Pour beaucoup, Internet, c'est un peu le monde des Bisounours

Cyril Bras est Directeur Cybersécurité chez Whaller

1/ Qu'est-ce qui domine selon vous la « bataille » de la cybersécurité : la sophistication technique ou l'engagement éthique des combattants ?

Je dirai que c'est une combinaison des deux mais il y a clairement une dominante sur la sophistication technique. Il existe une fuite en avant manifeste bien avant le numérique, dans le domaine militaire. Lorsque votre bouclier arrête les frappes d'un glaive alors il faut créer une épée plus lourde qui passera au travers du bouclier, il faudra donc renforcer le bouclier… Ce phénomène s'observe bien évidemment dans la cyberdéfense. Nous disposons de toujours plus de dispositifs de protection, des pare-feu agissant sur toutes les couches du modèle OSI, des anti-virus nouvelle génération appelés aussi EDR qui détectent des comportements anormaux ou encore plus récemment les capacités de l'IA générative. Les attaquants vont devoir à chaque fois s'adapter ou détourner les outils de défense pour en faire des outils offensifs [1]. Simplement il y a une différence fondamentale entre l'attaque et la défense et c'est là que l'éthique entre en considération. L'attaquant lui peut échouer 999 fois et réussir une fois. Le défenseur devra lui réussir 1000 fois ! La défense est donc plus exigeante mais aussi beaucoup plus encadrée que l'attaque. En effet, en France vous ne pouvez par exemple pas riposter à une cyberattaque (ce qui est une bonne chose) mais cela nécessite donc un engagement éthique que l'on ne trouvera pas nécessairement chez tous les attaquants excepté les White Hats. Ces derniers vont en effet informer sur des faiblesses

qu’ils peuvent découvrir dans des systèmes/logiciels.

2/ Quelle est selon vous la probabilité pour qu’Internet connaisse un jour une avarie mondiale d’origine criminelle ?

En 2017 Wannacry et Not Petya [2]ont démontré qu’une cyber attaque pouvait frapper à l’échelle planétaire et rendre inopérantes plusieurs entreprises simultanément. Ces attaques avaient mis en évidence plusieurs facteurs, le premier sur la non application des règles d’hygiène numérique comme l’application des correctifs de sécurité, le second sur le phénomène de dépendance client fournisseur d’offres logicielles. Un an plus tôt, une attaque mondiale s’appuyant sur un malware nommé MIRAI [3] avait rendu inaccessibles de nombreux sites web d’acteurs majeurs comme Twitter, Spotify ou encore Netflix. Cette attaque s’est appuyée sur des milliers de caméras connectées à Internet compromises et ajoutées à un réseau de BotNet. Ces caméras ont alors simultanément réalisé des requêtes vers plusieurs serveurs, conduisant à une situation proche du blackout. Là encore les attaquants exploitent des vulnérabilités logicielles non corrigées pour prendre le contrôle de matériels informatique. Ce code malveillant est toujours actif… Donc pour répondre à votre question, c’est très fortement probable d’autant que le numérique est de plus en plus présent dans nos vies quotidiennes sans que nous nous en rendions compte.

3/ Y-a-t-il plusieurs visions de la cybersécurité et le cas échéant, quelle est la vôtre ?

C’est évident ! La première étant celle qui consiste à confondre sécurité informatique et Cybersécurité. Elle est malheureusement encore trop souvent observable dans des organisations, qu’elles soient publiques ou privées. C’est une vision qui consiste à se contenter d’une approche exclusivement technique du sujet. La traduction dans le monde réel sera visible par le positionnement du RSSI (Responsable Sécurité des Systèmes d’Information) au sein des services

informatique ou des DSI. Est-ce que lorsque vous louez une voiture vous aimeriez que le contrôle technique soit réalisé par le loueur ?

Seconde vision, l'approche par la conformité que je nomme la « Cybersécurité de salon ». Cette approche est très bien mais il y a un risque d'avoir des « experts » un peu hors sol qui par manque de recul ou de pragmatisme vont vouloir appliquer strictement certains référentiels.

