Un article sur les concepts élémentaires en sécurité de l'information

Daniel Miessler
daniel(at)dmiessler.com

Publié par :

Philippe Latu
philippe.latu(at)inetdoc.net

https://www.inetdoc.net

Résumé

Cet article est une traduction libre d'une page publiée sur le blog de Daniel Miessler. Il présente les concepts de base en sécurité de l'information de façon succincte et imagée. C'est une excellente introduction au vocabulaire usuel de ce domaine sensible des technologies de l'information.

Table des matières

1. Meta-information

Copyright et Licence

Outils de publication

Cet article est écrit avec DocBook XML sur un système Debian GNU/Linux. Il est disponible en version imprimable au format PDF : `infosecconcepts.pdf`.

2. Un article sur les concepts élémentaires en Sécurité de l'Information

Le domaine de la sécurité de l'information est si vaste qu'il est facile de s'enfermer dans un secteur spécifique et de perdre ainsi la perspective générale. Ce domaine couvre tout ; de la hauteur de la clôture autour de l'entreprise jusqu'aux méthodes et outils pour durcir un système Windows server.

Il est important de se rappeler qu'il ne faut pas se laisser absorber par les détails. Chaque document sur les «bonnes pratiques» est lié directement à un concept de sécurité de plus haut niveau philosophique. Ce sont ces concepts que j'ai l'intention de présenter ici.

2.1. Les 4 principes de base en sécurité selon Eric Cole

Pour commencer, je voudrais couvrir les quatre principes de base en sécurité d'Eric Cole. Ces quatre concepts devraient constamment être à l'esprit de tous les professionnels de la sécurité de l'information.

Connaissez Votre Système

La connaissance de son système est probablement la chose la plus importante lorsque l'on essaie de le défendre. Peu importe qu'il s'agisse d'un château ou d'un serveur Linux ; si vous ne connaissez pas réellement les entrées et les sorties de ce que vous défendez, vous avez peu de chances de succès.

La connaissance exacte des logiciels exécutés sur vos systèmes est un bon exemple dans le monde de la sécurité de l'information. Quels sont les démons actifs ? Quel genre d'exposition engendrent-ils ? Un bon auto-test pour quelqu'un travaillant dans un environnement de taille moyenne serait de choisir aléatoirement une adresse IP dans la liste des systèmes et de voir si il connaît la liste exacte des ports qui sont ouverts sur les machines.

Un bon administrateur système devrait être capable de dire, par exemple, «c'est un serveur Web, donc il fonctionne seulement avec les ports 80, 443 et 22 pour l'administration à distance ; voilà.» ; et ainsi de suite pour chaque type de serveur dans l'environnement. Il ne devrait pas y avoir de surprises en examinant les résultats des scans de ports.

Ce que l'on ne veut pas entendre dans ce genre de test c'est : «Waouh, qu'est-ce que c'est que ce port ?». Avoir à se poser la question est un signe que l'administrateur n'est pas entièrement au courant de tout ce qui fonctionne sur la machine en question et c'est précisément la situation que l'on doit éviter.

Moindre privilège

Le concept suivant super important est celui du moindre privilège. Il indique simplement que les utilisateurs et les éléments du système d'information devraient pouvoir accéder seulement à ce dont ils ont besoin pour effectuer leurs tâches, et rien d'autre. La raison pour laquelle j'inclus les «éléments» c'est que les administrateurs configurent souvent des tâches automatisées qui ont besoin de pouvoir faire certaines choses : des sauvegardes par exemple. Et bien, ce qui se produit souvent c'est que les administrateurs se contentent de placer l'utilisateur qui effectue les opérations de sauvegarde dans le groupe d'administration du domaine ; même si ils pourraient faire fonctionner le service d'une autre manière. Pourquoi ? Parce que c'est plus facile.

Finalement c'est un principe conçu pour entrer directement en conflit avec la nature humaine, c'est-à-dire la paresse. Il est toujours plus difficile de donner un accès granulaire qui permet seulement d'effectuer des tâches spécifiques que de donner accès à un échelon plus élevé qui inclut les besoins à satisfaire.

