99,39 %.

weniger Bot-Traffic an unserem VPN-Login.

Keine KI. Keine neue Appliance. Kein Buzzword.

MEHR NUTZER. WENIGER BOTS.

Eine Gästeliste für IP-Adressen — was sie gebracht hat und was wir gelernt haben

Moritz Hamminger
Netzwerk & IT-Security, DESY

07.10.2026

HELMHOLTZ

DESY.

Worum es heute geht

1

Das Problem

Warum eine offene Tür nicht offen für alle sein muss

2

Die Ergebnisse

Was die Gästeliste in Zahlen gebracht hat

3

Die Kehrseite

Blocken, und warum das ein hartes Eisen ist

4

Zum Mitnehmen

Was wir heute anders machen würden

KAPITEL 01

Das Problem: Eine Tür, die jeder findet

Jeder Dienst, der aus dem Internet erreichbar ist, wird gefunden. Nicht irgendwann — sondern innerhalb von Minuten.

Die Ausgangslage

Ein VPN-Login muss erreichbar sein. Für alle Mitarbeitenden — und damit für alle anderen auch.

Dauerbeschuss

Bots probieren rund um die Uhr Benutzernamen und Passwörter am öffentlichen VPN-Zugang durch.

Rauschen

Scans und Login-Versuche fluten die Logs. Die echten Auffälligkeiten gehen darin unter.

Kein passendes Werkzeug

Die vorhandenen Lösungen waren entweder zu starr für den Alltag oder zu invasiv für die Nutzer.

Die Idee.

Nutzer schalten ihre eigene IP-Adresse frei. Alle anderen sehen die Tür gar nicht erst.

1

Anmelden

Login mit dem ganz normalen Konto über Single Sign-On.

2

IP erkennen

Das Portal sieht, von wo du kommst — IPv4 und IPv6.

3

Tür auf

Ein Klick, und deine Adresse steht auf der Gästeliste. Innerhalb einer halben Minute.

Self-Service statt Ticket. Die Gäste pflegen die Liste — nicht die IT.

Was IT-Access ist — und was nicht

Ehrliche Erwartungen sparen später Diskussionen

Ist

- Ein Self-Service-Portal, um sich selbst freizuschalten/entsperren
- Angebunden an das zentrale Login (Keycloak)
- Eine Schutzschicht vor öffentlichen Diensten
- Eine Sperrliste für nachweislich bösartige IPs
- Wirkt ganz vorne am Internet-Übergang

Ist nicht

- Kein Ersatz für VPN oder internes Netz
- Keine Anmeldung am Dienst selbst
- Keine Web Application Firewall, kein Proxy
- Kein vollständiger Bot-Schutz
- Keine Sperre ganzer Netze



Vordertür zu, Fenster offen
KI-Generiert

Eine Säule.
Nicht das Konzept.

IT-Access schließt die Vordertür.
Nicht das Fenster.

Es ist kein Sicherheitskonzept. Es kann eine Säule davon sein.

KAPITEL 02

Die Ergebnisse: Was die Gästeliste gebracht hat

Zahlen aus dem laufenden Betrieb.

