International Cybersecurity Forum

SECURITY AND PRIVACY BY DESIGN

Europe kicks off !

Lille Grand Palais

22nd and 23rd January 2019

Biais cognitifs et organisationnels : comment ~~rater~~ réussir sa sécurité (enfin, essayer)

forum-fic.com

whoami

Inti Rossenbach
Expert et manager en cybersécurité depuis le siècle dernier
www.cryptosec.org | @secucrypt

Remerciements & Avertissement

Yannick Meiller
ESCP Europe

Stéphane Calé
Commission « cyber » du CDSE

Avertissement
Mes propos n’engagent que moi et en aucun cas mon employeur
Les exemples que je cite ne sont pas issus de mon employeur actuel

Biais vs. Sécurité : 1 – 0

Mai - juin 2017, attaques WannaCry et NotPetya

EternalBlue, exploit développé par la NSA et révélé par le groupe Shadow Brokers en avril 2017

EternalBlue génère du trafic SMB

Au sein d’un SOC, quelques mois plus tard, découverte de trafic entrant SMB

Les analystes en déduisent qu’une attaque similaire est en cours

Alors ?

Biais vs. Sécurité : 1 – 0

Que s’est-il passé ?

> Erreur de raisonnement

Dans ce cas :

On sait que si A, alors B.

B arrive.

Déduction: alors c’est que A

Biais vs. Sécurité : 2 – 0

Deepwater Horizon, golfe du Mexique
La plateforme explose le 20 avril 2010

L’alarme générale automatique avait été désactivée pour éviter que des fausses alertes ne réveillent l’équipage et n’altèrent la productivité

Elle n’est activée qu’après l’explosion

11 morts, immense marée noire

Biais vs. Sécurité : 2 – 0

Que s’est-il passé ?

Causes multiples : alarmes défectueuses, erreurs humaines, dysfonctionnements techniques, etc.

Mais dans ce cas, ils se sont aussi habitués au « confort » de l’alarme générale désactivée, sans résoudre le problème. Et ils ont oublié, normalisé le risque...

> Normalisation du danger

Alors, **comment bien gérer un incident, une crise** ?

> Il faut des hommes de sang-froid

> Des experts

> Des plans et procédures de secours

> Il faut être préparé, exercé

> Une bonne communication…

C’est tout?

Alors, **comment bien gérer un incident, une crise** ?

> Il faut des **hommes** de s

> Des experts

> Des plans et procédures

> Il faut être préparé, exerc

> Une bonne communication…

Il faut des **femmes**!
Parce que c'est juste
Parce que c'est efficace

Étude parue dans Science en 2010

Abstract : « 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** »

http://www.chabris.com/Woolley2010a.pdf

Mais si la parité est redoutablement efficace, les biais cognitifs sont unisexe…

Comment éviter que des biais cognitifs ou organisationnels n'impactent la sécurité ?

Travail de recherche effectué dans le cadre de la formation « Sécurité / Sûreté et management » de l'ESCP Europe

www.cryptosec.org/docs/Memoire2017/Memoire_SecEmpiriqueSecu_v4.pdf

Quelle fiabilité des prises de décisions sécurité ?

Reposent souvent sur:
- Avis d'experts
- De fournisseurs
- Évaluations comparative (*benchmark*)
- Echanges avec les pairs

Relativement **inefficace** dans le cas de la **gestion de crise**

Comment améliorer la fiabilité des décisions sécurité ?
Évaluer les risques en situation de stress et d'incertitude?
Comment décider s'il faut réduire ou éviter des risques ?
Comment organiser la réaction à la matérialisation d'un risque ?