Cette règle du moindre privilège nous rappelle simplement de ne pas céder à la tentation et d'agir de cette façon. Il ne faut jamais céder et prendre le temps de rendre tout accès granulaire, au niveau le plus bas possible.

Défense en profondeur

La défense en profondeur est peut-être le concept le moins bien compris des quatre. Beaucoup pensent qu'il s'agit d'empiler trois pare-feux au lieu d'un, ou d'employer deux programmes d'antivirus plutôt qu'un. Techniquement c'est réalisable, mais ça ne correspond pas à la vraie nature de la défense en profondeur.

La véritable idée est d'empiler des couches de protection multiples entre un attaquant et des biens. Et ces couches n'ont pas besoin d'être des produits ; elles peuvent être l'application d'autres concepts, tel que le moindre privilège.

Prenons l'exemple d'un attaquant sur l'Internet qui essaie de compromettre un serveur web dans la DMZ. Ce pourrait être relativement facile en présence d'une vulnérabilité importante dans le système. Mais, avec une infrastructure construite en utilisant la défense en profondeur, ça peut être beaucoup plus difficile.

Qu'il s'agisse du durcissement des routeurs et des pare-feux, de l'introduction d'IPS/IDS, du durcissement du serveur cible, de la présence d'un IPS hôte sur le serveur, de l'antivirus sur le serveur, etc. ; une seule de ces étapes peut suffire à empêcher le succès complet d'une attaque.

L'idée, c'est que nous devrions penser à l'envers ; plutôt que de penser à ce qui doit être mis en place pour arrêter une attaque, il faut justement penser à tout ce qui doit se passer pour qu'elle soit réussie. Il faut donc envisager qu'une attaque doive passer par le routeur externe, le pare-feu, le commutateur, accéder au serveur, exécuter ceci, établir une connexion sortante vers un hôte extérieur, télécharger du contenu, exécuter cela, etc., etc.

Et si l'une de ces étapes échouait ? C'est la clef à la défense en profondeur ; placer des barrières sur autant de points que possible. Verrouiller les listes de contrôle d'accès (ACLs) du réseau. Verrouiller les accès aux fichiers. Utiliser la prévention d'intrusion réseau, utiliser la détection d'intrusion, rendre l'exécution de code hostile plus difficile sur les systèmes, s'assurer que les démons sont exécutés avec les moindres privilèges utilisateur, etc., etc.

Le bénéfice de cette démarche est simple à comprendre : vous avez plus de chances d'empêcher qu'une attaque soit couronnée de succès. Il est possible que quelqu'un parvienne à passer, à accéder à la machine en question, et soit arrêté par le fait que le code malveillant en question ne soit pas exécutable sur le serveur. Et même si ce code malveillant a été corrigé de sorte qu'il fonctionne, il sera alors bloqué par un IPS mis à jour ou un contrôle d'accès (ACL) plus restrictif sur un pare-feu. L'idée est de verrouiller tout ce que l'on peut à chaque niveau. Pas simplement un élément, l'ensemble : les permissions sur les systèmes de fichiers, les protections d'accès sur les piles mémoire des systèmes, les ACLs, l'IPS hôte, la limitation des accès d'administration, l'exécution avec des droits limités. La liste continue indéfiniment.

Le concept fondamental est simple : ne pas compter sur des solutions uniques pour défendre les biens à protéger. Traiter chaque élément de défense comme si c'était la seule couche disponible. Lorsque l'on adopte cette approche on est plus à même de bloquer les attaques avant qu'elles n'atteignent leur but.

La prévention est idéale, mais la détection est une obligation

Le concept final est plutôt simple à énoncer mais extrêmement important. L'idée est que même s'il vaut mieux qu'une attaque soit stoppée avant qu'elle ait atteint son but, il est absolument crucial de savoir au moins ce qui s'est produit. À titre d'exemple, ont peut avoir des protections en place qui essaient d'empêcher l'exécution de code malveillant sur le système, mais si un code de ce type est exécuté et que quelque chose est fait, il est indispensable d'être alerté et de pouvoir réagir rapidement.

