Dernière modification : 15/07/2020 12:16
Auteur : Gilles Lerat
Version : 0.2

Mise en œuvre d'une stratégie de sécurité informatique au moyen de solutions « open source »

L'augmentation significative des usages, des échanges et des technologies Internet va de pair avec une explosion des risques.
Ces risques sont potentiellement meurtriers pour l'activité de l'entreprise quelle que soit son activité. Ils concernent, sans que la liste ci-dessous soit limitative :

- Vol de données par des pirates informatiques
- Transfert d'informations par un employé indélicat
- Chiffrement des données
- Utilisation des ressources de l'entreprises à des fins malicieuses (envoi de spams, « cryptojacking »)
- Attaques par déni de service pour empêcher l'accès aux produits et services de l'entreprise

Le marché de la sécurité informatique s'est depuis longtemps structuré pour répondre à l'ensemble de ces problématiques et permettre de protéger la confidentialité et l'intégrité des données tout en assurant leur disponibilité et la traçabilité des flux d'information.
Le marché est ainsi conduit par un certain nombre de grandes sociétés en provenance principalement des Etats-Unis ou d'Israël. Les solutions purement françaises sont plutôt rares, à l'exception d'entreprises telles que Wallix, Stormshield ou Purplemet.

En parallèle, un grand nombre de solutions ouvertes (« open source ») existent, celles-ci permettent de couvrir la quasi-totalité des besoins des entreprises sur ces sujets de cybersécurité.
La notion de solution open source recouvre des logiciels qui sont le plus souvent gratuits d'utilisation et dont le code source est ouvert, c'est-à-dire qu'il est possible à tout un chacun de l'inspecter pour vérifier qu'il ne contient pas de « backdoor », c'est-à-dire du code malicieux laissé intentionnellement par les créateurs du logiciel. La recherche de vulnérabilités et donc leur correction est ainsi facilitée, voire encouragée par la recherche de « bug bounty ».

Bien qu'en matière d'open source, les entreprises soient en priorité, voire exclusivement attirées par le premier point, la gratuité, c'est en fait le côté ouvert du code qui est, dans une logique de sécurité, le plus intéressant.

Un autre aspect essentiel des projets open source est leur résilience.
Cette résilience vient tout d'abord de ce qu'un projet se compose le plus généralement d'une multitude de contributeurs, ce qui combinés à certains outils tels que Github rend les corrections de bugs et de vulnérabilité très rapides.

A cet égard, le différentiel de traitement des bugs entre le noyau (« kernel ») Linux et Windows est très parlant : les kernel Linux sont patchés très rapidement alors que les correctifs pour Windows sont parfois sujets à de longues semaines d'attentes.

Cette résilience s'exprime aussi par le fait que lorsqu'un projet périclite, il y a le plus souvent, une migration vers un nouveau projet de même type, plus prometteur. Cette migration des développeurs s'accompagne en général de procédures permettant de passer vers cette nouvelle solution. C'est ce qui a été observé en particulier lors de l'arrivée de la solution NextCloud, en remplacement d'OwnCloud.

Dans ce papier, nous examinerons un ensemble de solutions « open source » permettant de constituer une stratégie presque exhaustive de cybersécurité.

Bien entendu, le fait que la solution en elle-même soit gratuite ne signifie pas que le coût total d'acquisition soit négligeable. La complexité d'intégration et d'administration rentre en jeu et peut alourdir significativement le budget.

La contrepartie d'une solution open source est, en règle générale, une implication étendue de la part des équipes informatiques pour comprendre le produit, l'intégrer, le paramétrer et l'exploiter au quotidien. Le modèle d'affaires des éditeurs de solutions open source repose d'ailleurs sur une assistance à destination des entreprises qui ne disposent pas du temps et/ou des compétences nécessaires pour l'exploitation des solutions qu'elles retiennent.

Malgré toute la complexité réelle ou apparente, les solutions de sécurité open source sont un véritable atout au niveau des entreprises.
Il serait dommage pour les TPEs et les PMEs françaises de se priver de leur exploitation.
Au regard des solutions commerciales, les gains financiers sont parfois spectaculaires. En période de difficulté économique, c'est un avantage concurrentiel certain.