Objectif

Établir une méthodologie qui aide à
fiabiliser les décisions sécurité

L’étude complète porte sur trois domaines :

- analyse de risques
- définition de mesures de sécurité
- gestion de crise

Théorie

L’impossibilité ou la difficulté à établir des **modèles déterministes** pour gérer les risques a pour conséquence que cette activité dépend énormément des **décisions humaines**

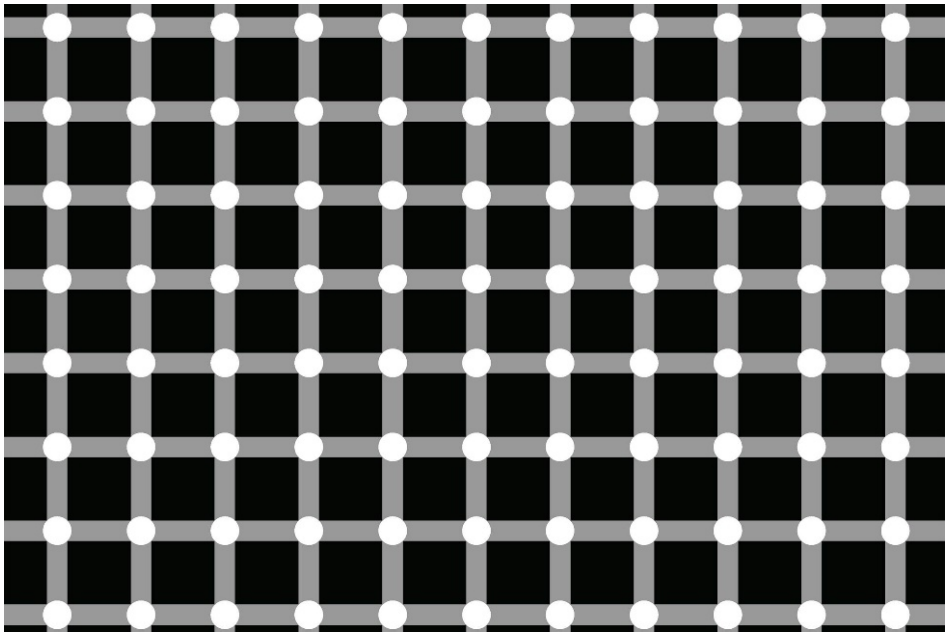
La rationalité de la pensée humaine et des comportements collectifs est limitée et ne peut être modélisée

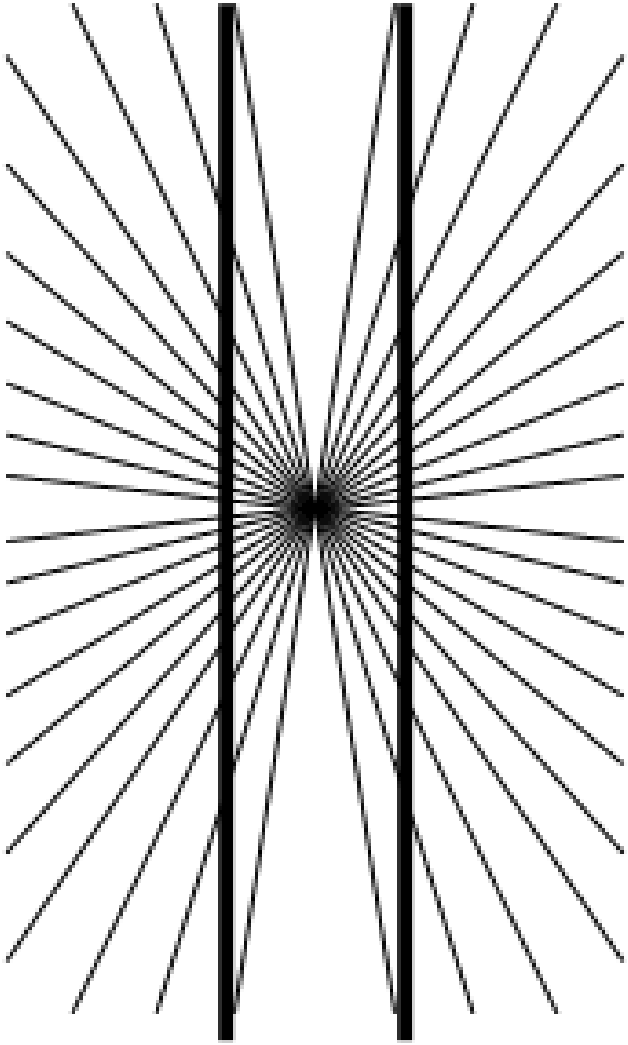
Mais il existe de nombreux travaux sur la psychologie, le management et la réaction des organisations humaines

Ainsi que des descriptions de cas d’incidents, de crises, de désastres

Théorie

Biais cognitif ?





