OPRISKO.ch

Observatoire des Risques Opérationnels

Cybercriminalité

perception du risque pour des entreprises suisses et motivations des hackers

Cyrille Reynard

Operational Risk Observatory

OpRiskO

15.09.2017 SwissMadeSecurity

Oprisko.ch – c.reynard@oprisko.ch

OPRISKO.ch

Observatoire des Risques Opérationnels

OBJECTIFS DE L'ÉTUDE MENEE PAR

L'OBSERVATOIRE DES RISQUES OPÉRATIONNELS

- **Définir** « la cybercriminalité ».
- **Comprendre qui sont les hackers**, leurs motivations, comment sont sélectionnées les entreprises ciblées par des attaques ainsi que le mode opératoire des attaquants.
- **Comprendre les principaux risques** pour les organisations, les menaces actuelles et mesures de défense.
- **Rôle attendu de l'état** du point de vue de l'entreprise.

OPRISKO.ch

Observatoire des Risques Opérationnels

MÉTHODOLOGIE DE RECHERCHE ET POPULATION SONDÉE

- Définition du sujet 2017 d'intérêt public : **cybercriminalité**
- Méthode de recherche encadrée par du personnel académique et enquête de terrain menée par Oprisko.
- Méthodologie qualitative de recherche par interviews.
- Distribution de 2 types de questionnaires :
  1 pour les entreprise / 1 pour les hackers.
- 26 entreprises suisses et 7 hackers sondés.
- Codage et analyse des données qualitatives.
- Rédaction d'un rapport (en cours d'élaboration).

OPRISKO.ch

Observatoire des Risques Opérationnels

Cybercriminalité - Contexte

- **Marché de plus de USD 445 milliard de profits illégaux**.

- Supérieur au produit intérieur brut de UAE ou Irlande, ou Finlande. (Caleb Barlow,2016)

OPRISKO.ch

Observatoire des Risques Opérationnels

DEFINITION DE LA CYBERCRIMINALITE

Selon nos répondants :

i. « Ensemble des agissements malveillants commis à l'aide de moyens informatiques et d'un réseau de télécommunication. »

ii. Un répondant hacker liste les infractions commises à l'aide d'un ordinateur :

« Accès non autorisé aux systèmes d'information et aux réseaux, vol, revente de comptes et d'informations personnelles, espionnage industriel et blanchiment d'argent. »

iii. Le secteur industriel spécifie le type d'infraction : vol de propriété intellectuelle, espionnage industriel, sabotage.

OPRISKO.ch

Observatoire des Risques Opérationnels

DEFINITION DU HACKER

Epistémologie :
A l'origine, un hacker manipule un instrument informatique avec génie pour résoudre des problèmes à l'aide de cet outil. (JH. Morin)

« *une personne qui, par jeu, goût du défi ou souci de notoriété, cherche à contourner les protections d'un logiciel, à s'introduire frauduleusement dans un système ou un réseau informatique* ». (Larousse)

Le hacker **s'auto-définit** comme « quelqu'un de curieux qui souhaite connaître le fonctionnement des systèmes en général, afin d'en comprendre les rouages et in fine de les maîtriser ». Nombre de nos répondants pensent que le hacker est avant tout quelqu'un de passionné.

OPRISKO.ch

Observatoire des Risques Opérationnels

MOTIVATIONS DU HACKER

Selon nos répondants :

a) Hacker white hat

Les hackers interviewés pensent que les « white hats » **sont curieux, aiment comprendre les systèmes, bricoler, détourner des produits,** services, ou systèmes de leur usage premier et mettent à profit leurs compétences au service de l'industrie.

b) Hacker black hat

Ceux qui violent les systèmes d'information, avec ou sans avantage personnel. Ils sont rassemblés sur le «mauvais» côté, traversant la ligne de démarcation claire entre «l'amour pour le piratage» et l'exécution délibérée des actions criminelles. Pour ces acteurs, il est normal de violer un système d'information et de le pénétrer son méandre le plus secret, en volant des informations et, compte tenu du profil de leur pirate informatique, les revendre.

OPRISKO.ch

Observatoire des Risques Opérationnels

COMMENT UN WHITE HAT DEVIENT BLACK HAT

Have your motivations for hacking ever changed over time?

« At the very beginning it was all about curiosity and learning. Then I decided to step forward into the real world, where people pay you money because they don't know how to play as I do. Right now it's just money. People can hire me, I do the job, get the money, and disappear»

What is your main aspiration ?

