

Registrierung zum Wettbewerb

Informationen zur Teamleiter:in

Titel:

Name:

Vorname:

Organisation/Institution:

Straße und Hausnummer:

PLZ und Ort:

E-Mail-Adresse:

Team

Teamname:

Teammitglieder (falls zutreffend):

Vorname, Name	E-Mail-Adresse

Hiermit erkläre ich, dass ich und alle Teammitglieder den nachfolgenden Teilnahmebedingungen des Wettbewerbs zustimmen. Die Einhaltung aller relevanten Gesetze und Vorschriften ist Voraussetzung für die Teilnahme am Wettbewerb.

Alle in diesem Formular erhobenen Daten werden nach Art. 5 Abs. 1 lit. b DSGVO nur für die ordnungsgemäße Durchführung des Wettbewerbs erfasst, gespeichert und weiterverwendet. Es gilt die Datenschutzerklärung des efzn, welche unter folgendem Link abrufbar ist: <https://www.efzn.de/datenschutz>.

Ort, Datum

Unterschrift Teamleiter:in

Teilnahmebedingungen des „CHALLENGE.efzn“-Wettbewerbs

1. Veranstalter des Wettbewerbs

Energie-Forschungszentrum Niedersachsen (efzn)

Das efzn ist ein gemeinsames wissenschaftliches Zentrum der Universitäten Braunschweig, Clausthal, Göttingen, Hannover und Oldenburg.

Ansprechpartner:

efzn-Geschäftsstelle

Am Stollen 19A

38640 Goslar, Deutschland

geschaeftsstelle@efzn.de

www.efzn.de

2. Titel des Wettbewerbs

„CHALLENGE.efzn“-Wettbewerb 2026

3. Gegenstand des Wettbewerbs

Der in Berlin öffentlich diskutierte Angriff bzw. Vorfall im Umfeld der Stromversorgung hat die Debatte darüber verstärkt, dass bereits der Zugriff auf frei zugängliche Infrastrukturdaten – etwa zu Leitungsverläufen oder Netzstrukturen – in falschen Händen missbraucht werden kann. Solche Daten stehen im Internet teilweise legal, offen und leicht zugänglich zur Verfügung. Gleichzeitig existieren viele weitere Informationsquellen, etwa Marktdaten, Lastzeitreihen, Erzeugungsdaten, Wetterinformationen, demografische Indikatoren oder geografische Daten. Jedes dieser Datensegmente wirkt isoliert betrachtet oft unkritisch – in Kombination und mit den Möglichkeiten moderner Datenanalyse und KI entstehen jedoch neue Einsichten in potenziell verwundbare Systeme. Einzelne Institutionen verfügen in der Regel nicht über die nötige interdisziplinäre Breite, die erforderlich ist, um diese Vielfalt an Informationen zu kombinieren. Der Wettbewerb bringt Fachleute aus IT-Sicherheit, Energietechnik, Data Science, Ingenieur- und Geowissenschaften sowie aus Sozial- und Wirtschaftswissenschaften zusammen, um gemeinsam neue Perspektiven zu entwickeln. Erst diese Vielfalt ermöglicht es, komplexe, sektorübergreifende Abhängigkeiten und Verwundbarkeiten zu erkennen und realitätsnahe Lösungsansätze zu formulieren. Der Wettbewerb soll aufzeigen, wie durch die Verknüpfung bislang in Industrie, Verwaltung und Forschung isoliert betrachteter Datenquellen neue Risikoindikatoren und Schwachstellenhypothesen erkannt werden können – bevor sie von unbefugten Dritten entdeckt oder ausgenutzt werden. Ziel ist es, die Resilienz kritischer Infrastrukturen in Niedersachsen zu erhöhen und so einen Beitrag zur gesamtgesellschaftlichen Gefahrenprävention zu leisten.

4. Teilnahmezeitraum

Die Registrierung für den „CHALLENGE.efzn“ Wettbewerb ist ab sofort möglich und bleibt auch während des gesamten Teilnahmezeitraums bis zum 31. Oktober 2026 geöffnet. Die Einsendung der Ergebnisse ist zwischen dem 01. und 31. Oktober 2026, 23:59 Uhr MEZ möglich.

5. Teilnahmeberechtigung

Der Wettbewerb richtet sich deutschlandweit an interdisziplinäre Teams aus Wissenschaft, Wirtschaft und Zivilgesellschaft. Die Teilnahme von Teams aus nur einem der genannten Bereiche ist ebenfalls möglich. Ebenso sind auch Einzelbeiträge zugelassen.

Teams müssen sich über eine:n entsprechende:n Teamleiter:in registrieren. Die Teilnehmenden müssen sicherstellen, dass alle Teammitglieder den vorliegenden Teilnahmebedingungen zustimmen.

