LIVRE BLANC

« Secure by design » : intégrer la cybersécurité dès la conception

L'importance de cette philosophie et son rôle dans la réduction de votre surface d'attaque depuis l'intérieur

SOPHOS

Résumé

«Secure by Design» est une philosophie de développement logiciel qui considère la sécurité comme une exigence primaire plutôt que comme un élément secondaire.

Au lieu de développer un produit dans un premier temps et d'y ajouter des correctifs de sécurité dans un second temps, l'approche Secure by Design exige que les considérations de cybersécurité soient intégrées à chaque étape du cycle de vie du développement — de l'architecture et de la conception jusqu'au codage, aux tests, au déploiement et à la maintenance.

Le principe est simple : si vous concevez un système sécurisé dès le départ, vos utilisateurs sont protégés par défaut, même s'ils ne savent pas comment configurer les paramètres appropriés ou si les failles de sécurité ne sont corrigées qu'après coup.

Concrètement, cela implique d'adopter des principes tels que le moindre privilège (qui consiste à n'accorder aux utilisateurs et aux processus que l'accès minimal dont ils ont besoin), des paramètres par défaut sécurisés (qui consistent à livrer les produits avec la configuration la plus sûre dès leur sortie de l'emballage), une défense en profondeur (qui consiste à superposer plusieurs couches de contrôles de sécurité afin qu'aucune

défaillance isolée ne soit catastrophique), ainsi que l'élimination de catégories entières de vulnérabilités grâce à des langages, des frameworks et des modèles de conception plus sûrs.

Le principe est simple :

Si vous concevez un système sécurisé dès le départ, vos utilisateurs sont protégés par défaut, même s'ils ne savent pas comment configurer les paramètres appropriés ou si les failles de sécurité ne sont corrigées qu'après coup.

L'importance de l'approche Secure by Design

Pendant des décennies, de nombreux acteurs du secteur technologique ont fonctionné selon le modèle «ship fast, fix later», ou «livrer vite, corriger ensuite». L'une des conséquences de cet héritage est que la cybersécurité peut être perçue comme un simple centre de coûts — un élément qui ralentit les mises en production et frustre les développeurs. Les répercussions se font sentir en temps réel : des failles de sécurité régulièrement révélées, des correctifs d'urgence mis en place à la hâte et des vols de données qui coûtent des milliards aux organisations tout en exposant les données personnelles de centaines de millions de personnes.

Les vulnérabilités d'Ivanti Connect Secure, l'exploitation de Log4Shell dans une bibliothèque open source très répandue et les vulnérabilités de MOVEit Transfer ont toutes démontré que la sécurité réactive ne peut tout simplement pas suivre le rythme d'adversaires déterminés.

Consciente de ce déséquilibre, la CISA (Cybersecurity and Infrastructure Security Agency) américaine, en collaboration avec des partenaires internationaux, a publié en 2023 des directives Secure by Design officielles, exhortant les fabricants de technologies à assumer la responsabilité des résultats de sécurité de leurs clients.

Les principes Secure by Design stipulent que la responsabilité en matière de sécurité doit incomber aux éditeurs qui développent les produits et non aux utilisateurs finaux qui effectuent le déploiement. Cela a modifié la manière dont les éditeurs abordaient la question de la sécurité des produits technologiques, faisant passer le débat de la responsabilité individuelle («les utilisateurs doivent installer les correctifs sans tarder») à la responsabilité des fabricants («les éditeurs doivent commercialiser des produits sécurisés dès le premier jour»).

Une approche primordiale pour les solutions de cybersécurité

Nous sommes ainsi brutalement rappelés à l'ordre : même les outils de cybersécurité peuvent parfois servir de point d'entrée à une attaque. Et cela se produit avec une régularité inquiétante.

Cela révèle une faiblesse majeure dont souffrent de nombreuses organisations : une fois qu'un appareil périmétrique est compromis, les attaquants continueront de s'en servir jusqu'à ce que celui-ci soit entièrement sécurisé. Les pare-feux et autres systèmes périphériques restent souvent vulnérables même après la mise à disposition d'un correctif. Selon une analyse récente des incidents traités par Sophos portant sur l'ensemble des vulnérabilités confirmées ayant été exploitées, le délai médian entre la publication d'un avis ou d'un correctif par l'éditeur et l'exploitation de cette faille par un attaquant s'élevait à 322 jours — soit près d'une année entière de possibilités pour les cybercriminels! Les éditeurs de solutions de cybersécurité ne peuvent pas partir du principe que les utilisateurs vont installer les correctifs immédiatement.