"Stop working in 2 or 3 years, retiring, giving money to my family, buy my own house."

- Propos recueillis par Raoul Chiesa en coordination avec

OPRISKO.ch

Observatoire des Risques Opérationnels

QUI SONT LES HACKERS ?

unicri
United Nations
Interregional Crime and Justice
Research Institute

Profil des hackers selon UNICRI :
96% d'hommes

Niveau d'éducation:
40% université
29% maturité

Age:
80% ont <30 ans

Personnalité:
Curieux
Heureux
Paresseux
Passionné

OPRISKO.ch

Observatoire des Risques Opérationnels

COMMENT SONT DÉSIGNÉES LES ENTREPRISES ATTAQUÉES ?

«Je vais faire une réponse simple à cette question : souvent par hasard.»

«Ce n'est pas forcement simple d'attaquer directement une entreprise. Il existe 3 façons pour qu'une entreprise soit attaquée :

i. À cause d'une faille informatique (serveur ou ordinateur non mis à jour par exemple) ou humaine (mot de passe non sécurisé). Attaque directe. **Rare.**

ii. Parce qu'un espion informatique (troyen) a été intentionnellement installé par quelqu'un qui a eu accès au réseau interne de l'entreprise. Attaque directe. **Très Rare**.

iii. Parce qu'au moins un ordinateur de l'entreprise a été victime d'un malware (ou certain type de virus, ou Troyens) à large spectre. **C'est le plus courant des cas**.»

OPRISKO.ch

Observatoire des Risques Opérationnels

BUDGET DES ENTREPRISES FACE A LA CYBERCRIMINALITE

- Les entreprises relèvent que la cybercriminalité est sous-estimée, ou que le risque est accepté car peu investissent réellement. Certains suggèrent de se doter de ressources externes pour gérer le risque cyber.

- « cela n'est pas pris au sérieux donc peu, voire pas de budget, les entreprises ne veulent pas investir continuellement dans les technologies car elle évolue vite » « organizations are not investing enough money, thus most of their measures are at the basic level »

Nos entreprises interviewées pensent :

i. Que la problématique cyber est un risque IT et non un risque d'entreprise.

ii. Que seules les entreprises d'envergure ont déployé des moyens pour se prémunir de la cybercriminalité.

iii. Que le risque cyber est en augmentation. Les menaces se complexifient et ne sont pas prises au sérieux par les PME.

OPRISKO.ch

Observatoire des Risques Opérationnels

EVOLUTION PROBABLE DU RISQUE CYBER POUR LES ENTREPRISES 2/2

Une personne interviewée déclare :

«Le risque va clairement augmenter dans les banques. Il fait référence à une étude qui dit que les banques sont 300 fois plus ciblées que les autres entreprises. Il pense qu'au niveau bancaire il s'agit en tout premier lieu protéger le trafic des paiements, et améliorer les moyens de détection pour réagir vite à une attaque.»

Avec la disparition du secret bancaire, les données des clients privés sont maintenant moins intéressantes. Par contre, avec la banque numérique ce qui est attrayant maintenant c'est les applications bancaires pour détourner de l'argent.