Der Betrieb in vier Zahlen

Stand: 02.10.2026

99,39 %

Bot-Reduktion
am VPN-Login

9538

Netze auf der Gästeliste
dürfen überhaupt anklopfen

190.827

IPs auf der Sperrliste
mit nachgewiesen bösartigem Verhalten

300

Netze von Nutzern selbst registriert
ohne Ticket, ohne Anruf

WAS 99,39 % IM ALLTAG BEDEUTEN

Von Dauerrauschen zu Einzelfällen

Saubere Logs

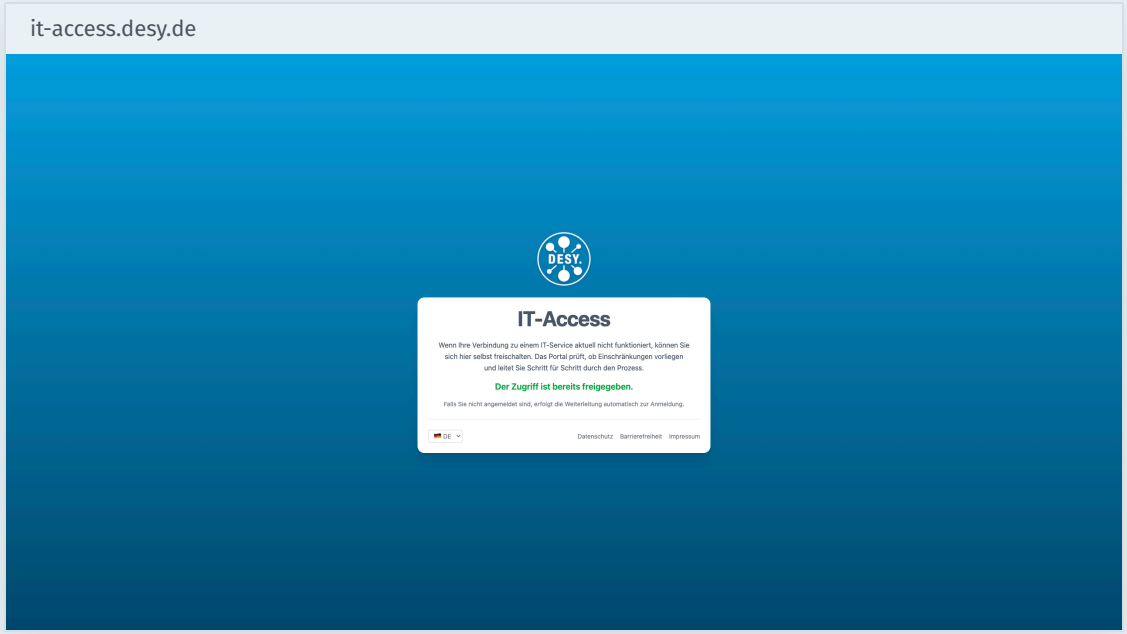
Was jetzt noch am Login auftaucht, ist fast immer ein Mensch. Auffälligkeiten fallen wieder auf.

Kleinere Angriffsfläche

Wer nicht auf der Liste steht, erreicht den Dienst gar nicht — auch nicht mit einer frischen Schwachstelle.

Weniger Aufwand

Freischaltung per Self-Service. Die IT muss nicht jede Home-Office-Adresse von Hand pflegen.



Aus Sicht der Nutzer

Ein Klick bis zur Freischaltung

- Login mit dem Konto, das man sowieso hat
- IPv4 und IPv6 werden automatisch erkannt
- Freischaltung vollautomatisch — kein Ticket
- Hilfeseite für die Fälle, in denen es hakt
- Andere Dienste können die Funktion einbinden

Wie es funktioniert — in einer Minute

Vom Browser bis zum Router

1

Portal

Web-App mit Single Sign-On. Erkennt die Adresse des Nutzers.

2

Registry

Prüft und speichert jede Freischaltung zentral in einer Datenbank.

3

Router

Zweimal pro Minute wird die Liste automatisch in die WAN-Router-Regeln am Internet-Übergang geschrieben.

Für die Neugierigen: Go, PostgreSQL, Kubernetes, NETCONF auf Juniper — Details gerne nach dem Vortrag.

KAPITEL 03

Die Kehrseite: Wenn eine Gästeliste nicht reicht

Manche Dienste müssen für alle offen bleiben.
Dann bleibt nur der umgekehrte Weg: die Störer aussperren.

Blocken ist ein hartes Eisen

Wer gesperrt ist, sieht keine Fehlermeldung. Er sieht einfach — nichts.

Die Folgen

- Kein freundlicher Hinweis für Betroffene
- Entsperren nur manuell durch das Betriebsteam

Die Auslöser

- Angriffe auf das VPN
- Portscans auf das ganze Netz
- Schutzmechanismen gegen Fehlsperren

Die Regeln

- Nur einzelne IPs, nie ganze Netze
- Jeder IP muss bösartiges Verhalten nachgewiesen werden
- Neue Sperrgründe brauchen eine Freigabe



