwortlichkeiten und Rollen.

- Erstellung von eindeutigen Referenzwerten zum Netzwerk-Traffic zur leichteren Erkennung von Abweichungen/Angriffen.

- Erkunden von Skalierungsmöglichkeiten bei der Infrastruktur im Falle eines Angriffs, besonders bei Cloud-basierten Instanzen (beispielsweise Azure).

- Durchführen regelmäßiger Stresstests als Soll-/Ist-Vergleich bei Infrastruktur und Maßnahmen.

- Vorhalten eines separaten Kommunikationskanals („Out-of-Band“) in Form einer sicheren Kommunikationsplattform, die nicht im angegriffenen Netzwerk läuft. Beispiele: Telefon (nicht sicher), Signal, Threema usw. Auch ist im Voraus festzulegen, welche Gruppen welche Kommunikationsmittel verwenden.

- Erstellen einer Liste von offline erreichbaren Kontaktpersonen: Die Liste muss offline (auf Papier) vorliegen und die Personen nennen, die helfen können oder informiert werden müssen. Das können interne Personen sein (Geschäftsführung, Beschäftigte, IT-Abteilung) oder auch externe (ISP, Sicherheitsfachleute, Kunden).

- Neben den technischen Fachleuten müssen auch Beschäftigte verfügbar sein, die Führungsentscheidungen treffen können. Diese Rollen möglichst in einem Business-Continuity-/Notfallplan dokumentieren.

- Führen einer Liste bekannter Bedrohungen (Botnets und böswillige IP-Adressen). Diese sollten permanent blockiert oder auf die Liste bei Bedarf schnell zugegriffen werden können.

- Verteilen der einzelnen Dienste über den gesamten IP-Raum zur Minimierung möglicher Nebenwirkungen und Erleichterung der Gegenmaßnahmen. Unter der gleichen IP-Adresse sollten nicht mehrere, voneinander unabhängige Dienste vereint sein.

- Für die Dienste/Anwendungen und Internetzugänge der Beschäftigten niemals dieselbe öffentliche IP-Adresse verwenden.

3. Einzelschritte der Reaktion auf DDoS-Angriffe

Kapitel 3 beschreibt mögliche Reaktionen auf einen DDoS-Angriff. Die nachfolgend skizzierten Schutzvorkehrungen stellen die Maßnahmen dar, die ein Unternehmen nach einem DDoS-Angriff mindestens ergreifen muss. Es gibt jedoch keine allgemeingültige Lösung.

Dem Opfer eines DDoS-Angriffs muss bewusst sein, dass für den Ablauf technisches Wissen, aber auch ein Zugriff auf die technischen Mittel vor Ort benötigt wird.

3.1. UMFANG DES ANGRIFFS ERMITTELN UND BESTÄTIGEN

Die Feststellung eines laufenden DDoS-Angriffs bedingt zunächst eine Einschätzung, ob und wie stark die Ressourcenverfügbarkeit eingeschränkt ist (beispielsweise nur für einige oder für alle Nutzer).

Dazu möglichst viele Informationen über den Angriff sammeln. Ein Inventar der betroffenen Systeme unterstützt die Beurteilung der Auswirkungen. Das lässt sich zum Beispiel anhand von Nutzerbeschwerden erstellen.

3.2. EINBLICK IN DEN ANGRIFF ERHALTEN

Wurde die Auswirkung des Angriffs dokumentiert und verstanden, ist als Nächstes die Ursache der Nichtverfügbarkeit zu untersuchen. Ein genaues Verständnis von der Funktionsweise des Angriffs ist die Grundlage für wirksame Gegenmaßnahmen.

- Ein SIEM- oder NSM-System kann dabei äußerst hilfreich sein.
- Ist keine Lösung für die Überwachung/Protokollierung vorhanden, können die Protokolle der Netzwerkgeräte/-anwendungen auch direkt ausgelesen werden.
- Sofern Referenzwerte zum Netzwerk-Traffic vorliegen, lassen sich damit die jeweiligen Angriffsmuster erkennen. Das können zum Beispiel rasant ansteigende Anfragen an einen Webserver oder (zunehmende) Anfragen nach nichtexistierenden Domains (DNS) sein.
- Möglichkeiten der Verbesserung und proaktiven Überwachung sind am besten mit dem ISP abzustimmen.

