Engineer

Zugriffskontrolle

das Erlauben oder Ablehnen jeder Ressourcenanfrage

Was es ist

Zugriffskontrolle ist der Teil eines Systems, der viele Male pro Sekunde dieselbe Frage beantwortet: Darf dieser Aufrufer jetzt diese Handlung an dieser Ressource ausführen? Der Aufrufer kann ein Mensch, ein Dienst oder ein geplanter Auftrag sein. Die Ressource kann eine Datei, eine Datenbankzeile, ein API-Endpunkt, ein Git-Repository oder eine Tür sein. Die einzelnen Mechanismen, die diese Frage beantworten, heißen Zugriffskontrollen. Das NIST-Glossar führt Autorisierung als Synonym für das gesamte Konzept auf. Seine Definitionen umfassen beide Hälften der Aufgabe: „die Entscheidung, einem Subjekt Zugriff auf Systemobjekte zu gewähren oder zu verweigern“, und „das Verfahren, bestimmten Anfragen stattzugeben oder sie abzulehnen“, um Informationen und zugehörige Verarbeitungsdienste abzurufen und zu nutzen oder bestimmte physische Einrichtungen zu betreten.

Die Verwechslung mit Authentifizierung liegt nahe, doch es sind getrennte Schritte. NIST SP 800-162 sagt es ausdrücklich: „Authentifizierung ist nicht dasselbe wie Zugriffskontrolle“. Die Authentifizierung stellt fest, wer fragt. Die Zugriffskontrolle verwendet diese Identität und alles Weitere, was über die Anfrage bekannt ist, um zu entscheiden, was der Aufrufer damit tun darf. Ein System kann eine Person einwandfrei überprüfen und sie trotzdem fremde Datensätze lesen lassen, weil die zweite Frage nie gestellt wurde.

Derselbe Leitfaden teilt die Arbeit in zwei Teile. Ein Policy Decision Point berechnet die Entscheidung, ein Policy Enforcement Point liegt im Anfragepfad und setzt sie durch. Beide können im selben Prozess liegen. Die Unterscheidung bleibt dennoch nützlich, denn eine Entscheidung, die niemand durchsetzt, schützt nichts. NIST SP 800-53 hält dies in zwei Maßnahmen fest: AC-24 verlangt, dass Entscheidungen vor der Durchsetzung auf jede Zugriffsanfrage angewendet werden; AC-3 verlangt, dass genehmigte Berechtigungen durchgesetzt werden.

Die Regeln können unterschiedliche Formen haben: eine Liste erlaubter Identitäten pro Objekt, Rollen wie bei RBAC oder Attribute des Aufrufers, des Objekts, der Handlung und der Umgebung, wie sie SP 800-162 behandelt. Unabhängig von der Form muss die Frage weiterhin bei jeder Anfrage gestellt werden.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist Zugriffskontrolle?“ für eine konkrete Entscheidung. Wir können helfen, das Konzept mit dem System in Verbindung zu bringen, das Sie entwickeln oder einkaufen. Konten, Passwörter und Berechtigungen werden so geordnet, dass alle genau den beruflich erforderlichen Zugriff haben und ihn am Tag ihres Ausscheidens verlieren.

Unsere Leistungen entdecken Kontakt aufnehmen →

Die Annahmen hinter dem Begriff prüfen

Nutzen Sie die Erklärung und die verlinkten Arbeiten, um Fragen für Ihr Projekt zu formulieren. Wir können die Annahmen gemeinsam mit Ihnen prüfen, bevor ein Werkzeug ausgewählt wird. 1.000 RBAC-Regeln für sichere Linux-Server — 1,000 Zugriffsregeln zum Schließen einer Sicherheitslücke

1.000 RBAC-Regeln für sichere Linux-Server Kontakt aufnehmen →

Warum es wichtig ist

Nach der Anmeldung entscheidet die Zugriffskontrolle über fast alles, was jemand erreichen kann. Starke Authentifizierung vor schwacher Zugriffskontrolle hält lediglich fest, welches Konto die Daten abgerufen hat. Für ein Unternehmen, das Informationen anderer Menschen verwahrt, entscheidet sich hier, ob das Versprechen darüber, wer was sehen darf, eingehalten wird.

