Engineer

Sécurité de l’information

Protection des données et systèmes contre abus et dommages

Ce que c’est

La sécurité de l’information consiste à maintenir les informations, et les systèmes qui les stockent et les transportent, dans l’état voulu par leurs propriétaires : lisibles uniquement par les personnes autorisées, modifiables uniquement de la manière prévue et disponibles au moment nécessaire. Dans la langue courante et dans la plupart des intitulés de poste, on parle simplement de sécurité. La définition du glossaire du NIST provient de la loi fédérale américaine, 44 U.S.C. 3552, qui nomme trois propriétés. La confidentialité préserve les restrictions autorisées d’accès et de divulgation. L’intégrité protège contre les modifications ou destructions indues et comprend la possibilité de démontrer l’authenticité d’une information et de montrer que son expéditeur ne peut pas nier de façon crédible l’avoir envoyée. La disponibilité désigne un accès fiable aux informations et leur utilisation en temps voulu.

Ces trois propriétés tirent dans des directions différentes, et cette tension explique l’essentiel de la difficulté du métier. Une base de données à laquelle personne ne peut accéder est parfaitement confidentielle et inutile à tous. Une sauvegarde conservée en trois endroits améliore la disponibilité et donne à un voleur trois lieux où chercher. La plupart des décisions consistent à trouver un équilibre entre ces exigences pour un type d’information précis. La réponse pour une liste publique de prix diffère beaucoup de celle pour le dossier médical d’un patient.

Le travail repose sur des mesures de protection, chacune répondant à un objectif précis. Certaines sont techniques : chiffrement, authentification, pare-feu, contrôle d’accès. D’autres sont procédurales : une revue avant de livrer un changement, une règle retirant les accès d’un salarié le jour de son départ, un plan écrit en cas d’incident. D’autres encore sont physiques, comme une pièce fermée à clé. NIST SP 800-53 est un catalogue de ces mesures, regroupées en familles et rédigées pour qu’une organisation puisse choisir celles qui répondent

à ses risques. Le NIST Cybersecurity Framework 2.0 se situe un niveau plus haut. Il décrit des résultats au travers de six fonctions : gouverner (Govern), identifier (Identify), protéger (Protect), détecter (Detect), répondre (Respond) et rétablir (Recover), et précise qu'il ne prescrit pas la manière de les atteindre.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce que la sécurité de l'information ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Des comptes, mots de passe et droits attribués selon les besoins exacts de chaque poste, puis retirés le jour du départ.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

Pourquoi c'est important

Les dommages causés aux informations sont difficiles à réparer. Une fuite de données reste une fuite, quelles que soient les corrections ultérieures. Un enregistrement modifié à l'insu de tous rend suspecte chaque décision prise ensuite sur cette base. Une panne le jour du traitement de la paie ou d'une échéance d'appel d'offres coûte davantage que les heures qu'elle dure. Les personnes concernées par les données en supportent généralement le coût en premier, puis l'entreprise qui les détenait.

Pour un acheteur, la difficulté tient à ce que la sécurité est invisible lorsqu'elle fonctionne. Deux fournisseurs peuvent énumérer les mêmes outils dans les mêmes termes, et un seul peut avoir vérifié qu'ils font effectivement ce qui est annoncé. Les questions utiles portent donc sur les preuves : quelles protections sont en place, comment sait-on qu'elles fonctionnent aujourd'hui et pas seulement le jour de leur installation, et que se passe-t-il lorsque l'une d'elles signale un problème ? Un fournisseur qui répond par un rapport issu du système en service n'est pas dans la même situation que celui qui répond par un document de politique interne.

Les compromis sont réels et concernent surtout le temps et les contraintes d'utilisation. Chaque analyseur produit des constats, et chacun exige qu'une personne juge de son importance. Chaque étape supplémentaire de connexion est une étape que les utilisateurs chercheront à contourner. Toute mesure ajoutée doit être entretenue, faute de quoi elle devient discrètement une protection qui n'existe que sur le papier. La fonction « gouverner » (Govern) ouvre

le cadre, car ces décisions relèvent autant de la gestion que de la technique : quelqu'un doit décider du risque acceptable, des données qui méritent le plus de soin et du coût des autres protections.

