BIAIS COGNITIFS ET ORGANISATIONNELS : COMMENT RÉUSSIR SA SÉCURITÉ (ENFIN, ESSAYER)

I. ROSSENBACH
RandoriSec (@secucrypt)

Les biais psychologiques, affectifs, organisationnels ont souvent le champ libre pour nous entraîner dans les tréfonds de l'erreur lorsque nous avons à gérer des incidents et situations de crise. Façon enclume aux chevilles. En nous inspirant de la manière dont les développeurs peuvent expurger leur code des vulnérabilités les plus courantes et les plus dangereuses, nous verrons comment il est possible d'éviter les affres des biais cognitifs et organisationnels.

1. BIAIS COGNITIFS VS. SÉCURITÉ : 1-0

Fin juin 2017, quelque part en Europe, au sein du CERT/SOC d'une grande entreprise : depuis mai, toutes les équipes sécurité sont sur les dents : WannaCry, puis NotPetya ont déjà fait des ravages. Rançongiciel, *wiper* déguisé en rançongiciel, les deux logiciels malveillants se propagent via SMB en utilisant EternalBlue, un exploit développé par la NSA et révélé par le mystérieux groupe Shadow Brokers en avril 2017. Un matin, des analystes du CERT/SOC identifient un flux SMB entrant, jamais vu auparavant. Le branle-bas de combat est déclenché et en quelques heures des mesures de fermeture de flux drastiques et handicapantes sont mises en œuvre. Pour rien. L'entreprise n'était pas attaquée, il s'agissait simplement d'un flux légitime qui n'avait jamais été répertorié.

Que s'est-il passé ?

Le CERT/SOC a simplement commis une erreur de raisonnement et a ensuite déroulé, sans s'en rendre compte. En l'occurrence, l'erreur était : nous avons un lien de cause à conséquence du type : si A, alors B (si EternalBlue, alors il y a du SMB). On constate B (flux SMB). Alors on en déduit – c'est l'erreur – que A est vrai (présence d'EternalBlue).

2. BIAIS COGNITIFS VS. SÉCURITÉ : 2-0

20 avril 2010, plateforme pétrolière Deepwater Horizon, golfe du Mexique : une explosion puis un incendie dévastent la plateforme, entraînant la mort de onze personnes et une immense marée noire.

Que s'est-il passé ?

Comme toujours, les causes sont multiples : erreurs humaines, dysfonctionnements techniques... Mais les équipes avaient aussi désactivé les alarmes générales qui avaient tendance à se déclencher intempestivement (à cause de bugs, virus, écrans bleus à répétition sur un Windows NT...), sans résoudre la cause de ces fausses alertes – malgré le travail acharné de certains techniciens qui ont essayé de rétablir le bon fonctionnement du système jusqu'au bout. La compagnie (BP), elle, avait les yeux rivés sur la production. L'équipage a peu à peu oublié l'importance de ces alarmes, et ils se sont habitués à vivre avec ce risque. Ils ont normalisé le danger et n'ont pas pu évacuer à temps lorsque l'accident est arrivé **[1]**.

3. UNE MÉTHODE

Ces deux expériences illustrent la difficulté de fiabiliser les décisions sécurité. Il est en effet impossible – ou très difficile – de définir des modèles déterministes en matière de sécurité (essentiellement parce que sa matière première est l'incertitude, l'imprévu, d'où découle la difficulté à évaluer le nombre et la nature des facteurs défavorables). La conséquence est que ces décisions dépendent énormément des choix humains. Or la rationalité de la pensée humaine et des comportements collectifs est limitée, souvent défaillante, et ne peut pas non plus être modélisée.

Dès lors se pose une question : comment fiabiliser les décisions sécurité qu'il est nécessaire de prendre au cours et à la suite d'un incident majeur ou d'une crise ?

Il faut des hommes et des femmes de sang froid, des experts, des plans et procédures de secours, il faut être préparé, avoir fait des exercices, il faut une bonne communication, avoir en tête ce qu'ont fait les pairs...

