Außenblick: Technische Anforderungen

14. Nov. 2026 · @Gerd

Worum es geht

Mit dem Außenblick prüft @gerds-it.de regelmäßig von außen, ob deine im Internet erreichbaren Systeme bekannte Sicherheitslücken haben. Dieses Dokument beschreibt, was dafür auf deiner Seite nötig ist und wie die Prüfung technisch abläuft. Es richtet sich an dich und an deinen IT-Dienstleister oder Hoster.

Der Ablauf in Kürze:

1. Du nennst uns die Adressen, die geprüft werden sollen, und gibst sie schriftlich frei.
2. Dein Dienstleister schaltet unseren Prüfserver für Web-Anfragen frei, falls bei dir ein Sperrsystem läuft.
3. Die Prüfung läuft danach von selbst: jede Woche vollständig, jede Nacht zusätzlich auf neu bekannt gewordene Lücken.
4. Du bekommst einen Bericht und wirst informiert, wenn etwas Neues gefunden wird.

Was wir von dir brauchen

- **Die Adressen.** Alle Domains und, falls vorhanden, IP-Adressen, die geprüft werden sollen: Webseite, Shop, Kundenportal, Fernzugang, Mailserver und ähnliche Dienste. Die Checkliste am Ende hilft beim Sammeln.
- **Die IP-Adressen dahinter.** Zu jeder Domain die IP-Adressen des Servers, auf dem sie läuft, für IPv4 und, falls vorhanden, für IPv6. Dein Dienstleister oder Hoster kennt sie. Wir brauchen sie für die Schutzregel, die weiter unten beschrieben ist.
- **Die schriftliche Freigabe.** Geprüft wird nur, was du schriftlich freigegeben hast. Die Freigabe nennt die Adressen und ein Ablaufdatum. Freigeben kann nur, wer über die Systeme verfügen darf.
- **Einen technischen Ansprechpartner.** Jemand, den wir bei einem dringenden Fund erreichen: du selbst oder dein IT-Dienstleister, mit E-Mail-Adresse und Telefonnummer.
- **Die Information an Hoster und Dienstleister.** Liegt ein System bei einem Hoster oder wird es von einem Dienstleister betreut, informierst du ihn vorab über die Prüfung. Manche Hoster verlangen dafür eine eigene Zustimmung. Dieses Dokument kannst du dafür weitergeben.

Technische Eckdaten des Prüfservers

An diesen Angaben erkennt dein Dienstleister unsere Prüfung in seinen Protokollen.

Merkmal	Wert
IP-Adresse (IPv4)	185.183.181.178
IP-Adresse (IPv6)	2602:fc16:2:52b::eda2
Name (Reverse DNS)	scanner.gerds-it.de
Standort	Deutschland
Kennung in jeder Anfrage (User-Agent)	`@gerds-it.de Schwachstellenscan (+https://scanner.gerds-it.de; nuclei01-scanner@gerds-support.de)`
Infoseite	https://scanner.gerds-it.de
Kontakt	nuclei01-scanner@gerds-support.de
Werkzeug	Nuclei (Open Source) mit täglich aktualisierten Prüfvorlagen
Zeit	nachts ab 1:30 Uhr

Vollständige Prüfung	einmal pro Woche, am vereinbarten Tag
Prüfung auf neue Lücken	jede Nacht, nur mit den neu hinzugekommenen Prüfvorlagen
Geschwindigkeit	gedrosselt, im Standard höchstens 20 Anfragen pro Sekunde, auf Wunsch weniger

Freischaltung auf deiner Seite

Viele Systeme sperren automatisch Adressen, die viele ungewöhnliche Anfragen schicken. Genau so sieht unsere Prüfung aus. Ohne Freischaltung wird der Prüfserver nach kurzer Zeit gesperrt, und das Ergebnis ist unvollständig.

Bitte freischalten: die beiden IP-Adressen des Prüfservers (IPv4 und IPv6, siehe Eckdaten), und zwar nur für Web-Anfragen (HTTP und HTTPS) auf die freigegebenen Adressen.

Bitte nicht freischalten: Anmeldeversuche per SSH oder an anderen Verwaltungszugängen. Unsere Prüfung meldet sich nirgends an. Kommt von unserer Adresse ein solcher Versuch, soll dein System ihn sperren wie jeden anderen.

Wo die Freischaltung typischerweise nötig ist:

System	Was zu tun ist
Web-Firewall (WAF)	Ausnahme für die IP-Adresse auf den freigegebenen Adressen
CrowdSec	Whitelist nur für HTTP-Ereignisse der IP-Adresse
fail2ban	`ignoreip` in den Web-Jails, nicht im SSH-Jail
Angriffserkennung des Hosters oder der Firewall (IPS)	Ausnahme für die IP-Adresse, beim Hoster anfragen
Vorgeschalteter Dienst wie Cloudflare (CDN)	Ausnahme dort einrichten und uns den Dienst nennen, siehe Schutzregeln
Mailserver mit eigener Sperre	Ausnahme für die IP-Adresse in der Verwaltungsoberfläche

Wenn du nicht freischalten möchtest, ist das deine Entscheidung. Die Prüfung zeigt dann, was ein Angreifer sieht, bis er gesperrt wird. Im Bericht steht in diesem Fall, dass das Ergebnis unvollständig ist.