NIST beschreibt den idealen Durchsetzungsmechanismus als Reference Monitor. Maßnahme AC-25 in SP 800-53 verlangt, dass er manipulationssicher ist, immer aufgerufen wird und klein genug bleibt, um analysiert und getestet zu werden. Diese drei Eigenschaften sind eine praktische Prüfung für jede Kontrolle in einem echten Produkt. Kann der Aufrufer die Eingaben verändern, auf denen die Prüfung beruht, ist die erste verletzt. Erreicht ein Pfad die Daten, ohne die Prüfung zu passieren, ist die zweite verletzt. Ist die Logik auf Hunderte von Handlern verteilt, sodass niemand sie von Anfang bis Ende lesen kann, ist die dritte verletzt.

Der OWASP Application Security Verification Standard übersetzt dies in prüfbare Anforderungen. Sein Kapitel zur Autorisierung verlangt, den Zugriff auf Funktionen auf ausdrücklich berechtigte Aufrufer zu beschränken und einzelne Datenelemente ebenso zu schützen. Die Regeln müssen in einer vertrauenswürdigen Dienstschicht durchgesetzt werden, statt sich auf etwas zu verlassen, das ein nicht vertrauenswürdiger Client manipulieren könnte, etwa

JavaScript im Browser. Änderungen an den Werten, von denen eine Entscheidung abhängt, müssen außerdem sofort wirksam werden. Wo das nicht möglich ist, soll eine kompensierende Kontrolle Alarm schlagen, wenn jemand handelt, nachdem die Berechtigung entzogen wurde.

Der Preis ist zusätzlicher Aufwand im Anfragepfad. Jede Entscheidung braucht Fakten, und jeder Fakt muss nachgeschlagen werden. Wer das Nachschlagen auslässt, verlagert die Prüfung leicht dorthin, wo sie am billigsten ist. Das ist häufig der Ort, den der Aufrufer kontrolliert.

Wie es in der Praxis aussieht

Auf einer maritimen Plattform, auf der eine Person für mehrere Organisationen handeln kann, wurde die Zuständigkeit dadurch geklärt, wo die Entscheidung fällt: Die aktive Organisation wird im Client gehalten, aber für Zugriffsentscheidungen wird keiner dieser Angaben vertraut. Ein OrganizationContext speichert die aktuelle Auswahl in localStorage, damit der Wechsel sofort erfolgt. Ein serverseitiges Cookie spiegelt sie, damit serverseitig gerenderte Seiten denselben Kontext auflösen. Bei jeder Anfrage wird die Autorisierung auf dem Server erneut geprüft. Die Seite zieht die Grenze in einem Satz: Nur der Server entscheidet, was erlaubt ist. Wer localStorage manipuliert, verändert lediglich die eigene Oberfläche, weil der Server weiterhin Nein sagt.

Auf derselben Art von Plattform wurden Zahlungsannahme und Berechtigungsvergabe als zwei Systeme gebaut. Kartenzahlungen über Stripe und In-App-Käufe bei Apple und Google laufen in einem Zahlungsschema mit 9 Tabellen und 34 Funktionen zusammen. Ein getrenntes Zugriffsschema mit 11 Tabellen und 34 Funktionen beantwortet „Darf dieses Konto das?“, ohne zu wissen, welcher Store die Zahlung abgewickelt hat. Diese Antwort steuert Unternehmensverzeichnis, Suche und Datenexport. Sie wird bei jeder Anfrage serverseitig erneut geprüft, denn eine ausgeblendete Schaltfläche ist eine Gefälligkeit und keine Kontrolle. Ein zusätzlicher Store betrifft nun nur die Zahlungsseite. Eine Supportfrage zum Zugriff führt zu einer Tabelle statt zu drei. Die Seite benennt den Preis: zwei Schemas und eine Berechtigungsabfrage bei Anfragen, die diesen Aufwand sonst nicht hätten.

Als das Unternehmen seinen Quellcode auf eigene Hardware verlagerte, wurde die Git-Forge so eingerichtet, dass sie standardmäßig ablehnt. Die Seite zählt Zugriffskontrolle zu den Aufgaben, die mit dem Betrieb einer Forge einhergehen. Gewählt wurde eine Forge ohne administrative Weboberfläche: Je

weniger Oberfläche es gibt, desto weniger muss verteidigt werden. Die Richtlinie beginnt mit Ablehnung. Ein Aufrufer ohne Identität erhält nichts, ein Aufrufer ohne Schlüssel ebenfalls nichts. Jedes deklarierte Repository ist zudem als privat markiert, sodass die Vertraulichkeit auf Regeln und nicht auf Unauffindbarkeit beruht. Erreichbarkeit gehört zur selben Richtlinie. Port 23231 antwortet nur auf der Loopback-Schnittstelle; von außen führt deshalb nur ein Weg über einen Sprunghost hinein. Der Multiplexer, der Git über den öffentlichen Port zugänglich machen könnte, steht mit ausgeschaltetem Schalter im Code: Auch ein ungenutzter Listener ist Angriffsfläche.

