Dialog für Cybersicherheit

Ergebnisbericht

Cyberresilience-Framework.

In IT-Krisen schneller agieren. (Kurz: RESI)

Handreichung kommunales DDoS-Szenario

Dialog für Cybersicherheit

Version 1.0

Stand: März 2026

1 Cyberresilience-Framework. In IT-Krisen schneller reagieren. © 2025 by Bundesamt für Sicherheit in der Informationstechnik, Dialog für Cybersicherheit Workstream RESI

Der Bericht dokumentiert die Fortführung des Workstreams „Cyberresilience-Framework. In IT-Krisen schneller agieren“. (Kurz: RESI), der von Dezember 2023 bis November 2024 im Dialog für Cybersicherheit durchgeführt wurde. Seitdem sind einige der beteiligten Mitarbeiter:innen des Workstreams weiterhin ehrenamtlich tätig, um den Ergebnisbericht des Workstreams aktuell zu halten. Zudem entstand der vorliegende Bericht (von März 2025 bis März 2026), der sich nun einem DDoS-Angriff (Distributed Denial of Service) widmet. Das Framework befähigt Kommunen, schneller und zielgerichteter zu handeln. Mit dem ausgearbeiteten Framework sollen Kommunen gestärkt werden, schneller auf einen DDoS-Angriff reagieren und rasch zum regulären Tagesablauf zurückkehren zu können.

Beteiligte Personen:

Marc Arnold (Stadt Heilbronn), Ralf Benzmüller (G DATA), Nils Brinker, Daniel Burdach (Gemeinde Grünheide), Sabine Griebsch (GovThings), Esther Kern (BIGS), Janka Kreißl (Dunkelblau GmbH & Co. KG), Franz Lantenhammer, Doris Rehn (BSI).

Der Dialog für Cybersicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist ein partizipativ ausgerichteter, gesamtgesellschaftlicher Dialog, um die Vielschichtigkeit der Perspektiven auf das Thema „Cybersicherheit“ möglichst breit und realitätsnah abzubilden und allen Beteiligten einen Austausch bzw. eine Mitwirkung auf Augenhöhe zu ermöglichen.

Der Dialog für Cybersicherheit soll daher ausdrücklich den verschiedenen Meinungen und Ansätzen zur Annäherung an das Thema „Cybersicherheit“ aus Sicht der Zivilgesellschaft Raum und die Möglichkeit zum Austausch geben, ohne dies durch eine engmaschige Steuerung des BSI zu beschränken.

Der vorliegende Bericht wurde von der BSI-Geschäftsstelle und Arbeitsgruppe RESI eigenständig erarbeitet. Die dort wiedergegebenen Ansichten spiegeln nicht zwangsläufig die Ansicht des BSI bzw. aller Teilnehmenden wider.

Weitere Informationen zum Dialog für Cybersicherheit:

https://www.dialog-cybersicherheit.de

Kontakt Geschäftsstelle: projekt-digitalegesellschaft@bsi.bund.de

Kontakt Projektgruppe: resi@dialog-cybersicherheit.de

Inhaltsverzeichnis

Die Anlage „Merkblätter und Checklisten“ wird in der aktuellen Version als eigenständiges Dokument bereitgestellt:
(Anlage „Merkplätter und Checklisten“ bzw. https://www.dialog-cybersicherheit.de/media/)

Einleitung

Aktuell konnten vermehrt DDoS-Angriffe (Distributed Denial of Service) auf Kommunen festgestellt werden. Kartiert wurden diese Angriffe in ehrenamtlicher Tätigkeit von Jens Lange im Projekt „Kommunaler Notbetrieb“[2], welches das einzige für Kommunen zugängliche Lagebild darstellt. So wurden im Frühjahr 2025 unter anderem die Webpräsenzen der Städte Nürnberg, Stuttgart, Dresden und Berlin angegriffen und waren bis zu mehreren Tagen nicht erreichbar. In der Folge war das Angebot an Dienstleistungen für die Bürger:innen teilweise eingeschränkt. Ende Juli 2025 waren die Webseiten von rund 30 Städten und Landkreisen teilweise stundenlang nicht erreichbar, sodass digitale Dienste wie Online-Antragsstellungen oder das Herunterladen von Formularen nicht möglich waren.

Die Angriffe konnten unter anderem der pro-russischen Hackergruppe NoName057(16) zugeordnet werden. Obwohl die Gruppe im Juli 2025 durch Sicherheitsbehörden mehrerer Länder ausgeschaltet wurde, war sie bereits nach wenigen Tagen wieder aktiv. Die Hauptziele der Gruppe waren unter anderem Verwaltungsstrukturen in Deutschland und Italien. Die Angriffe wurden angekündigt.

Diese Beispiele zeigen aber nur einen Ausschnitt der breiten Palette von unterschiedlichen DDoS-Angriffen und den Angreifern, von denen sie ausgeführt werden. Die Täter:innen und ihre Motivation reichen von Hacktivisten mit politischen oder ideologischen Motiven über Kriminelle, die Schutzgeld erpressen wollen bis hin zu unzufriedenen Kunden oder Beschäftigten. Sie alle können sich aus einer großen Auswahl an leicht zugänglichen und günstigen, aber professionellen DDoS-Dienstleistungen in kriminellen Untergrundforen bedienen. Je nach Angreifer und Motivation können unterschiedliche Gegenmaßnahmen notwendig sein.

Häufiges Ziel von DDoS-Angriffen sind Webseiten und die dort verfügbaren Dienste. Aber auch die Server anderer Internetdienste wie E-Mail, DNS[3], VPN[4] oder die Firewalls der Organisation sind mögliche Ziele.

Auch für die technische Umsetzung der DDoS-Angriffe gibt es vielfältige Vorgehensweisen, die häufig in verschiedenen Angriffswellen variiert werden. Grundlage der meisten Angriffe sind sogenannte Botnetze, die aus vielen kompromittierten Rechnern oder schlecht konfigurierten Webcams oder anderen IoT-Geräten[5] bestehen. Die Angriffstechniken lassen sich grob in drei Gruppen zusammenfassen:

2 https://kommunaler-notbetrieb.de
3 Domain Name System
4 Virtual Private Network
5 Internet of Things

- Volumenbasierte Angriffe senden sehr viele Datenpakete an die anvisierten Rechner (z. B. UDP-Flood[6]). Viel effektiver sind aber Reflection-Angriffe: Hier werden mit fehlerhaften Datenpaketen Fehlermeldungen auf schlecht konfigurierten Systemen im Internet erzeugt und an das Opfersystem geschickt.
- Die Kommunikation zwischen Geräten im Internet ist in Protokollen geregelt (z.B. HTTPS, POP3, FTP, SSH, DNS). In protokollbasierten Angriffen werden Eigenschaften der Kommunikation missbraucht, um die Systeme und häufiger die Ressourcen der Systeme auszulasten. Z. B. ist Anzahl der Netzwerkverbindungen bei vielen Netzwerkgeräten auf maximal 65554 begrenzt. Wenn diese alle belegt sind, können keine weiteren Anfragen bearbeitet werden.
- Die meisten Internetdienste werden durch Anwendungen zugänglich. Diese Anwendungen bieten weitere Möglichkeiten, um Systeme zu überlasten. Z. B. können rechenintensive Datenbankabfragen die darauf basierenden Webseiten unbenutzbar machen.

Es zeigt sich also, dass DDoS-Angriffe von unterschiedlichen Tätergruppen mit unterschiedlichen Motiven ausgeführt werden. Die Angriffe zielen auf vielfältige Geräte und Services und die Angreifer können auf professionelle Unterstützung von DDoS-Dienstleistern zurückgreifen. Beim Umgang mit DDoS-Angriffen ist Unterstützung von Abwehrprofis bei Providern oder DDoS-Abwehrspezialisten für die technische Bewältigung notwendig.

Mit dieser Handreichung möchten wir Kommunen ein Dokument an die Hand geben, wie sie

- einen DDos-Angriff schnell erfolgreich abwehren und wieder in den Normalbetrieb übergehen können
- sich auf einen DDoS-Angriff vorbereiten können beziehungsweise dieser Notfall mit einer geringeren Wahrscheinlichkeit eintritt.

In den meisten Fällen führt ein DDoS-Angriff zu einer temporären Einschränkung der Verfügbarkeit von Diensten. Ist die Kommune oder Institution darauf vorbereitet, kann sie diese Einschränkungen in der Regel schnell beseitigen, so dass der Schaden eher gering ist. Die Erstellung eines Business Continuity Management Plan auf Grundlage einer Risikoanalyse und/oder einer Business Impact Analyse mit Prozessen für das Störungsmanagement und einem Notfallplan helfen dabei.

Sollte es jedoch keine entsprechenden vorbereitenden Maßnahmen geben, kann sich der Ausfall von Systemen und Diensten auch zu einer Krise entwickeln.

