

Premium

Monitoring, Sicherheitslagebild, Port-Scan und Geheimnisse teilen, für angemeldete Konten.

- [Monitoring](#)
- [Benachrichtigungs-Kanäle](#)
- [Sicherheitslagebild](#)
- [Port-Scan](#)
- [Geheimnis teilen](#)

Monitoring

Das [Monitoring](#) prüft deine Dienste regelmäßig von außen und meldet sich, wenn etwas nicht stimmt. Pro Konto sind bis zu 25 Prüfungen möglich.

Arten von Prüfungen

Art	Prüft	Intervall
Webseite	HTTP-Status und Antwortzeit, optional erwarteten Statuscode und ein Stichwort im Inhalt	1 min bis 1 h
Port	ob ein Dienst auf <code>host:port</code> antwortet, z. B. <code>mail.example.de:25</code>	1 min bis 1 h
Zertifikat	Ablauf des TLS-Zertifikats, Warnung ab einer Zahl von Tagen (Standard 14)	1 h bis 1 Tag
Blacklist	ob IP oder Domain auf Spam-Sperrlisten auftaucht	1 h bis 1 Tag
DNS	ob sich ein DNS-Eintrag ändert, z. B. MX oder A	1 min bis 1 h

Störung oder Warnung

- **Störung:** Das Ziel ist nicht erreichbar oder antwortet falsch. Bei Webseiten und Ports erst nach **zwei Fehlschlägen in Folge**, damit ein kurzer Wackler keinen Alarm auslöst.
- **Warnung:** Etwas ist auffällig, aber noch nicht kaputt, etwa ein Zertifikat, das bald abläuft.
- **Wieder in Ordnung:** Auch das wird gemeldet, mit der Dauer der Störung.

Bei einer **DNS-Prüfung** gilt eine Änderung als Warnung. War sie gewollt, übernimmst du den neuen Wert mit einem Klick als Sollzustand.

Verlauf

Zu jeder Prüfung gibt es die letzten 24 Stunden als Grafik, die letzten 90 Tage als Balken und eine Liste der Vorfälle. Änderst du Art oder Ziel, beginnt der Verlauf von vorn.

Benachrichtigungen

Ohne Kanal siehst du Störungen nur auf der Seite. Wie du Mail, ntfy, Telegram und andere einrichtest, steht auf der nächsten Seite.

Benachrichtigungs-Kanäle

Kanäle legst du im [Monitoring](#) unter **Benachrichtigungen** an, bis zu 5 Stück. Jede Meldung von Monitoring und Sicherheitslagebild geht an alle deine Kanäle. Mit **Test** prüfst du, ob ein Kanal funktioniert.

Kanal	Was du brauchst
E-Mail	eine Adresse. Sie bekommt zuerst einen Bestätigungslink, erst danach kommen Meldungen.
ntfy	eine Topic-Adresse, z. B. <code>https://ntfy.sh/mein-geheimes-topic</code> . In der ntfy-App das Topic abonnieren.
Telegram	ein Bot-Token von @BotFather und deine Chat-ID
Discord	eine Webhook-Adresse aus den Kanal-Einstellungen (Integrationen → Webhooks)
Slack / Mattermost	eine Incoming-Webhook-Adresse
Webhook (JSON)	eine beliebige Adresse. Sie bekommt alle Felder als JSON, gut für eigene Automatisierung.

Tipps

- **ntfy** ist am schnellsten eingerichtet: App installieren, ein schwer zu erratendes Topic ausdenken, fertig. Wer das Topic kennt, liest mit, also kein „test“ oder „server“ nehmen.
- **Telegram:** Schreib deinem Bot einmal etwas. Die Chat-ID findest du dann unter `https://api.telegram.org/bot<TOKEN>/getUpdates` im Feld `chat.id`.
- Mails gehen höchstens 20-mal pro Stunde je Kanal raus, damit ein flatterndes Ziel nicht dein Postfach flutet.