3.3. HILFE VOM ISP ODER DRITTLÖSUNG ZUR DDOS-ABWEHR

- Der ISP oder Drittanbieter sollte möglichst umgehend informiert und mit möglichst vielen Angaben zum laufenden Angriff versehen werden. Dazu gehören mindestens das angegriffene IPS, die Art des DDoS-Angriffs (siehe 1.4. Arten von DDoS-), mögliche Angriffsvektoren usw.
- Anhand der Informationen zu den Auswirkungen kann der ISP die Situation besser erfassen und konkrete Gegenmaßnahmen vorschlagen.
- Referenzwerte zu berechtigtem Traffic erleichtern die Feststellung der Menge an Traffic, der zu blockieren ist.
- Mit einem separaten Kommunikationskanal kann der ISP den Austausch während des Angriffs unterstützen. Angreifer versuchen die Abwehrmaßnahmen oft zu umgehen, indem sie ihre Vektoren während eines Angriffs ändern. Damit ist es aber auch möglich, Angaben zu den ergriffenen Maßnahmen zu machen. Der ISP kann dann schneller auf Maßnahmen reagieren, die entweder zu stark sind und berechtigten Traffic behindern, oder zu schwach, um hinreichend viele Pakete des Angriffs abzuwehren.
- Obwohl der ISP gegen Schicht-7-Angriffe wahrscheinlich machtlos ist, wenn er die betroffenen Anwendungen nicht selbst hostet oder managt, sollte er trotzdem eingebunden sein, weil er einige gleichzeitig eingesetzte Vektoren immerhin bekämpfen kann.
- Generell gilt, dass der ISP mit seinem eigenen oder einem zugekauften DDoS-Schutz zwar viele volumetrische Angriffe auf die Schicht 3 oder 4 abwehren, aber keinen vollständigen Schutz gewährleisten kann.
- Ist eine ganz bestimmte IP-Adresse (kein Perimetergerät) Ziel des Angriffs und der Schutz erweist sich

als unzureichend, besteht eine letzte Möglichkeit darin, beim ISP ein vorübergehendes Ignorieren („Blackhole") dieser IP-Adresse anzufragen. Das zieht natürlich die Nichtverfügbarkeit der jeweiligen Ressource und damit ein Scheitern dieses Angriffs teilweise erfolgreich ist, minimiert aber wenigstens die Begleiterscheinungen und erhält den Betrieb in einem gewissen Umfang aufrecht.

3.4. MÖGLICHKEITEN DES ANGEGRIFFENEN

Bei den nachfolgenden Schritten wird davon ausgegangen, dass Verbindungen nach außen weiterhin verfügbar sind. Ist das Gateway oder die externe Firewall wegen des Angriffs vollständig ausgefallen, kann der ISP womöglich weiterhelfen.

Vorhandene Ergebnisse der Überwachung/Protokollierung sind gegebenenfalls zu untersuchen. Andernfalls kann die externe Seite der Firewall auch mittels PCAP (Paketerfassungsanalyse) untersucht oder das Protokoll der betroffenen Anwendungen/Geräte auch direkt ausgelesen werden.

3.4.1. EINSICHT IN DEN ANGRIFF

- Worin besteht das Angriffsziel?
- Auf welche Ressourcen zielt der Angreifer ab?
- Um welche Art von DDOS-Angriff handelt es sich (OSI-Schicht 3-4 oder bis Schicht 7)?
- Auswertungsstatistik zum Ausgangspunkt des Angriffs erstellen: Kommen bestimmte Ausgangspunkte oder Länder in Frage? Kommen bestimmte ASNs in Frage? Das lässt sich besonders anhand der für ein NSM typischen Visualisierungen/Dashboards ermitteln.