6 User Datagram Protocol

Vorgehen

Im Rahmen der Recherche zum möglichen Ablauf eines DDoS-Angriffs und der Reaktion darauf analysierten die Beteiligten aktuelle Hilfestellungen für Kommunen und andere Behörden. Dabei wurde erfasst, welche Anleitungen bereits existieren und welche Unterstützung darüber hinaus möglich ist.

In Weiterführung der Recherchen zum Szenario „Ransomware“ wurden vor allem die dort erlangten Erkenntnisse genutzt und für das Szenario „DDoS-Angriff“ eingesetzt.

Das Framework stellt erprobte Ansätze und Erfahrungswissen bereit. Der praxisorientierte Leitfaden, „Handreichung Kommunales DDoS-Szenario“ bietet konkrete Hilfestellungen, die in einem solchen Vorfall die Arbeit wesentlich erleichtern können.

Die hier vorgestellten Materialien und Empfehlungen sind nicht nur theoretisch fundiert, sondern basieren auf fachlicher Expertise und Erfahrung. Sie bieten eine solide Grundlage, um sich in entsprechenden Situationen zu orientieren und im Ernstfall handlungsfähig zu bleiben. Diese Einblicke und Hilfestellungen machen den vorliegenden Bericht zu einer Unterstützung für alle, die für die Organisation, Sicherheit und Funktionsfähigkeit kommunaler Strukturen verantwortlich sind.

Wichtige Tipps

- ! Haben Sie eine Taschenkarte mit den wichtigsten Kontakten und Arbeitsschritten griffbereit (auch außerhalb der Dienstzeiten).
- ! Verwahren Sie essenzielle Hilfestellungen auch in Papierform auf und überprüfen Sie diese mindestens alle 6 Monate auf ihre Aktualität:
    - Adresslisten, Telefonnummern und E-Mail-Adressen von Behörden, Mitarbeiter:innen, Dienstleistern, Ansprechpartner:innen aus Nachbarkommunen
    - Notfallpläne, Checklisten
- ! Schulen Sie regelmäßig Ihre Mitarbeiter:innen zum Thema IT-Sicherheit.
- ! Führen Sie regelmäßig Notfallübungen durch, prüfen Sie Abläufe und dokumentieren Sie Änderungen.
- ! Nach einem IT-Sicherheitsvorfall: Der Vorfall und die Dokumentation der Vorfallbearbeitung sollen ausgewertet werden und Lehren für die Verbesserung der Reaktionsprozesse erarbeitet werden. Diese sind in die Notfalldokumentation aufzunehmen und offline verfügbar gehalten werden, so dass sie bei einem eventuellen weiteren Vorfall uneingeschränkt zugänglich ist.

Handreichung Kommunales DDoS-Szenario als Blaupause

Das Framework basiert auf einem fiktiven kommunalen DDoS-Szenario, welches als Blaupause dient. Dies soll einen konzeptionellen Rahmen bieten, der Kommunen bei der Organisation und Bewertung des IT-Sicherheitsvorfalls unterstützt. In diesem Szenario werden die verschiedenen Schritte exemplarisch für die Behörde durchgespielt. Dabei werden vor allem die behördeninternen Abläufe, die Aufgaben der IT-Administration und der Kommunikation betrachtet.

Um ein verständliches Schaubild des fiktiven kommunalen DDoS-Szenarios zu gewährleisten, wurden drei Handlungsstränge identifiziert:

- Behördeninterne Organisation,
- Technik/Systeme/IT-Sicherheit und
- Kommunikation

und der Ablauf entsprechend grafisch dargestellt.

Damit das Schaubild nachvollziehbar bleibt, wurde auf Querverbindungen zwischen den Handlungssträngen verzichtet. Dennoch sind diese während eines IT-Sicherheitsvorfalls vorhanden.

Auch wenn ein DDoS-Angriff in den meisten Fällen nach wenigen Stunden eingedämmt oder beendet ist und mit einem vorbereitetem Notfallplan oder einem funktionierenden Störungsmanagement bewältigt werden kann, wollen wir in dem Szenario den extremen Fall durchspielen, bei dem der Vorfall sich krisenhaft entwickelt. Dies ist meist auf eine fehlende oder nicht hinreichende Vorbereitung zurückzuführen.

Ziel: In solchen Situationen sollen Kommunen schneller und zielgerichteter handeln können.

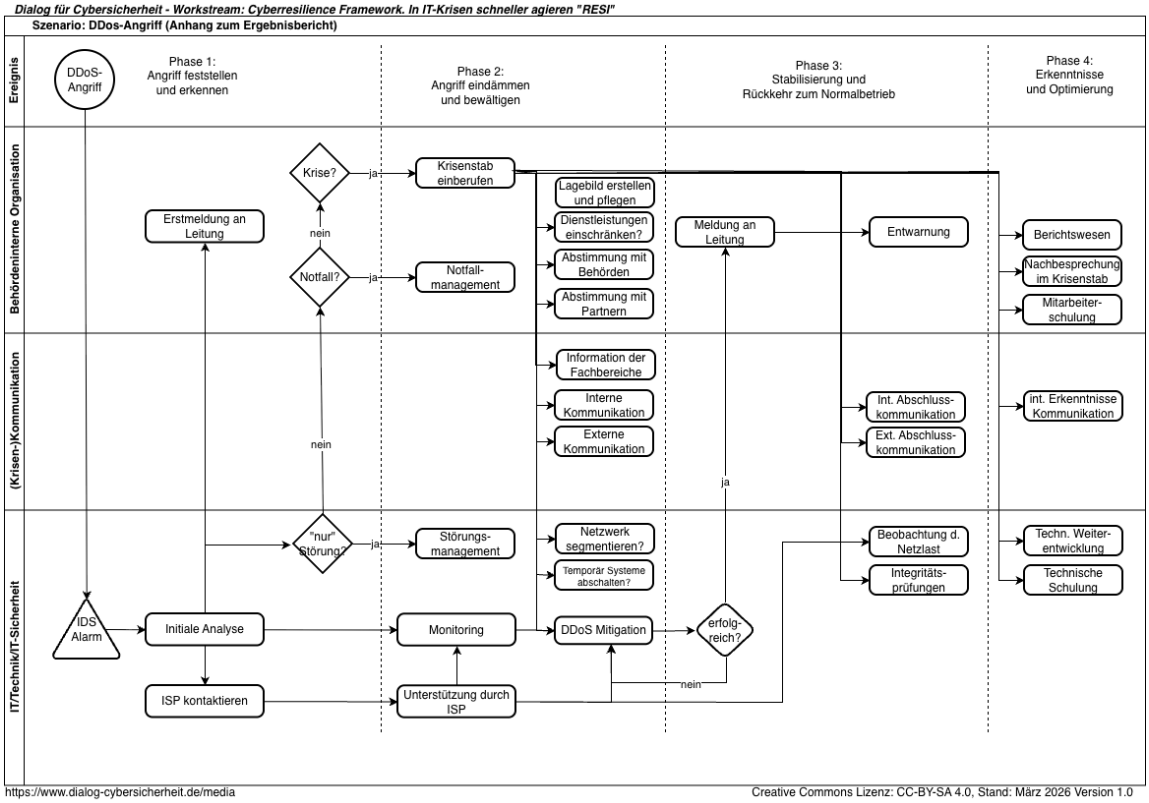

Abbildung 1- Überblick DDoS-Szenario

Das voranstehende Schaubild zeigt einen Gesamtüberblick. Im Folgenden werden die einzelnen Phasen des Angriffs noch einmal separat grafisch dargestellt, um die Schwerpunktprozesse der einzelnen Phasen zu beschreiben und zu verdeutlichen.

Anders als beim Szenario „Ransomware“, bei dem eine Organisation in der Regel unmittelbar vollständig betroffen ist und sämtliche Dienstleistungen ausfallen oder zumindest eingeschränkt sind, stellt es sich bei einem DDoS-Angriff anders dar.

Bei einem DDoS-Angriff werden meist nicht alle Verfahren und Dienstleistungen betroffen sein, sondern vor allem solche, die von außen, das heißt von den Bürger:innen oder Vertragspartner:innen online erreichbar sind. Hier liegt auch der maßgebliche Unterschied in der technischen Zuständigkeit.

Unabhängig von der technischen Zuständigkeit trägt die Kommune immer die Verantwortung für die von ihr betriebenen oder genutzten IT-Systeme und Verfahren sowie der damit verarbeiteten und gespeicherten (Personen-)Daten. Die Verantwortung für den Datenschutz und die Informationssicherheit bleibt immer in der Hand der Kommune. Es ist wichtig und hilfreich, wenn die Kommune im Rahmen einer Risikobewertung die Kritikalität der von ihr betriebenen und genutzten Systeme vorab festgestellt und Prioritäten festgelegt hat. Daraus lässt sich auch ableiten, ob es sich bei dem Vorfall um eine Störung, einen Notfall oder eine Krise handelt. Das BSI hat den BSI

Standard 200-4 Business Continuity Management[7] bereitgestellt, der Business Impact Analyse und Risikomanagement unterstützt.