Sicherheitslagebild

Das [Sicherheitslagebild](#) sammelt neue Sicherheitslücken an einer Stelle:

- **BSI / CERT-Bund:** Sicherheitshinweise, stündlich aktualisiert, die letzten 30 Tage
- **CISA KEV:** Lücken, die nachweislich **aktiv ausgenutzt** werden, alle 3 Stunden, die letzten 90 Tage
- **EPSS:** Wahrscheinlichkeit, dass eine Lücke in den nächsten 30 Tagen ausgenutzt wird, täglich

Merkliste: nur was dich betrifft

Trag unter **Meine Produkte** ein, was du betreibst, z. B. „Proxmox“, „FortiOS“, „Exchange Server“, „Vaultwarden“. Neue Einträge zu diesen Produkten werden hervorgehoben und als Meldung an deine Kanäle geschickt.

Mit Version wird es genauer: Trag zum Produkt deine Version ein (z. B. FortiOS 7.4.3). Ist deine Version laut Quelle nicht betroffen, gibt es keine Meldung.

Wo du die Version findest:

- in der Weboberfläche meist unter „Info“ oder „System“
- unter Linux mit dem Paketmanager: `dpkg -l | grep name` oder `rpm -q name`
- bei Windows-Software unter „Apps“

Unter **Melden ab** legst du fest, ab welcher Schwere du Meldungen bekommst.

Die Detailseite

Zu jedem Eintrag gibt es eine eigene Seite mit:

- **Was macht die Lücke?** Beschreibung, CVSS-Wert und Art der Schwachstelle auf Deutsch erklärt
- **Welche Systeme sind betroffen?** Produkte und Versionen, mit Abgleich gegen deine Version
- **Wie schütze ich mich?** Hinweise und Links des Herstellers
- **Bin ich schon betroffen?** Eine Checkliste, wie du Angriffsspuren findest

Bei Sonderversionen (LTS, Hotfix, Distributionspakete) im Zweifel die Hinweise des Herstellers prüfen.

Port-Scan

Mit dem [Port-Scan](#) prüfst du deine **eigenen Server** von außen: Welche Ports sind offen, was meldet sich dort?

Freigaben

Gescannt werden nur Ziele, die der Admin für dein Konto freigegeben hat. So lässt sich der Scan nicht gegen fremde Server einsetzen. Möglich sind:

- einzelne IP-Adressen
- Netze bis /24 (IPv4) bzw. /48 (IPv6)
- Hostnamen. Sie werden beim Scan aufgelöst, gescannt wird genau die eine IP.

Für eine neue Freigabe schreib dem Admin über [Feedback](#), welche Adressen dir gehören.

Scannen

Ziel wählen, Ports angeben (bis 100, mit Vorlagen für gängige Ports) und starten. Das Ergebnis:

- **offen:** Ein Dienst antwortet. Ist das so gewollt?
- **geschlossen:** Das Ziel lehnt ab.
- **gefiltert:** Keine Antwort, eine Firewall verwirft die Pakete.

Jeder Scan landet im Protokoll. Den eigenen Internetanschluss prüfst du einfacher mit dem [Port-Check](#).

Geheimnis teilen

Mit [Geheimnis teilen](#) gibst du Passwörter, Zugangsdaten oder Schlüssel per **Einmal-Link** weiter, statt sie in Mail oder Chat zu schreiben.

So funktioniert es

1. Text eingeben, Gültigkeit wählen (1 Stunde bis 7 Tage), optional ein Passwort.
2. Link kopieren und dem Empfänger schicken. Er wird nur dieses eine Mal angezeigt.
3. Der Empfänger öffnet den Link und klickt auf **Anzeigen**. Danach ist das Geheimnis auf dem Server gelöscht.

Warum das sicher ist

- Dein **Browser verschlüsselt** den Text (AES-256-GCM), bevor er zum Server geht.
- Der Schlüssel steht hinter dem `#` im Link. Diesen Teil schicken Browser nie an einen Server. Der Server kennt den Inhalt also nicht.
- **Linkvorschauen** in Messengern verbrauchen den Link nicht, erst der Klick auf „Anzeigen“.
- Mit Passwort braucht man zusätzlich das Passwort. Nach 5 falschen Versuchen ist das Geheimnis weg. Teile das Passwort auf einem anderen Weg, z. B. Link per Mail und Passwort per Telefon.

In deiner Liste siehst du nur, ob ein Link schon geöffnet wurde. Meldet der Empfänger, dass der Link schon benutzt war, hat ihn jemand anderes geöffnet: Dann das Passwort bzw. den Schlüssel austauschen.