La différence entre apprendre qu'une attaque est réussie dans un délai de 5 ou 10 minutes et le découvrir des semaines est plus tard est astronomique. Souvent, avoir connaissance assez tôt d'une attaque peut entraîner son échec. Même si des attaquants obtiennent un accès sur la machine et ajoutent un compte utilisateur, il doit être possible de placer rapidement cette machine hors-ligne avant qu'ils ne puissent faire n'importe quoi avec.

Quel que soit le contexte, la détection est un devoir absolu parce que les démarches préventives n'ont aucune garantie de succès à 100%.

2.2. La triade CIA (aka. CIA Triad)

La triade de CIA est un acronyme très important dans le domaine de la sécurité de l'information. Il correspond à : confidentialité (Confidentiality), intégrité (Integrity) et disponibilité (Availability). Ce sont les trois éléments que tout professionnel essaie de protéger. Examinons les brièvement.

Confidentialité, Confidentiality

> La protection de la confidentialité consiste à préserver des informations secrètes. Ces informations peuvent aller de la propriété intellectuelle d'une société à la collection photo personnelle d'un utilisateur. Tout ce qui attaque la capacité de chacun à préserver ce qu'il veut garder secret est une attaque contre la confidentialité.

Intégrité, Integrity

> L'intégrité consiste à s'assurer que les informations n'ont pas été modifiées relativement à leur forme authentique. Les attaques contre l'intégrité sont celles qui essaient de modifier une information en vue d'une utilisation ultérieure. Des modifications de prix dans une base de données commerciale ou la modification du niveau de paie de quelqu'un sur une feuille de calcul de tableur sont des exemples de ce type d'attaque.

Disponibilité, Availability

> La disponibilité est un élément tout à fait critique du puzzle CIA. Comme on peut s'y attendre, les attaques contre la disponibilité sont celles qui font que la victime ne peut plus accéder à une ressource particulière. L'exemple le plus célèbre de ce type d'attaque est le déni de service (Denial of Service ou DoS). Le principe, c'est qu'avec ce type d'attaque rien n'est volé ni modifié. L'attaquant vous empêche d'accéder à tous les services visés. Les ressources attaquées peuvent être un serveur isolé ou bien même un réseau entier dans le cas des attaques basées sur la bande passante (Distributed Denial of Service ou DDoS).

Il est assez pratique de classer selon les termes de la triade CIA les attaques contre la sécurité de l'information et les défenses correspondantes. Considérons quelques techniques communes employées par les attaquants : la capture de trafic (sniffing), le reformatage de disques durs et les modifications sur un système de fichiers.

La capture de trafic est une attaque sur la confidentialité parce qu'elle permet d'analyser des informations qui ne sont pas censées être visibles. Un attaquant qui reformate le disque dur d'une victime a attaqué la disponibilité de son système. Enfin, quelqu'un qui a édité et modifié le système de fichiers a compromis l'intégrité de ce système. Penser en ces termes peut nous aider à progresser et comprendre les diverses techniques offensives et défensives.

2.3. La terminologie

Maintenant je voudrais revoir quelques termes techniques extrêmement importants. Les explications peuvent devenir un peu «académiques» mais je vais faire de mon mieux pour aller à l'essentiel.

Vulnérabilité, Vulnerability

> Une vulnérabilité est une faiblesse dans un système. C'est assez simple à comprendre parce que l'on emploie généralement ce terme exact dans les avis (advisories) et même dans les médias. Comme exemple, on trouve l'avis LSASS CVE-2004-0894 qui permet à un attaquant de prendre le contrôle des systèmes à distance. Quand on applique un correctif (patch) à un système, on le fait pour supprimer une vulnérabilité.