DE L'IMPORTANCE DE LA MIXITÉ POUR BIEN PENSER…
Étude parue dans *Science* en 2010

Extrait : ***« Converging evidence of a general collective intelligence factor that explains a group's performance on a wide variety of tasks. This "c factor" is not strongly correlated with the average or maximum individual intelligence of group members but is correlated with the average social sensitivity of group members, the equality in distribution of conversational turn-taking, and the proportion of females in the group »*** **[2].**

Mais ces éléments ne suffisent pas quand l'urgence, l'incertitude et le stress sont à leur comble. C'est-à-dire quand les circonstances sont particulièrement favorables à l'entrée en scène de biais cognitifs.

4. BIAIS COGNITIFS ?

Ce sont des mécanismes de pensée – des traitements cognitifs – relativement systématiques qui provoquent une altération du raisonnement et du jugement tout en préservant l'apparence de la raison logique.

Citons quelques exemples pour fixer les idées :

- L'hubris : que l'on pourrait traduire en français par « orgueil démesuré », qui est un narcissisme et une excessive confiance en soi qui peuvent conduire à une surestimation de ses capacités (relativement courant dans la communauté cyber).
- Le group think : proche du biais de conformité, phénomène de groupe par lequel le désir d'harmonie ou de conformité perturbe ou rend irrationnel les processus de décision. Les membres du groupe essayent de minimiser les conflits et parviennent rapidement à prendre des décisions par consensus sans analyse critique des alternatives vite écartées et en s'isolant des influences extérieures.
- La dilution de la responsabilité : les décisions de groupe, portées par le groupe, aboutissent à des prises de risque plus élevées que les décisions portées individuellement (ce phénomène est aussi connu pour provoquer nombre d'accidents en montagne, en milieux hostiles, ou dans les bars).

Ainsi, gérer un incident majeur ou une crise consiste à gérer des situations peu ou pas modélisées en utilisant nos cerveaux et nos corps dont les comportements sont souvent erratiques, soumis à des biais cognitifs et évoluant au sein d'organisations imparfaites.

5. UNE ANALOGIE FERTILE

Ces dernières années ont vu se développer exponentiellement les « applications » accessibles par des utilisateurs et rendant d'innombrables services en matière de traitement de l'information. Il existe des centaines de langages de programmation qui permettent de développer des applications, des milliers de configurations matérielles, des centaines de milliers de personnes dans le monde possèdent les compétences pour les développer. La sécurité de ces applications est devenue un enjeu clé. Quelques statistiques sur plusieurs années de tests de sécurité réalisés par une équipe que nous avons animée montrent que plus de 60% des

vulnérabilités découvertes sont des vulnérabilités applicatives (dans le contexte d'une grande entreprise). Il existe des méthodes et des outils d'analyse des codes sources qui permettent de détecter les erreurs de programmation, et donc de limiter les vulnérabilités potentielles. Néanmoins ces analyses sont très coûteuses et peu efficaces pour déceler les erreurs fonctionnelles (c'est-à-dire les erreurs de spécification).

Au cours des premières années du siècle a vu le jour une communauté, Open Web Application Security Project (OWASP) dont les travaux sont librement accessibles, et dont la vocation est de construire et proposer des recommandations, méthodes et outils de sécurisation des applications web. Le projet qui a rapidement connu un grand succès et est aujourd'hui une référence en matière de sécurité des applications est l'« OWASP Top Ten Project » **[3]** (cette liste est référencée par nombre de standards de sécurité, comme MITRE, PCI DSS, DISA, FTC, etc.). Il a pour but d'identifier et de lister les dix risques de sécurité applicatifs web les plus critiques.

La particularité de cette liste est qu'elle n'est pas le fruit de « bonnes pratiques » ou d'avis d'experts (comme peuvent l'être les référentiels ISO), mais le résultat de l'analyse de centaines de milliers vulnérabilités effectivement découvertes chez des milliers de clients.

Dans la même logique, le Center for Internet Security publie les CIS Controls **[4]**, liste de vingt recommandations de sécurité à appliquer pour sécuriser un système d'information. S'il s'agit dans ce cas de mesures de sécurité couvrant tout le spectre de la cybersécurité, la conception de cette liste et la priorisation de ses items relèvent du même principe : elles sont le résultat de l'observation d'un panel significatif d'attaques réelles.

Le principe sous-jacent de ces deux listes est qu'en l'absence de modèle de sécurité déterministe, un élément clé – mais non suffisant – pour sécuriser une application ou un système d'information est de vérifier que les vulnérabilités les pires et les plus fréquentes sont évitées.