Le problème des privilèges

Les outils de cybersécurité sont au cœur des infrastructures les plus sensibles d'une organisation. Les agents de détection Endpoint s'exécutent avec un accès au niveau du noyau. Les plateformes SIEM collectent les journaux de tous les systèmes. Les fournisseurs d'identité détiennent les clés de chaque compte. Les pare-feux sont les gardes-frontières entre réseaux fiables et réseaux non fiables.

Lorsque les produits de cybersécurité constituent le cœur du dispositif de défense d'une organisation, ils ont le devoir accru de respecter les principes Secure by Design. Les éditeurs de notre secteur jouent un rôle essentiel dans la protection des clients, et cette confiance s'accompagne d'attentes quant à la conception des produits.

Cette position privilégiée signifie qu'une faille dans un produit de cybersécurité n'expose pas seulement ce produit lui-même, mais également tout ce qu'il est censé protéger. Un attaquant qui parvient à compromettre un agent EDR (Endpoint Detection and Response) ne dispose pas seulement d'un outil, il prend le contrôle de l'appareil doté des privilèges les plus élevés. Une faille dans une appliance VPN ne se contente pas de perturber l'accès à distance, elle offre aux adversaires un accès direct qui contourne tous les contrôles périmétriques.

Les conséquences du non-respect du principe Secure by Design

Les conséquences du non-respect des principes Secure by Design sont bien documentées et, s'ils ne sont pas correctement appliqués, ils compromettent la sécurité des entreprises, des utilisateurs et de l'Internet dans son ensemble.

- **Escalade des coûts liés aux violations.** Lorsque des vulnérabilités sont découvertes après la mise en production, leur correction coûte exponentiellement plus cher que si elles avaient été corrigées pendant la phase de développement.
- **Érosion de la confiance.** Les clients, les autorités de régulation et les partenaires perdent confiance dans les organisations qui sont régulièrement victimes d'incidents de sécurité. Les répercussions sur la réputation peuvent perdurer pendant des années après la remédiation technique.
- **Risques réglementaires et juridiques.** Partout dans le monde, les gouvernements renforcent la réglementation en matière de cybersécurité. La Cyber Resilience Act de l'Union européenne, par exemple, imposera des exigences de sécurité obligatoires aux produits comportant des éléments numériques vendus en Europe. Les organisations qui ne respectent pas les principes Secure by Design s'exposent à des risques de non-conformité, à des amendes et à une exclusion du marché.
- **Risques pour la sécurité nationale.** Les infrastructures critiques, telles que les réseaux électriques, les stations d'épuration et les systèmes de santé, dépendent de plus en plus d'appareils et de systèmes connectés à Internet. Dans ces environnements, les produits non sécurisés par défaut sont une porte ouverte aux acteurs malveillants soutenus par des États et aux auteurs de ransomware, avec des conséquences potentielles susceptibles de bouleverser la vie quotidienne des personnes concernées.
- **Fatigue liée aux correctifs incessants.** Sans bases solides, les organisations se retrouvent prises dans un cercle réactif sans fin : elles doivent rechercher les vulnérabilités, prioriser les correctifs, tester les mises à jour et déployer les correctifs — inlassablement. Cela mobilise des ressources qui pourraient être consacrées à des investigations de cybersécurité plus approfondies.

Comment choisir un pare-feu Secure by Design ?