Théorie

Biais cognitif ?

Un biais cognitif est un **mécanisme** de pensée – un traitement cognitif – relativement systématique qui provoque une **altération du raisonnement** et du jugement tout en préservant l’apparence de la raison logique

Théorie

Nous devons ainsi gérer des situations **peu ou pas modélisées** en utilisant nos cerveaux et nos corps dont les comportements sont souvent **erratiques,** soumis à biais cognitifs et des organisations imparfaites

Une analogie fertile

Open Web Application Security Project (OWASP)
Projet *open source* : recommandations, méthodes et outils pour améliorer la sécurité des applications

A1:2017-Injection
A2:2017-Broken Authentication
A3:2017-Sensitive Data Exposure
A4:2017-XML External Entities (XXE)
A5:2017-Broken Access Control
A6:2017-Security Misconfiguration
A7:2017-Cross-Site Scripting (XSS)
A8:2017-Insecure Deserialization
A9:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging&Monitoring

Une analogie fertile - OWASP

Exemples

Top 10-2017 A1-Injection
http://www.cryptosec.org/app/accountView?id=' or '1'='1

Top 10-2017
A2-Broken Authentication
Has missing or ineffective
multi-factor authentication

Une analogie fertile - OWASP

OWASP n’est pas le résultat de « bonnes pratiques » d’origine indéterminée, ou d’avis d’experts

Résulte de l’analyse de centaines de milliers de vulnérabilités effectivement découvertes chez des milliers de clients

Autre référentiel similaire :
CIS Controls
du Center for Internet Security
(ex SANS Top 20)

Une analogie fertile - OWASP

Principe

Vu les coûts des audits de code et leur piètre efficacité pour détecter les vulnérabilités fonctionnelles ou de configuration

une approche efficace pour améliorer la sécurité d’un système ou d’une application est **d’éliminer les vulnérabilités les plus dangereuses et les plus fréquentes**

Une analogie fertile - OWASP

Par **analogie**

lister les **biais cognitifs**, **problèmes organisationnels** et **erreurs communément commises** lors des prises de décision en situation de crise

Puis essayer de trouver des questions qui permettent de les mettre en lumière lorsqu'ils adviennent

Au lieu de chercher à optimiser les décisions (trouver les meilleures), **éviter les mauvaises**.
Les checklists sont adaptées

Paye ton biais
(cas pratiques)

Cas 1

Une organisation mène un exercice de *redteaming*

Suite à une première détection, l’équipe en charge de la détection / réaction recherche en priorité dans le SIEM les éléments qui confirment qu’il s’agit d’un exercice

Cas 1

> Biais de confirmation

Tendance à favoriser l’information connue ou l’idée admise et à ne pas rechercher, à ignorer ou à rejeter les informations et les données qui la contredisent. Nous cherchons à confirmer nos idées, plus qu’à les remettre en question

Cas 1

Biais de confirmation

Question de révélation
Des options ont-elles été rejetées sans analyse, sur la base d’un argument unique et rapidement traité?

Cas 2

Vendredi 5 février 2016, 10h30, dans une banque

Un cadre dirigeant constate que le récapitulatif des transactions SWIFT de la veille n’a pas été imprimé

Il essaie de les imprimer, sans succès
L’imprimante a déjà dysfonctionné dans le passé, il ne s’inquiète pas

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

Cas 2

> Normalisation du danger

Situation où des individus ou organisations sont confrontés à des risques (initialement jugés importants) suffisamment longtemps pour qu'ils deviennent la norme (et ne soient plus considérés comme exceptionnels)

Cas 2

Normalisation du danger

Question de révélation

Y a-t-il des risques ou des dangers qui sont acceptés « parce que nous nous y sommes habitués » ?

