Sécurité by-design : analyse des 3 grands principes

Principe n°1 : minimiser la surface d'attaque

La surface d'attaque représente tous les points d'entrée et les points de communication qu'un système d'information possède avec l'extérieur. Elle peut être logicielle (OS, librairie, accès en lecture/écriture), réseau (ports ouverts, IP actives, flux réseaux, protocoles utilisés), humaine (phishing, social engineering) ou encore physique (intrusion dans les locaux).

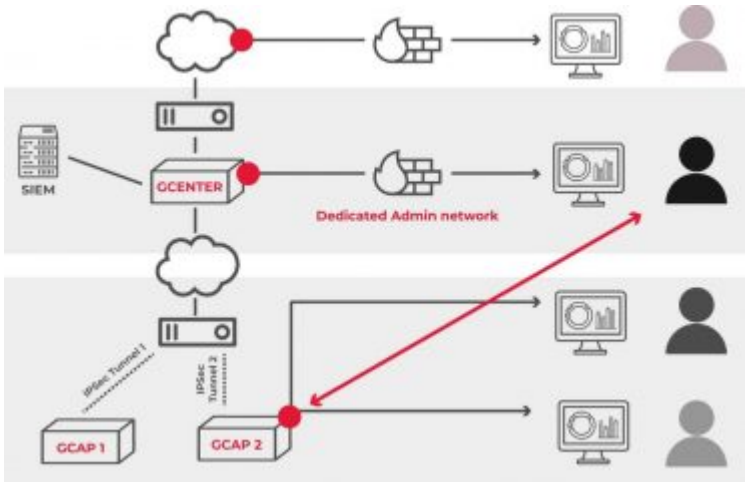
Un SI disposant d'une surface d'attaque étendue sera plus vulnérable aux attaques car les moyens de filtrage et de contrôle sont plus complexes à mettre en place et à organiser. Une fois que tous les points de la surface d'attaque ont été identifiés, il faut mettre en place des outils de surveillance ou de protection avancés sur ces points. Pour les systèmes très exposés, il est également conseillé de réaliser des analyses de sécurité régulières.

Parmi les solutions envisageables pour réduire la surface d'attaque d'un système d'exploitation, on retrouve également un principe bien connu mais peu appliqué : le durcissement. Il consiste à analyser tout ce qui n'est pas ou peu utilisé sur le système, dans le but de fermer des services et des ports pour limiter les possibilités d'interaction à distance avec ce système. C'est ce principe qui a été appliqué dans la conception de nos sondes de détection de menaces.

Principe n°2 : le moindre privilège

Selon l'ANSSI, le principe du moindre privilège stipule qu'un administrateur donné n'a accès qu'à la ou les zones d'administration dont il a le juste besoin opérationnel, sans possibilité technique d'accéder à une autre zone. Dans les cas spécifiques des droits les plus privilégiés sur l'annuaire lui-même, seuls des administrateurs du SI d'administration peuvent en disposer.

Ce principe est indissociable de la sécurité by-design. Une répartition claire des tâche, rôles et droits attribués c'est garantir le cloisonnement d'un environnement. Une fois le principe du moindre privilège mis en place, la compromission d'une sous-partie de l'environnement devient plus difficile car sa surface d'attaque est fortement réduite. Une corruption n'aura dans ce cas-là que des conséquences limitées. L'application de ce principe dès la conception va de pair avec l'idée de séparation des rôles.



Opérateur : consultation des alertes, recherche IOC, forensics.

Administrateur système : création des rôles, gestion des droits, configuration des sondes et gestion des appliances.

Administrateur local : consultation des alertes et des logs système, activation/désactivation des remontées d'informations.

Auditeur : consultation des alertes, consultation des logs des sondes.

Principe n°3 : la défense en profondeur

Dans cette même logique, nous retrouvons le principe de défense en profondeur ou « defense in depth ». Terme emprunté à une technique militaire destinée à retarder l'ennemi, la défense en profondeur consiste à exploiter plusieurs techniques de sécurité afin de réduire le risque lorsqu'un composant est compromis ou défaillant. L'idée est d'opposer aux menaces des lignes de défense coordonnées et indépendantes afin de faire reposer la sécurité sur un ensemble cohérent et non sur un élément. En tant que « barrière », un produit de sécurité doit être surveillé, protégé et bénéficier de plan de réaction en cas d'incident. Pour mettre en place cette défense en profondeur, les étapes recommandées sont les suivantes :

 Détermination des objectifs de sécurité pour construire la stratégie de défense en profondeur,

 Élaboration de l'organisation et de l'architecture générale du système pour définir les points de contrôle et d'évaluation,

 Élaboration de la politique de défense,

 Qualification du système au regard des critères de défense en profondeur,

 Évaluation de la défense permanente et périodique à partir des méthodes d'attaques et du retour d'expérience (contrôle et audit).

Bien sûr, l'application seule de ces trois grands principes dans la conception d'une application, d'un système, d'un objet connecté ou d'un logiciel, ne saurait garantir son imperméabilité aux attaques et aux intrusions.

La démarche de la sécurité by-design doit être étendue au-delà de la phase de conception, elle doit être prise en compte tout au long du cycle de vie du produit et doit être l'affaire de tous les acteurs du développement produit.