Engineer Beratung

So arbeiten wir sicher

Wie Engineer ApS sicher entwickelt und betreibt: unsere Arbeitspraktiken, die Absicherung dieser Website und die Meldestelle für Schwachstellen.

Sicherheit ist keine separat verkaufte Leistung. Sie bestimmt die Arbeitsweise: Das Bedrohungsmodell gehört zum Entwurf, die Härtung zur Umsetzung und der Nachweis zur Übergabe.

Die Kontrollen von Anfang an einplanen

Machen Sie Zugriff, Bereitstellung und Wiederherstellung von Anfang an zum Teil der technischen Arbeit.

Unsere Leistungen entdecken Kontakt aufnehmen →

Hinter eine Sicherheitsbehauptung schauen

Fragen Sie nach der Konfiguration und den Tests hinter einer Sicherheitsbehauptung, mit ausdrücklich benanntem Geltungsbereich.

Fallstudien Kontakt aufnehmen →

Wie wir entwickeln

- **Standardmäßig minimale Rechte.** Dienste laufen unter eigenen unprivilegierten Benutzern mit genau dem Zugriff, den sie für ihre Aufgabe benötigen. Zugriffsgrenzen sind darauf ausgelegt, die Ausbreitung zwischen Komponenten einzuschränken, falls eine davon kompromittiert wird.
- **Geheimnisse gelangen nie ins Repository.** Zugangsdaten liegen in einem Secret Store oder in der Bereitstellungsschicht, nie im Quellcode oder in einem Build-Artefakt. Jeder Commit wird automatisch geprüft; ein Treffer verhindert den Commit.
- **Infrastruktur als Code beschrieben.** Server entstehen aus einer lesbaren, prüfbaren und erneut ausführbaren Beschreibung. Die Maschinenkonfiguration ist damit ein versioniertes Dokument statt einer Erinnerung im Kopf einer Person.

- **Abhängigkeiten mit festgelegten Versionen und Sicherheitsprüfung.** Die Bestandteile eines Systems sind dokumentiert. Diese Liste wird mit veröffentlichten Sicherheitshinweisen abgeglichen; dass letzten Monat alles funktionierte, genügt nicht als Vertrauensgrundlage.
- **Durchgehend verschlüsselte Übertragung.** Zertifikate werden automatisch ausgestellt und erneuert, und die Erneuerung wird überwacht. Denn häufig scheitert TLS an einem Zertifikat, das niemand im Blick hatte.
- **Automatisierte Sicherungen mit separaten Wiederherstellungstests.** Eine Sicherung ist zunächst nur eine Behauptung, bis jemand daraus Daten wiederherstellt. Wir implementieren getrennte Abläufe für Sicherungen und Wiederherstellungstests; die Verifizierung stützt sich auf die tatsächlich wiederhergestellten und geprüften Daten.

Jede Zeile oben ist **ein gewöhnlicher Arbeitstag** — keine Phase, die man am Ende ergänzt.

Vereinbaren Sie Sicherheitsgrenzen, Verantwortlichkeiten und Prüfungen als Teil des Entwurfs.

Wie diese Website aufgebaut ist

Für unsere eigene Website gelten dieselben Maßstäbe. Sie können jede dieser Aussagen im eigenen Browser überprüfen.

- **Kein Backend, keine Datenbank, kein Admin-Login.** Jede Seite ist eine statische Datei, die erzeugt wird, bevor sie angefordert wird. Dadurch entfallen Anwendungssitzungen und Endpunkte für Datenbankabfragen; die anwendungsbezogene Angriffsfläche der Website wird kleiner.
- **Kein ausführbares JavaScript.** Seiten, Menüs und Links nutzen natives HTML und CSS; die strukturierten Daten sind inertes JSON-LD. Es gibt kein Browserskript, das Anfragen stellen oder Einstellungen speichern könnte.
- **Eine strenge Content Security Policy** direkt in der Seite, mit `form-action 'none'` — die Website sendet keinerlei Formulare ab.
- **Subresource Integrity für das Stylesheet.** Das Bundle erhält beim Build einen Fingerprint und einen Hash, damit Ihr Browser die unveränderte Übertragung prüfen kann.
- **Keine Anfragen an Dritte.** Keine Analysewerkzeuge, Schriftdienste oder Karten-Widgets von Drittanbietern und kein Einwilligungsbanner. Öffnen Sie die Netzwerkansicht Ihres Browsers und zählen Sie die Hosts: Es gibt genau einen, unseren.

- **Keine Cookies.** Was gespeichert wird und was nicht, steht vollständig auf der Cookie-Seite.
- **Eine maschinenlesbare Richtlinie zur Schwachstellenmeldung** unter `/.well-known/security.txt`, damit Forschende ohne Nachfrage wissen, wohin sie einen Fund melden können.

Wie sie betrieben wird

Ein kleiner Server in Toronto, als Code beschrieben, mit einem Zugriffsprotokoll, das bereits beim Schreiben maskiert und ungefähr dreißig Tage aufbewahrt wird. Die Danksagungen und Quellen nennen jede Software darauf; die Datenschutzseite beschreibt genau, was er bei der Beantwortung von Anfragen erfasst.

Eine Schwachstelle melden

Wenn Sie eine Schwachstelle in dieser Website oder in einem von uns betriebenen System gefunden haben, schreiben Sie an welcome@engineer.company und beschreiben Sie den Fund und die Schritte zur Reproduktion. Wir bestätigen den Eingang, erläutern unser Vorgehen und nennen Sie auf Wunsch als Finder. Es gibt weder ein Prämienprogramm noch juristische Drohungen — nur eine Adresse, die eine Ingenieurin erreicht.

Wünschen Sie dieselbe Sorgfalt für Ihre eigenen Systeme?
Lassen Sie uns nachsehen.

Diese Seite enthält Aussagen, **die Sie prüfen können** — direkt in dem Browser, in dem Sie sie lesen.

Kein Backend, keine Cookies, kein ausführbares JavaScript und eine Richtlinie, die die Seite selbst deklariert.

Bitten Sie uns, Ihre Website zu prüfen Was wir anbieten →

Feststellen, was Schutz benötigt

Beginnen Sie mit den Schutzgütern, Vertrauensgrenzen und Berechtigungen des Systems, das Sie schützen müssen.

Preise ansehen Kontakt aufnehmen →

Einen gezielten Sicherheitsauftrag vereinbaren

Besprechen Sie eine gezielte Prüfung oder Umsetzung mit konkreten Kontrollen und Abnahmeprüfungen.

Unsere Leistungen entdecken

welcome@engineer.company +45 50 10 61 84 Kopenhagen, Dänemark

Nehmen Sie diese Seite mit

Kontaktkarte

Mit Sorgfalt und Liebe gestaltet von D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Copyright © 2025 – heute · Engineer ApS · Alle Rechte vorbehalten.

Gedruckt von https://advisory.engineer.company/de/security/