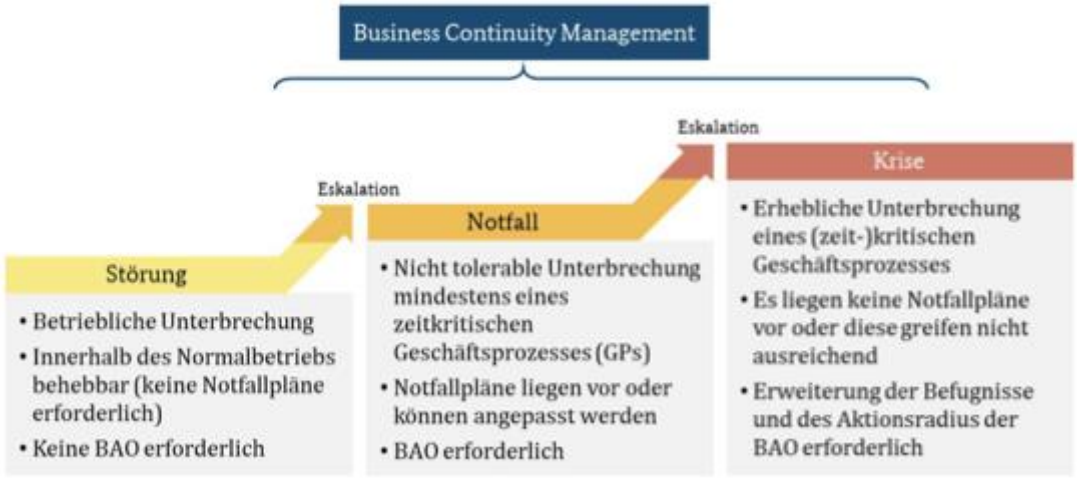

Abbildung 2 Abgrenzung von Störung, Notfall und Krise (BSI Standard 200-4, S. 20)

Wird das betroffene System von der Kommune oder Organisation selbst betrieben, liegt die alleinige Zuständigkeit für die Behebung des Vorfalls auch bei dieser. Ist diese nicht dazu in der Lage, sollte ein qualifizierter Dienstleister hinzugezogen werden.

Sind Systeme einer anderen Behörde oder Organisation betroffen, von denen die Kommune abhängig ist, liegt die technische Zuständigkeit bei der Organisation, die die Systeme bereitstellt.

Werden die betroffenen Systeme von einem Dienstleister betrieben, sei es durch einen kommunalen Zweckverband oder einen externen Dienstleister, trägt dieser die Verantwortung für die Schadensbehebung (IT-Dienstleister, Software-as-a-Service-Fachverfahren (SaaS), Webhoster).

Nicht zuletzt kann das betroffene System auch an einen Internet Service Provider ausgelagert sein. In diesem Fall erbringt dieser die vertraglich festgelegten Maßnahmen zur Wiederherstellung der vollen Funktionalität der vereinbarten Dienstleistung binnen einer vorgegebenen Frist.

7 https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

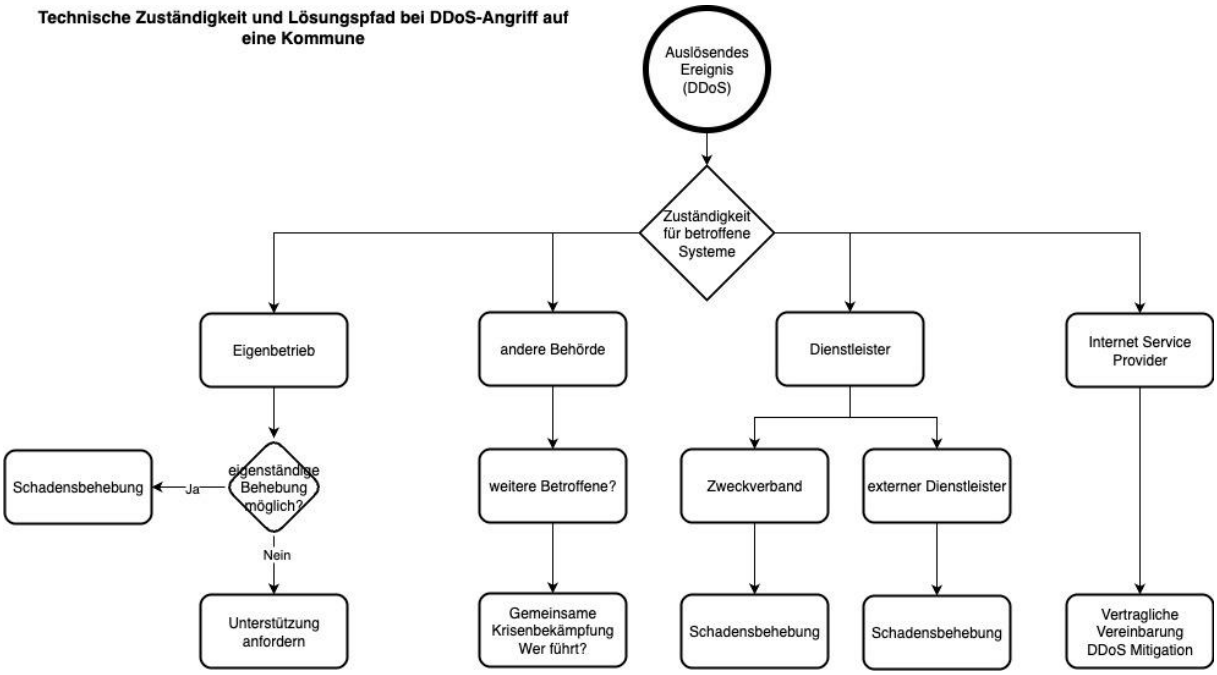

Abbildung 3 - Technische Zuständigkeit

Häufig sind im Falle eines DDoS-Angriffs jedoch gleichzeitig mehrere technische Zuständigkeiten gegeben. Dann ist die enge Abstimmung zwischen den beteiligten Stellen und klare Absprachen für die jeweiligen Zuständigkeiten für ein erfolgreiches Bestehen des Vorfalls ausschlaggebend. In den Fällen, in denen die Systeme von Dienstleistern oder anderen Behörden betrieben werden, sind vorab vertragliche Regelungen wie Service Level Agreements (SLA) zu treffen, die bei einem Vorfall die jeweiligen Verpflichtungen beinhalten.

Unabhängig von der jeweiligen technischen Zuständigkeit liegt die Verantwortung für die behördeninternen Abläufe und die Kommunikation stets bei der betroffenen Kommune oder Institution. Daher werden wir im Folgenden vor allem auf die Prozesse und Abläufe in diesen beiden Handlungssträngen detailliert eingehen. Die Leitung der betroffenen Kommune oder Institution trägt unabhängig von der Schwere des Vorfalls die Gesamtverantwortung. Vorbereitete Verfahren wie Störungsmanagement, Notfallpläne oder eingeübtes Krisenmanagement helfen bei der Bewältigung eines DDoS-Angriffs.

In einigen Fällen stellt die Kommune auch Dienste für andere Behörden bereit (efa-Prinzip). Dann ist die Kommune in diesem Zusammenhang für die Information der betroffenen Dienststellen verantwortlich.

1. Phase 1: Angriff feststellen und erkennen

Früherkennung - Event

Die Vorfallbewältigung bei einem IT-Sicherheitsvorfall beginnt mit der Meldung. Entsprechend des Ursprungs und Art der Meldung sind bereits erste Schlussfolgerungen und Maßnahmen möglich (z. B. Vertrauenswürdigkeit und Plausibilität der Meldung).

Ein DDos-Angriff wird häufig erkannt, wenn Nutzer:innen die Nichterreichbarkeit von Diensten feststellen und melden. Allerdings kann ein solcher Angriff auch durch entsprechende Warn- und Alarmierungssysteme in der Infrastruktur sowie das (Social)-Media-Monitoring in Bezug auf die einschlägigen Gruppierungen und Netzwerke erkannt werden.