OPRISKO.ch

Observatoire des Risques Opérationnels

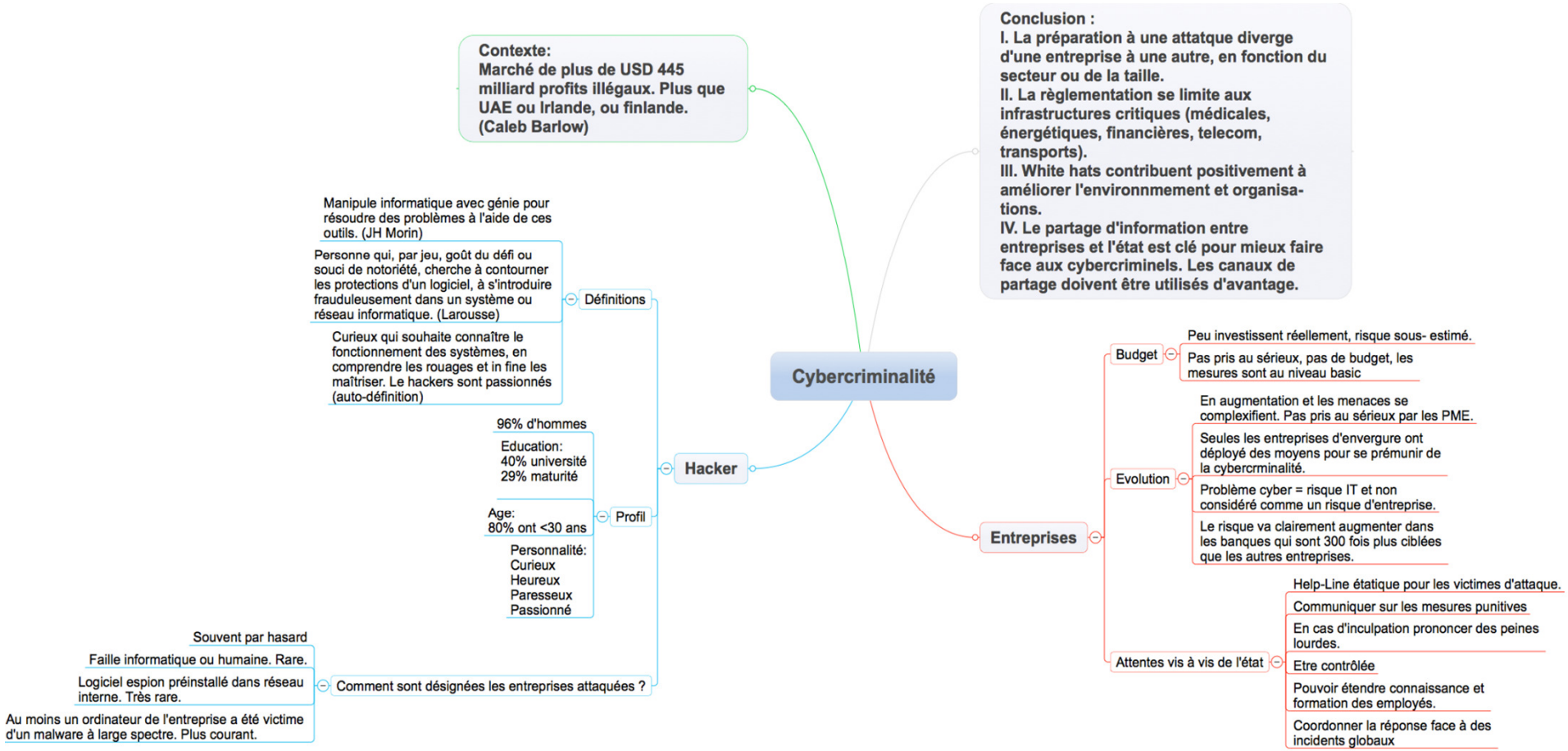
ATTENTES DES ENTREPRISES SONDÉES VIS-À-VIS DE L'ETAT.

- Communiquer sur les mesures punitives.
- Mise en place d'une help-line étatique pour les entreprises victimes d'attaques.
- En cas d'inculpation, prononcer des peines lourdes.
- Etre contrôlée : exemple des contrôles d'hygiène dans les restaurants, chaque entreprise devrait pouvoir démontrer un programme cybercriminalité.
- Etendre les compétences des employés : définir une politique de formation étatique.
- Coordonner la réponse face à des incidents globaux.

OPRISKO.ch

Observatoire des Risques Opérationnels

Synthèse étude Cybercriminalité



OPRISKO.ch

Observatoire des Risques Opérationnels

Conclusion Cybercriminalité

- L'état de préparation à une attaque diverge d'une entreprise à une autre, en fonction du secteur ou de la taille.

- La réglementation se limite aux infrastructures critiques (médicales, financières, énergétiques, de télécommunications, transports) et impose des obligations en matière de contrôles de sécurité et de notification d'incidents.

- Les hackers "white hat" contribuent positivement à améliorer l'environnement en décelant des failles dans les organisations et les systèmes.

- Le partage d'information entre les entreprises et l'Etat est clé pour mieux faire face aux cybercriminels. Les canaux de partage d'information doivent être utilisés d'avantage.

OPRISKO.ch

Observatoire des Risques Opérationnels

Merci pour votre attention et

- Aux sponsors.
- Enrico Vigano et Raoul Diez.
- Les membres d'Oprisko qui ont contribués activement à cette présentation et qui participent aujourd'hui à cet évènement.
- Le professeur Fragnière pour avoir validé la recherche d'Oprisko.
- Le professeur Jean-Henry Morin pour avoir apporté un regard critique sur cette présentation.

Oprisko.ch accueille avec plaisir de nouveaux membres (actifs, passifs, étudiants)