Seminars, Challenges, Serious Games and Casus

Année académique 2019-2020

Compte rendu analytique de la première conférence : sécurité et gouvernance en milieu professionnel

Redcactus

Conférence présentée par Monsieur Antoine COX et Monsieur Clement LAURENS, tous deux membres de la société Redcactus.

Sous la supervision de Monsieur Bob MULUMBA, professeur de *Seminars, Challenges, Serious Games and Casus* .

Compte rendu de 3ème année de bachelier, option sécurité des systèmes, Hénallux.

5 Novembre 2019.

Thomas Matis

Table des matières

1 Présentations

1.1 Présentation des conférenciers

Cette conférence a été majoritairement présentée par Monsieur Antoine COX, cybersecurity technical leader dans la société Redcactus. Il est par ailleurs cofondateur de la Cyber Security Agency.

Monsieur Clément LAURENS, co-fondateur et sales lead de la société Redcactus, est intervenu.
Il est diplômé du master Human Resources Management/Personnel Administration de l'université de Paris XII - Val-De-Marnes.

Pour finir, Monsieur Bob MULUMBA, professeur et responsable notamment de l'unité d'enseignement *Seminars, challenges, serious games and Casus*, est également intervenu plusieurs fois afin de faire le lien entre ce qu'il nous avait enseigné et ce que monsieur COX nous démontrait.

1.2 Présentation de la société Redcactus

Redcactus est une société de sécurité informatique implémentée dans la ville de Bruxelles.

Cette société est spécialisée dans les domaines suivants : IAM [1], le cloud, la protection des données, la sécurité informatique et le DevSecOps [2].

1.3 Présentation des sujets abordés

Voici l'agenda des sujets abordés :

1. Politique de sécurité et gouvernance dans l'amélioration journalière de la sécurité.
2. Hacking Tools : C99 Shell dans un wordpress accompagné d'une démonstration selon une politique de sécurité.
3. Les caractéristiques d'un consultant 'Junior' en sécurité.
4. Session de questions-réponses.

Tous ces sujets ont été discutés sur base de l'idée suivante : *Une bonne politique de sécurité* ***doit*** *prendre en compte le fait que les gens ne s'y connaissent parfois, voire souvent, pas du tout en informatique, et plus précisément en* ***sécurité*** *informatique.*

De plus, au vu de l'importance et du pouvoir que détient le chef de la sécurité informatique, cette idée est à mettre encore plus en application.

1. Identity and Access Management - GIA en français (Gestion des identités et des Accès)
2. DevSecOps est une méthode de gestion qui fait le lien entre équipes de sécurité et d'exploitation.

2 Conférence

2.1 Politique de sécurité et gouvernance dans l'amélioration journalière de la sécurité

Monsieur COX a débuté sa conférence en posant quelques questions à l'assemblée sur le début de son powerpoint et, lorsqu'il a eut fini de juger nos connaissances en sécurité informatique (qu'il a sans doute jugé suffisantes), a simplement quitté son powerpoint pour directement rentrer dans le vif du sujet.
Je pense qu'il aurait été intéressant de tout de même passer en revue ces slides, étant donné que l'ensemble et je pense la majorité des étudiants n'avaient pas toutes les connaissances qui avaient été jugées comme acquises par le conférencier.

Ce dernier nous a parlé des réalités du terrain : une attaque intervient toutes les 5 minutes, 70% des SOC [3] ne sont pas préparés, les attaques peuvent coûter jusqu'à 6 milliards de dollars, le temps de réaction moyen à une attaque est de 50 jours, etc.

Il a bien insisté sur la différence entre la théorie et la pratique : rien n'est jamais parfait, il faut faire au mieux avec ce que l'on possède. Pour cela, il faut sécuriser un élément en fonction de sa criticité, de la valeur qu'il détient, etc.
Cela recoupe effectivement ce qui nous a été enseigné, notamment par Monsieur MULUMBA, qui fit à ce moment-là le lien entre ses enseignements et ceux du conférencier.

De plus, Monsieur COX a insisté sur le fait que tout était business. Il faut pouvoir expliquer sa solution de sécurité à des gens qui ne s'y connaissent pas forcément ,et que cette dernière ait une plus-value.