Par analogie, nous avons donc essayé d'énumérer les erreurs les plus fréquemment commises en matière de prise de décision, du fait de biais cognitifs ou de problèmes organisationnels, puis nous avons instancié cette liste aux situations de gestion de crise. Concrètement, cela se traduit par des questions ouvertes qui peuvent révéler, au cœur de l'action, l'émergence de biais cognitifs qui pourraient défavorablement influencer des décisions. Nous les appellerons questions de révélation.

6. PAYE TON BIAIS (CAS PRATIQUES D'APPLICATION DE LA MÉTHODE)

Rouge confirmation

Le service de sécurité opérationnelle d'une grande entreprise est divisé en deux équipes, une Blue Team et une Red Team. Régulièrement sont organisés des exercices au cours desquels les défenseurs (les bleus) essaient de détecter et caractériser les attaques lancées par les pentesters (les rouges). Un jour, un équipement de sécurité (une sonde) remonte une alerte. La Blue Team, persuadée qu'il s'agit d'une attaque dans le cadre d'un exercice, recherche dans le SIEM et les diverses autres sources de traces, les éléments qui confirmeraient qu'il s'agit d'un exercice, pendant plusieurs heures. Cette équipe a été victime d'un biais de confirmation, qui est une tendance à favoriser l'information connue ou l'idée admise et à ne pas recher-

cher, à ignorer ou à rejeter les informations et les données qui la contredisent. Nous cherchons davantage à confirmer nos idées qu'à les mettre en cause. Une question aurait pu révéler ce biais : « Des options ont-elles été rejetées sans analyse, sur la base d'un argument unique et rapidement traité ? ».

Ça imprime pô

Vendredi 5 février 2016, 10h30, banque centrale du Bangladesh. Un cadre dirigeant constate que le récapitulatif des transactions SWIFT de la veille n'a pas été imprimé. Il essaie de les sortir, sans succès. Mais il ne s'en inquiète pas outre mesure, l'imprimante dysfonctionnait régulièrement. En réalité, l'impression ne fonctionne pas, car une attaque est en cours, et l'un des 6 malwares introduits est dédié au blocage des impressions. Cette attaque, au cours de laquelle plus de 60 millions de dollars ont été dérobés, reste à ce jour le plus important cyber braquage. Le biais cognitif dont ont été victimes les équipes de la banque est la normalisation du danger, une situation où des individus ou organisations sont confrontés à des risques (initialement jugés importants – une imprimante qui sert à des contrôles importants qui dysfonctionne) suffisamment longtemps pour qu'ils deviennent la norme (et ne soient plus considérés comme exceptionnels). Les équipes auraient pu déceler un tel biais s'ils s'étaient posé la question : « Y a-t-il des risques ou des dangers qui sont acceptés « parce que nous nous y sommes habitués ? » » (probablement auraient-ils répondu : « on ne peut pas négliger les dysfonctionnements de l'imprimante qui sert à vérifier que nos paiements de la veille étaient corrects » et auraient-ils essayé de résoudre le problème, évitant ainsi de le trouver « normal » lors de l'attaque).

sudo shutdown -r now

Un incident majeur est en cours, d'origine incertaine (il n'est pas établi qu'il s'agisse d'une attaque). Une cellule de crise a été convoquée. Elle est présidée par un directeur autoritaire qui décide qu'il faut redémarrer certains serveurs en DMZ. Au moins deux personnes, présentes dans la salle, savent que cela n'a aucune chance de résoudre le problème, ni de l'élucider et encore moins d'aider à déterminer s'il s'agit d'une attaque ou non. Pire, cela peut même être contre-productif. L'un d'entre eux le dit, mais il n'est pas

écouté. Un chef de service dit : « on pourrait nous reprocher de ne pas l'avoir tenté ». La décision de redémarrer les serveurs est entérinée. Le redémarrage d'un serveur (et une bascule) ne permet aucune avancée et a coûté 45 minutes. Décision est pourtant prise de redémarrer les autres (sur d'autres liens réseau). Le biais cognitif qui s'est matérialisé dans ce cas est le biais d'engagement : un lien d'attachement entre un individu ou une organisation et son action, résultant de plusieurs types de facteurs psychologiques : calcul stratégique, crainte de « perdre » un investissement, obligation de se justifier à ses propres yeux, obligation de se justifier aux yeux d'autrui... Deux questions de révélation auraient pu permettre de sortir de cet engagement stérile : « Y a-t-il des responsables qui s'impliquent trop dans la technique, par exemple du fait de leurs anciennes fonctions techniques ? » ou « Y a-t-il des intervenants qui semblent trop impliqués émotionnellement dans la gestion de crise ? ».