Lorsque vous évaluerez votre prochain pare-feu, vous devrez veiller en priorité à ce qu'il soit véritablement «Secure by Design». Toutefois, il peut être difficile de faire abstraction des arguments marketing des éditeurs pour comprendre quelles fonctionnalités une solution offre réellement. Les critères suivants vous aideront à identifier les caractéristiques essentielles à prendre en compte lors du choix d'un pare-feu conçu selon les véritables principes Secure by Design :

1. Architecture renforcée

Comme nous l'avons vu, il est essentiel que l'architecture du pare-feu soit conçue, du code jusqu'au cœur du système, selon le principe Secure by Design. Mais il est souvent difficile de savoir ce qu'un éditeur de pare-feu en particulier a fait pour renforcer la sécurité de son produit. La plupart des éditeurs affirment que leurs produits sont sûrs, mais au final, ce sont leurs résultats concrets et vérifiables qui révéleront la vérité.

Voici quelques points évidents à vérifier :

- La prise en charge de l'authentification multifacteur dans toutes les zones du pare-feu (administration, VPN, portails).
- La prise en charge intégrée de l'accès réseau Zero Trust (ZTNA) pour vous affranchir de l'utilisation d'un VPN d'accès à distance.
- Une gestion à distance sécurisée qui ne nécessite PAS l'utilisation du protocole SSH ni la connexion à distance à l'appareil depuis Internet.
- Des portails utilisateurs sécurisés et conteneurisés s'ils sont exposés à Internet.
- La mention dans leurs dernières notes de publications de la mise en œuvre des principes Secure by Design.

2. Correction automatique des vulnérabilités sans interruption de service

L'un des principaux vecteurs d'attaque contre les infrastructures réseau réside dans les vulnérabilités non corrigées. Une fois qu'une faille de sécurité a été découverte, plusieurs semaines peuvent s'écouler avant qu'un correctif ne soit effectivement appliqué. De nombreux utilisateurs souffrent d'une «fatigue liée aux correctifs», car ils sont constamment contraints d'appliquer de nouveaux correctifs et de subir les temps d'arrêt qui en découlent à intervalles réguliers.

Simplifiez-vous la vie et assurez-vous que votre système soit mis à jour rapidement en faisant appel à un éditeur proposant des mises à jour automatiques over-the-air (OTA) qui ne nécessitent aucun temps d'arrêt. Ne vous laissez pas séduire par le marketing autour des soi-disant «mises à jour automatiques» : vérifiez bien ce que cela signifie. Si une mise à jour nécessite toujours un redémarrage et une interruption de service, elle n'est pas «automatique».

3. Audit automatique des risques liés à la configuration

Un autre facteur courant à l'origine d'incidents de sécurité est la mauvaise configuration du pare-feu. Malheureusement, la plupart des pare-feux ne vous signalent pas les erreurs de configuration, laissant ainsi une brèche potentielle susceptible d'être exploitée. Exigez que votre prochain pare-feu vérifie automatiquement et en continu les configurations importantes et signale les paramètres à haut risque afin que vous puissiez y remédier aisément.

4. Suivi proactif par l'éditeur

Souvent, lorsqu'un pare-feu est attaqué, vous ne vous en rendrez probablement compte que lorsqu'il sera trop tard. Heureusement, ce n'est pas le cas de tous les pare-feux. Choisissez un éditeur qui surveille ses propres produits à distance et recueille des données de télémétrie afin de détecter les signes d'une intrusion dès les premières phases d'une attaque. Les éditeurs doivent être disposés et capables d'agir rapidement en cas de détection d'une activité anormale, en vous contactant sans délai ou en contactant votre partenaire de cybersécurité afin de vous aider à identifier l'attaque et à y remédier.

5. Éditeur engagé en faveur du principe Secure by Design

Cela va sans dire, mais si vous êtes arrivé jusqu'ici, vous avez sans doute déjà en tête un éditeur qui adhère clairement aux principes Secure by Design. Mais ne vous contentez pas de les croire sur parole. Consultez leur historique récent, leurs rapports d'avancement et leurs notes de publications pour vous rendre compte précisément de leur engagement en matière de cybersécurité.

L'engagement de Sophos en faveur du principe Secure by Design

Le 8 mai 2024, Sophos a été l'une des premières organisations à s'engager en faveur de l'initiative «Secure by Design» de la CISA (Cybersecurity and Infrastructure Security Agency) américaine, qui s'articule autour de sept piliers fondamentaux de la sécurité de la technologie et des produits :

1. Authentification multifacteur.
2. Mots de passe par défaut.
3. Réduction de catégories entières de vulnérabilités.
4. Correctifs de sécurité.
5. Politique de signalement des vulnérabilités.
6. CVE.
7. Preuves d'intrusion.