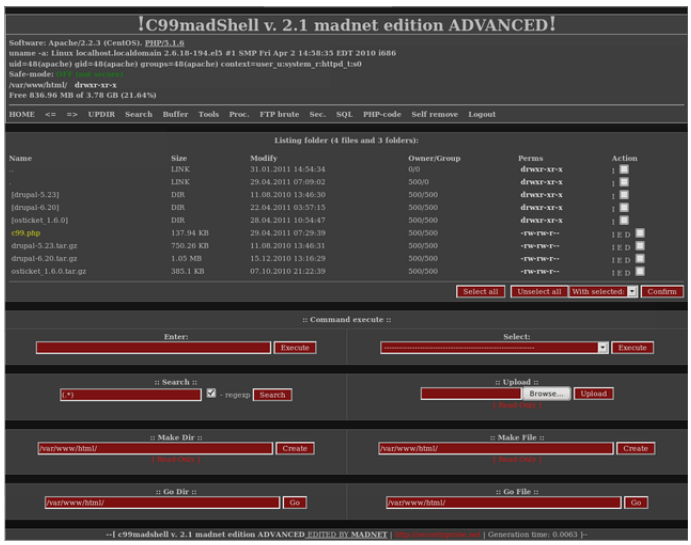
Pour finir cette partie, il faut toujours réviser de manière récurrente ce que l'on a mis en place : la sécurité change très vite, il faut toujours se remettre en question pour avancer.
En effet, chaque jour de nombreuses failles de sécurité apparaissent [4] : une solution de sécurité peut donc passer de quasi inviolable à très vulnérable à cause d'une seule faille, qui peut apparaître n'importe quand.
Il faut donc se tenir informer en permanence sur les nouvelles vulnérabilités, et toujours repenser ses stratégies.

2.2 Hacking Tools : C99 Shell dans un wordpress accompagné d'une démonstration selon une politique de sécurité

Afin de nous démontrer que les systèmes les plus utilisés sont loin d'être infaillibles et qu'il ne faut pas être un expert en cybersécurité pour les exploiter, Monsieur COX nous a fait une démonstration d'une injection de shell C99 dans un wordpress.

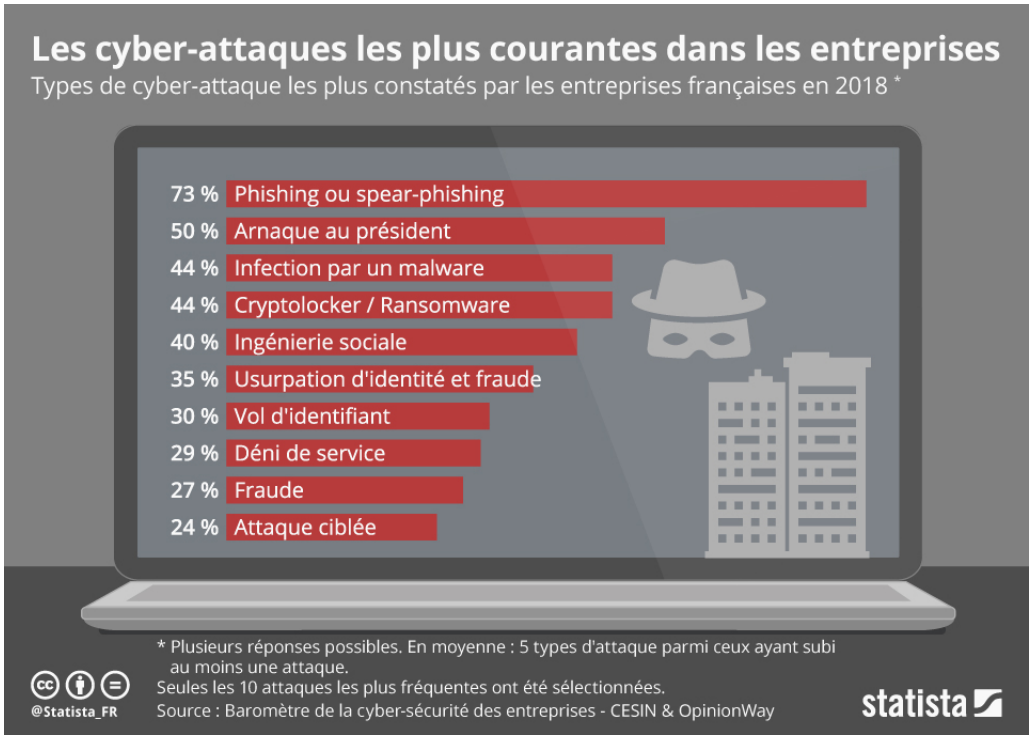
Il ne lui a effectivement pas fallu plus d'une petite dizaine de minute pour pouvoir l'injecter : rajouter /robots.txt à la fin de l'url, aller au fichier de connexion admin et y entrer les identifiants de base : admin/admin, copier-coller le shell et voici ce que cela donne :

3. Security Operations Center
4. `https://cyware.com/category/breaches-and-incidents-news`



Il a un accès complet au site web.
On peut se rendre compte de la gravité de la chose lorsque l'on apprend que 34% des sites webs sur l'internet sont des sites wordpress.
En terme de CMS [5], wordpress détient 60% des parts du marché !