Je suis partisan d'une approche qui combine les deux visions précédentes. En effet, il est indispensable d'une part de cadrer/normer le SSI dans une structure mais cela doit se faire en cohérence avec la réalité du terrain. Ensuite il faut comprendre les 3 couches de Cybersécurité : physique, logique et sémantique qui permettent de mettre en évidence qu'il faut aller au-delà du cadre technique car les cyberattaques s'y déroulent.

4/ Dans quelle mesure le secteur public, garant de l'intérêt général et détenteur de la puissance publique, vous semble-t-il devoir montrer le chemin à suivre en matière de cybersécurité ?

Les données détenues par les administrations, les collectivités ou encore les hôpitaux revêtent souvent un caractère sensible et nous pouvons difficilement nous opposer à leur collecte (impôts, examens médicaux, aides sociales…). Il est donc essentiel que les différentes composantes du secteur public soient robustes et exemplaires.

Malheureusement, la presse relaye tous les jours des cyberattaques frappant des établissements publics comme des hôpitaux ou des collectivités territoriales, ce qui démontre que la prise en considération du sujet est encore faible. Il y a encore du chemin à parcourir pour que la Cybersécurité soit adressée au bon niveau dans ces entités. Trop souvent le RSSI, lorsqu'il existe est rattaché au service informatique ou à la DSI (quand en plus il ne cumule pas des fonctions techniques).

Ce rattachement génère des situations de juge et partie qui peuvent être préjudiciables à la prise en considération du sujet par les dirigeants de la structure. Il conviendrait de revoir la fonction SSI en général, qui reste encore trop souvent perçue comme exclusivement technique et incompréhensible. La fonction RSSI devrait évaluer vers un directeur Cybersécurité à minima au même niveau que les DSI. Il conviendrait de faire évoluer les fiches métiers en s'appuyant sur le panorama des métiers de la Cybersécurité publié en 2020 par l'ANSSI [4].

Du côté de la protection à présent, des efforts importants ont été réalisés avec la montée en puissance de l'ANSSI afin d'accompagner le secteur public et par extension le secteur privé qui est bien souvent un sous-traitant du secteur public. La création d'un commandement cyber dans la gendarmerie nationale est aussi un signal fort pour montrer l'engagement de l'état à lutter contre la cybercriminalité.

5/ Quelle est selon vous la nature du lien qui unit souveraineté et cybersécurité ?

L'un ne va pas sans l'autre, il y a un lien d'interdépendance évident. La souveraineté numérique permet de garantir une indépendance légale, contre les lois extra-territoriales pouvant affecter les données. La Cybersécurité va permettre d'assurer, de garantir la souveraineté numérique en protégeant l'information. Toutefois comment se protéger efficacement si les solutions de Cybersécurité ne sont pas souveraines ?

6/ Diriez-vous que nous vivons les derniers moments d'un été indien de la « cyber-naïveté » ? Comment intégrer dans nos sociétés du confort l'idée d'une omniprésente menace ?

Il est vrai que depuis 2020 [5], les cyberattaques sont devenues plus visibles car bien plus reportées par la presse locale ou nationale ouvrant la voie à une acculturation généralisée plutôt douloureuse [6]. Dans le même temps la part

du numérique dans notre vie de tous les jours n'a fait que s'accroitre augmentant par la même occasion les opportunités laissées aux cyber criminels. Le chemin est encore long dans le changement des habitudes. Les récentes attaques sur les systèmes VMWare ESxi [7] en est une belle illustration puisque les attaquants ont exploité une vulnérabilité corrigée depuis de nombreux mois mais laissée béante sur de trop nombreux systèmes. J'aime bien le terme de cyber naïveté de votre question car il illustre bien cette naïveté propre au numérique qui n'existe pas dans le reste des activités. Qui laisse les clefs de sa voiture sur le contact dans la rue pour aller au cinéma ou utilise la même clef pour sa voiture sa boite aux lettres sa maison ? Personne, enfin je l'espère ; pour beaucoup Internet c'est un peu le monde des Bisounours, un lieu de partage, d'échange… alors que l'on y retrouve les mêmes menaces que dans le monde réel. La seule différence c'est que les agressions sont permanentes et peuvent provenir de votre voisin comme d'une personne située à l'autre bout du Monde. Alors nous devons juste nous comporter comme nous le faisons dans le monde réel.