À quoi cela ressemble en pratique

Sur une plateforme applicative, la sécurité est devenue un résultat de construction plutôt qu'une opinion, grâce à un programme continu d'analyses de sécurité. L'analyse statique passe par CodeQL, les tests dynamiques par ZAP, et les dépendances Go sont vérifiées avec govulncheck. Une nomenclature logicielle est générée à chaque construction avec Anchore et Syft, et Gitleaks analyse l'historique à la recherche d'identifiants d'accès. La chaîne d'approvisionnement du processus de construction est elle aussi couverte : les Actions externes appelées par les workflows sont fixées à des commits précis, jamais à des étiquettes que quelqu'un pourrait déplacer. Dependabot surveille 6 écosystèmes. À cette automatisation s'ajoutent 21 audits de sécurité écrits, dont un modèle de menaces et une évaluation selon le guide de tests OWASP. Une vulnérabilité reconnue par les contrôles configurés peut faire échouer la construction. Le coût réside dans le volume de constats et le tri continu nécessaire pour conserver un signal exploitable.

L'hôte de l'entreprise dispose de 464 MB de mémoire, trop peu pour une pile de métriques. Sa sécurité est donc documentée par sept rôles en lecture seule qui décrivent l'hôte en service en Markdown. Le rapport d'accès couvre les comptes, le périmètre sudo, les empreintes de clés, les utilisateurs de la forge et les rôles de base de données. Le rapport de sécurité détermine si le durcissement est effectivement appliqué, plutôt que simplement configuré, en affichant les règles de pare-feu dans leur ordre de correspondance et les règles de bannissement actives. Aucun nombre n'est affiché si l'exécution ne l'a pas mesuré. Les rapports ont notamment découvert deux protections de sécurité inactives et un port d'écoute non déclaré.

L'écart entre configuration et application effective s'était déjà révélé sur ce même hôte. Une limitation de débit est restée pendant un an sous une règle de pare-feu plus large qui s'appliquait en premier : aucun paquet ne l'atteignait. Les vérifications lisent désormais la liste numérotée des règles et la chaîne de filtrage active, puis vérifient cet ordre par des assertions. Chaque port a exactement une règle, toujours assortie d'un protocole. Le port SSH a une règle de limitation de débit, jamais de règle d'autorisation à côté, et la surface publique déclarée de cinq ports est vérifiée dans son ensemble.

Où les problèmes surviennent

Une protection est configurée sans jamais être appliquée. Un paramètre dans un fichier, une règle dans une liste ou une politique sur un wiki consigne une intention. Seule une vérification du système en fonctionnement montre la réalité. Un programme qui compte les protections au lieu de les tester annonce une couverture complète alors que les failles restent ouvertes. Le premier vrai test vient alors de quelqu'un d'autre.

Tout repose sur une seule couche. Un périmètre solide derrière lequel l'accès est grand ouvert signifie qu'une seule erreur expose tout. La défense en profondeur suppose que chaque couche finira par céder et en place une autre derrière : un mot de passe volé rencontre encore un second facteur, et un service compromis se heurte encore à un rôle de base de données aux droits limités.

Les constats arrivent plus vite qu'on ne les lit. Un analyseur qui signale tous les problèmes possibles avec la même urgence apprend à ses utilisateurs à ne plus le lire. Des responsables clairement identifiés, des seuils de gravité et une règle écrite déterminant quand un constat bloque une publication préservent l'utilité de ses résultats.

On ne pense à la disponibilité qu'au moment de la panne. La confidentialité capte l'essentiel de l'attention, car les fuites font l'actualité. Des sauvegardes jamais restaurées, un serveur unique sans plan de remplacement et des certificats qui expirent sans qu'on le remarque mettent tous à mal la troisième propriété. Et ces défaillances surviennent souvent le pire jour possible.

Les personnes extérieures ne savent pas où signaler un problème. Qui trouve une faiblesse dans un service accessible au public doit savoir où la signaler. La RFC 9116 définit un fichier security.txt, servi à l'adresse /.well-known/security.txt, avec un champ Contact obligatoire indiquant où envoyer les signalements et un champ Expires obligatoire indiquant jusqu'à quand le fichier est fiable. Sans lui, les signalements arrivent dans une boîte générique ou chez la première personne qui répond.

Pour aller plus loin

- La sécurité de l'information dans le glossaire du NIST CSRC — la définition issue de FIPS 200 et de 44 U.S.C. 3552, avec ses trois propriétés.
- 44 U.S.C. 3552 — la loi qui définit confidentialité, intégrité et disponibilité.

- NIST SP 800-53 Rev. 5 — le catalogue de mesures de sécurité et de protection de la vie privée, regroupées en familles.
- Le NIST Cybersecurity Framework 2.0 — six fonctions qui décrivent les résultats de sécurité, de « gouverner » (Govern) à « rétablir » (Recover).
- RFC 9116 — le format security.txt, qui indique aux chercheurs où signaler une vulnérabilité.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu'est-ce que la sécurité de l'information ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

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

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/security/