Menace, Threat

> Une menace est un événement, naturel ou artificiel, qui peut endommager un système. Les types de menaces comprennent les gens qui essaient de pénétrer dans un réseau pour voler des informations, les feux, les tornades, les inondations, l'ingénierie sociale, les salariés malveillants, etc. Tout ce qui peut endommager les systèmes est essentiellement une menace pour ces systèmes. Souvenons nous aussi qu'une menace est habituellement évaluée comme une probabilité, ou une chance, que cet événement puisse survenir. Comme exemple, on pourrait prendre la menace d'utilisation de code malveillant contre une vulnérabilité particulière. S'il n'existe aucun code malveillant connu dans la nature le niveau de cette menace est assez bas. Mais si un nouveau code malveillant apparaît en force dans les listes de diffusion majeures, le niveau de la menace augmente significativement.

Risque, Risk

Le risque est peut-être la plus importante de toutes ces définitions puisque la mission principale des responsables de la sécurité de l'information est de gérer ce risque. L'explication la plus simple que j'ai entendue est que le risque est la chance de quelque chose de mauvais arrive. C'est un peu trop simpliste et je pense que la meilleure façon d'expliquer ce terme est d'utiliser deux ou trois formules :

```
Risk = Threat x Vulnerability
```

La multiplication est utilisée ici pour une raison très spécifique. Dès que l'un des deux termes vaut zéro, le résultat devient nul. Autrement dit, il n'y a aucun risque s'il n'y a pas de menace ou de vulnérabilité.

À titre d'exemple, si notre serveur Linux est totalement vulnérable selon la publication de l'avis CVE-XYZ mais qu'il n'existe aucun moyen d'exploiter la vulnérabilité, alors le risque devient nul. De même, s'il existe quantité de façons d'exploiter une vulnérabilité et que nous avons déjà appliqué le correctif (nous ne sommes donc plus vulnérable), nous n'encourrons de nouveau aucun risque.

Une formule plus élaborée inclut l'impact, ou le coût, à l'équation (littéralement) :

```
Risk = Threat x Vulnerability x Cost
```

Ce facteur permet à un décideur d'affecter une valeur quantitative au problème. Ce n'est pas toujours une science exacte, mais si nous savons qu'un vol de propriété intellectuelle vitale pour votre société nous coûterait 4 milliards de $, alors c'est une bonne information à considérer pour traiter le risque.

Cette dernière partie est importante. L'objectif global de l'affectation d'une valeur au risque est que les responsables puissent prendre les décisions sur ce qui doit être traité ou pas. S'il existe un risque associé à l'hébergement de certaines données sur un serveur FTP public, mais que ce risque n'est pas assez sérieux pour dépasser les bénéfices attendus, alors c'est une bonne affaire de continuer à héberger ces données.

C'est tout l'enjeu. Les responsables chargés de la sécurité de l'information doivent en savoir assez sur les menaces et les vulnérabilités pour être capables de prendre des décisions pertinentes sur la façon de développer l'infrastructure informatique. La gestion des risques justifie pleinement le travail sur la sécurité de l'information.

Politique, Policy

Une politique de sécurité est une prise de position affirmée de la direction établissant ce qui est permis dans l'entreprise et ce qui ne l'est pas. Une politique de sécurité dira, par exemple, que vous pouvez lire votre courrier électronique personnel au travail mais que vous ne pouvez pas consulter votre banque en ligne, etc. Une politique devrait être assez large pour englober l'entreprise entière et devrait avoir l'aval de ses instances.

2.4. Réflexions personnelles

Dans cette section, je voudrais rassembler une série d'idées personnelles importantes sur la sécurité de l'information. Nombre d'entre elles ne sont pas des règles et ne sont que le reflet d'une opinion. C'est le genre d'opinion que l'on n'apprend probablement pas en classe. Heureusement, on peut considérer qu'un bon nombre de spécialistes du domaine est d'accord avec ces avis.

Le but de la Sécurité de L'information est de faire en sorte que la mission principale de l'entreprise soit remplie avec succès.
Un sentiment de frustration important émerge lorsque les professionnels de la sécurité de l'information perdent de vue ce concept clé. La sécurité de l'information n'est pas simplement là pour «faire bien». Elle doit aider l'entreprise à faire son travail. Si cette mission est de gagner de l'argent, la mission principale du groupe de sécurité, à son niveau le plus haut, est de faire que cette société gagne de l'argent. Pour le dire autrement, la raison d'être du groupe de sécurité est, en premier lieu, d'empêcher que l'entreprise perde de l'argent.