La liste présentée ci-dessous, bien que non exhaustive, a le mérite de couvrir un large rayon d'action des solutions de cybersécurité :

- Gestion des mots de passe
- Authentification et authentification forte (MFA – Multi Factor Authentication)
- Accès distant (par réseau privé virtuel de type IPSEC, RDP, SSH, etc.)
- Pare feu applicatif (WAF)
- Système de détection et de prévention d'intrusion (IDS/IPS)
- Supervision des infrastructures
- Collecteur et analyseur de logs (SIEM – Security Information and Event Management)
- Prise en main à distance

La gestion des mots de passe

Les mots de passe sont la première et souvent l'unique barrière qui permet de sécuriser l'accès aux données.
Une majorité des infractions à distance impliquent un vol de mots de passe.
L'utilisation d'un gestionnaire de mot de passe est souvent un préalable indispensable.
Dès lors que les mots de passe doivent être partagés, pour gérer les différents accès aux équipements ainsi qu'aux applications, ou pour gérer le cycle de vie, une mise en œuvre globale doit être implémentée.
Par ailleurs, il est souvent indispensable de gérer la force des mots de passe, de rappeler aux utilisateurs le besoin de les changer à intervalles réguliers. Pour ce faire, des gestionnaires de mots de passe collaboratif existent.
Il est en particulier, important de pouvoir vérifier la force des mots de passe. L'API HaveIbeenPwnd permet de vérifier les mots de passe qui ont été compromis suite à des fuites de donnée, le plus souvent accessible sur « le Dark Web ».
Parmi les solutions de gestionnaires de mots de passe collaboratifs, deux produits se distinguent : Psono et Bitwarden. Tous les deux sont gratuits et open source.

L'authentification forte.

Aujourd'hui, l'utilisation d'un mot de passe ne suffit pas à sécuriser un accès sensible. Dans ce cas de figure, on utilise en complément une autre méthode basée sur un « token » logiciel ou matériel (ce que l'on a) ou bien une authentification biométrique (ce que l'on est). On parle d'une authentification à facteurs multiples (en anglais Multiple Factor Authentication ou bien MFA).

Une autre problématique de l'authentification est en rapport avec le confort d'usage : si l'utilisateur doit s'authentifier sur trois applications distinctes de l'entreprise avec à chaque fois, deux ou trois facteurs, cela devient rapidement contraignant. C'est là qu'interviennent les solutions de Single Sign On (SSO) et Single Log Out (SLO).
Ces solutions permettent de ne s'authentifier qu'une seule fois : l'approbation ainsi obtenue est transférée aux autres services afin de ne pas être obligé de renouveler systématiquement la procédure d'authentification.
A titre d'exemple, on peut citer les sites qui permettent de s'authentifier via un compte de réseau social ou de messagerie (tel que Twitter, Google, Facebook). L'authentification fédérative sur l'un de ces services donne l'accès aux autres.
Plusieurs solutions open source permettent de mettre en place de tels mécanismes. Citons en particulier : PrivacyIDEA, KeyCloak, SimpleSAMLphp.

L'accès distant

Les problématiques d'accès distant regroupent plusieurs protocoles et méthodes d'accès : IPSEC, RDP, SSH, etc..

La crise du COVID a montré de manière éclatante le besoin d'un accès distant et donc d'un accès sécurisé aux ressources informatiques de l'entreprise.
Les protocoles natifs, telles que RDP et SSH montrent rapidement leurs limites.

L'une des solutions est de mettre en place des plateformes assurant un relais sécurisé sur les serveurs internes : on parle alors de bastions.
Une autre solution, fréquemment utilisée, consiste à mettre en place des tunnels VPN de type IPSEC. L'établissement du tunnel permet d'offrir une adresse IP locale aux utilisateurs distants et leur donne plus de flexibilité pour lancer un grand nombre d'applications.

A l'instar de Google qui a lancé la solution BeyondCorp, utilisant le modèle Zero Trust, il est désormais possible d'accéder aux services à distance, en utilisant uniquement un navigateur Web.

Là encore, les entreprises ont l'embarras du choix quant aux produits open source à déployer : OpenVPN et Nginx en premier lieu, mais également Pritunl, Pritunl Zero et Apache Guacamole.

