Gestion du patrimoine informatique - Gemalto

Lors de mon stage chez Gemalto, j'ai été capable d'observer la gestion du patrimoine informatique au sein d'une entreprise de taille importante. Avant de commencer, penchons nous sur ce qu'est la gestion du patrimoine informatique. Le terme "parc informatique" désigne ici le matériel informatique physique de l'entreprise, mais aussi les actifs logiciels et réseaux. Une gestion de parc informatique consiste donc à répertorier et localiser le contenu du parc informatique, afin de gérer son évolution dans le temps, son bon fonctionnement, et de répondre au plus vite aux potentiels incidents ou problèmes. La gestion du parc informatique désigne aussi la gestion des documentations produites, des sauvegardes et de la formations des utilisateurs.

Puisque au sein de la société Gemalto, le nombre de serveurs en production avoisine les 400 machines, et puisque de très nombreux postes utilisateurs sont déployés dans tous les services, un outil de centralisation des informations a été nécessaire. Cet outil open-source se nomme "iTop". C'est une CMDB, ou en français une base de données de gestion de configuration. Le principe d'une CMDB est de centraliser l'ensemble des actifs informatiques d'une entreprise. Celui-ci se présente sous la forme d'un moteur de recherche interne, dans lequel il est possible de chercher le nom d'une machine ou une IP. Lorsque l'on accède aux informations d'une machines dans la base de données, il est possible d'accéder à son emplacement physique, à ses différentes adresses, à son système d'exploitation, à son emplacement dans la topologie réseau, à la documentation relatives aux services ou à la machine, etc … Les serveurs sont répertoriés, ainsi que les éléments d'interconnexions (routeurs, commutateurs, firewall), les postes clients, etc … Cette CMDB a été implémentée en suivant les normes ITIL. Cette solution est accessible en fonction des autorisations des utilisateurs dans l'AD. Ainsi, certains utilisateurs ne seront capables que de lire les informations, là où d'autres peuvent uploader, et ou d'autres encore peuvent remplacer et supprimer des informations. Cette solution est très pratique au quotidien, puisqu'elle sert de point centrales pour toutes les informations réseaux, mais aussi pour les documentations et les services. En revanche, une solution de la sorte nécessite d'être continuellement mise à jour manuellement, ce qui demande un temps de travail non considérable.

Puisque Gemalto est un acteur de la sécurité numérique, d'autres normes et certifications sont requises pour ne pas rompre certains contrats avec des clients. La norme PCI DSS est ici obligatoire pour que Gemalto puisse assurer des services au monde bancaires. Cette norme est celle de la sécurité de l'industrie des cartes de paiements pour les principaux groupes tels que Visa ou MasterCard (*Payment Card Industry Data Security Standard*). Celle-ci impose la présence de certains éléments

de sécurité au sein de l'architecture de l'entreprise, de certaines méthodes afin d'archiver les actions utilisateurs, et de procédure des plus sécurisées.
Toujours relatif à la sécurité, la norme internationale ISO 27001 (*Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences)* impose d'autres contraintes sécuritaires à Gemalto. La norme ISO 27001 est en effet composée de plusieurs points distincts. Le but de cette norme est de garantir la protection des actifs de l'organisation, en passant par une évaluation des risques, la mise en place de règles strictes de sécurités, une organisation de la sécurité de l'information, une gestion des actifs, une protection des ressources humaines, la mise en place de sécurités physiques, de protocoles de communications sécurisé, un contrôle des accès poussé. Le déploiement d'un système d'acquisition de données sur les systèmes d'informations et également de rigueur, tout comme la présence d'un management des incidents de sécurité, de continuité de service et de mise en conformité.

Puisque les serveurs de production de Gemalto hébergent directement des applications clientes, ou puisqu'ils participent à une architecture plus global, en authentifiant des flux par exemple, une attention toute particulière est attribuée à la gestion d'incident. En effet, une équipe de permanents est mobilisée 24h/24 afin de résoudre les différents incidents pouvant survenir sur les serveurs. Des procédures leurs sont fournies pour résoudre les problèmes le plus rapidement possible. D'un point de vue technique, une console de supervision générale affiche les alertes de sécurité et les différentes erreurs et problèmes rencontrés sur les machines sensibles. La remontée d'information se fait via via un utilitaire HP dénommé "Operation Manager", qui, couplé à un SIEM (*Security Information and Event Management*) et à diverses sondes autonomes, est capable de superviser l'ensemble des serveurs, que ce soit sur la couche physique, réseau, ou applicative.

La mise à jour des logiciels sur les postes clients se fait de manière centralisée, via un outil de déploiement de logiciels. Les utilisateurs n'ont donc pas la main sur l'ensemble des logiciels installés sur la machine, mais uniquement sur un catalogue d'applications approuvées en interne. Les utilisateurs peuvent donc télécharger certains logiciels à la demande. Les mises à jour applicatives sont déployées de la même manière, au redémarrage des postes.
Sur les serveurs de productions, une équipe est chargée d'analyser les mises à jours, de les tester sur un environnement de laboratoire, d'observer les conséquences de tels mises à jours, avant de les déployer pendant les périodes creuses (donc typiquement dans la nuit du samedi soir). A titre d'exemple, lorsque j'étais en stage, l'équipe chargée d'analyser l'impact des mises à jours travaillait sur les patchs pour les vulnérabilités Spectre et Meltdown. Après plusieurs tests, ils se sont rendu comptes que les mises à jour officielles n'étaient pas stables, et que le déploiement de ces dernières risquerait de causer des instabilités sur les services de

productions. Cette étape de réflexion est réalisée pour tous les déploiements de mises à jours en environnement de production.

Les utilisateurs disposent tous d'un temps de formation annuel pour participer à des séminaires techniques. En parallèle, Gemalto propose des conférences accessibles par tous les employés, via internet, sur des sujets techniques divers et variés. J'ai pu observer qu'une grosse majorité des employés du pôle informatique écoutaient régulièrement ces conférences sur leur temps de travail.

Au niveau de la veille technologique, j'ai pu observer une personne dont la fonction était chargée d'effectuer les recherches sur des nouvelles technologies. Celui-ci avait donc un environnement de test à sa disposition, sur lequel il devait produire des PoC (*Proof of Concept*) de nouvelles technologies à jauger, et potentiellement à déployer sur l'environnement de production du site.