Séminaire du 16 décembre 2021

Rapport sur le séminaire : Normes de sécurité

Auteur :
Sénéchal Julien

Sécurité des systèmes
Hénallux
Troisième Bloc, groupe A
Année académique 2021-2022

18 Décembre 2021

1 Compte rendu informatif

1.1 Présentation du conférencier

Il s'agissait de monsieur David Blampain. Après être sorti de technique en informatique de gestion à Louvain, il a commencé ses études dans le marketing avant de se réorienter dans l'informatique et plus particulièrement la gouvernance. Il est en possession d'un master en marketing et advertising. Il à également fait chercheur en philosophie à l'ULB.
Il possède de nombreuses certifications comme les ISO 25005, 27001, 27032 (+ NIST), formé aux règles du RGPD et actuellement en train de suivre le CISSP.

1.2 Les conseils

Nous avons eu beaucoup de conseils de la part du conférencier. Pour commencer, il nous a tout d'abord recommandés d'utilisation un framework organisationnel comme le NIST. Selon lui, c'est très important pour assurer la continuité de la politique de sécurité dans le temps et cela permet aussi de ne passer à côté de rien.

Puis, il nous a énuméré les divers points faibles récurrents des entreprises afin d'y faire plus attention : il soulignait, par exemple, le fait que la première chose à faire et de former les gens qui ne connaissent rien à la sécurité et qui devraient utiliser le système d'information. Pour cela, il nous a recommandé de suivre une formation en marketing ou communication pour savoir communiquer et intéresser les personnes que l'on veut former. Ensuite, de faire attention à la sécurité physique. En effet, certains groupes sont spécialisés dans le social engineering et pourraient arriver à compromettre le système d'informations simplement avec une imprimante. Pour cela, il nous a donnés comme exemple une personne qui se ferait passer pour une femme de ménage et qui viendrait simplement mettre une clé USB sur l'imprimante et corrompre de cette manière celle-ci afin d'obtenir tous les fichiers qui y transiteraient. Pour ce qui est de la sécurité physique, il est recommandé de sous-traiter car bien souvent les spécialistes ont une meilleure vision du point de vue 'voleur'.

Ensuite, pour commencer à mettre en place notre politique de sécurité, tout doit être écrit. Si une chose n'est pas écrite, c'est qu'elle n'existe pas. Puis, nous devons faire les divers points suivants avant de commencer :
- Faire la liste des actifs à protéger
- Liste du matériel
- Revoir les règles et la sécurité de l'Active Directory (très important)
- Classifier les informations à protéger
- Chiffrer les données sensibles (+ toutes les règles liés au RGPD)

Nous avons aussi pu avoir une petite explication sur les menaces potentielles. Il en existe 3 type :
- Interne : Employé, IT, Ouvrier, etc.
- In/Out : Stagiaire, Consultant, etc.
- Out : Clients, Etats, Concurrent, etc.

Étant donné que les états sont des menaces, nous devons faire attention également aux éditeurs de logiciels que nous utilisons sur notre système d'information. Nous avons eu l'exemple d'une entreprise voulant mettre Kaspersky comme antivirus sur tout le système d'information. Sauf que celui-ci est édité par des développeurs Russes qui sont connus pour leur cyber espionnage.

Il est également important de collecter un maximum de logs, de telle manière à pouvoir aider l'équipe de forensics au cas où l'on subirait une attaque ou s'il y a tentative.

L'importance également du 2FA à été rappelée. Non seulement il est très important de mettre en place un système multi-authentificateur mais il est également très important d'imprimer les clés de récupération et de faire attention à la sécurité physique de ceux-ci.

Enfin, il nous expliquait qu'une chose assez rare dans les entreprises est de chiffrer les disques. En effet, beaucoup d'appareils deviennent mobiles, et des informations importantes peuvent s'y trouver.

1.3 Quelques explications sur ISO

Il y a 2 types de document :

- Les normes :
  Uniquement les certifications finissant par 1 permettant d'obtenir la certification (pour l'entreprise)

- Les clauses :
  Nombreux documents qui expliquent comment obtenir la certification en détails.

2 Compte rendu personnel

Ce que j'ai personnellement apprécié, c'est le fait que ce soit une personne qui travaille dans le domaine de la consultance en sécurité qui nous parle de son expérience et ce qu'il a déjà pu vivre dans une entreprise. Il a pu ainsi nous souligner des points importants que l'on peut sous-estimer en tant que technicien sans grande expérience. Néanmoins, j'ai trouvé que l'explication des différentes étapes du framework NIST et des différents documents de l'ISO 27000 était un peu trop théorique. J'aurais en effet préféré une approche plus pratique. Par exemple, en prenant l'exemple d'une entreprise fictive dans laquelle on aurait dû faire l'audit ensemble étape par étape.