KPMG

Faire face aux nouvelles menaces en cybersécurité

Octobre 2017

Avec vous aujourd'hui

Jean-Francois Allard
Associé
Gestion des risques
KPMG au Canada
jeanfrancoisallard@kpmg.ca
514-840-2645

Ordre du jour:

1. Évolution de la Cyber Criminalité
2. Les attentes du Conseil d’administration

Évolution de la Cyber Criminalité

Définition

Qu’est-ce que la cybercriminalité ?

Selon la Gendarmerie Royale du Canada, elle se divise en deux types :

La cible est la technologie

- Piratage à des fins criminelles - ex. autoriser des transactions frauduleuses
- Réseaux zombies et installation de logiciels malveillants (malware)
- Dénis de services distribués (Ddos)
- Rançonnage

La technologie est l’instrument

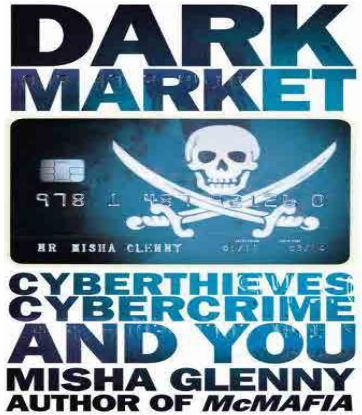
- Le vol et la fraude
- Le vol d’identité
- La violation de propriété intellectuelle
- Le blanchiment d’argent
- Le trafic de drogues
- La traite de personnes
- La cyber intimidation

Mise en contexte

Pourquoi y a-t-il recrudescence de la cybercriminalité?

Essentiellement cinq phénomènes sont responsables :

1. Digitalisation de l'économie
2. Dépendance importante aux infrastructures TI critiques
3. Habilité accrue des jeunes avec les TI
4. Apparition en 2010 d'un protocole de communication appelé « TOR » et anonymisation des échanges sur Internet
5. Apparition des marchés noirs électroniques « Dark Market »



Qui sont les acteurs ?

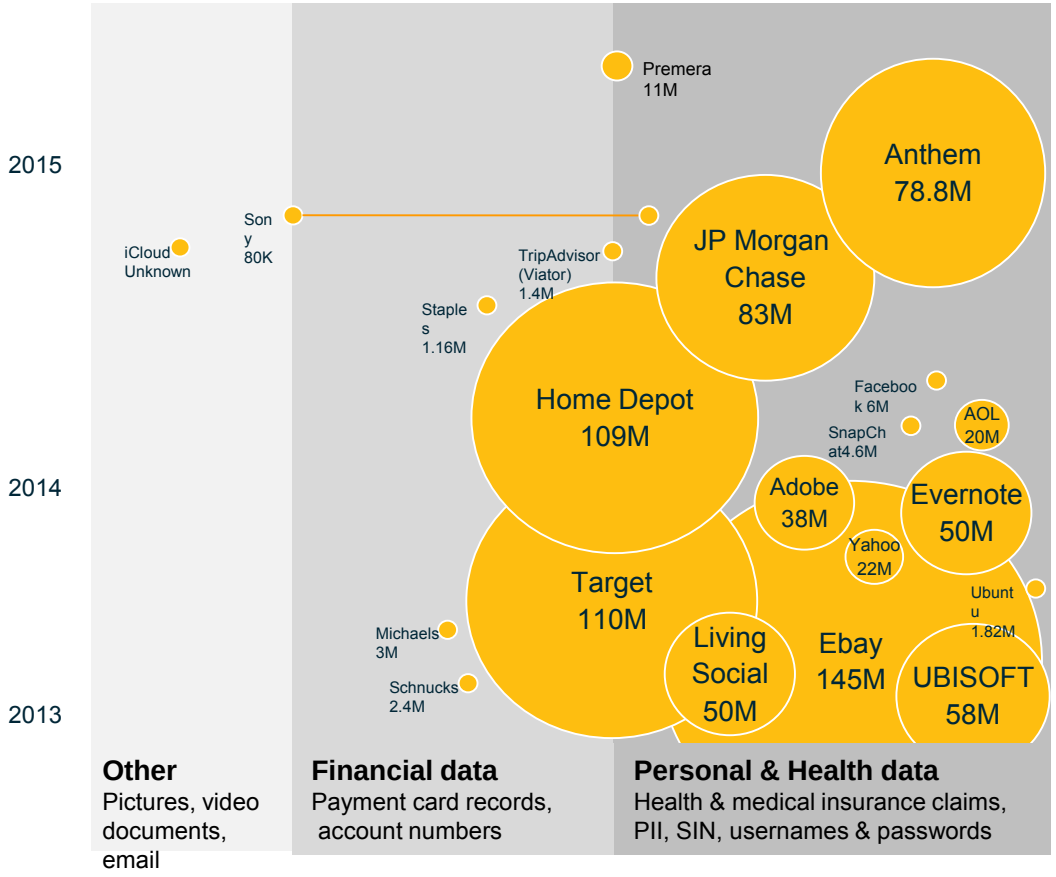
Petits criminels / Motifs: Gains financiers