Die Einhaltung aller relevanten Gesetze und Vorschriften ist Voraussetzung für die Teilnahme am Wettbewerb.

6. Teilnahme und Anerkennung der Teilnahmebedingungen

Um teilzunehmen, müssen sich Einzelpersonen oder Teams vor Aufnahme der Arbeiten an dem Wettbewerbsbeitrag über das dafür vorgesehene Webformular auf der Wettbewerbswebseite (www.efzn.de/challenge) registrieren. Mit der Registrierung erklären sich die Teilnehmenden mit allen Punkten der vorliegenden Teilnahmebedingungen des „CHALLENGE.efzn“ Wettbewerbs einverstanden.

Insbesondere gilt:

- Registrierung mit benannter verantwortlicher Kontaktperson pro Team – Teilnahme nur nach Anerkennung der Teilnahmebedingungen.
- Keine eigenständigen Kontakte zu Betreibern/Behörden im Namen des Wettbewerbs ohne Abstimmung mit der efzn-Geschäftsstelle.
- Verstöße gegen die vorliegenden Teilnahmebedingungen führen zum Ausschluss.

7. Geltungsbereich (Scope) und Abgrenzung

Im Vordergrund stehen nachvollziehbare Methoden, belastbare Herleitungen und konkrete Handlungsempfehlungen für Betreiber von kritischen Infrastrukturen, Behörden und Forschung.

Geographische Fokusregion ist Niedersachsen. Sachlich liegt der primäre Fokus auf dem Energiesystem (Strom, perspektivisch auch Wärme/Gas, sofern datenbasiert abbildbar). Abhängigkeiten zu weiteren Sektoren können berücksichtigt werden, insbesondere Telekommunikation (Kommunikationsfähigkeit im Krisenfall), Wetter und Verkehr.

Ergebnisse dürfen keine operative Handlungsanleitung enthalten – sie sollen Vorsorge und Verteidigung verbessern, nicht Risiken erhöhen. Potenziell sicherheitsrelevante Erkenntnisse dürfen ausschließlich über den vorgesehenen Responsible-Disclosure-Kanal gemeldet werden. Teams verpflichten sich, sicherheitsrelevante Zwischenresultate nicht öffentlich zu speichern oder weiterzugeben.

In Scope (erlaubt):

- Analyse und Verknüpfung offener Daten (z.B. Last-, Erzeugungs-, Markt-, Wetter-, Geo- und Demografie-Daten) zur Ableitung von Risiko-Hypothesen.

- Modellierung und Visualisierung von Abhängigkeiten im Energiesystem (und optional angrenzenden Sektoren).
- Bewertung von Ergebnissen auf aggregierter Ebene (Cluster, Regionen, Klassen von Assets) sowie Vorschläge für Schutz- und Resilienzmaßnahmen.
- Reproduzierbare Dokumentation der Datenquellen, Annahmen und Analyseschritte.

Out of Scope (ausdrücklich untersagt!):

- Jegliche Versuche, reale Systeme zu stören, zu testen oder anzugreifen (z.B. Penetrationstests, Scans, Exploits, Social Engineering, physische Erkundung).
- Die Veröffentlichung oder Weitergabe von detailscharfen Informationen zu konkreten verwundbaren Objekten, Standorten oder Angriffswegen.
- Nutzung nicht-öffentlicher Betriebsdaten oder personenbezogener Daten ohne ausdrückliche Freigabe im Rahmen des Wettbewerbs.

8. Datenbasis und Umgang mit Daten

Zugelassen sind ausschließlich frei verfügbare Datenquellen, die rechtmäßig genutzt werden können (Open Data, offizielle Transparenzdaten, frei zugängliche Karten-/Geodaten, wissenschaftliche Publikationen). Ein ständig aktualisierter Datenkatalog wird über die Wettbewerbswebseite bereitgestellt. Der Katalog verweist auf öffentlich zugängliche Quellen und Datentypen – er stellt keine zentral zusammengeführten oder heruntergeladenen Kopien detailscharfer Infrastrukturdaten bereit, um die Auffindbarkeit sensibler Informationen nicht zusätzlich zu erhöhen. Zur Risikominderung werden Ergebnisse, die eine konkrete Ausnutzung erleichtern könnten, nur über einen vertraulichen Meldeweg eingereicht (*Responsible Disclosure*).

9. Einreichungen

Einzureichen sind mindestens:

- Profil des Teams (bspw. Studierende und Mitarbeitende aus Hochschulen, Fachleute aus Unternehmen, engagierte Personen aus der Zivilgesellschaft oder Schulgruppen).
- Kurzbericht (Problemstellung, Datenquellen, Methode, Ergebnisse, Unsicherheiten, Empfehlungen).
- Reproduzierbarkeit: Code oder detaillierte Schrittfolge inkl. Parametern.
- Impact- und Risikoabwägung: Warum hilft das Ergebnis Verteidigern, ohne Missbrauch zu erleichtern?