Il était effectivement intéressant de nous montrer que les attaques peuvent être réalisées sans grandes connaissances, ce qui nous pousse à faire le maximum pour défendre nos infrastructures.
Surtout lorsque l'on sait que l'attaque la plus réalisée dans les entreprises françaises en 2018 est le phishing, qui ne nécessite quasi voire aucune connaissance en sécurité informatique.



[6]

5. Content management system - système de gestion de contenu, en français
6. Confer source : image n°2

2.3 Les caractéristiques d'un consultant 'Junior' en sécurité

Le conférencier nous a expliqué qu'il fallait rapidement trouver un domaine en particulier qui nous intéressait et nous plaisait pour pouvoir se spécialiser.

Il nous a donné différentes voies à suivre :

- Réseau
- Pentesting
- Forensics
- IAM [7]
- Cryptographie

Ensuite, il ne faut pas se fermer complètement à une option, mais c'est toujours bien de se spécialiser. La réalité fait que la majorité des experts en sécurité informatique sont freelance (moins stable qu'un CDI), car il n'est pas nécessaire d'avoir un expert à temps plein et qu'il coûte très cher à la boite. Encore une fois, tout est business.

Enfin, il y a également le métier de CISO [8] qui permet de toucher à tout, mais toucher à tout signifie n'exceller dans rien. C'est un choix personnel à faire.

Il est effectivement essentiel de se trouver une spécialité à approfondir. Néanmoins, le choix est tellement vaste qu'il est quasi impossible de pouvoir faire ce choix dès la fin de nos études.

Je pense plutôt qu'il faudrait, comme dans ce schéma, se déplacer de branche en branche pour découvrir ce qu'il nous plaît et pouvoir choisir au mieux.

2.4 Session de questions-réponses

Voici les différentes questions qui ont été posées, ainsi que leur réponse respective :

7. Gestion des Identités et des Accès
8. Chief Information Security Officer

1. Quelles études avez-vous fait ?
   -> Le conférencier n'a pas préféré répondre à cette question en public. Il s'avère qu'il n'a pas fait d'études supérieures. Il est, selon moi, encore plus honorable d'arriver où ce Monsieur en est arrivé en n'ayant pas fait d'études.
2. Auriez-vous des références, ouvrages ou autres documents à nous conseiller pour pouvoir nous entraîner ?
   -> Google est le meilleur de nos alliés. Voici quelques références pêle-mêle :
   - Hackthis ![9]
   - Root-me [10]
   - SANS [11]
   - Offensive security [12]

   Pour finir, le plus important : l'expérience sur le terrain.
3. Cherchez-vous toujours des stagiaires ?
   -> Oui.
4. Comment choisissez-vous vos solutions de sécurité ? Par réputation ?
   -> Les solutions ne sont pas prises en fonction de leur réputation, ce serait trop dangereux. Pour limiter les coûts, ils commencent par tester les solutions open-source. Si elles ne conviennent pas, ils testent donc les solutions propriétaires.

9. `https://defendtheweb.net/?hackthis`, désormais appelé defendtheweb
10. `https://www.root-me.org/`
11. `https://www.sans.org/`
12. `https://www.offensive-security.com/`

3 Sources

1. Linkedin :
   - https://www.linkedin.com/company/redcactus-by-positivethinkingc
     about/
   - https://www.linkedin.com/in/antoine-cox-ab4598137/
   - https://www.linkedin.com/in/claurens1/
2. Sites webs :
   - https://red-cactus.io/
   - https://steemit.com/steemit/@bassemm/got-wordpress-php-c99-webs
   - https://kinsta.com/fr/part-de-marche-de-wordpress/
   - https://www.lemagit.fr/definition/SecOps
3. Images :
   (a) https://2.bp.blogspot.com/-OgGmvicsBPk/WNEl5_R2xpI/AAAAAAAAfvQ/
   gFEk1qkhaT805_R4MBzcc7MtjaNm2-YRACLcB/s640/cybersecurity%
   2Bdomains%2Bv2-0%2Bhenry%2Bjiang.png
   (b) https://infographic.statista.com/normal/chartoftheday_15871_
   types_de_cyber_attaque_les_plus_courantes_entreprises_francaise
   n.jpg