Les pare-feux applicatifs (Web Application Firewall)

Les solutions vues précédemment mettent souvent en œuvre une interface Web, en particulier pour des besoins d'administrations. Dans ce cas de figure, il est alors nécessaire soit de restreindre très fortement l'accès à cette interface, soit de la protéger contre les vulnérabilités de type 0 Day, c'est-à-dire celles pour lesquelles n'existe aucun patch correctif.
La protection implique, le plus souvent, la mise en place d'une solution de type WAF (Web Application Firewall) qui permet de se protéger contre différents types d'attaques : injection SQL, cross site scripting (XSS),…
Parmi la myriade de solutions open source dédiées à ce segment de marché, trois se détachent spécifiquement : ModSecurity (pour Apache), NAXSI (pour Nginx) et WebKnight (pour IIS).

Les systèmes de détection et de prévention d'intrusion (IPS)

En complément des méthodes décrites, il est conseillé de mettre en place des solutions de détection voire de prévention des intrusions (IDS et IPS). Lorsque ces solutions sont installées sur les postes de travail, on parle de HIDS (Host Intrusion Detection Systems) ou plus récemment EDR (Endpoint Detection and Response) pour détecter les intrusions au niveau du poste de travail.
Au niveau du réseau, on parle de NIDS (Network Intrusion Detection System) voire tout simplement d'IDS.
Ces solutions collectent et analysent des informations à l'aide d'outils de « big data » afin de détecter et d'empêcher une intrusion qui pourrait conduire à une compromission système ou applicative.

Parmi les solutions les plus réputées sur ce segment de marché, on peut citer : Snort, Suricata, Wazuh, Fail2ban.

Supervision des infrastructures

L'augmentation des systèmes de sécurité rend nécessaire la supervision des serveurs et des applications.
Plusieurs protocoles sont utilisés pour effectuer cette supervision en temps réel. Le plus fréquemment utilisé est SNMP, mais d'autres protocoles sont possibles, notamment SSH.
La supervision est l'un des domaines dans lesquels les solutions open source sont très répandues. On pense naturellement à Nagios. En complément de cette solution, Grafana est souvent utilisé pour produire des tableaux de bords visuels personnalisés et adaptés à chaque infrastructure.
Les bases de données traditionnelles n'étant pas très bien adaptées, on va plutôt mettre en œuvre le système de gestion de base de données InfluxDB.
D'autres solutions intéressantes sont disponibles sur ce marché qui en regorge : Cacti et EyesOfNetwork (distribution basée sur CentOS et regroupant Nagios, Cacti, GLPI, OCS, Grafana, InfluxDB, etc..)

Collecteur et analyseur de logs

L'utilisation de l'ensemble des solutions décrites ci-dessus nécessite de centraliser l'ensemble des logs afin d'avoir une vue d'ensemble et de pouvoir les corréler pour en tirer des alertes pertinentes.
De nos jours, le standard largement utilisé est le protocole Syslog que soit pour le système de stockage ou bien les échanges entre les périphériques émettant des logs et le collecteur central.
Pour répondre à ce besoin, nous pensons immédiatement à la "stack" ELK (Elasticsearch, Logstash et Kibana), Elasticsearch va stocker et indexer les logs, Logstash va avoir la fonction de serveur chargé d'effectuer les échanges avec les différents périphériques qui envoient des logs et Kibana permet de créer des tableaux de bord afin de mette en forme et visualiser des statistiques pertinentes.
Une autre solution intéressante dans ce domaine est nommée Graylog, elle utilise aussi Elasticsearch, mais aussi MongoDB. Le choix d'entre ELK et Graylog diffère en fonction des besoins, mais en règle générale, ELK est plus adaptée aux petites équipes alors que Graylog est lui plus adapté aux équipes nombreuses avec un système d'authentification des utilisateurs et une meilleure gestion des alertes pour agir rapidement.