Cas 3

Un incident majeur est en cours, d’origine incertaine (pas certain 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

Au moins deux personnes dans la salle savent que cela n’a aucune chance de résoudre le problème (et peut être contreproductif)

Cas 3

L’un d’entre eux le dit, mais il n’est pas écouté

Quelqu’un dit: « on pourrait nous reprocher de ne pas l’avoir tenté »

La décision de redémarrer les serveurs est confirmée

Le redémarrage d’un serveur ne permet aucune avancée et a coûté 45 mn

Décision est pourtant prise de redémarrer les autres

Cas 3

> Biais d’engagement

Lien d’attachement entre un individu ou une organisation et son action, résultant de plusieurs types de facteurs psychologiques : calcul stratégique, « coûts perdus », obligation de se justifier à ses propres yeux, obligation de se justifier aux yeux d’autrui

Cas 3

Biais d’engagement

Questions de révélation

Y a-t-il des responsables qui s’impliquent trop dans la technique du fait de leurs anciennes fonctions techniques ?

Y a-t-il des intervenants qui semblent trop impliqués émotionnellement dans la gestion de crise ?

Cas 3

Ou il peut s’agir du biais **des solutions préférées**

Il s’agit de celles qui sont ou semblent :
- Évidentes, qui tombent « sous le sens »
- Irrésistibles
- Commodes
- Disponibles, validées ou expérimentées par d’autres
- Faciles à justifier

Question de révélation
Y a-t-il des décisions techniques qui ne sont décidées que par crainte que ne pas l’avoir fait soit reproché ultérieurement ?

Cas 4

Au cours d’un exercice, le responsable 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 verbale importante pour que le problème soit identifié et jugulé **au plus vite** et de façon **autonome par le SOC**

Le responsable du SOC ne peut presque plus gérer son équipe et consacre l’essentiel de son temps à préparer et effectuer son reporting

(Dessin: Philippe Geluck)

Cas 4

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.

Question de révélation

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 d'instructions techniques de la hiérarchie) ?

Cas 5

2011 – 2012, une société française vend un système qu’elle a conçu, permettant des écoutes, surveillances et interceptions automatisées à l'échelle d'une nation à la Libye, dictature alors dirigée par le colonel Kadhafi

Cas 5

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. Ils cessent de penser, démissionnent et ne se voient plus que comme un rouage qui n'a pas son mot à dire

Question de révélation

Les décisions ou actions dans lesquelles **je** suis impliqué ou auxquelles **j'assiste** sont-elles éthiquement légitimes ?

Cas 6

Mars 2013, la chaîne de supermarchés Target est victime d'une fuite de données majeure : 40 millions de cartes et informations personnelles de plus de 110 millions de clients

L'équipe de sécurité à Bangalore a détecté l'attaque et contacté le siège à Minneapolis

Mais l'alerte a été négligée

Cas 6

> Dysfonctionnements d’équipe

Et plus précisément il s’agit dans ce cas d’un problème de **communication** (qui aurait pu être révélé au cours d’un exercice – pourvu qu’il ait été suffisamment réaliste)

Question de révélation

(par exemple au cours d’un exercice)
La communication au sein de l’équipe est-elle défaillante ?

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

Rationalité limitée
Biais de confirmation
Biais de *l'énaction*
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

À chacun nous associons une liste de **questions de révélation**

Un outil !

Présentation de l’ébauche d’outil que j’ai développé lorsque j’ai su que je venais au FIC

www.cryptosec.org/biais

Utilisation:

- sur grand écran
- chacun sur son écran
- une personne en charge...

La méthode doit être **polie** par son utilisation

En situation réélle, mais surtout en **exercice**

Autre axe de développement, considérer les aspects **temporels:**

- Moment adéquat pour prendre une décision sécurité ?

- Éviter que les précautions prises (pour éviter de mauvaises décisions) ne retardent trop le processus de décision ?

- Prendre en compte l'évolution des risques (probabilités et menaces) avec le temps ?

Conclusion

Le principal intérêt de la méthode est de poser des questions

Inviter à la **réflexion**

Se poser des questions

Les réponses dépendront toujours de qui sera en charge et du contexte

Ainsi, ce n’est pas un outil d’aide à la prise de bonnes décisions sécurité, mais un **outil qui peut aider à ne pas prendre de mauvaises décisions**

¡ Merci !

www.cryptosec.org/docs/Memoire2017/
Memoire_SecEmpiriqueSecu_v4.pdf

www.cryptosec.org

@secucrypt