Cyberattaque

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 août 2019

https://www.bortzmeyer.org/cyberattaque.html

Auteur(s) : Angeline Vagabulle
ISBN n°978-2-9555452-7-0
Éditeur : Les funambulles
Publié en 2018

Des livres parlant de « cyberattaques » ou de « cybersécurité », il y en a plein. C'est un thème à la mode et les historiens du futur, lorsqu'ils étudieront la littérature du passé, noteront sans doute que les années 2010 étaient marquées par l'importance de ce thème. Mais ce livre a un angle original : ni un roman, ni un « reportage » sensationnaliste, ni une pseudo-réflexion sur la « cyberguerre », c'est un récit vu de l'intérieur d'une grosse perturbation, le passage de NotPetya dans l'entreprise où travaille l'auteure. Derrière le passionnant récit « sur le terrain », c'est peut-être l'occasion de se poser quelques questions sur l'informatique et la sécurité.

J'avoue ne pas savoir dans quelle mesure ce récit est authentique. L'auteure raconte à la première personne ce qu'a vécu l'entreprise où elle travaillait. Angeline Vagabulle est un pseudonyme, soit parce que l'entreprise ne souhaitait pas que ses cafouillages internes soient associés à son nom, soit parce que l'auteure a fait preuve d'imagination et romancé la réalité. Mais le récit est très réaliste et, même si cette entreprise particulière n'existe pas, les évènements relatés dans ce livre ont tous bien eu lieu dans au moins une grande entreprise dans le monde.

Ceux et celles qui ont vécu un gros problème informatique dans une grande entreprise multinationale les reconnaitront : le DSI qui se vante dans des messages verbeux et mal écrits que l'entreprise est bien protégée et que cela ne pourrait pas arriver, les conseils absurdes (« ne cliquez pas sur un lien avant d'être certain de son authenticité »), l'absence de communication interne une fois que le problème commence (ou bien son caractère contradictoire « éteignez tout de suite vos ordinateurs » suivi de « surtout n'éteignez pas vos ordinateurs »), la langue de bois "*corporate*" (« nous travaillons très dur pour rétablir la situation »), la découverte de dépendances que personne n'avait sérieusement étudié avant (« ah, sans les serveurs informatiques, on ne peut plus téléphoner ? »), l'absence de moyens de communications alternatifs. Il faut dire que l'entreprise décrite ici a fait fort : non seulement les postes de travail sur le bureau mais tous les serveurs étaient sous Windows, évidemment pas tenus à jour, et donc vulnérables à la faille EternalBlue. Au passage de NotPetya, tous les fichiers sont détruits et plus rien ne marche, on ne peut plus envoyer de propositions commerciales aux clients, on ne peut plus organiser une réunion,

on ne peut même plus regarder le site Web public de la boîte (qui, lui, a tenu, peut-être était-il sur Unix ?) Et cela pendant plusieurs semaines.

Le ton un peu trop « léger », et le fait que l'héroïne du livre surjoue la naïve qui ne comprend rien peuvent agacer mais ce livre n'est pas censé être un guide technique du logiciel malveillant, c'est un récit par une témoin qui ne comprend pas ce qui se passe, mais qui décrit de manière très vivante la crise. (En italique, des encarts donnent des informations plus concrètes sur la cybersécurité. Mais celles-ci sont parfois non vérifiés, comme les chiffres de cyberattaques <https://www.bortzmeyer.org/compter-attaques.html>, a fortiori comme leur évaluation financière.)

(Le titre est clairement sensationnaliste : il n'y a pas eu d'attaque, cyber ou pas, NotPetya se propageait automatiquement et ne visait pas spécialement cette entreprise.)

En revanche, j'ai particulièrement apprécié les solutions que mettent en place les employés, pour faire face à la défaillance de l'informatique officielle. Comme les ordiphones ont survécu, WhatsApp est largement adopté, et devient l'outil de communication de fait. (Ne me citez pas les inconvénients de WhatsApp, je les connais, et je connais l'entreprise qui est derrière. Mais, ici, il faut se rappeler que les différents sites de la boîte n'avaient **plus aucune** communication.) Il reste à reconstituer les carnets d'adresses, ce qui occupe du monde (« C'est John, du bureau de Dublin, qui demande si quelqu'un a le numéro de Kate, à Bruxelles, c'est pour pouvoir contacter Peter à Dubaï. ») Beaucoup de débrouillardise est déployée, pour pallier les conséquences du problème. Une nouvelle victoire du "*shadow IT*", et la partie la plus passionnante du livre.

Ce livre peut aussi être lu comme une critique de l'entreprise. Avant même le problème informatique, l'auteure note que sa journée se passait en réunion « sans même le temps d'aller aux toilettes ». On peut se demander s'il est normal qu'une journée de travail se passe exclusivement en réunions et en fabrication de "*reportings*", sans rien produire. Il est symptomatique, d'ailleurs, qu'on ne sait pas exactement quel travail fait l'héroïne dans son entreprise, ni dans quel service elle travaille, ni d'ailleurs ce que fait l'entreprise.

L'auteure s'aventure à supposer que le problème est partiellement de la faute des informaticiens. « Ils feraient mieux de se concentrer sur leur boulot, en l'occurrence le développement d'applications et de systèmes sans failles. » C'est non seulement très yakafokon (développer un système sans faille est vraiment difficile) mais surtout bien à côté de la plaque. On sait, sinon faire des applications sans faille, du moins faire des applications avec moins de failles. On sait sécuriser les systèmes informatiques, pas parfaitement, bien sûr, mais en tout cas bien mieux que ce qu'avait fait l'entreprise en question. On le sait. Il n'y a pas de problème d'ignorance. En revanche, savoir n'est pas tout. Encore faut-il appliquer et c'est là que le bât blesse. Les solutions connues ne sont pas appliquées, à la fois pour de bonnes et de mauvaises raisons. Elles coûtent trop cher, elles ne plaisent pas aux utilisateurs (« le système que tu nous dis d'utiliser, j'ai essayé, il est peut-être plus sécurisé, mais qu'est-ce qu'il est moche ») et/ou aux décideurs (« ce n'est pas "*enterprise-grade*" » ou bien « on n'a pas le temps, il faut d'abord finir le "*reporting*" du trimestre précédent »). D'ailleurs, après une panne d'une telle ampleur, est-ce que l'entreprise en question a changé ses pratiques ? Gageons qu'elle aura continué comme avant. Par exemple, au moment du passage de NotPetya, l'informatique était sous-traitée au Portugal et en Inde. Aucun informaticien compétent dans les bureaux. Est-ce que ça a changé ? Probablement pas. L'expérience ne sert à rien, surtout en matière de cybersécurité.

Déclaration de potentiel conflit d'intérêt : j'ai reçu un exemplaire gratuitement.

---

https://www.bortzmeyer.org/cyberattaque.html