Engineer

Informationssicherheit

Schutz von Daten und Systemen vor Missbrauch und Schäden

Was es ist

Informationssicherheit sorgt dafür, dass Informationen und die Systeme, die sie speichern und übertragen, im von ihren Eigentümern vorgesehenen Zustand bleiben: Nur die dafür vorgesehenen Menschen können sie lesen, Änderungen geschehen nur auf die vorgesehene Weise, und bei Bedarf sind die Informationen verfügbar. Im Alltag und in den meisten Stellenbezeichnungen wird das zu Sicherheit verkürzt. Die Definition im NIST-Glossar stammt aus dem US-Bundesgesetz 44 U.S.C. 3552 und nennt drei Eigenschaften. Vertraulichkeit wahrt die autorisierten Beschränkungen von Zugriff und Offenlegung. Integrität schützt vor unzulässiger Veränderung oder Zerstörung. Sie umfasst auch den Nachweis, dass Informationen echt sind und ihr Absender den Versand nicht glaubhaft abstreiten kann. Verfügbarkeit bedeutet rechtzeitigen und verlässlichen Zugriff auf die Informationen sowie ihre Nutzung.

Die drei stehen in einem Spannungsverhältnis. Das macht den größten Teil der Schwierigkeit aus. Eine Datenbank, die niemand erreicht, ist vollkommen vertraulich und für niemanden brauchbar. Eine an drei Orten aufbewahrte Sicherung erhöht die Verfügbarkeit und gibt einem Dieb drei Orte zum Suchen. Bei den meisten Entscheidungen in diesem Bereich geht es darum, für eine konkrete Art von Information diese Ansprüche gegeneinander abzuwägen. Für eine öffentliche Preisliste fällt die Antwort ganz anders aus als für die Krankenakte eines Patienten.

Dazu dienen Kontrollen, jeweils konkrete Schutzmaßnahmen für einen bestimmten Zweck. Manche sind technisch: Verschlüsselung, Authentifizierung, Firewall, Zugriffskontrolle. Manche sind organisatorisch: eine Prüfung vor der Auslieferung einer Änderung, der Entzug von Zugängen am letzten Arbeitstag ausscheidender Mitarbeiter oder ein schriftlicher Vorfallplan. Andere sind physisch, etwa ein abgeschlossener Raum. NIST SP 800-53 ist ein nach Familien gegliederter Katalog solcher Kontrollen, aus dem eine Organisation passend zu

ihren Risiken auswählen kann. Das NIST Cybersecurity Framework 2.0 setzt eine Ebene höher an. Es beschreibt Ergebnisse unter sechs Funktionen, Steuern, Identifizieren, Schützen, Erkennen, Reagieren und Wiederherstellen, und schreibt ausdrücklich nicht vor, wie diese Ergebnisse zu erreichen sind.

Das Konzept für eine Entscheidung nutzen

Nutzen Sie „Was ist Informationssicherheit?“ 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

Schäden an Informationen lassen sich schwer rückgängig machen. Einmal offengelegte Daten bleiben offengelegt, gleichgültig, was anschließend behoben wird. Ein unbemerkt veränderter Datensatz macht jede spätere darauf gestützte Entscheidung fragwürdig. Ein Ausfall am Tag einer Gehaltsabrechnung oder einer Ausschreibungsfrist kostet mehr als die Stunden, die er dauert. Meist tragen zuerst die Menschen die Kosten, deren Daten es waren, und danach das Unternehmen, das sie verwahrte.

Für einen Auftraggeber besteht die Schwierigkeit darin, dass Sicherheit unsichtbar bleibt, solange sie funktioniert. Zwei Anbieter können dieselben Werkzeuge mit denselben Worten aufzählen, und nur einer hat vielleicht geprüft, ob diese Werkzeuge das Behauptete tatsächlich leisten. Die nützlichen Fragen betreffen deshalb die Belege: Welche Kontrollen sind eingerichtet? Woher weiß jemand, dass sie heute funktionieren und nicht nur am Installationstag? Was geschieht, wenn eine ein Problem meldet? Ein Anbieter, der mit einem Bericht aus dem laufenden System antwortet, steht anders da als einer, der ein Richtliniendokument vorlegt.

Die Zielkonflikte sind real und betreffen vor allem Zeit und Reibungsverluste. Jeder Scanner liefert Befunde, und bei jedem muss ein Mensch entscheiden, ob er wichtig ist. Jeder zusätzliche Anmeldeschritt lädt dazu ein, einen Weg daran vorbei zu suchen. Jede neue Kontrolle muss gepflegt werden, sonst existiert sie irgendwann unbemerkt nur noch auf dem Papier. Die Funktion Steuern eröffnet

das Framework, weil dies ebenso Managemententscheidungen wie technische Entscheidungen sind: Jemand muss festlegen, welches Risiko akzeptabel ist, welche Daten die größte Sorgfalt verdienen und was der übrige Schutz kostet.

