L'édito des *"Cyberlundi de la cybersécurité"*

Du fait de la crise sanitaire, et, en particulier, des mesures de confinement, **l'Université de Paris** s'est trouvée dans l'incapacité d'accueillir la conférence mensuelle des "*Lundi de la cybersécurité*".

Déterminés à maintenir la programmation de ce très bel évènement, les fondateurs, Béatrice Laurent et Gérard Peliks, ont décidé de l'organiser, le 1er avril dernier, sous la forme d'un ***"Cyberlundi de la cybersécurité"***.

Grâce à l'exceptionnelle implication de l'intervenant, la société Yogosha, ce webinar, consacré à la "*Security by design"* et à *"l'apport du Bug Bounty dans la culture du DevSecOps*", **fût un véritable succès !**

De la culture de *"la sécurité offensive"* [1] au pilotage de réseaux d'intelligence.

[1] Cyril Quillien, International Sales and Channel Manager - Private Bug Bounty Platform at Yogosha. Webinar du 1er avr2020.

Yassir Kazar, CEO & co-fondateur de Yogosha, a souhaité ouvrir la séance par une introduction sur la question du Développement-Sécurité-Opérations (**DevSecOps**).

Fruit d'une longue gestation au sein des organisations, cette approche prône le principe de la **Security by design**. Autrement dit, la sécurité du projet est pensée en amont, et ce, dès la phase de conception.

Dans ce cadre, chaque intervenant sur **la chaîne de production devient co-responsable** de la sécurité de l'ensemble de l'infrastructure et/ou de ses diverses applications.

Cette méthode de gestion a été conçue, notamment, afin d'optimiser la communication entre les différentes équipes. Il est à noter que "*des technologies **d'automatisation** ont aidé les entreprises à adopter des pratiques **plus agiles**"* [2].

Néanmoins, si ces outils s'avèrent nécessaires, il apparaît qu'ils ne sauraient être suffisants.

Aussi, les structures qui souhaiteraient s'inscrire dans une démarche *DevSecOps* devront, en premier lieu, repenser leur modèle de gouvernance et envisager un nouveau management d'expertises devenues à la fois **pluridisciplinaires et transverses**.

En second lieu, il conviendra pour les RSSI/DSI/ Directeurs de la cybersécurité **de fédérer et/ou de piloter des réseaux d'intelligences externalisés** ; le cas échéant, en vue de "*sécuriser de manière continue tout périmètre applicatif IT critique (site marchand, plateforme SaaS, espace client, site web, API...)*" [3].

Le bug Bounty, (qui est à distinguer des tests d'intrusion dont il est conseillé qu'ils soient préalablement réalisés par des experts en cybersécurité), en est une parfaite illustration.

Souvenons-nous de cette affaire médiatisée par la presse américaine en janvier 2019 qui révélait qu'un jeune américain de quatorze ans avait décelé une faille de sécurité majeure dans l'application Facetime d'Apple[4].

Né en 1995, le premier programme de "***chasse aux bugs***" a été mené par un ingénieur américain Jarrett Ridlingghafer. [5]

Il est coutumier de distinguer **les programmes publics,** ouverts à tous et directement organisés par les entreprises, **des programmes privés**, gérés par des plateformes de Bug Bounty qui assurent un rôle d'interface entre les structures et les chercheurs "chasseurs de prime".

---

[2] https://www.redhat.com/fr/topics/devops/what-is-devsecops
[3] Communiqué de presse consultable sur le lien qui suit : https://yogosha.com/wp-content/uploads/2019/05/10-Yogosha-remportele-prix-de-la-startupFIC2019-BugBounty.pdf
[4] Deux jours après, le 21 janvier, Yogosha, se voyait remettre par le FIC le Prix spécial du jury dans la catégorie Prix de la start - up 2019.
[5] https://fr.wikipedia.org/wiki/Bug_bounty_(chasse_aux_bugs)

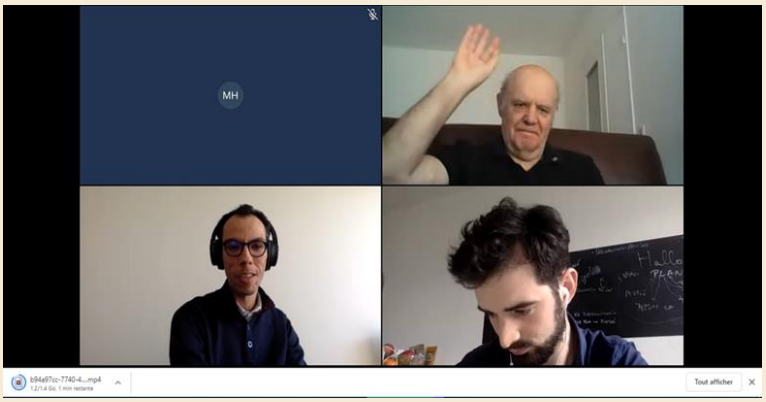
Nonobstant la nature de cette rémunération, s'agirait-il d'une forme de crowdsourcing [6] appliquée au pentest ?

En effet, *"grâce à une communauté de hackers, chercheurs en sécurité, rigoureusement sélectionnée, et à une plateforme collaborative, les entreprises peuvent monitorer des programmes de recherche et optimiser la détection et la remédiation de leurs failles"[7].*

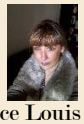
Afin de garantir la constitution d'un écosystème de confiance, il est précisé en propos conclusifs, que les compétences des hackers sont testées en ligne suivant une double notation (la communauté et les clients) avant leur "recrutement". En outre, leur identité est validée par un tiers de confiance.

Par ailleurs, s'agissant de la criticité de l'application, celle-ci est évaluée selon des critères objectifs et mesurables, en particulier, avec l'aide du **standard ISO/IEC 29147**.

In fine, le hacker éthique bénéficie d'une protection régie par l'**article 47 de la loi n°2016-1321 du 7 octobre 2017 pour une république numérique** qui vient compléter l'article L.2321-4 du Code de la défense.



Gérard Peliks,
Yassir Kazar et Cyril Quillien
Ils étaient accompagnés de Béatrice Laurent et de Meriem Hamada.



Edito écrit par Alice Louis
Mél : alice.louis@netcourrier.com
Membre de l'AFCDP, du CEFCYS, de l'IE-IHEDN
Directrice du projet de création du fonds de dotation
"Fonds Cyber Ethique pour une Souveraineté Numérique"
Juriste en droit des médias (IP/IT) et Major 2019 du MBA
Management de la Cybersécurité de l'Institut Léonard de Vinci

[6] Le crowdsourcing est une forme d'externalisation. Cf https://www.cairn.info/revue-management-et-avenir-2011-1-page-254.htm#
[7] Communiqué de presse consultable sur le lien qui suit : https://yogosha.com/wp-content/uploads/2019/05/10-Yogosha-remportele-prix-de-la-startupFIC2019-BugBounty.pdf