Ce n'est pas une façon très «originale» de voir les choses pour ceux qui ont un peu d'expérience dans le monde de la sécurité de l'information ; mais c'est un état d'esprit à adopter pour qui veut durer dans ce domaine. Ce phénomène devient de plus en plus important avec toutes les sociétés qui commencent à attribuer des primes aux professionnels qui voient la sécurité comme une source d'affaires plutôt que comme un exercice purement technique.

L'infrastructure informatique actuelle facilite le piratage.
Alors que la plupart des attaquants les plus qualifiés peuvent inventer (et inventent) des façons ingénieuses d'introduire des vulnérabilités dans les systèmes, la capacité nécessaire à réaliser ce que nous observons au

quotidien dans le monde de la sécurité est essentiellement basée sur une architecture terriblement défectueuse. Qu'il s'agisse de la gestion mémoire, des langages de programmation ou de la conception d'architectures de sécurité complètes ; aucun des éléments que nous utilisons aujourd'hui n'a été conçu en prenant les aspects sécurité en compte. Tous ces éléments ont été conçus par des universitaires pour des universitaires.

Pour employer une analogie, je pense que nous construisons des gratte-ciel avec du bois comme le guano ou le balsa. Les pirates franchissent régulièrement ces parois en bois et n'avons d'autre solution que de reboucher les trous et prier. Pourquoi ? Parce que nous essayons de construire des édifices hauts quelques dizaines de mètres avec des matériaux beaucoup trop fragiles. Les bois comme le balsa et le guano font d'excellentes huttes qui résistent à une tempête de pluie occasionnelle et un choc ou deux. Mais ils ne résistent pas aux tornades, aux tremblements de terre ou plus particulièrement à des hooligans avec des torches.

Pour construire tout ça, nous avons besoin d'acier. Aujourd'hui nous n'en avons pas. Nous continuons à construire en utilisant les mêmes matériaux anciens. On retrouve les mêmes problèmes de gestion mémoire qui permettent encore et encore les débordements de tampons et les mêmes problèmes de langage de programmation qui permettent d'écrire du code dangereux plus facilement que du code sécurisé. Jusqu'à ce que nous ayons de nouveaux matériaux pour construire nous subirons toujours. Il est encore trop facile de faire flamber le bois ou d'y percer un trou.

Ainsi, toute analogie mise à part, je pense que dans la prochaine décennie nous verrons l'apparition de nouveaux modèles d'architecture système ; des modèles avec des conditions d'utilisation et d'exécution fortement restrictives selon le paradigme «fermé par défaut». Nous devrions aussi voir apparaître de nouveaux langages de programmation, de nouveaux environnements de développement (IDE), de nouveaux compilateurs et de nouvelles techniques de gestion mémoire. Le tout conçu à partir de zéro pour être sûr et robuste.

Avec toutes ces nouveautés, je pense qu'à cette époque nous verrons des systèmes exposés seuls sur le réseau public pendant des années avec peu de chance de compromission. Des attaques réussies arriveront toujours, bien sûr, mais elles seront extrêmement rares comparé à aujourd'hui. Les problèmes de sécurité ne disparaîtront jamais, nous le savons tous, mais ils reviendront à des questions de conception/configuration humaine plutôt qu'à des questions de corrections de défauts technologiques.

La sécurité par l'obscurité est mauvaise, mais la sécurité avec de l'obscurité ne l'est pas.
J'ai participé à beaucoup de débats en ligne au cours des années autour du concept de Sécurité par l'Obscurité. À la base, il y a une croyance populaire qui veut que si tous les aspects de notre défense reposent sur le secret, celle-ci est nécessairement défectueuse. Ce n'est simplement pas le cas.