7/ Lorsque l'on assure la cybersécurité d'une plateforme collaborative comme Whaller, quel genre de promesse fait-on à ses utilisateurs ?

De garantir un haut niveau de sécurité pour protéger les données qui nous sont confiées.

Mon recrutement au poste de directeur Cybersécurité en mars 2022, dénote une volonté encore peu répandue dans les PME de faire de la Cybersécurité un avantage stratégique. Thomas Fauré, le président fondateur de Whaller est un fervent défenseur de cette position. Ceci n'est atteignable , qu'en faisant en sorte que la Cybersécurité ne soit pas juste la préoccupation de la direction cyber mais bien l'affaire des tous les collaborateurs de Whaller. Une autre illustration c'est l'engagement de Whaller dans la course à la qualification SecNumCloud de sa plateforme. Cette dernière

affirme la volonté au plus haut niveau de faire de la Cybersécurité un gage de confiance dans l'usage de notre plateforme.

8/ Considérez-vous que notre arsenal juridique en matière pénale est suffisamment dissuasif face au terrorisme aveugle des « black hats » ?

Je ne sais pas si l'on peut parler de terrorisme aveugle, dans la plupart des cas ce sont des criminels qui se sont déplacés dans l'environnement numérique car celui-ci présente deux avantages, il est lucratif et la prise de risque bien plus faible [8]. Ils sont très loin d'être aveugles dans leurs frappes simplement ces dernières sont d'ordre criminel donc sans éthique ; raison pour laquelle elles touchent des hôpitaux et n'hésitent pas à publier des données sur les patients pour arriver à leurs fins [9]. Pour beaucoup les risques juridiques encourus sont faibles, pour peu qu'ils soient dans un pays ne disposant pas de législation cyber ou pire qui encourage la cybercriminalité envers les ennemis de leur nation.

Ce qui est certain c'est qu'augmenter les exigences cyber des entreprises et des entités étatiques par le vecteur juridique me semble une bonne direction à prendre à défaut de pouvoir sanctionner les cybercriminels. Le RGPD lors de son entrée en vigueur en 2018 a commencé à faire bouger les lignes même si cela ne concernait que les données personnelles, ce règlement a imposé de la sécurité par défaut dans les solutions numériques. L'arrivée de la directive NIS 2 au second semestre 2024 [10] va étendre le périmètre des entités pour lesquelles la Cybersécurité ne sera plus une option mais bien obligatoire. Pour assurer la bonne mise en œuvre des sanctions basées sur le chiffre d'affaire sont prévues.

9/ Comment bâtir la sécurité sur la confiance quand on apprend qu'une unité de l'armée américaine entend

recourir aux deepfakes dans le cadre de campagnes de déstabilisation ?

Ce n'est pas nouveau, les campagnes de déstabilisation sont des moyens utilisés depuis très longtemps en s'appuyant à chaque fois sur les moyens technologiques contemporains. C'est une forme de ruse de guerre, déjà présente dans les périodes antiques [11]. D'une certaine façon le cheval de Troie en était une illustration. Il faut donc apprendre à composer avec ce nouveau risque et ajouter des mesures pour garantir l'authenticité des vidéos.

10/ Comment seconder au mieux la démarche de sensibilisation et de vulgarisation entreprise par l'ANSSI ?

Il est indispensable que chacun des acteurs de la Cybersécurité relaye les messages de l'ANSSI à leur niveau. Le sujet cyber parait obscur et inintéressant pour bon nombre de nos concitoyens, il est donc essentiel d'arriver à le vulgariser et le rendre sexy [12]. Les directeurs Cybersécurité, les RSSI doivent se mettre au niveau des utilisateurs et s'appuyer sur les éléments fournis par l'agence pour acculturer de façon large.