3.4.2. ALLGEMEINE DDOS-SCHUTZMASSNAHMEN

Ganz allgemein empfiehlt sich eine schnelle Filterung des Angreifer-Traffics, um dem eigenen Netzwerk etwas Luft zu verschaffen. Zu diesem Zeitpunkt ist ein restriktives Sperrverhalten wahrscheinlich hinnehmbar. Jetzt geht es vor allem um die Gesundheit des Netzwerks und der Anwendungen sowie die Verfügbarkeit für die potentiell betroffenen Organisationen. Die so gewonnene Zeit lässt sich zur genaueren Untersuchung und Ergreifung eleganterer/gezielterer Schutzmaßnahmen gegen den jeweiligen Angriffsvektor nutzen.

- Vorübergehendes Sperren der angreifenden IP-Adressen: Die (vorübergehend) zu sperrenden IP-Adressen in eine (vorzugsweise separate) Negativliste eintragen. Wird eine anfragende IP-Adresse in der Negativliste gefunden, fängt das System die Verbindung ab und verweigert ihr den Zugriff. Das kann auf unterschiedliche Weise geschehen, indem zum Beispiel eine Fehlermeldung eingeblendet, der Anwender auf eine andere Seite weitergeleitet oder die Verbindung reaktionslos getrennt wird.

- Vorübergehendes Geoblocking/Geofencing bestimmter IP-Adressbereiche: Der Zugriff aus einer kompletten geografischen Region wird gesperrt.

- ASN-Sperre: Stammt der böswillige Traffic von bestimmten ASNs, werden diese oder zugehörige Netzwerkblöcke gesperrt.

- Loadbalancing und Skalierung: Mit dem Loadbalancing wird ankommender Traffic über mehrere Server oder Rechenzentren verteilt. Durch die Verteilung der Last werden einzelne Server oder Ressourcen vor Überlastung durch einen DDoS-Angriff geschützt. Mit der einstweiligen Erhöhung der Dienstkapazität wird die Wirkung des Angriffs begrenzt.

- Isolieren: Läuft der angegriffene Dienst mit mehreren anderen Diensten auf dem gleichen Server, wird der betroffene Dienst auf ein eigenes Gerät verlagert und Kollateralschäden des Angriffs dadurch minimiert.

- Beschränken: Den betroffenen Dienst auf das Minimum beschränken.

- Fernausgelöst ignorieren: Der gesamte Traffic wird auf eine bestimmte Ziel-IP an einer „Nullschnittstelle" umgeleitet, wodurch der böswillige Traffic ins Leere läuft, bevor er sein Ziel erreicht.

- Angegriffene Dienste/Anwendungen beenden: Diese Maßnahme wehrt Angriffe zwar nicht ab, schützt sie aber vor Funktionsstörungen. Allerdings können dabei auch erhebliche Datenverluste und Dienstausfälle entstehen.

3.4.3. SPEZIELLE ABWEHRMASSNAHMEN NACH ANGRIFFSVEKTOR

Im Falle eines DDoS-Angriffs auf Muster achten, die für Protokolle (Schicht 3/4) bzw. Anwendungen (Schicht 7) typisch sind, zum Beispiel:

Überblick Schicht 3 und 4

Protokoll	Angriffsvektor	Abwehrmaßnahmen
UPD	Reflection/Amplifikation	• Sperrbar, wenn der Traffic vom Zielsystem nicht benutzt/erwartet wird. Ansonsten helfen nur volumetrische/DDoS-Normalisierungen.
TCP	SYN-Flood	• Syn-Cookie einsetzen. • Timeouteinstellungen anpassen. • Wiederverwendung der ältesten nur halb geöffneten TCP-Sitzung.

Überblick Schicht 7

Anwendung	Angriffsvektor	Abwehrmaßnahmen
DNS	NX-Flood (Berechtigte) Anfrageflut	• Cache des DNS-Servers vor Überschwemmung mit NX-Antworten schützen. • DNS-Anfragen anhand einer Positivliste mit (Sub-)Domains beenden. • Begrenzung nach Quell-IP vornehmen.
HTTP/HTTPS	Slowloris Gezielte URL-Flood	• Timeouteinstellungen strenger anpassen. • Begrenzung nach Ziel-URLs einengen. • Bei weitgefächerter Auswirkung auf den Webserver: möglicherweise alle Anfragen an die meisten Ziel-URLs beenden (Ziel-URLs sind damit nicht mehr erreichbar). • Wenn zugänglich: Referrer-URL untersuchen.