Hacktivists / Motifs: Support politique

Crime organisé / Motifs: Gains financiers

États/ Motifs: Agenda politique

Cybersécurité | Sélection d'incidents



Top data breaches 2013 – Present

The number of breached records per recognized company by data type (>1M records)

References:

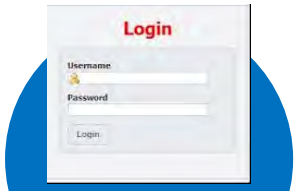
-http://blogs.wsj.com/corporate-intelligence/2014/03/28/whats-more-valuable-a-stolen-twitter-account-or-a-stolen-credit-card/

http://blogs.wsj.com/riskandcompliance/2013/06/26/passwords-more-valuable-than-credit-card-data/

http://www.foxbusiness.com/technology/2014/01/15/e-bazaar-crooks-hawk-your-info-in-online-black-market/

Combien vaut votre identité sur Internet ?

Prix en USD de données volées dans les marchés au noir



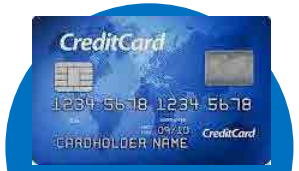
Username / Passwords
$5.60

Debit Card (#)
$9.55

Health Record / SSN
$47.62

Loyalty Rewards
$.50 for 50k points

Social Media
$.05 - $8.00



Credit Card (#)
$.25 - $100

References:
- http://blogs.wsj.com/corporate-intelligence/2015/03/28/whats-more-valuable-a-stolen-twitter-account-or-a-stolen-credit-card/
- http://blogs.wsj.com/riskandcompliance/2013/06/26/passwords-more-valuable-than-credit-card-data/
- http://www.tripwire.com/state-of-security/vulnerability-management/how-stolen-target-credit-cards-are-used-on-the-black-market/
- http://www.foxbusiness.com/technology/2015/01/15/e-bazaar-crooks-hawk-your-info-in-online-black-market/
- http://www.theregister.co.uk/2015/11/05/hilton_honor_cards_breached/

Attentes du Conseil d'Administration en cybersécurité

Attentes du Conseil d'Administration

Le rôle du Conseil d'Administration est essentiel pour l'efficacité de la cybersécurité :

- Obtenir et être d'accord avec les réponses aux trois questions fondamentales relatives à la cybersécurité :
  1. Où en sommes-nous?
  2. Où voulons-nous être (votre position de défense)?
  3. Comment pouvons-nous y arriver?
- Ceci ne devrait pas être un débat sur la cybersécurité, mais plutôt une discussion d'affaires sur la protection des actifs de l'entreprise.
- Comprendre la valeur des divers sous-ensembles de données, et s'assurer que les ressources appropriées sont consacrées à la classification et à la sécurisation des actifs les plus critiques.
- S'assurer que la cybersécurité est un sujet d'actualité et le diviser en trois éléments: Information, Action, Décision.
- S'assurer de l'obtention régulière des informations de gestion et indicateurs de performance de la sécurité et les analyses adéquatement.
- Demander des rapports d'incidents de cybersécurité régulièrement afin de surveiller les attaques et les tendances.
- S'assurer que tous les membres du Conseil sont conscients qu'ils font partie du risque.
- Être un participant actif dans le plan de réponse aux incidents de cybersécurité de votre entreprise.
- Effectuer des évaluations périodiques de risques de cybersécurité et examiner la nécessité d'une évaluation indépendante des risques.
- Finalement, si un cyber-risque est soulevé, atténuer ou accepter le risque; **ne pas l'ignorer**.

KPMG

Questions

kpmg.ca/cyber