RAPPORT DE PRESOUTENANCE DE

NKAN MASSOM Calvin Rodrigue

2e année Master SIGL

Dans la perspective de l’obtention d’un master en Système d’Information et Génie Logiciel, NKAN MASSOM Calvin Rodrigue a réalisé un projet sous le thème de

« Audit et optimisation de la sécurisation d’un SaaS ».

L’objectif est de réaliser d’optimiser la réalisation d’audit de sécurité d’application SaaS le logiciel afin qu’il puisse permettre à une entreprise de réaliser des applications de type Software As A Service de manière aussi sécurisée et fiable que possible et ainsi avoir un impact croissant sur le chiffre d’affaire.

Ce mémoire est divisé en plusieurs parties dans les grandes lignes à savoir, une introduction générale, 4 chapitres répandus, une conclusion générale et quelques références. Le premier chapitre sera consacré à l’étude de l’art, le second sur la présentation du projet, le troisième sur l’analyse et conception du système et le dernier sur la réalisation proprement dite.

En effet, la sécurité est un état d’esprit confiant et tranquille d’une personne qui se croit ou se sent à l’abri du danger; ce qui signifie qu’elle dépend de la personne qui ressent cela, du contexte dans lequel elle se trouve, du type de menaces qu’il peut avoir, et bien d’autre encore. Autrement dit, la sécurité dépend de tout un écosystème et donc il n’y a pas véritablement de sécurité, encore moins de cybersécurité, ce qui complique assez le problème.

Selon *Le Petit Larousse,* <<un produit représente chacun des articles, objets, biens, ou services proposes sur le marché par une entreprise>>. Aujourd’hui, lorsqu’une entreprise réalise un produit a commercialiser, il peut s’agir :

* D’un produit embarque,
* D’un sous-système,
* D’une solution,
* D’un logiciel ou suite de logiciel.

L’idée étant de les fournir à l’utilisateur, pour une utilisation dans un contexte propre a lui. Donc l’entreprise réalise un produit, pensant comprendre de quelle manière le client va s’en servir, d’autant plus que c’est son domaine. Ce qui est vrai dans un contexte fonctionnel, dans la mesure où le produit répond a un besoin du client.

Aussi dans le domaine de la cybersécurité, c’est le contexte d’utilisation qui dimensionne le type de risque et d’exposition dont le client peut être victime. Faisant ainsi de la sécurisation des produits un domaine à prendre en compte.

En matière de cybersécurité, trois éléments clés sont a retenir :

* La confidentialité : les données ne doivent pas être divulguées
* L’intégrité : les données ne doivent pas être falsifiables ou fausses
* La disponibilité : l’accès aux données doit être contrôlée

A ce niveau, la sécurisation se restreint a la fonctionnalité d’un produit. A ceux-là, nous pouvons ajouter les notions de :

* Traçabilité : pour répertorier les transactions d’un système
* La non-répudiation : pour éviter de nier tout participation a une transaction

Et même avec ceux-ci, comme dans le contexte actuel, les choses évoluent de manière exponentielle, dans le sens de rendre rapidement des moyens de sécurité mis en place obsolètes, la validité d’un produit en matière de sécurité, ne tient que le temps de se faire dépasser, ce qui arrive assez rapidement dans bien des cas.

Autrement un produit quel qu’il soit, finira bien par être compromis, s’il n’est pas amélioré de manière permanente. Et donc un jour tout produit finit par être compromis. Cependant il ne faut pas s’arrêter là, mais pouvoir retrouver ce qui s’est passé, de remonter à la cause, de circonscrire les effets et évidemment d’analyser et de remonter toutes les informations nécessaire la compréhension de ce qui s’est passé. Ceci afin d’améliorer les processus afin que la compromission ne se reproduise pas. Mais aussi qu’en cas d’attaque, de compromission et de dégâts occasionnes, que le produit permette de remonter les informations (accès, nature des dégâts, éléments modifiées) y afférant (grâce aux logs par exemple). Ce qui permettra aux assurances de louer, aux clients de porter plainte au niveau de la justice, et en gros d’avoir tout un écosystème d’éléments permettant de minimiser la portée des effets de la compromission d’un produit.

Au terme de ce travail, nous avons pu mettre sur pied un rapport d’audit logiciel comprenant les informations nécessaires à l’amélioration des applications SaaS de l’entreprise ne matière de sécurité. Mais aussi l’entreprise dispose désormais de mois de prévenir les failles de sécurité, en agissant non plus après la réalisation complète de l’application, mais pendant la réalisation de celle-ci.