Überwachungssysteme müssen nicht angepasst werden. Sie dürfen und sollen die Prüfung anzeigen.

Was geprüft wird und was nicht

Geprüft wird:

- bekannte Sicherheitslücken in Web-Anwendungen und Diensten, die unter den freigegebenen Adressen erreichbar sind
- typische Fehlkonfigurationen, zum Beispiel offen liegende Verwaltungsseiten, Sicherungsdateien oder Konfigurationsdateien
- veraltete Softwarestände, für die Lücken bekannt sind

Gemeldet werden Funde der Stufen kritisch, hoch und mittel.

Nicht gemacht wird:

- keine Angriffe, die Systeme lahmlegen können (Denial of Service)
- kein massenhaftes Durchprobieren von Eingaben (Fuzzing) und keine eingreifenden Tests
- kein Erraten von Passwörtern und keine Anmeldung an deinen Systemen
- keine Änderung und kein Abruf deiner Daten
- keine Prüfung von innen: Was nur in deinem Netz erreichbar ist, sieht der Außenblick nicht

Der Außenblick ersetzt keine gründliche Einzelprüfung. Wenn ein System genauer untersucht werden soll, machen wir das gesondert und nach Absprache.

Schutzregeln

Damit nie ein fremdes System geprüft wird, gelten feste Regeln:

- **Nur freigegebene Adressen.** Was nicht in der Freigabe steht, wird nicht geprüft.
- **Prüfung vor jedem Lauf.** Vor jeder Prüfung wird jede Domain aufgelöst. Zeigt sie nicht auf eine der IP-Adressen aus deiner Freigabe, wird sie übersprungen, und wir melden uns bei dir. Das passiert zum Beispiel nach einem Umzug zu einem anderen Hoster.
- **IPv4 und IPv6.** Geprüft wird über beide Wege, denn Firewall-Regeln werden für IPv6 oft anders gepflegt als für IPv4. Die Schutzregel gilt für beide: Auch über IPv6 prüfen wir nur Adressen, die in deiner Freigabe stehen.
- **Vorgeschaltete Dienste nur ausdrücklich.** Läuft eine Adresse über einen Dienst wie Cloudflare, prüfen wir sie nur, wenn das in der Freigabe steht und der Dienst solche Prüfungen zulässt.
- **Freigabe mit Ablaufdatum.** Nach dem Ablaufdatum stoppt die Prüfung von selbst. Wir melden uns rechtzeitig vorher wegen der Verlängerung.

Ergebnisse und Meldewege

- **Bericht.** Nach jeder vollständigen Prüfung gibt es einen Bericht: welche Adressen geprüft wurden, welche Funde offen sind und wie dringend sie sind. Adressen, die übersprungen wurden, stehen mit Grund darin.
- **Meldung bei neuen Funden.** Wird ein neuer Fund der Stufe kritisch oder hoch entdeckt, informieren wir deinen technischen Ansprechpartner.
- **Kein Fund heißt nicht sicher.** Die Prüfung findet bekannte Lücken, die von außen sichtbar sind. Sie ist ein Baustein, kein Nachweis für lückenlose Sicherheit.
- **Umgang mit den Ergebnissen.** Die Ergebnisse liegen auf unserem eigenen Server in Deutschland und werden nicht an Dritte weitergegeben. Du bekommst nur die Ergebnisse zu deinen eigenen Adressen.

Änderungen, Stopp und Kontakt

Bitte melde uns vorab:

- neue Adressen oder Systeme, die mit geprüft werden sollen
- einen Wechsel der IP-Adresse oder des Hosters
- Systeme, die abgeschaltet werden
- einen neuen technischen Ansprechpartner
- Zeiten, in denen nicht geprüft werden soll, zum Beispiel während einer Umstellung

Prüfung stoppen: Eine Nachricht an die Kontaktadresse genügt. Wir nehmen die genannte Adresse oder alle Adressen aus der Prüfung.

Kontakt: nuclei01-scanner@gerds-support.de · www.gerds-it.de

Checkliste

Adressen

Adresse (Domain oder IP)	IP-Adressen des Servers (IPv4, IPv6)	Hoster oder Dienstleister	Hoster informiert	Freischaltung erledigt

Angaben zur Freigabe

Angabe	Eintrag
Unternehmen	
Technischer Ansprechpartner (Name, E-Mail, Telefon)	
Gewünschter Tag für die vollständige Prüfung	
Geringere Geschwindigkeit gewünscht	
Vorgeschalteter Dienst (zum Beispiel Cloudflare)	
Freigabe gültig bis	
Ort, Datum, Unterschrift	

Revision #2
Created 2026-11-14 15:43:12 UTC by Gerd
Updated 2026-11-14 15:44:13 UTC by Gerd