3.4.4. WEITERE ABWEHRMASSNAHMEN

- Einsatz eines Geräts, das DDoS-Angriffe abwehren kann. Das ist allerdings eine teure Lösung, die sich jedoch rechnen kann, wenn es häufiger zu DDoS-Angriffen in der jeweiligen Umgebung kommt.

- Bei Webanwendungen: Dynamischen durch statischen Inhalt ersetzen. Statischer Inhalt zum Beispiel in Suchmasken, aber auch niedrigaufgelöste Bilder und komprimierte und verkleinerte CSS- und JavaScript-Dateien verringern den Datenverkehr.

- Resilienz durch (dauerhaften) Einsatz einer CDN-Lösung erhöhen.
- Das Netzwerk gegebenenfalls weiter untergliedern. Möglichst keine gemeinsam genutzte Infrastruktur!
- DNS-Einträge: längere TTL-Zeit einstellen. Ein Tag (24 Std.) als TTL-Zeit kann die Auswirkungen auf andere Dienste bei Ausfall der DNS-Server begrenzen. Eine längere TTL-Zeit wirkt sich allerdings auch auf die Übernahme von Änderungen aus.
- Bei Webanwendungen, zum Beispiel Webseiten: Einsatz einer WAF und eines Advanced Global CDN (AGCDN). Webseiten/Server werden von der WAF überwacht und böswilliger Traffic anhand verschiedener Regeln gesperrt. Die WAF erkennt und sperrt bekannte böswillige IP-Adressen, verdächtige User Agents und weitere ungewöhnliche Aktivitäten wie wiederholt versuchte Brute-Force-Angriffe auf die eigene Webseite. Das AGCDN verstärkt diesen Schutz, indem es plötzlich stark zunehmende Anfragen am Erreichen des Hauptservers (Ursprung) hindert, was ansonsten zur Nichterreichbarkeit der Webseite führen kann. Viele CDN-Anbieter haben die WAF als Teil der Bezahldienste bei sich laufen.
- Werden vom öffentlichen Internet aus erreichbare Cloud-Ressourcen verwendet, können auch die DDoS-Schutzvorrichtungen des Cloud-Anbieters aktiviert werden.

3.5. BEWEISAUFNAHME

Wird ein Vorfall dem ISP, dem nationalen CSIRT, den Behörden oder anderen Partnern nachträglich gemeldet, ist immer ein Nachweis zu führen. Dies kann auf NetFlow-, Netzwerk- oder Anwendungsebene erfolgen. Idealerweise lassen sich Nachweise auf allen Ebenen beibringen.

3.6. WIEDERHERSTELLUNG

Der DDoS-Angriff ist beendet, wenn der Netzwerk-Traffic wieder bei den früheren Referenzwerten liegt.

Diese Angriffe laufen manchmal allerdings in mehreren Wellen ab, die die Angreifer nacheinander auslösen. Werden die Schutzmaßnahmen daher bereits eingestellt, folgt eine weitere und noch gefährlichere Angriffswelle. Die Angriffsweise kann sich von Welle zu Welle auch ändern, um die Wirkung der eingesetzten Techniken auszuloten. Ist der DDoS-Angriff aber wirklich vorbei, können die deaktivierten Dienste neu gestartet werden.

Anschließend muss noch geprüft werden, ob alles wieder normal läuft. Wenn ja, sollte den Nutzern das entsprechend mitgeteilt werden.

3.7. AUSWERTUNG

Im Anschluss an den beendeten Angriff ist ein Meeting für den Erfahrungsrückfluss von allen Beteiligten anzuraten. Dabei werden auch die einzelnen Maßnahmen bewertet. Regelmäßige Stresstests können als Soll-/Ist-Vergleich bei Infrastruktur und Maßnahmen dienen.

Eine Auswertung der Schwachstellen erbringt bei der weiteren Vorbereitung abzuarbeitende konkrete Aktionen und führt zur Anpassung der Störfallbehandlung.