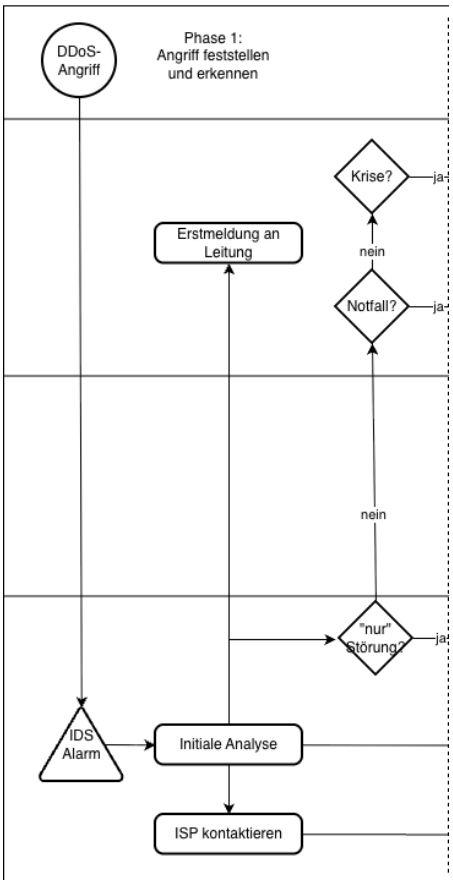

Abbildung 4 - Phase 1 (Angriff feststellen und Erkennen)

Die Meldung kann kommen

- intern:
  - Mitarbeiter:innen (fallen z. B. Unregelmäßigkeiten beim Erreichen der Webseite auf)
    - Internetauftritt oder weitere Onlineangebote der Kommune nicht mehr erreichbar
  - Eigene Warn-Systeme (z. B. das Security-Monitoring / Intrusion-Detection-System schlägt Alarm bei ungewöhnlich hoher Last, z. B. hohe Auslastung des Internetzugangs, ungewöhnlich viele gleichzeitige Verbindungen oder einseitiger Traffic-Anstieg)
  - IT bzw. Teile der IT sind nicht mehr funktionsfähig
- Extern:
  - Eigener IT-Dienstleister bzw. Erkennungsmechanismen des Dienstleisters
  - Behörde
  - Bürger:innen, Unternehmen
  - Presse, Medien (Social Media, Internet etc.)

Angriffsart einordnen und bestätigen

Um die Angriffsart einzuordnen, sollte die eingegangene Meldung in einem ersten Schritt durch das verantwortliche IT-Team bzw. IT-Sicherheitsteam analysiert werden. Erste Indizien können auf einen DDoS-Angriff hindeuten. Hierzu zählen z. B. Logdateien,

die IPs/Herkunftsländer der Anfragen, die Netzauslastung oder Traffic-Muster (wiederkehrende Wellen des Datenverkehrs).

Die Auswertung kann verdeutlichen, ob es sich um einen gezielten DDoS-Angriff handelt oder um einen DDoS-Angriff, der vorgeschaltet ist, um ein weiteres negatives Ereignis zu verschleiern, beispielsweise Malware-, Phishing- oder Ransomware-Angriffe. In dem vorliegenden, ausgearbeiteten Beispielszenario wird von einem gezielten DDoS-Angriff ausgegangen.

Meldung einschätzen

Eine Abgrenzung und den Eskalationsmechanismus für das Schadensereignis stellen die Begriffe Störung, Notfall und Krise dar. Die eingegangene Meldung sollte intern bewertet werden, um zu verifizieren, worum es sich laut BSI-Standard 200-4[8] handelt:

- technische Störung, die mit Standardmaßnahmen und Allgemeiner Aufbauorganisation (AAO) bewältigt werden kann
- Notfall oder Krise, die nur mithilfe einer „Besonderen Aufbauorganisation“ (BAO) bewältigt werden kann

Eskalation und Alarmierung:

Im Falle eines DDoS-Szenarios informiert das zuständige IT-(Sicherheits)team die zuständigen Führungskräfte. Auf Basis der Erstmeldung und der Indizien der Erstuntersuchung erfolgt eine Entscheidung darüber, welche Eskalationsstufe (Störung, Notfall oder Krise) festgestellt wird und welche Form der Aufbauorganisation (AAO/BAO) herangezogen wird.

8 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8

2. Phase 2: Angriff bewältigen/eindämmen

2.1. Sofortmaßnahmen

In den parallel ablaufenden Handlungssträngen:

- „behördeninterne Organisation“,
- „Technik/Systeme/IT-Sicherheit“
- „Kommunikation“

sind erste Sofortmaßnahmen zu ergreifen.

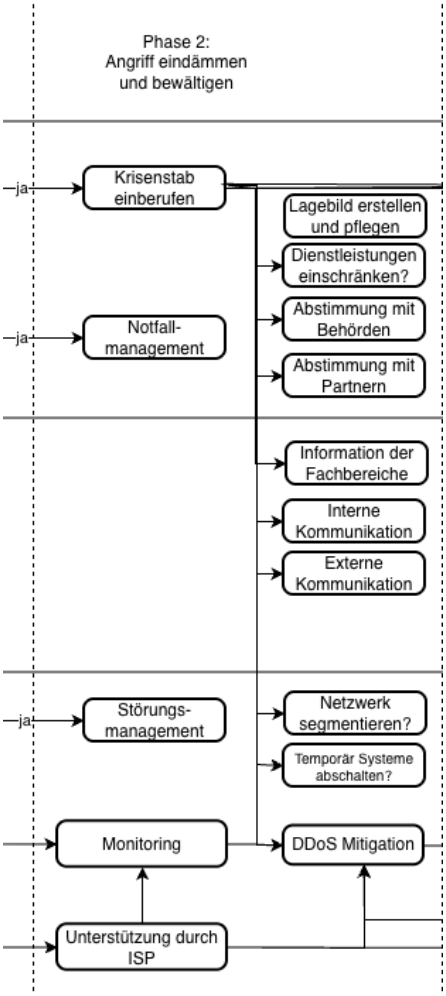

Abbildung 5 - Phase 2 (Angriff eindämmen und bewältigen)

2.2. Behördeninterne Organisation

Krisenstabsleitung

Wenn die Erstinformationen ergeben haben, dass ein Krisenstab notwendig ist, um den IT-Sicherheitsvorfall organisiert zu bearbeiten, muss dieser entsprechend eingerichtet werden. Der Krisenstab leitet das Krisenmanagement und trifft die Entscheidungen. Der/die Leiter:in des Krisenstabs trägt die Verantwortung. Er/sie muss dabei alle Aspekte, die für die Bewältigung der Krise relevant sind, berücksichtigen. Dazu holt er/sie sich die Erkenntnisse des Krisenstabes ein. Diesem sollten neben der Management-Ebene ebenfalls der/die IT-Sicherheitsbeauftragte sowie die IT-Leitung, der/die Datenschutzverantwortliche und ein/e Verantwortliche/r/ für die Kommunikation angehören. Auch die für das Personal zuständigen Stellen (Personal-Management) sollten einbezogen werden.[9] Ggf. kann bzw. muss der Personenkreis noch erweitert werden, z. B. um Jurist:innen oder externe Fachexpertise. Der/die Leiter:in des Krisenstabs kann fachlichen Expert:innen die Leitung von Teilaufgaben übertragen. Diese verantworten dann eigenständig ihren Bereich und berichten laufend an den/die Leiter:in des Krisenstabs.

- *Interne Koordination*

- [Prozedur] Notfallteam / Krisenstab startet Reaktion nach festgelegtem Protokoll
- [Information] Fachbereiche über Situation informieren

9 Der Personalrat ist zu beteiligen und kann als Multiplikator genutzt werden, ist aber nicht Mitglied des Krisenstabes.

- [Reaktion] Aufrechterhaltung essenzieller Verwaltungsprozesse[10]
- [Reaktion] Lückenlose Protokollierung aller Schritte Erkenntnisse, Maßnahmen, Beauftragungen und Kosten