Wo es schiefgeht

Die Prüfung sitzt in der Oberfläche. Eine Schaltfläche ist verborgen oder ausgegraut, doch der dahinterliegende Endpunkt antwortet jedem direkten Aufrufer. Der Server muss bei jeder Anfrage erneut entscheiden, gestützt auf Fakten, die der Aufrufer nicht bearbeiten kann.

Die Funktion wird geprüft, der Datensatz nicht. Eine Anfrage nennt eine Rechnung, ein Dokument oder ein Konto anhand seiner Kennung. Der Server bestätigt, dass der Aufrufer Rechnungen ansehen darf, und gibt die angeforderte zurück, ohne ihre Zugehörigkeit zu prüfen. ASVS nennt diese Lücke Insecure Direct Object Reference (IDOR) oder Broken Object Level Authorization (BOLA). Erkennbar ist sie an einer Kennung in der Anfrage, die der Server ungeprüft übernimmt. Lösen Sie jedes Objekt innerhalb des eigenen Zugriffsbereichs des Aufrufers auf. In einem Produkt mit mehreren Mandanten muss der Mandant aus der serverseitigen Sitzung stammen und niemals aus der Anfrage.

Alles Neue ist offen, bis jemand es schließt. Eine neue Route, Tabelle oder ein neues Repository beginnt mit der Voreinstellung. Lautet sie „erlauben“, bleibt die Lücke bestehen, bis jemand sie bemerkt. SP 800-53 formuliert das Gegenteil für Netzwerke als „standardmäßig verweigern, ausnahmsweise erlauben“. Dieselbe Regel passt auf jede Schicht: Was nie gewährt wurde, wird verweigert.

Berechtigungen wachsen nur. SP 800-162 weist darauf hin, dass Nutzer mit der Zeit Rechte ansammeln, wenn Zugriffe nicht entfernt oder widerrufen werden. Menschen wechseln Teams, Projekte enden und Auftragnehmer gehen. Jeder dieser Zeitpunkte verlangt, etwas zu entziehen. Ein Widerruf, der erst Stunden später beim Ablauf einer Sitzung wirkt, ist eine abgeschwächte Form derselben Lücke.

Niemand kann erklären, warum eine Anfrage erlaubt wurde. Werden Entscheidungen an vielen Stellen getroffen und nirgends protokolliert, fehlt einer Untersuchung die Grundlage. Zeichnen Sie Erlaubnisse und Ablehnungen mit der jeweils maßgeblichen Regel auf und schützen Sie das Protokoll: SP 800-162 warnt, dass Entscheidungsmuster Eigenschaften der Menschen hinter den Anfragen offenlegen können.

Weiterführende Lektüre

- Zugriffskontrolle im NIST-CSRC-Glossar — Definitionen aus FIPS 201-3 und CNSSI 4009, mit Autorisierung als Synonym.
- NIST SP 800-53 Rev. 5 — die Maßnahmenfamilie zur Zugriffskontrolle, einschließlich AC-3 zur Durchsetzung, AC-24 zu Entscheidungen und AC-25.
- NIST SP 800-162 — attributbasierte Zugriffskontrolle mit Entscheidungs- und Durchsetzungspunkten.
- OWASP Application Security Verification Standard — prüfbare Autorisierungsanforderungen auf Funktions-, Daten- und Feldebene.

Glossar

Für Ihre tatsächlichen Rahmenbedingungen auswählen

Beschreiben Sie den Bereitstellungsweg, die Betriebsrisiken und die Bereitschaftsverantwortlichen. Wir können eine Änderung mit Prüfungen, einem Wiederherstellungsweg und klaren Zuständigkeiten abgrenzen.

Preise ansehen Kontakt aufnehmen →

Die Begriffe praktisch nutzbar machen

Fragen Sie, wie „Was ist Zugriffskontrolle?“ auf Ihre Organisation zutrifft. Ein konkretes Beispiel aus Ihrem bestehenden System reicht aus, um das Gespräch zu beginnen.

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://engineer.company/de/glossary/access-control/