Prise en main à distance

Toutes les équipes informatiques ont déjà été confrontées aux problématiques de prise en main à distance sur le poste d'un utilisateur qui fait face à un problème.
Dans la pratique, nous constatons l'utilisation de logiciels commerciaux comme TeamViewer, Anydesk et bien d'autre.
Une solution open source, disposant de fonctionnalités équivalentes existe : MeshCentral.
MeshCentral propose une interface web permettant aux administrateurs de gérer les postes connectés par le biais d'un agent. Cet agent est compatible avec tous les systèmes Windows, Unix et MacOS. Un système d'invitation par lien ou par email permet de demander à un collaborateur de télécharger puis installer l'agent afin de prendre la main à distance, naviguer dans le système de fichier et même avoir

un accès en ligne de commande. Pour finir, MeshCentral offre la possibilité de discuter via un onglet de navigateur.
Pour une équipe qui souhaiterait contrôler son parc à l'aide de MeshCentral, il est très facile de déployer l'agent par GPO.

Signature électronique

Le souci croissant pour les problématiques en rapport avec l'écologie ont mis au goût du jour les solutions de signature numérique.

Pour que de telles solutions deviennent contractuelles, il est nécessaire d'une part de faire évoluer l'environnement législatif et d'autre part, de mettre en place des mécanismes techniques permettant d'assurer le même niveau de protection qu'avec une signature manuscrite.
Pour cela, on utilise la cryptographie, notamment des algorithmes de chiffrement de type asymétrique (avec une paire de clés publiques / privées) et de signature numérique (qui génèrent un « hash » ou condensat). Ces algorithmes permettent d'authentifier la personne signataire d'un document et partant d'en assurer la non-répudiation. Ils garantissent également l'intégrité du document.

Une solution open source permettant de mettre en place ce genre de procédé existe : il s'agit de SignServer.
Elle respecte tous les standards de signature électronique de document (PDF, XML, etc.), de code (Authentification MS, Java incluant les APK), l'horodatage (RFC3161, ETSI, etc.) et ePassport, en assurant la conformité avec les spécifications de l'OACI.
Une fois déployé, SignServer propose une interface pour que les administrateurs puissent configurer la solution (ajout d'utilisateur, configuration des clés, etc.) ainsi qu'une seconde interface pour assurer l'enrôlement des utilisateurs.
A l'issue de cette seconde étape, ces derniers pourront signer et vérifier la signature des documents qui leur auront été transmis.

Plateforme de gestion de tickets

Nous avons vu précédemment qu'il est souvent nécessaire de prendre la main à distance sur le poste d'un collaborateur. Toutefois au préalable, celui-ci a sollicité votre aide par un biais quelconque.

Pour cela, la plupart des entreprises ont recours à des solutions de gestion des tickets (des demandes, des remontées de bug, etc.). Il en existe de très nombreuses sur le marché.
Après avoir étudié les différentes solutions open source disponibles, Secureware a retenu la solution Zammad pour gérer sa plateforme de support. En effet, Zammad est une solution facile à déployer et à maintenir dans le temps, et son atout majeur est une interface graphique épurée et intuitive.
De nombreuses fonctionnalités sont mises à disposition : il est ainsi possible d'ouvrir des tickets via l'interface web, par email, par un chat disponible sur le Web par exemple, ou encore sur plusieurs réseaux sociaux.

Différents groupes prédéfinis permettent de gérer les administrateurs, les agents qui travaillent sur les tickets et les utilisateurs qui effectuent des demandes. Le système de « macros » permet de personnaliser le fonctionnement très efficacement.

Une autre solution intéressante est Request Tracker (RT). Ses fonctionnalités sont beaucoup plus étendues que celles de Zammad, car cela va de la gestion projet, à la démarche qualité en passant par la gestion des relations clients. RT est presque un ERP ; en particulier cette solution permet de respecter la norme ISO20000 à travers la mise en place d'une démarche ITIL.

Conclusion

L'open source est un modèle commercial rentable, qui a fait ses preuves à maintes reprises. Le rachat de Red Hat par IBM pour près de 34 milliards de dollars en est une preuve éclatante : Red Hat a été l'un des premiers grands fournisseurs IT à s'investir dans l'open source.

Les solutions Open Source n'ont donc plus à rougir devant les solutions propriétaires et représentent une alternative souvent séduisante. Compte tenu des contraintes, il est toutefois essentiel d'être conseillé par un expert qui maîtrise le sujet, afin de peser les avantages et les inconvénients en fonction des besoins, des contraintes et des ressources.