2.3. IT/Technik/IT-Sicherheit

Technische Gegenmaßnahmen

Kurzfristige Abwehr

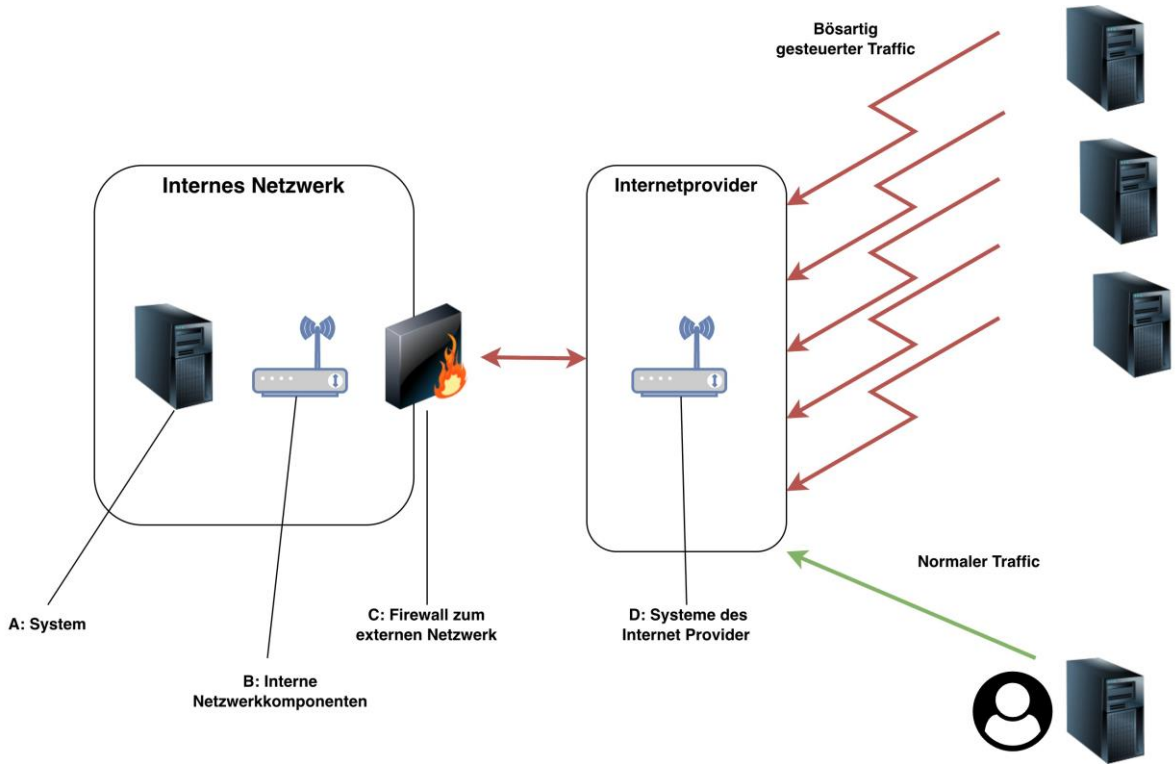

Abbildung 6 - Überblick DDoS-Angriff auf Netzwerk (eigene Darstellung)

Im Rahmen der initialen technischen Gegenmaßnahmen, kommt es vor allem darauf an, die Last auf die eigenen Systeme zu mindern. Dies kann grundsätzlich an sämtlichen Stellen geschehen, an denen der Verkehr aus dem offenen Internet zugespitzt auf die eigenen Systeme bündelt. Entsprechend ist eine Filterung an mehr oder weniger allen Stellen, durch welche der Internetverkehr fließt und die (direkt oder indirekt) unter eigener Kontrolle stehen, möglich. Knotenpunkte hierbei sind üblicherweise und unter anderem der Internetprovider (siehe Punkt D in Abbildung 6) und an den Grenzen des eigenen Netzwerkes die Firewalls (siehe Punkt C in Abbildung 6). Je nach betroffenen Systemen haben diese oft auch dezidierte Filterungsmöglichkeiten, wie etwa eine App-Firewall (siehe Punkt A und B in Abbildung 6).

10 Frage „Worauf kann ich nicht verzichten?“ (priorisierte Leistungen) umkehren zu „Auf welche Leistungen kann (vorübergehend) verzichtet werden (zu Gunsten von priorisierten Leistungen).“

Im Rahmen der initialen Reaktion gilt es, mögliche Knotenpunkte auszumachen, insbesondere solche die unter eigener Kontrolle stehen. Neben der grundsätzlichen Verfügungsgewalt ist weiterhin kurzfristig vorhandenes Know-how notwendig, um eine effektive Filterung umzusetzen (bspw. eine effektive Anpassung der Firewall-Konfiguration).

Es ist nicht unüblich, dass entweder das betroffene System insgesamt oder Teile der Infrastruktur, welche vom Angriff betroffen ist, von Dienstleistern betrieben werden. In diesem Fall ist dieser zu kontaktieren und gegebenenfalls sind weitere Maßnahmen abzustimmen.

Ein elementarer erster Schritt ist vor allem der Kontakt zum Internetprovider. Als erstes Nadelöhr aus dem offenen Internet zum eigenen Netzwerk sind Maßnahmen hier besonders effektiv. Weiterhin verfügt dieser aufgrund seiner Tätigkeit meist über entsprechendes Know-how, um DDoS-Attacken entsprechend abzuwehren.

Ebenfalls ist es ratsam, sich nicht unbedingt auf eine einzelne Maßnahme zu verlassen. Mithilfe einer mehrstufigen Filterung des Netzwerkverkehrs erreicht man kumulativ den maximalen Effekt.

Kurzfristig lässt sich eine Sperrung des Zugangs vornehmen, um die Überlastung zu unterbinden und die Netzinfrastruktur nicht zu gefährden. Die Abwehr des DDos-Angriffs erfolgt durch

- eine Anpassung von Firewall-Regeln und Traffic-Filterung (Blockieren unbekannter schädlicher IP-Bereiche),
- die Aktivierung von DDoS-Schutzfunktionen in vorhandenen Systemen (Rate Limiting, Connection Limits),
- eine Kontaktaufnahme zum Internet-Provider (z. B. Upstream-Filterung)
- Einbindung externer Dienstleister, wenn nur sehr wenig oder kein Know-how in der Kommune vorhanden ist[11]
- Einbindung des Internetproviders und der der Webseiten-Hoster
- die Auswertung und Meldung der Protokolle der IP-Adressen der angreifenden Systeme und einer Abuse-Meldung (Missbrauchsmeldung) an die zuständigen Provider, damit diese eine Sperrung des Zugangs vornehmen, um die Überlastungsangriffe zu unterbinden und die Netzinfrastruktur nicht zu gefährden.

Evaluierung und Durchführung Trennung kritischer Systeme

- [Reaktion] Segmentierung des Netzwerks soweit dies in der Situation kurzfristig möglich ist, damit wichtige Dienste vom Angriffsverkehr isoliert bleiben

11 Auf der BSI-Website findet sich eine Liste qualifizierter DDoS-Mitigation-Dienstleister im Sinne § 3 BSIG: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.html

- [Reaktion] Sicherstellen, dass keine Kompromittierung der Daten stattfindet, Monitoring für mögliche Parallelangriffe (z.B. Datenabfluss, Verschlüsselung von IT-Systemen und Daten (siehe hierzu das RESI-Szenario Ransomware[12])

Stufenweiser Rückzug nicht-essenzieller Dienste

- [Reaktion] Temporäres Abschalten weniger wichtiger Online-Dienste (Schonen von Ressourcen für kritische Systeme) / ggf. Umschalten auf Bypässe

2.4. Kommunikation (Beispielvorlagen siehe Anhang)

Interne Kommunikation:

Inhalte der Erstinformation an Mitarbeitende

- Was ist passiert / passiert gerade (möglicherweise auch mit einfacher Begründung wie „technische Probleme“)
- Welche Systeme und Dienste funktionieren, auf welche Systeme und Services muss vorübergehend verzichtet werden
- Welche Tätigkeiten sollten vorübergehend vermieden werden
- Wie sehen vorübergehende Behelfslösungen/manuelle Workarounds aus, wo werden diese ggf. vorgenommen
- Wer kann aktuell arbeiten und wer nicht/ wer kann sich wie/wo einbringen und ggf. unterstützen
- Welche Informationen müssen/dürfen nach außen gegeben werden (Verweis auf zentrale Pressestelle)
- Kontaktdaten für Rückfragen (sofern möglich), z. B. Support / HelpDesk

Externe Kommunikation:

Inhalte der Erstinformation an Bürger:innen/Medien

- Was ist passiert / passiert gerade (möglicherweise auch mit einfacher Begründung wie „technische Probleme“)
- Information, dass an der Behebung des Vorfalls gearbeitet wird
- Wie stellt die Kommune weiterhin wesentliche Dienstleistungen sicher.
- Welche (wichtigen) Systeme funktionieren, auf welche Services muss vorübergehend verzichtet werden
- Wie sehen vorübergehende Behelfslösungen/manuelle Workarounds aus und wo werden diese vorgenommen
- Kontaktdaten für Rückfragen (sofern möglich) / Hotline

Inhalte der Erstinformation an Behörden

12 https://www.dialog-cybersicherheit.de/media/

- (je nach Bundesland freiwillige) Meldung an das Landes-CERT und ggf. weitere Stellen gem. rechtlicher Vorgaben (siehe Übersicht Meldepflichten). Ggf. Meldung an zuständige Behörde für den Landesverfassungsschutz (bei Verdachtsfall auf Sabotage)
- Freiwillige Meldung an die zuständige Zentrale Ansprechstelle Cybercrime der Polizei (ZAC), ggf. Anzeige
- ggf. Meldung (nach Art. 33) an die zuständige Datenschutzaufsicht, sofern Systeme oder Dienste, die personenbezogene Daten verarbeiten, betroffen sein könnten. Auch bei einer Störung der Verfügbarkeit kann es sich um eine Verletzung des Schutzes personenbezogener Daten handeln. Die Pflicht zur Meldung kann im Falle eines geringen Risikos unterbleiben (bspw. eine bloße Störung einer Informations-Website). Eine Meldepflicht ist jedoch eher zu bejahen, sofern etwa E-Services, welche über registrierte Nutzerkonten erreichbar sind, betroffen sind. Die Meldung ist innerhalb von 72 Stunden ab Erkennen des Angriffs abzugeben. Die tatsächliche Bewertung, ob eine Meldung notwendig ist, obliegt der/dem internen oder externen Datenschutzbeauftragten.