Le GIP ACYMA plus connu sous le nom cybermalveillance.gouv.fr propose de nombreux support de communication accessibles qu'il peut être pertinent de relayer. Cette entité a pour mission l'acculturation aux enjeux cyber mais également de mise en relation en cas d'incident avec des prestataires qualifiés.

La proposition récente formulée par BFM Business de relayer les alertes Cyber du GIP me parait être une excellente initiative qui mériterait d'être reproduite par d'autres médias. [13]

11/ À tort ou à raison, l'Union européenne est souvent invoquée comme un facteur de supériorité en matière

d'échelle, par rapport à la France seule. Est-il plus efficace à vos yeux d'envisager la cybersécurité de notre « village gaulois » ou celle de « l'empire romain » ?

C'est certainement un compromis des deux à l'image de la tortue romaine, inventée par les gaulois et utilisée par les romains. Je pense qu'il faut combiner l'ensemble des savoirs individuels européens pour en faire une force. Globalement le village gaulois est précurseur sur le sujet Cyber, la création des opérateurs d'importance vitale il y a plus de 10 ans et sa déclinaison à l'échelle européenne avec la directive NIS en est une belle illustration. Il faut donc essayer de s'appuyer sur ce qui se fait de mieux à l'échelle européenne en combinant les solutions. L'unité fait la force.

Il convient d'encourager les démarches de partage d'information Cyber entre les différents acteurs de la SSI y compris dans les petites structures afin que chacun à son niveau puisse mettre en place des mesures adaptées. L'exemple récent du réseau des RSSI [14] de collectivités dont j'ai été un des initiateur est dans cet esprit de partage. Les cybercriminels partagent de l'information sur leurs cibles, il est plus que temps d'en faire de même au niveau de la défense.

C'est également une démarche que j'ai poussé lors de mon arrivée chez Whaller où j'ai mis en place une plateforme d'échange d'IOC avec nos clients et partenaires [15].

12/ Vous êtes un auditeur de l'IHEDN. Pouvez-vous nous décrire en profondeur cette « mise à jour » humaine ?

Au-delà du titre conféré d'auditeur IHEDN, ce fût une superbe expérience qui a confirmé pour moi l'attrait pour les sujets de souveraineté numérique et de Cybersécurité, mais également mes choix professionnels. De façon plus personnelle, les différentes intervention auxquelles j'ai pu assister mais également les nombreux échanges représentaient des bouffées d'oxygène intellectuelles. Ce fut aussi une expérience humaine

riche permettant de faire se rencontrer des profils divers et variés ayant ces sujets en commun, le tout animé par le foisonnement et la richesse intellectuelle du général (2S) Watin-Augouard.

C’est un passage très rapide qui marque et c’est un engagement que l’on souhaite poursuivre au-delà.