Mais dans ce cas un autre biais cognitif a également joué un rôle : celui des solutions préférées. Il s'agit des options qui semblent évidentes, qui tombent sous le sens, qui sont irrésistibles, commodes, faciles à justifier. Mais pas toujours les meilleures. Et dans ce cas une question de révélation qui peut déceler certains de ces biais est : « Y a-t-il des décisions techniques qui ne sont décidées que par crainte que ne pas l'avoir fait soit reproché ultérieurement ? ».

Soyez autonomes, mais faites ce que je dis

Au cours d'un exercice, un directeur demande à l'équipe en charge de la réaction cybersécurité de lui faire un reporting toutes les 30 minutes. Dans le même temps, il exerce une pression importante (courriels, appels téléphoniques, présence physique) pour que le problème soit identifié et jugulé au plus vite et de façon autonome par le SOC (il veut que son efficacité soit vue et reconnue). Le responsable du SOC ne peut presque plus gérer son équipe et consacre l'essentiel de son temps à préparer et effectuer son reporting. Le problème auquel il est soumis est l'injonction paradoxale : un individu ou un groupe est face à une injonction paradoxale lorsqu'il doit répondre à des attentes ou des directives contradictoires et/ou impossibles à réaliser. Une question de révélation peut être : « Au cours de la gestion d'une crise, y a-t-il des demandes paradoxales (par exemple exiger que les techniciens travaillent et proposent des solutions tout en tenant compte des instructions techniques de la hiérarchie) ? ».

Je n'ai fait que mon travail...

Le cas suivant est tiré d'articles de presse. 2011 – 2012, une société française conçoit et vend à la Libye un système permettant des écoutes, surveillances et interceptions automatisées à l'échelle d'une nation. Le pays est alors une dictature dirigée par le colonel Kadhafi. Ce dernier se sert de cette solution pour repérer, persécuter et parfois exécuter des membres de l'opposition. Dans ce cas, les gens qui ont participé à la conception et à la commercialisation de ce système se sont abandonnés au renoncement éthique : les individus peuvent renoncer à formuler des jugements éthiques et moraux sur leurs actions ou celles qui les entourent, se contentant d'obéir aux instructions ou aux procédures, par exemple pour un salaire ou une progression hiérarchique. Ils cessent de penser, démissionnent, et ne se voient plus que comme un rouage qui n'a pas son mot à dire. Une question de révélation, simple, permet de mettre en lumière un tel problème – pourvu que l'on y réponde honnêtement, c'est-à-dire sans se livrer à des contorsions de justifications fallacieuses : « les décisions ou actions dans lesquelles je suis impliqué ou auxquelles j'assiste sont-elles éthiquement légitimes ? ».

7. MÉTHODOLOGIE D'UTILISATION

Dans l'étude que nous avons consacrée au sujet, nous avons identifié 22 biais cognitifs et problèmes organisationnels qui peuvent constituer des facteurs de risques significatifs pour les prises de décision en cas de gestion de crise.

À chacune de ces thématiques, nous avons associé des questions de révélation qui peuvent permettre de les identifier, et donc d'infléchir nos décisions. Il faut bien comprendre que notre méthodologie a vocation à détecter des problèmes, pas à les résoudre.

La liste exhaustive des questions de révélation se trouve dans l'étude complète **[5]**. Nous avons aussi développé une interface simpliste permettant de voir défiler les questions et, le cas échéant, de repérer le biais ou problème organisationnel auquel elles se rapportent **[6]**.

Une proportion élevée de ces questions est dédiée à relever des problèmes de fonctionnements collectifs, c'est-à-dire que ses lieux d'exercice privilégiés sont les réunions, comités, groupes de travail, cellules de crise. Mais elles pourront également être utili-

sées par des individus, sur eux-mêmes, pendant ou après leurs activités. Elles peuvent alors servir de garde-fous concernant leur propre travail, ou comme outil de vérification du travail d'autres équipes.