Sonstige:

- Benachrichtigung an den IT-Dienstleister, insbesondere falls hierzu eine gesetzliche oder vertragliche Verpflichtung besteht

Auf die Erstinformation folgen – sofern der Vorfall länger andauert – kontinuierliche Status-Updates in angemessenen Abständen. Darin wird über den aktuellen Stand, erzielte Ergebnisse, die Verfügbarkeit der Systeme bzw. Services und nächste Schritte informiert.

Beispielvorlagen für die o.g. Meldungen finden Sie im Anhang. Für die behördlichen Meldungen stellen die Empfängerstellen i.d.R. ein Template oder ein Webformular bereit. Eine Übersicht der Kontaktadressen für die jeweilige Behörde finden Sie in den Anlagen.

3. Phase 3: Stabilisierung und Rückkehr in den Normalbetrieb

3.1. Weitere Maßnahmen

Nachdem die Sofortmaßnahmen gegriffen haben und sich die Lage beginnt zu normalisieren, ist es wichtig, dass weiterhin alle Systeme überwacht werden, um bei einer möglichen weiteren DDoS-Angriffswelle sofort reagieren zu können. Dabei ist ein besonderes Augenmerk auf die enge Abstimmung zwischen behördeninterner Organisation, technischer Leitung (IT-Notfallstab/Dienstleister) und Kommunikationsverantwortlichen zu richten.

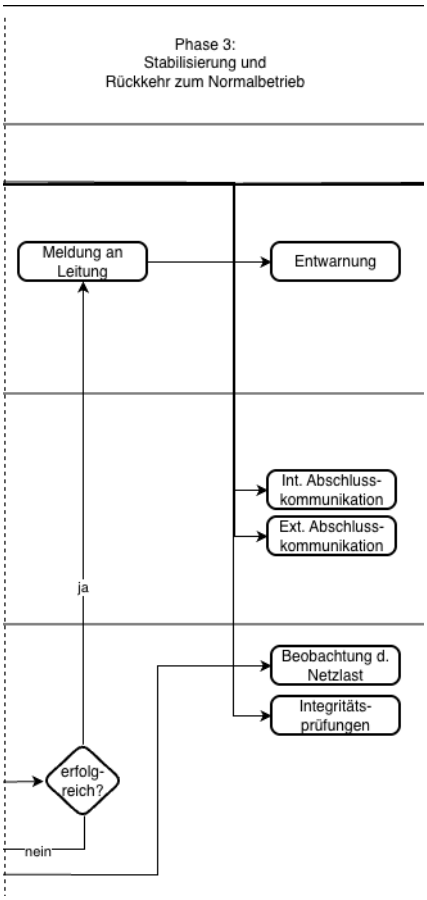

Abbildung 7 - Phase 3 (Stabilisierung und Rückkehr zum Normalbetrieb)

3.2. Behördeninterne Organisation

Krisenstabsleitung:

Solange die Einschränkungen durch den DDoS-Angriff anhalten, setzt der Krisenstab seine Aufgabenwahrnehmung weiter fort. Sobald die Erreichbarkeit der einzelnen gestörten Systeme wieder hergestellt ist, können die regulären Prozesse wieder in Gang gebracht werden. Dabei hat der Krisenstab weiterhin die Aufgabe, die Rückkehr in den Normalbetrieb zu begleiten, um im Falle einer erneuten Angriffswelle sofort wieder in den Krisenmodus zu wechseln.

3.3. IT/Technik/IT-Sicherheit

Die Beobachtung der Netzlast ist ein wesentlicher Bestandteil. Hieraus können wichtige Schlussfolgerungen gezogen und weitere Maßnahmen abgeleitet werden:

- Ein engmaschig fortgeführtes Monitoring zeigt auf, ob die Angriffslast nachlässt oder weiter besteht (DDoS-Angriffe laufen häufig in Wellen ab)
- Entsprechend der Auswertung des Monitorings kann das schrittweise Wiederhochfahren der betroffenen Dienste / Fachverfahren angestoßen werden oder zeitlich begrenzter Zugang je nach Kapazität ermöglicht werden.
- Integritätsprüfungen

- Technische Forensik, um sicherzustellen, dass kein zusätzlicher Schaden (heimliche Malware-Installation) entstanden ist[13]
- Prüfen aller wichtigen Datenbanken und Anwendungen

3.4. Kommunikation (Beispielvorlagen siehe Anhang)

Interne Kommunikation:

Inhalte der Abschlussinformation an Mitarbeitende

- Information zur wiederhergestellten Erreichbarkeit der Systeme/Dienste
- Information zu kurz-/mittelfristigen (Präventions-)Maßnahmen
- Danke an Beteiligte für Unterstützung
- Ggf. Zusammenfassung für Gremien und Öffentlichkeit mit Kommunikation der wichtigsten Erkenntnisse

Externe Kommunikation:

Inhalte der Abschlussinformation an Bürger:innen/Medien

- Information zur wiederhergestellten Erreichbarkeit der Systeme/Dienste
- Information zu kurz-/mittelfristigen (Präventions-)Maßnahmen
- Danke für Geduld und Verständnis

Inhalte der Abschlussinformation an Behörden

- Unterschiedlich, je nach Art der Meldung. In der Regel Konkretisierung der Informationen der Erstmeldung, bzw. Ergänzung um nun gesicherte Erkenntnisse. Der genau geforderte Inhalt kann bestenfalls mit der bestehenden Kontaktperson abgeklärt werden.
- Insbesondere relevant für operativ tätige Stellen, in der Regel jedoch zumindest die Information der Beendigung der Akutphase.

13 Weitere Informationen zur IT-Forensik finden sich hier: https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Sicherheitspruefungen/IT-Forensik/forensik_node.html.

4. Phase 4: Erkenntnisse / Optimierung

4.1. Folgerungen

Nachdem der Vorfall bereinigt ist und die Organisation zum Normalbetrieb übergegangen ist, müssen die Erkenntnisse sowohl in der Vorbereitung als auch in der Durchführung des Vorfalls ausgewertet werden. Dabei ist es wichtig, die Mitarbeiter:innen und alle Bereiche eng mit einzubinden. Eine offene Fehlerkultur hilft dabei, die gewonnenen Erfahrungen für zukünftige Verbesserungen zu nutzen.

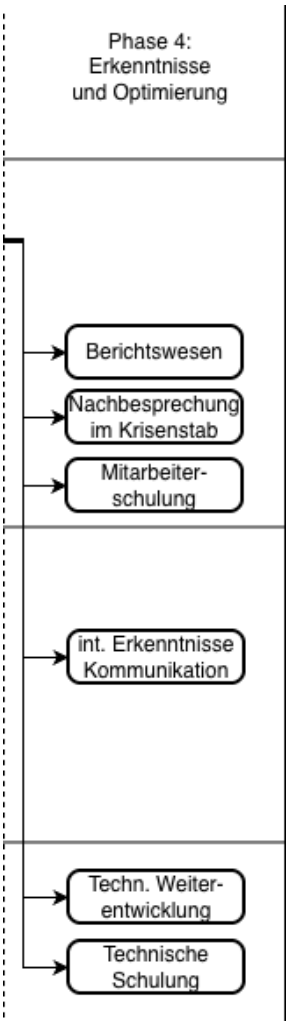

Abbildung 8 - Phase 4 (Erkenntnisse und Optimierung)

4.2. Behördeninterne Organisation

Nachbesprechung im Krisenstab

- Dokumentation und Bewertung, welche Maßnahmen gut funktioniert haben / Bewertung: Welche Maßnahmen waren wirksam? Wo gab es Lücken?
- Ggf. Anpassung / Erweiterung der Notfallpläne

Mitarbeiterschulungen

- Bewusstsein der Mitarbeitenden schärfen
- Verdeutlichen, wie schnell an IT gemeldet werden muss. / Was ist auffällig?

4.3. IT/Technik/IT-Sicherheit

Technische Weiterentwicklung

- Systemkomponenten aktualisieren und gegebenenfalls härten (z. B. durch stärkere Zugangsfilter)
- Gegebenenfalls dauerhafte Implementierung eines DDoS-Schutzdienstes und Erhöhung der Bandbreite
- Erneute Überprüfung der Segmentierung des Netzwerks

4.4. Kommunikation (Beispielvorlagen siehe Anhang)

Interne Kommunikation

– Erkenntnisse aus dem Vorfall sollten in jeweils notwendigem Maß den entsprechenden Gremien vorgelegt werden, inklusive Nachweis und Aufschlüsselung der Kosten, Dauer der Bewältigung, Personaleinsatz.