Das umfasst zum Beispiel:

- Den Angreifern bekannte IP-Adressen der Backend-Server ändern.
- Die Bandbreite der Internetverbindung korrekt anpassen; die Aktivitäten des Tagesgeschäfts sollten nur etwa 50 Prozent der gesamten Bandbreite ausmachen.
- Die Architektur anhand der erkannten Schwachstellen überprüfen.

4. Checkliste

Die nachfolgende Checkliste besteht aus zwei Teilen. Im ersten Teil geht es um proaktive Maßnahmen. Der zweite Teil fasst die in Kapitel 3 beschriebenen Reaktionen in Listenform zusammen.

4.1. PROAKTIVE CHECKLISTE

☐ Exponierte Netzwerke, Hosts und Dienste kennen, die Inventarliste regelmäßig aktualisieren und jederzeit mit möglichen Engpässen rechnen:

- Die Risiken und die Bedeutung der exponierten Systeme und Geräte des Unternehmens beurteilen.
- Schriftliche Liste der Diensteigentümer erstellen und freigeben.
- Aktuelle Netzwerk- und Dienstdiagramme erstellen.
- Separate Kommunikationskanäle vorhalten.
- Eine Liste von Ansprechpartnern offline oder auf Papier erstellen.

☐ ISP, nationales CSIRT und das eigene Unternehmen müssen einander samt Ansprechpartnern bekannt sein.

☐ Möglichkeiten und Grenzen des ISP im DDoS-Angriffsfall kennen.

☐ SLAs mit dem ISP für den DDoS-Angriffsfall vorbereiten.

☐ Firewall-Regeln regelmäßig überprüfen.

☐ Sicherheitsupdates von Betriebssystemen, Programmen und Routern automatisch aufspielen.

☐ Möglichst Cloud-Dienste verwenden; auf lokalen Servern gehostete Webseiten, Mailservices und andere Onlineplattformen sind äußerst verwundbar. Cloud-Dienste sind wegen ihrer breiten Verfügbarkeit weniger anfällig für DDoS-Angriffe.

☐ Krisenkommunikation planen.

4.2. REAKTIONEN AUF ANGRIFFSEREIGNISSE

☐ Interne Reaktionsmöglichkeiten bereitstellen.

☐ Load Balancer und Skalierung einsetzen und korrekt konfigurieren.

☐ Mit einem Reverse-Proxy arbeiten.

☐ Eine WAF und ein ADCDN einrichten.

☐ Die Netzwerkgeräte überprüfen und stärken und bewährte Praktiken verwenden.

☐ Eingeschränkte Dienste vorbereiten und bei einem Angriff verwenden.

☐ Webanwendungen: Dynamischen durch statischen Inhalt ersetzen.

☐ Resilienz durch eine CDN-Lösung erhöhen.

☐ Interne und öffentliche DNS-Infrastruktur ggf. weiter untergliedern.

☐ DNS-Einträge: eine längere TTL-Zeit einstellen. Ein Tag (24 Std.) als TTL-Zeit kann die Auswirkungen auf andere Dienste bei Ausfall der DNS-Server nach künftigen Angriffen begrenzen.

☐ Webanwendungen (zum Beispiel Drupal): Einsatz einer WAF und eines ADCDN.

☐ DDoS-Schutz der (Cloud-)Dienstanbieter aktivieren/anfragen.

☐ Böswillige IP-Adressen vorübergehend sperren.

☐ Vorübergehendes Geoblocking/Geofencing bestimmter IP-Adressbereiche.

☐ ASN-Sperrung: Stammt der böswillige Traffic von bestimmten ASNs, werden diese oder zugehörige Netzwerkblöcke gesperrt.

☐ Loadbalancing und Skalierung: Mit dem Loadbalancing wird ankommender Traffic über mehrere Server oder Rechenzentren verteilt. Durch die Verteilung der Last werden einzelne Server oder Ressourcen vor Überlastung durch einen DDoS-Angriff geschützt.

☐ Paket-Normalisierung: Der Traffic für einen bestimmten IP-Adressbereich wird in Rechenzentren umgeleitet, wo er „normalisiert", d. h. gereinigt wird. Nur sauberer Traffic wird in den Zielbereich weitergeleitet.

☐ Angegriffene Dienste/Anwendungen beenden.

☐ Fernausgelöst ignorieren.