NOTE

22 biais cognitifs et problèmes organisationnels qui constituent des facteurs de risques humains pour les décisions sécurité :

- **rationalité limitée ;**
- **biais de confirmation ;**
- **biais de l'enaction ;**
- **histoires versus statistiques ;**
- **rôle du hasard ;**
- **fausseté des souvenirs ;**
- **non-partage de l'information ;**
- **biais de conformité ;**
- **groupthink ;**
- **faux consensus ;**
- **hubris ;**
- **biais d'engagement ;**
- **normalisation du danger ;**
- **injonctions paradoxales ;**
- **solutions préférées ;**
- **cadrage des situations ;**
- **dysfonctionnements d'équipe ;**
- **communication défaillante ;**
- **renoncement éthique ;**
- **oubli ;**
- **erreurs de raisonnement ;**
- **dilution de la responsabilité.**

Typiquement, ces questions devraient être posées de façon continue (c'est-à-dire que parvenu à la fin de la liste on la reprend au début, d'où la présentation en défilement que nous avons choisie sur notre petite application) tout au long de la gestion de crise/incident. La tâche nécessite un certain recul vis-à-vis des actions de résolutions elles-mêmes. Par exemple, en faisant l'hypothèse qu'une cellule de crise est présidée par un ou une responsable qui assume *in fine* les décisions importantes, qu'une autre personne anime la réunion, coordonne et prend des notes pour le compte-rendu, la tâche de dérouler le questionnaire devrait être dévolue à une troisième personne n'intervenant que lorsqu'il ou elle détecte un problème dans le déroulement de la gestion de crise.

CONCLUSION

Ces questions ne peuvent prétendre à l'exhaustivité. Comme les méthodologies de l'OWASP ou des CIS Controls. Il faut les considérer comme des tamis. Selon la précision des questions, l'expérience et l'expertise de celui qui les pose, elles peuvent permettre d'identifier des biais courants, mais qui s'expriment toujours de façon particulière.

Et tout comme ces méthodes, ils ne deviendront efficaces que polis par la confrontation avec la réalité. Leur pratique seule permettra d'affiner les questions, d'en réduire le nombre ou d'ajouter des catégories importantes de risques humains.

Afin de compléter l'efficacité de ces questions, il pourra s'avérer utile d'ajouter des questions « positives », c'est-à-dire ne visant pas à identifier des problèmes connus, mais à souligner des divergences avec certaines pratiques validées par l'expérience.

Un approfondissement de la méthode devra également affiner les aspects temporels : comment déterminer le bon moment pour prendre une décision sécurité ? Comment éviter que les précautions prises – pour éviter de mauvaises décisions – ne finissent pas elles-mêmes par détériorer le processus de décision, en le retardant ?

Enfin, soulignons qu'au début de l'élaboration de cette méthode nous avions à l'esprit de la compléter par des recommandations qui viendraient d'une certaine façon répondre aux questions soulevées. Il est apparu après quelques essais que l'utilité de la méthode en aurait été diminuée. En effet, si des recommandations étaient formalisées, elles seraient soit trop génériques et donc peu utiles, soit précises, mais peu adaptées aux situations particulières. De plus, des recommandations auraient probablement l'inconvénient de pousser les utilisateurs de la méthode à directement consulter « la solution », la recommandation. Or l'intérêt principal de la méthode est de soulever des questions. De pousser à la réflexion. D'inciter au doute. Charge à ceux qui l'utilisent d'apporter les réponses adaptées à leur contexte. Ainsi ouverte, cette méthode n'est donc pas un outil d'aide à la décision sécurité, mais bien plutôt un outil d'aide à la « non prise » de mauvaises décisions. ▌

RÉFÉRENCES

[1] **http://techrights.org/2010/10/12/deepwater-update/**

[2] **http://www.chabris.com/Woolley2010a.pdf**

[3] **https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project**

[4] **https://www.cisecurity.org/controls**

[5] **https://cryptosec.org/?Securisation-de-la-securite**

[6] **https://www.cryptosec.org/biais**