Weitergehende Literatur / Quellen

BSI Publikation: Maßnahmenkatalog Ransomware

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Schutz-vor-Ddos-Angriffen/schutz-vor-ddos-angriffen_node.html

BSI Publikation: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall, Arbeitspapier – Version 1.2 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

BSI Webseite - Checkliste Technik:
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Checkliste-Technik/ich-habe-einen-it-sicherheitsvorfall-checkliste-technik_node.html

BSI-Webseite: Liste zertifizierter IT-Sicherheitsdienstleister in den Geltungsbereichen IS-Revision und IS-Penetrationstests

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Anerkennung-von-Stellen-und-Zertifizierung-IT-Sicherheitsdienstleister/IS-Rev/Liste-IT-Sicherheitsdienstleister/liste-is-revi-is-pentester_node.html

BSI-Veröffentlichung: Liste der qualifizierten APT-Response-Dienstleister; Stand: 01.08.2024

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

Glossar und Abkürzungen

Begriff	Abkürzung	Beschreibung
Allgemeine Aufbauorganisation	AAO	Beschreibung festgelegter Hierarchie, Zuständigkeiten und Kommunikationswege - Grundstruktur
Besondere Aufbau- und Ablauforganisation	BAO	Beschreibung festgelegter Hierarchie, Zuständigkeiten und Kommunikationswege bei Großeinsätzen
Botnetz, Botnet		Ein Botnetz besteht aus einer Anzahl von IT-Systemen (Computer, Internet of Things Geräte etc.), die von Cyberkriminellen übernommen wurden und für Angriffe genutzt werden.
Command & Control Rechner/Server	CC-Server	Mit dem Command & Control Rechner/Server steuert der Angreifer die von ihm übernommene IT-Systeme, die sein Botnetz bilden
Denial of Service	DoS	Denial of Service (engl. Verweigerung des Dienstes) – kurz DoS – bedeutet so viel wie etwas unzugänglich machen oder außer Betrieb setzen. Man spricht auch von einem Überlastungsangriff.
Distributed Denial of Service	DDoS	Ein Distributed Denial of Service liegt vor, wenn der Überlastungsangriff von einer Vielzahl von verteilten Systemen ausgeht. Diese verteilten Systeme sind vom Angreifer übernommene Computer oder IT-Systeme, die auf Anweisung eines Command & Control-Rechners synchronisiert den Angriff durchführen.
Domain Name System	DNS	Hierarchisch unterteiltes Bezeichnungssystem in einem meist IP-basierten Netz zur Beantwortung von Anfragen zu Domain-Namen (Namensauflösung)
„Einer für Alle“-Prinzip	EfA	Mit dem Konzept EfA-Online-Dienste sollen digitale Dienste für die öffentliche

		Verwaltung an einer Stelle entwickelt und für andere/alle weiteren Dienststellen Länder- und Kommunenübergreifend bereitgestellt und genutzt werden. Nutzer:innen können mit einem einzigen Online-Dienst in Deutschland ihr Anliegen erledigen Dafür wird ein Online-Dienst für eine Verwaltungsleistung einmal attraktiv und nutzerfreundlich entwickelt und betrieben.
Internet of Things	IoT	Sammelbegriff für Technologien einer globalen Infrastruktur der Informationsgesellschaften, die es ermöglicht, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.
Ransomware		eine Art von Schadprogrammen, die durch Verschlüsselung den Zugriff auf Daten und Systeme einschränken oder unterbinden. Für die Freigabe wird dann ein Lösegeld (englisch: Ransom) verlangt.
Virtual Private Network	VPN	Ein virtuelles privates (in sich geschlossenes) Kommunikationsnetz bezeichnet eine Netzwerkverbindung, die von Unbeteiligten nicht einsehbar ist. Virtuell in dem Sinne, dass es sich nicht um eine eigene physische Verbindung handelt, sondern um ein bestehendes Kommunikationsnetz, das als Transportmedium verwendet wird. Das VPN dient dazu, Teilnehmer des bestehenden Kommunikationsnetzes an ein anderes Netz zu binden.

Anhang: Weiterführende Informationen zur Kommunikation und Vorlagen

Allgemeine Informationen zur Kommunikation

Sicherung von Notfallzugängen und Kontakten:

Bei einem DDoS-Angriff kann es sein, dass Sie auf wichtige Informationen nicht digital zugreifen können. Halten Sie daher alle wichtigen Kommunikationsmittel auch in Papierform bereit (Telefonnummern, E-Mail-Adressen, Messenger-Kontakte, Zugangsdaten inkl. zweitem Faktor für Social-Media-Accounts).

Sofern Sie über Ihre Website selbst nicht mehr kommunizieren können, kann eine Information der Bürgerinnen und Bürger über alternative Kommunikationswege erfolgen (z. B. Social-Media-Kanäle der Kommune, Newsletter, Veröffentlichungen in Zeitungen, Online-Nachrichtenportalen oder über Radiosender oder eine extern gehostete Landing Page (Darksite)).

Zentrale Kommunikationsverantwortung:

Legen Sie eine/n Verantwortlichen bzw. ein kleines Team fest, das Informationen einholt (z.B aus dem Krisenstab oder direkt bei der IT-Abteilung), kommunikationsstrategische Entscheidungen trifft (wann wird was an wen kommuniziert) und abgestimmte offizielle Informationen herausgibt. So verhindern Sie widersprüchliche Aussagen und Fehlinformationen. Auch Rückfragen sollten bei dieser Person/diesem Team zusammenlaufen und dort bearbeitet werden.

Zielgruppengerechte, klare Kommunikation:

Kommunizieren Sie eindeutig, verständlich und faktenbasiert, geben Sie nur gesicherte Informationen weiter und keine Spekulationen/Vermutungen oder Hoffnungen (z. B. zur Dauer der Behebung). Passen Sie Sprache und Informationsumfang stets an die jeweilige Zielgruppe an.

Interne Adressaten (Verwaltung, Gremien, IT) benötigen ggf. detaillierte technische Informationen. Informieren Sie Mitarbeitende laufend (z. B. via Intranet), damit diese wissen, auf welche Services vorübergehend verzichtet werden soll bzw. muss und wie sie alternativ dennoch arbeiten können bzw. wo sie ggf. auf manuelle Verfahren zurückgreifen müssen. Bedenken Sie auch, dass ggf. andere Behörden informiert werden müssen, wenn deren Dienste auf Ihrem Serviceportal ausgefallen sind (z. B. EfA-Leistungen oder vom Land gehostete Dienste, die im kommunalen Serviceportal eingebunden sind).

Externe Empfänger (Bürger:innen, Medien) müssen in einfach verständlichen Meldungen erfahren, welche Leistungen weiterhin verfügbar sind und bei welchen

Leistungen Einschränkungen bestehen und welche alternativen Kontakt- und Antragswege genutzt werden können, ohne zu viel Einblick in technischen Details zur Betroffenheit von Systemen o.ä. zu erhalten.

Kommunizieren Sie ruhig, professionell und empathisch und haben Sie die Erwartungen und Enttäuschungen ihrer Anspruchsgruppen im Blick. Vermitteln Sie glaubhaft, dass Sie die Lage im Griff haben und alle Betroffenen regelmäßig informiert werden.

Halten Sie Kontakt zum CERT / Landesdatennetz und berichten Sie kontinuierlich. Sind Verwaltungsleistungen betroffen, die Sie im übertragenen Wirkungskreis vornehmen, informieren Sie die entsprechenden Behörden.

Kontinuierliche Kommunikation:

Informieren Sie alle relevanten internen und externen Gruppen während des gesamten Vorfalls regelmäßig – auch und vor allem dann, wenn es länger dauert, aber keine neuen Erkenntnisse vorliegen. Geben Sie proaktiv Informationen weiter, um Gerüchten keinen Raum zu lassen. Kommunizieren Sie bei längerer Dauer zu festgelegten Kommunikationszeitpunkten.

Kommunikationsvorlagen

Interne Erstinformation (an Mitarbeitende)

Betreff: Information zur Verfügbarkeit der Website(n)

Liebe Kolleginnen und Kollegen,

aktuell haben wir technische Probleme, welche sich auf unsere Website auswirken. Es handelt sich hierbei mit hoher Wahrscheinlichkeit um einen DDoS-Angriff – das heißt, unsere Server/unser Netzwerk werden/wird mit einer großen Menge von Datenverkehr überlastet, was die technische Verfügbarkeit einschränkt.

Unsere IT-Abteilung arbeitet mit Hochdruck daran, die Erreichbarkeit der Seite und alle damit verbundenen Funktionen/Dienste schnellstmöglich wieder herzustellen.