Login-Versuche am VPN

SPERRGRUND 1

Bots am VPN

Wer ausprobiert, statt sich anzumelden

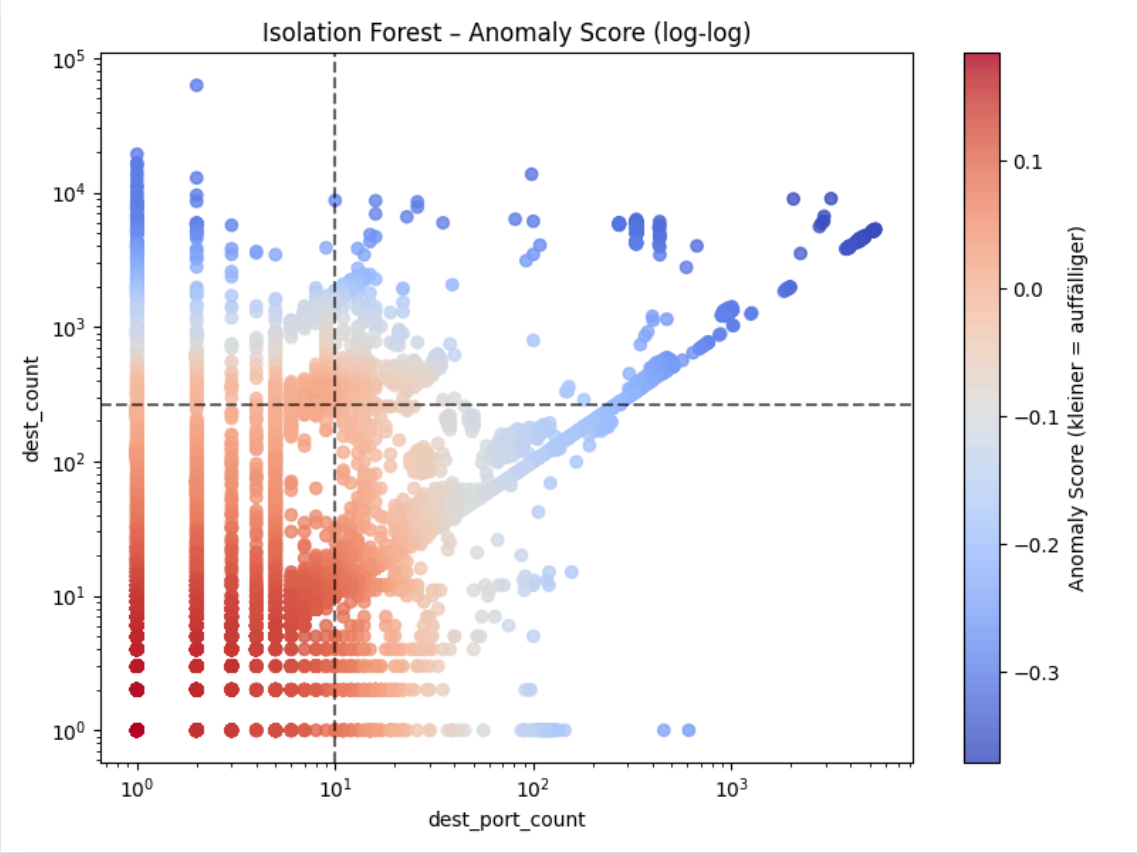
5

verschiedene Benutzernamen
in 30 Minuten

5

falsche Passwörter
in 30 Minuten

Gesperrt wird nur der VPN-Zugang — sonst nichts.



Abgelehnte Verbindungen in den Firewall-Logs

SPERRGRUND 2

Portscans

Wenn grep zu langsam wird, muss das Rauschen raus

25

verschiedene Ziel-IPs
in 5 Minuten

100

verschiedene Ports
in 5 Minuten

- Sperrt den kompletten Zugang ins Netz
- Die Gegenseite reagiert — mit gefälschten Absendern

KAPITEL 04

Was wir heute anders machen würden

Und was ihr euch sparen könnt.

Lessons Learned

Was wir gedacht haben — und was wir daraus gelernt haben

GEDACHT	GELERNT
„Validierung im Backend? Nutzt doch eh nur mein Frontend.“	→ Baue jede Schnittstelle so, als würden sie andere nutzen. Sie werden es tun.
„Das Portal muss nicht immer erreichbar sein.“	→ Self-Service ist Infrastruktur. Fällt er aus, sperrt man genau die aus, die rein sollen.
„Die Router schaffen das schon.“	→ Hardware-Grenzen sind Design-Grenzen. Früh messen, nicht erst im Betrieb.
„Nur fuer Institutsaccounts.“	→ Nächster Schritt: Verschiedene Zugangszones implementieren.
„Wer scannt ist böse.“	→ Dual Use Infrastruktur beachten

Drei Dinge zum Mitnehmen

1

Die Tür muss nicht für alle offen sein.
Nur für die Richtigen.

2

Self-Service ist ein Security-Feature.
Kein Komfort-Feature.

3

Eine Säule ist kein Konzept.
Das Fenster hinten müsst ihr trotzdem zumachen.

Wir haben keine höhere Mauer gebaut.
Wir haben eine Gästeliste an die Tür gehängt.

Fragen, Wünsche, Ideen?

KONTAKT
moritz.hamminger@desy.de

HELMHOLTZ

DESY.