Conformément à nos valeurs fondamentales en matière de transparence, le principe Secure by Design a été un fil conducteur qui nous a guidés dans l'évaluation et l'amélioration continues de nos pratiques de sécurité.

Nous avons publié notre engagement en matière d'amélioration et rendons publics les progrès que nous réalisons au regard des sept piliers fondamentaux du cadre Secure by Design. Bien sûr, la cybersécurité est en constante évolution et ce travail n'est jamais terminé. Le perfectionnement et l'amélioration constants de l'application des principes Secure by Design à l'ensemble de notre portefeuille constituent un élément central et permanent de notre philosophie.

Sophos se distingue en proposant plusieurs fonctionnalités Secure by Design clés qui renforcent considérablement la posture de sécurité de Sophos Firewall, tout en vous facilitant grandement la vie. Sophos Firewall est le seul pare-feu sur le marché à proposer des correctifs de sécurité véritablement automatiques, déployés à distance, qui ne nécessitent aucun temps d'arrêt. Nous sommes également le seul éditeur à surveiller activement l'ensemble de nos pare-feux installés chez nos clients. Cela nous permet de détecter tout signe d'attaque, de manière à pouvoir réagir rapidement pour vous aider, vous et votre partenaire de cybersécurité, à y remédier — et à garantir immédiatement que tous les autres clients sont protégés contre des attaques similaires.

Points à retenir

Conformément à nos valeurs fondamentales en matière de transparence, le principe Secure by Design a été un fil conducteur qui nous a guidés dans l'évaluation et l'amélioration continues de nos pratiques de sécurité.

La dernière version (v22) de Sophos Firewall renforce davantage ses fonctionnalités Secure by Design, améliorant considérablement la posture de sécurité du pare-feu. Ces fonctionnalités comprennent :

- Une nouvelle fonctionnalité 'État d'intégrité' pour réduire le risque qu'une erreur de configuration mène à une attaque potentielle.
- Un tout nouveau plan de contrôle repensé pour offrir une sécurité et une évolutivité optimales, qui élimine toute une catégorie de vulnérabilités.
- L'ajout de Sophos XDR Sensor pour Linux, qui renforce la surveillance en temps réel de l'intégrité des systèmes de l'ensemble de notre clientèle par nos propres équipes de sécurité, leur permettant ainsi d'identifier les attaques et d'y répondre plus rapidement.
- Les mises à jour du firmware sont désormais chiffrées et leur authenticité est garantie par un certificat.
- Une mise à niveau du dernier moteur anti-malware de Sophos pour offrir une détection en temps réel et renforcée des menaces émergentes, y compris celles de type zero-day.

Nos travaux de recherche autour de la campagne Pacific Rim nous a permis de voir de près comment opèrent les acteurs malveillants déterminés et dotés de moyens importants — et les mesures nécessaires pour s'en protéger. Cette campagne a mis en évidence le fait que les attaquants n'attendent pas que des failles apparaissent, ils recherchent activement les problèmes de conception, les erreurs de configuration et les systèmes non corrigés au sein des infrastructures à travers le monde. Cette expérience a directement influencé notre approche Secure by Design.

Nos travaux ont souligné la nécessité de mesures de sécurité modernes pour réduire la surface d'attaque au niveau des produits, intégrer des paramètres par défaut robustes, renforcer les procédures d'authentification et éliminer les possibilités d'utilisation abusive bien avant qu'une vulnérabilité ne soit concrètement exploitée.

Aller de l'avant

L'approche Secure by Design n'élimine pas toutes les vulnérabilités et ne dispense pas les organisations d'une vigilance constante. Mais elle est devenue un pilier fondamental de la cybersécurité pour réduire la surface d'attaque. La question n'est plus de savoir si cette approche est une bonne idée, mais la rapidité à laquelle elle est adoptée.

SOPHOS

Êtes-vous prêt à évaluer votre programme de cybersécurité ?

Discutez avec un expert Sophos dès aujourd'hui.

Sophos France
Tél. : 01 34 34 80 00

Email : info@sophos.fr