Références

[1]	A. Beky, «ChatGPT : les cybercriminels l’utilisent aussi,» Silicon.fr, 02 Mars 2023. [En ligne]. Available: https://www.silicon.fr/chatgpt-acteurs-menace-utilisent-aussi-459595.html. [Accès le 13 Mars 2023].
[2]	H. Le Fell, «WannaCry et (Not)Petya : retour sur ces cyberattaques,» Les Echos, 04 Août 2017. [En ligne]. Available: https://solutions.lesechos.fr/tech/c/ne-prendre-otage-identifiez-exposition-a-wannacry-notpetya-5356/. [Accès le 13 Mars 2023].
[3]	J. Absalon, «Mirai : comment un logiciel a été à l’origine de la cyberattaque mondiale,» RTL, 28 Ocotobre 2016. [En ligne]. Available: https://www.rtl.fr/actu/sciences-tech/mirai-comment-un-logiciel-a-ete-a-l-origine-de-la-cyberattaque-mondiale-7785481817. [Accès le 13 Mars 2023].
[4]	ANSSI, «Panorama des métiers de la Cybersécurité,» 2020. [En ligne]. Available: https://www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/. [Accès le 28 Mars 2023].
[5]	V. Rieß-Marchive, «2020 : l’Anssi et Acyma tirent le bilan d’une année explosive sur le front des cyberattaques,» 13 Janvier 2021. [En ligne]. Available: https://www.lemagit.fr/actualites/252494759/2020-lAnssi-et-Acyma-tirent-le-bilan-dune-annee-explosive-sur-le-front-des-cyberattaques. [Accès le 09 décembre 2022].
[6]	Antoine, «Cybersécurité – 50% des PME font faillite après une cyberattaque, le plan du gouvernement pour 2023,» Carnet de Bord, 06 Février 2023. [En ligne]. Available: https://www.carnetdebord.info/cybersecurite-50-pme-font-faillite-cyberattaque-plan-gouvernement-2023/. [Accès le 17 Mars 2023].
[7]	D. Filippone, «Salve mondiale de cyberattaques via une faille ESXi,» Le Monde Informatique, 06 Février 2023. [En ligne]. Available: https://www.lemondeinformatique.fr/actualites/lire-salve-mondiale-de-cyberattaques-via-une-faille-esxi-89445.html. [Accès le 17 Mars 2023].
[8]	S. Rolland, «La gendarmerie nationale en première ligne contre les cybercriminels,» La Tribune, 08 Septembre 2021. [En ligne]. Available: https://www.latribune.fr/technos-medias/internet/la-gendarmerie-nationale-en-premiere-ligne-contre-les-cybercriminels-891778.html. [Accès le 17 Mars 2023].
[9]	B. Bonar, «Des hackers publient des photos dénudées de malades pour faire chanter un hôpital,» Numerama, 1 Mars 2023. [En ligne]. Available: https://www.numerama.com/cyberguerre/1299068-des-hackers-publient-des-photos-denudees-de-malades-pour-faire-chanter-un-hopital.html. [Accès le 17 Mars 2023].
[10]	ANSSI, «Directive NIS 2 : ce qui va changer pour les entreprises et l’administration françaises,» [En ligne]. Available: https://www.ssi.gouv.fr/directive-nis-2-ce-qui-va-changer-pour-les-entreprises-et-ladministration-francaises/. [Accès le 29 Mars 2023].
[11]	P. Laederich, Stratégie et stratagèmes dans l’Antiquité grecque et romaine, Cairn, 2009.
[12]	H. Meddah, «Le patron de l’ANSSI veut rendre la cybersécurité « plus sexy »,» 06 Septembre 2018. [En ligne]. Available: https://www.usinenouvelle.com/article/le-patron-de-l-anssi-veut-rendre-la-cybersecurite-plus-sexy.N737689. [Accès le 17 Mars 2023].
[13]	BFM Tech&Co, «Cybersécurité: BFM Business s’engage pour renforcer le dispositif Alerte Cyber,» 28 Mars 2023. [En ligne]. Available: https://www.bfmtv.com/tech/cybersecurite/cybersecurite-bfm-business-s-engage-pour-renforcer-le-dispositif-alerte-cyber_AN-202303280475.html. [Accès le 29 Mars 2023].
[14]	J. Cheminat, «Les RSSI des collectivités territoriales créent un réseau de partage,» 16 Février 2021. [En ligne]. Available: https://www.lemondeinformatique.fr/actualites/lire-les-rssi-des-collectivites-territoriales-creent-un-reseau-de-partage-81985.html. [Accès le 28 Mars 2023].
[15]	WHALLER, «Whaller propose à ses partenaires une plateforme d’échange d’IOC (menaces cyber),» 05 Avril 2022. [En ligne]. Available: https://blog.whaller.com/2022/04/05/whaller-propose-a-ses-partenaires-une-plateforme-dechange-dioc-menaces-cyber/. [Accès le 29 Mars 2023].