La confusion est basée sur le fait que les gens ont entendu dire que la sécurité par l'obscurité est mauvaise et la plupart ne comprennent pas ce que le terme signifie en réalité. En conséquence, ils font la supposition terrible que le fait de compter sur l'obscurité, même comme une couche supplémentaire au dessus d'un bon niveau de sécurité, est mauvais. C'est malheureux.

Ce que l'expression sécurité par l'obscurité décrit en réalité est un système où le secret est le seul niveau de sécurité. Cette idée vient du monde de la cryptographie où des systèmes de chiffrage faibles sont souvent mis en œuvre de telle façon que la sécurité du système dépend du secret de l'algorithme plutôt que de la clé. C'est mauvais et c'est la raison pour laquelle la sécurité par l'obscurité est connue comme une idée à éviter.

Ce que beaucoup de gens ne comprennent pas c'est que l'ajout de l'obscurité à un niveau de sécurité déjà solide n'est pas une mauvaise chose. Le projet Portknocking est un exemple caractéristique. Cet outil intéressant permet de «cacher» les démons qui sont accessibles depuis l'Internet. Le logiciel analyse les journaux d'un pare-feu et reconnaît des séquences de connexion spécifiques qui proviennent de clients de confiance. Quand l'outil reconnaît la séquence (knock) sur le pare-feu, il ouvre le port. La clé c'est qu'il ne vous ouvre pas juste un shell ; ce qui reviendrait à de la sécurité par l'obscurité. Tout ce qu'il fait à ce niveau, c'est d'ouvrir une invite de connexion SSH habituelle comme si l'étape précédente n'avait pas eu lieu. C'est donc une couche supplémentaire, et non la seule couche de sécurité.

La sécurité est un processus plutôt qu'une finalité.
C'est assez commun mais ça mérite d'être répété. Nous n'arriverons jamais à atteindre l'objectif. Il n'y a rien à faire. C'est un objectif que nous cherchons à atteindre et pour lequel nous luttons. Plus tôt on l'apprend, mieux c'est.

La complexité est l'ennemie de la sécurité.
Vous pouvez me considérer comme un excentrique, mais je pense que le concept de simplicité est une belle chose. Cela s'applique à la conception Web, la programmation, l'organisation de sa vie et oui : à la sécurité. Il est tout à fait logique que la complexité entrave la sécurité parce que la capacité de chacun à défendre son système repose sur la compréhension complète de son architecture. La complexité rend les choses plus difficiles à comprendre. J'en ai assez dit.

2.5. Conclusion

Mon espoir est que cette petite collection d'idées sur la sécurité de l'information sera utile à quelqu'un. Si vous avez des questions ou des commentaires n'hésitez pas à m'envoyer un courrier électronique à `<daniel(at)dmiessler.com>`. Je suis sûr que j'ai oublié une tonne de trucs qui auraient dû être présentés ici et j'accepterai n'importe quelle réprimande sur ces lignes.

3. Termes techniques et documents de référence

An Information Security Concepts Primer

: Article original : An Information Security Concepts Primer .

Advisories, Common Vulnerabilities and Exposures, CVE-AAAA-NNNN

: Avis annonçant une vulnérabilité informatique suivant un format défini. Voir Common Vulnerabilities and Exposures.

: L'avis LSASS CVE-2004-0894 est cité en exemple.

Déni de Service, DoS

: Rendre un service Internet indisponible. Voir Déni de service.

DMZ

: Réseau isolé entre au moins deux pare-feux. Voir Zone démilitarisée.

Gestion du risque

: Identifier les risques qui pèsent sur les actifs et les personnels d'une entreprise. Voir Gestion des risques.

Packet sniffer, renifleur, sniffeur

: Logiciel de récupération des informations transitant sur un réseau. Voir Packet sniffer.

Pare-feu, firewall

: Élément logiciel et|ou matériel ayant pour rôle de filtrer les communications entre réseaux. Voir Pare-feu.

Portknocking

: Ouverture de port à la demande en fonction de séquences de connexions définies. Voir PORT KNOCKING.

Sécurité par l'obscurité

: Ne rien divulguer sur un système pour en protéger la sécurité. Voir Sécurité par l'obscurité.