Dialog für Cybersicherheit

April 2026: Mitteilung zur Handreichung kommunales DDoS-Szenario

Kommunale Verwaltungen sind seit einigen Jahren vermehrt von DDoS-Angriffen (Distributed-Denial-of-Service) betroffen. Häufige Ziele sind dabei Webseiten und die dort verfügbaren Dienste. Aber auch die Server anderer Internetdienste wie E-Mail, DNS (Domain Name System) oder die Firewalls der Organisation sind mögliche Ziele. DDoS-Angriffe können die Arbeit der Verwaltung zeitweise empfindlich stören. Zudem kann die Bereitstellung von kommunalen Onlinedienstleistungen für einen Zeitraum eingeschränkt bzw. nicht verfügbar sein.

Der vorliegende Bericht „Cyberresilience-Framework. In IT-Krisen schneller agieren. (Kurz: RESI) - Handreichung kommunales DDoS-Szenario“ 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.

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.

Die Handreichung ist kein Ersatz für die Vorbereitung von Notfallmaßnahmen bei Cybervorfällen oder für ein Business Continuity Management (BCM). Neben der Unterstützung von Kommunen, die mehr oder weniger in einen Cybervorfall geraten, soll der Bericht dazu anregen, Vorbereitungen auf den Cybernotfall anzugehen.

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. Im Rahmen dieser ehrenamtlichen Tätigkeit entstand der vorliegende Bericht (von März 2025 bis März 2026).

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.

Alle Ergebnisberichte sowie weitere Dokumente können auf der Seite vom Dialog für Cybersicherheit abgerufen werden: https://www.dialog-cybersicherheit.de/media/.

Kontakt
Arbeitsgruppe RESI
Dialog für Cybersicherheit
E-Mail: resi@dialog-cybersicherheit.de