Wie es in der Praxis aussieht

Auf einer Anwendungsplattform wurde Sicherheit durch ein kontinuierliches Sicherheitsprogramm für eine Anwendungsplattform zu einem Build-Ergebnis statt zu einer Meinung. CodeQL führt statische Analysen durch, ZAP dynamische Tests, und govulncheck prüft Go-Abhängigkeiten. Anchore und Syft erzeugen bei jedem Build eine Softwarestückliste, und Gitleaks durchsucht den Verlauf nach Zugangsdaten. Auch die Lieferkette des Builds selbst ist abgedeckt: Die externen Actions, die seine Workflows aufrufen, sind auf genaue Commits festgeschrieben, niemals auf verschiebbare Tags. Dependabot überwacht 6 Ökosysteme. Neben der Automatisierung stehen 21 schriftliche Sicherheitsaudits, darunter ein Bedrohungsmodell und eine Bewertung anhand des OWASP-Testleitfadens. Eine von den konfigurierten Prüfungen erkannte Schwachstelle kann den Build scheitern lassen. Der Preis ist die Menge der Befunde und die laufende Bewertung und Priorisierung, die nötig ist, damit das Signal brauchbar bleibt.

Der eigene Host des Unternehmens hat 464 MB Arbeitsspeicher, zu wenig für einen Metrik-Stack. Seine Sicherheit beschreiben deshalb sieben rein lesende Berichtsrollen, die den laufenden Host als Markdown darstellen. Der Zugriffsbericht erfasst Konten, sudo-Befugnisse, Schlüsselfingerabdrücke, Forge-Nutzer und Datenbankrollen. Der Sicherheitsbericht beantwortet, ob die Härtung tatsächlich greift, statt nur konfiguriert zu sein. Er gibt die Firewallregeln in Auswertungsreihenfolge und den aktiven Satz von Sperrregeln aus. Keine Zahl erscheint, die der Lauf nicht gemessen hat. Unter anderem fanden die Berichte zwei wirkungslose Sicherheitskontrollen und einen nicht deklarierten lauschenden Port.

Die Lücke zwischen konfiguriert und tatsächlich wirksam war auf demselben Host schon sichtbar geworden. Eine Ratenbegrenzung stand ein Jahr lang unter einer allgemeineren Firewallregel, die zuerst passte. Deshalb erreichte sie kein Paket. Die Prüfungen lesen nun die nummerierte Regelliste und die aktive Filterkette und prüfen die Reihenfolge. Pro Port gibt es genau eine Regel, stets mit Protokoll. Der SSH-Port hat eine Ratenbegrenzung und niemals zusätzlich eine Freigaberegel daneben. Die deklarierte öffentliche Angriffsfläche von fünf Ports wird als Ganzes geprüft.

Wo es schiefgeht

Eine Kontrolle ist konfiguriert und greift nie. Eine Einstellung in einer Datei, eine Regel in einer Liste oder eine Richtlinie im Wiki hält fest, was jemand beabsichtigte. Erst eine Prüfung am laufenden System zeigt, was tatsächlich gilt. Ein Sicherheitsprogramm, das Kontrollen zählt, statt sie zu testen, meldet vollständige Abdeckung, während Lücken offenbleiben. Den ersten echten Test führt dann jemand anderes aus.

Alles hängt an einer Schicht. Ein starker äußerer Schutz mit unbeschränktem Zugriff dahinter gibt bei einem einzigen Fehler alles preis. Gestaffelte Verteidigung geht davon aus, dass jede Schicht irgendwann versagt, und setzt eine weitere dahinter. Ein gestohlenes Passwort trifft so noch auf einen zweiten Faktor und ein kompromittierter Dienst auf eine eng begrenzte Datenbankrolle.

Befunde kommen schneller an, als jemand sie liest. Ein Scanner, der jedes denkbare Problem gleich dringend meldet, gewöhnt Menschen daran, seine Ausgabe nicht mehr zu lesen. Klare Verantwortliche, Schweregradschwellen und eine schriftliche Regel dafür, wann ein Befund eine Freigabe blockiert, halten die Ausgabe lesenswert.

An Verfügbarkeit wird erst während des Ausfalls gedacht. Vertraulichkeit erhält die meiste Aufmerksamkeit, weil Datenlecks Schlagzeilen machen. Nie wiederhergestellte Sicherungen, ein einzelner Server ohne Ersatzplan und unbemerkt ablaufende Zertifikate verfehlen alle die dritte Eigenschaft. Das geschieht meist am ungünstigsten Tag.

Außenstehende finden keine klare Meldestelle. Wer in einem öffentlich erreichbaren Dienst eine Schwachstelle entdeckt, muss wissen, wohin die Meldung gehört. RFC 9116 definiert eine Datei security.txt unter /.well-known/security.txt. Das Pflichtfeld Contact nennt die Meldestelle, das Pflichtfeld Expires den Zeitpunkt, bis zu dem der Datei vertraut werden kann. Ohne sie landen Meldungen in einem allgemeinen Postfach oder bei der ersten Person, die antwortet.

Weiterführende Lektüre

- Informationssicherheit im NIST-CSRC-Glossar — Die Definition aus FIPS 200 und 44 U.S.C. 3552 mit ihren drei Eigenschaften.

- 44 U.S.C. 3552 — Das Gesetz, das Vertraulichkeit, Integrität und Verfügbarkeit definiert.
- NIST SP 800-53, Revision 5 — Der nach Familien gegliederte Katalog von Sicherheits- und Datenschutzkontrollen.
- Das NIST Cybersecurity Framework 2.0 — Sechs Funktionen, die angestrebte Ergebnisse der Sicherheitsarbeit beschreiben, von Steuern bis Wiederherstellen.
- RFC 9116 — Das Format security.txt, das Forschern zeigt, wohin eine Schwachstelle zu melden ist.

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 Informationssicherheit?“ 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/security/