Bitte beachten Sie folgende Hinweise:

- Wichtigste/relevante funktionierende Systeme/Dienste: [Aufzählung einfügen]
- Eingeschränkte bzw. nicht verfügbare Systeme/Dienste: [Aufzählung einfügen]
- Behelfslösungen / manuelle Workarounds: [Angaben einfügen]

Nach derzeitigen Erkenntnissen handelt es sich bei diesem Vorfall ausschließlich um ein Problem der technischen Verfügbarkeit der Website und der daran angeschlossenen Funktionen bzw. Dienste. Es liegen keine Hinweise auf eine Verschlüsselung von Daten oder einen unbefugten Zugriff auf Systeme vor.

Bitte beachten Sie, dass ausschließlich [Verantwortliche Person/Team] offizielle Informationen nach außen gibt. Bitte geben Sie selbst keine Auskünfte an Bürger:innen oder Medien weiter. Sollten Sie Fragen zu Ihrem Arbeitsbereich haben, wenden Sie sich bitte an [Kontakt einfügen].

Sobald wir über neue Erkenntnisse verfügen, werden Sie umgehend informiert.

Vielen Dank für Ihre Unterstützung!

Mit freundlichen Grüßen

Vorname Name

Funktion

Externe Erstinformation (an Bürger:innen, Medien)

Sehr geehrte Bürgerinnen und Bürger,

unsere Website ist derzeit aufgrund technischer Probleme nur eingeschränkt/nicht erreichbar. Ursache ist mit hoher Wahrscheinlichkeit ein sogenannter DDoS-Angriff. Dabei wird der Server mit einer sehr großen Menge an Datenverkehr überlastet, sodass die Seite zeitweise nicht verfügbar ist.

Unsere IT-Abteilung arbeitet mit Hilfe externer Experten bereits mit Hochdruck daran, Ihnen unsere Online-Services schnellstmöglich wieder zur Verfügung zu stellen.

Derzeit sind folgende Online-Dienste nicht/nur eingeschränkt nutzbar:

- [Aufzählung einfügen], z. B. *Download von Dokumenten und Formularen, Terminbuchungen, Beantragung von Dokumenten*

Folgende Dienstleistungen stehen aktuell zur Verfügung:

- [Aufzählung einfügen]

Folgende Behelfslösungen haben wir für Sie etabliert:

- [Angaben einfügen]

Es handelt sich bei diesem Vorfall nach derzeitigen Erkenntnissen ausschließlich um ein Problem der technischen Verfügbarkeit der Website und der daran angeschlossenen Funktionen bzw. Dienste. Es liegen keine Hinweise auf eine Verschlüsselung von Daten oder einen unbefugten Zugriff auf Systeme vor.

Bsp.

- Sollten Sie bereits einen Termin für den heutigen Tag gebucht haben, können Sie diesen regulär wahrnehmen. Unsere Bürgerbüros sind vollständig arbeitsfähig.
- Falls Sie zur Bearbeitung Ihres Anliegens einen Termin benötigen, warten Sie bitte, bis Sie wieder einen Termin vereinbaren können. Sollten Sie keinen Termin

benötigen, können Sie wie gewohnt zu unseren regulären Öffnungszeiten in das Bürgerbüro kommen.
- Wenn Sie keinen Termin vereinbart haben oder für Ihr Anliegen keinen benötigen, bitten wir Sie dennoch darum, erst in das Bürgerbüro zu kommen, sobald die Website wieder zur Verfügung steht.

Für Rückfragen erreichen Sie uns unter [Telefonnummer/E-Mail].

Wir werden Sie umgehend informieren, sobald wir neue Informationen haben bzw. unsere Dienste wieder regulär verfügbar sind.

Vielen Dank für Ihr Verständnis und Ihre Geduld!

Ihre [Kommune/Stadtverwaltung]

Interne Folgeinformation (an Mitarbeitende)

Liebe Kolleginnen und Kollegen,

unsere Website sowie die daran angeschlossenen Dienste sind leider weiterhin nicht verfügbar. Unsere IT-Verantwortlichen arbeiten derzeit gemeinsam mit externen Experten mit Hochdruck an einer Lösung.

Wir hoffen/erwarten/gehen davon aus, das Problem bis XXX behoben zu haben und bitten Sie bis dahin weiter um Ihre Geduld.

Bitte verweisen Sie externe Anfragen an folgende Ansprechpartner:innen, die regulär erreichbar sind: [Name, Telefonnummer/E-Mail].

Bitte beachten Sie, dass ausschließlich [Verantwortliche Person/Team] offizielle Informationen nach außen gibt. Bitte geben Sie selbst keine Auskünfte an Bürger:innen oder Medien weiter. Sollten Sie Fragen zu Ihrem Arbeitsbereich haben, wenden Sie sich bitte an [Kontakt einfügen].

Wir melden uns umgehend bei Ihnen, sobald das Problem behoben ist.

Vielen Dank für Ihre Unterstützung!

Mit freundlichen Grüßen

Vorname Name

Funktion

Externe Folgeinformation (an Bürger:innen/Medien)

Liebe Bürgerinnen und Bürger,

unsere Website ist leider auch heute nur eingeschränkt erreichbar. Der Grund ist ein andauernder technischer Angriff, der die Systeme stark belastet.

Wir verstehen, dass dies für viele von Ihnen ärgerlich ist und möglicherweise auch Unannehmlichkeiten verursacht. Bitte seien Sie versichert:

- Ihre Daten sind sicher.
- Wir arbeiten mit Hochdruck und externer Unterstützung an einer Lösung.
- Alle wichtigen Dienstleistungen sind für Sie weiterhin erreichbar – entweder online oder über folgende Behelfslösungen: [Infos einfügen].

In dringenden Fällen (bspw. beim Ablauf wichtiger Fristen, für dringende Online-Anträge (bspw. für Sozialleistungen) oder bei sonstigen Notfällen (bspw. Kindeswohlgefährdung) erreichen Sie uns über unsere Notfall-Hotline XXX bzw. über XXX (anderen Kanal einfügen).

Bitte beachten Sie, dass eine Kontaktaufnahme über unsere Social-Media-Kanäle (z.B. Direktnachrichten oder Kommentare) auch aus Datenschutzgründen kein geeigneter Weg für eine Weiterbearbeitung ist.

Sobald wir neue Informationen haben, werden wir Sie umgehend informieren.

Vielen Dank für Ihre Geduld und Ihr Verständnis!

Ihre [Kommune/Stadtverwaltung]

Interne Abschlussinformation (an Mitarbeitende)

Betreff: Wiederhergestellte Erreichbarkeit unserer Systeme

Liebe Kolleginnen und Kollegen,

wir freuen uns, Ihnen mitteilen zu können, dass die durch den DDoS-Angriff verursachten Einschränkungen behoben sind und unsere Website sowie die betroffenen Systeme/Dienste wieder uneingeschränkt zur Verfügung stehen.

Kurzüberblick zur Situation:

- Betroffene Systeme/Dienste sind wieder funktionsfähig.
- Die Erreichbarkeit wurde durch [kurze Angabe, z. B. technische Maßnahmen, Unterstützung externer Dienstleister] wiederhergestellt.

Nächste Schritte / Präventionsmaßnahmen:

- Kurzfristig: [z. B. zusätzliche Monitoring-Maßnahmen, Anpassung der Firewall-Regeln, enger Austausch mit CERT]
- Mittelfristig: [z. B. Ausbau der Abwehrsysteme, Überprüfung und Aktualisierung von Notfallplänen, Schulung]

Wir danken allen, die in den vergangenen Tagen durch ihr Engagement, ihre Flexibilität und ihren Einsatz dazu beigetragen haben, dass wir den Angriff erfolgreich bewältigen konnten.

Mit freundlichen Grüßen

Vorname Name

Funktion

Externe Abschlussinformation (Bürger:innen, Medien)

Sehr geehrte Bürgerinnen und Bürger,

unsere Website sowie die daran angeschlossenen Online-Dienste stehen Ihnen ab sofort wieder uneingeschränkt zur Verfügung. Der Ausfall wurde durch einen sogenannten DDoS-Angriff verursacht, bei dem die Server mit einer großen Menge an Datenverkehr überlastet wurden.

Wichtig für Sie:

- Ihre Daten waren zu keinem Zeitpunkt gefährdet. Es handelte sich ausschließlich um eine Einschränkung der Verfügbarkeit.
- Die Erreichbarkeit wurde durch [kurze Angabe, z. B. technische Maßnahmen, Unterstützung externer Dienstleister] wiederhergestellt.

- Unsere IT-Abteilung hat gemeinsam mit externen Partnern Maßnahmen ergriffen, um die Erreichbarkeit wiederherzustellen und ähnliche Vorfälle künftig noch besser abzuwehren.

Wir danken Ihnen herzlich für Ihre Geduld und Ihr Verständnis während der Einschränkungen.

Ihre [Kommune/Stadtverwaltung]