Optional: Visualisierungen, Prototypen, Leitfaden für Betreiber oder Vorschläge für Daten-Governance (z.B. differenzierte Zugänge/Protokollierung).

10. Responsible Submission & Disclosure Process:

Zur technischen und organisatorischen Risikominderung gilt ein mehrstufiger Einreichungs- und Offenlegungsprozess. Die erste Stufe dient ausschließlich der Registrierung. Alle Projekte sind standardmäßig nicht öffentlich und unterliegen restriktiven Zugriffsrechten.

Befunde, die eine konkrete Ausnutzung erleichtern könnten, dürfen nicht per unverschlüsselter E-Mail versendet werden. Sie sind ausschließlich über den hierfür vorgesehenen Secure-Disclosure-Kanal einzureichen. Hierzu zählen insbesondere konkrete Objektbezüge, Koordinaten, detaillierte Standorthinweise, präzise Ausfall- oder Angriffspfade, technische Kombinationen mit hoher Missbrauchseignung sowie sonstige Inhalte, die nur einem eng begrenzten Evaluation Board zugänglich sein sollen. Der Eingang solcher Meldungen wird durch die efzn-Geschäftsstelle bestätigt; diese klassifiziert die Meldung, führt eine Erstprüfung durch und koordiniert die vertrauliche Weitergabe an zuständige Betreiber, Behörden oder weitere berechnigte Stellen.

Eine Reproduktion oder fachliche Prüfung sensibler Einreichungen erfolgt ausschließlich in einer isolierten Prüfungsumgebung. Das Evaluation Board erhält sicherheitsrelevante Details nur insoweit, wie dies für Bewertung, Priorisierung oder koordinierte Maßnahmen erforderlich ist. Für die öffentliche Kommunikation und Preiswürdigung werden Beiträge ausschließlich in abstrahierter, nicht-ausnutzungsgerechter Form freigegeben. Die vorliegenden Teilnahmebedingungen erteilen keine Befugnis zu Tests, Scans, Kontaktaufnahmen oder sonstigen Eingriffen in reale Systeme. Kontakt-, Verschlüsselungs- und Verfahrenshinweise zum Responsible-Disclosure-Kanal werden auf der Wettbewerbswebseite veröffentlicht.

11. Ermittlung des / der Gewinner:in

Die eingereichten Beiträge werden nach folgenden Bewertungskriterien durch das Evaluation Board bewertet:

- Originalität, Nachvollziehbarkeit und Reproduzierbarkeit der Datenverknüpfung
- Methodische Qualität (KI-Einsatz, Datenqualität, Unsicherheiten, Plausibilisierung)
- Beitrag zur Resilienz: konkrete, umsetzbare Empfehlungen für Schutzmaßnahmen
- Sicherer Umgang: Risikoabwägung, verantwortungsvolle Darstellung, Einhaltung der Regeln
- Interdisziplinärer Mehrwert und sektorübergreifende Perspektive (wo sinnvoll)

Das interdisziplinäre Evaluation Board unter Leitung des efzn bewertet die eingereichten Beiträge und legt die Gewinner:innen des Preisgeldes fest. Die Gewinner:innen werden per E-Mail benachrichtigt.

Das Evaluation Board setzt sich zusammen aus Vertreter:innen von Netzbetreibern (Übertragungs- und Verteilnetz), Telekommunikation, weiteren Infrastrukturdienstleistern, Sicherheitsbehörden, Politik sowie Wissenschaft.

12. Preisgeld und Weiterverwertung

Das Preisgeld wird in folgender Höhe vergeben:

Preisgeld 1. Platz: 3000,- Euro; Preisgeld 2. Platz: 2000,- Euro; Preisgeld 3. Platz: 1000,- Euro.

Das efzn nutzt die Ergebnisse zur Erarbeitung von Handlungsempfehlungen und zur Organisation geschlossener Rückkopplungsrunden mit betroffenen Betreibern / Institutionen.

13. Preisverleihung

Die Details der Preisverleihung werden zu einem späteren Zeitpunkt festgelegt. Grundsätzlich erfolgt eine Preisverleihung mit öffentlicher Würdigung nur auf abstrahierter Ebene. Etwaige Reise- und Übernachtungskosten für die Teilnahme an der Preisverleihung werden nicht übernommen.

14. Datenschutz

Es gilt die Datenschutzerklärung des efzn, welche unter folgendem Link abrufbar ist:
<https://www.efzn.de/datenschutz>

15. Haftungsausschluss, Ausschluss des Rechtsweges

Das efzn behält sich das Recht vor, diese Teilnahmebedingungen zu ändern und den Wettbewerb bei Bedarf abzusagen. Der Rechtsweg ist ausgeschlossen.