Cyber menaces et cyber assurances à l'épreuve de la crise Covid 19

Yann TONNELLIER– ANSSI
Jean BAYON de la TOUR – MARSH
Philippe COTELLE – AIRBUS/AMRAE

Agenda

- Gestion du risque cyber durant la Crise COVID
  - Enjeux
  - Impacts mesurés actuellement
- Etat de la Menace
  - Dimension technique
  - Garantie assurantielle
- La sortie de crise
  - Preparation et risk management
  - Renouvellement des couvertures assurance cyber

Gestion de la crise

- Les entreprises ont fait face à des enjeux potentiellement contradictoires:
  - Déployer le plus rapidement possible des ressources, des outils et des moyens pour permettre le télétravail du personnel et préserver l'avenir de l'entreprise
  - Maintenir les règles de sécurité pour préserver l'entreprise

Quel impact aujourd'hui?

- 40%-50% des personnels en tele travail
- 50% d'augmentation du trafic des données
- 30% d'augmentation sur les lignes fixes

Trafic mixte : usages professionnels
mais aussi souvent pour des usages personnels

Un test de resilience !

Vraies opportunitées pour les hackers

- +30% attaques DDos
- +667% campagnes phishing en février
- +80% augmentation des demandes d’assistance sur “cybermalveillance.gouv.fr”
- Mais pas pour l’instant de brèches majeures ou pertes sérieuses déclarées

Tous les risques sont présents

- Piratage de comptes professionnels de messagerie ou d'accès aux systèmes d'information de l'organisation
- Pertes d'exploitation, perte de données
- Atteinte à l'activité et à l'image de l'entreprise ou de l'organisation
- Fraude

Sinistralité en cyber assurance

- Faible augmentation de la sinistralité
- Quelques pistes pour l'expliquer :
  - Phishing est plutôt une problématique qui relèvent de polices Fraude (qui sont complémentaires aux polices cyber)
  - Grands groupes: gèrent bien cette fréquence (sous franchise donc)
  - PME (les principales victimes)
    - peu assurées en cyber assurance
    - gèrent d'autres priorités / déclareront plus tard (nous avons des déclarations 3 mois après l'incident chez les PME)
  - Préparation des sinistres futurs?

Etat de la menace

Observation lié à la crise

- ❖ Une sollicitation accentuée des sites internet d'équipements de protection (masques) et les produits pharmaceutiques
- ❖ Une position de faiblesse des citoyens et entreprises

- ➢ Augmentation du nombre d'acteurs de la menace
- ➢ Majoritairement cybercriminel à des fins financiers

Modes opératoires observés

- Vague de courriers électroniques non sollicités
- Spearphishing* et les attaques par "Point d'eau**"
- Applications Android
- Ramsomwares utilisant le covid-19 comme leurre

* Courrier électronique ciblé contenant une charge malveillante ou un lien malveillant
** compromission de sites légitime à des fins de collecte d'informations personnelles, bancaires et de mot de passe

Augmentation de la surface d'exposition

- Situation inédite et qui va s'inscrire dans la durée
- Augmentation des usages numériques de mobilité
  - Usage pro/perso
  - BYOD Institutionnel jusqu'au Shadow IT
- Des employeurs et des collaborateurs non préparés à la situation
- Augmentation des domaines Internet liés au thème du COVID-19 ou Coronavirus

Quel impact sur la cyber assurance

- Garanties acquises?
  - A priori oui (mais dépend du texte de police)

- Changement de risque avec COVID ?
  - Analyse technique : a priori oui (cf slides précédents)
  - Analyse légale (Art L 113.4 de Code des Ass.) : plus rassurant pour les assurés car lié au processus de souscription
  - Et pour preuves:
    - Télétravail existait déjà avant, donc rien de nouveau
    - Cyber est par essence un risque mouvant
    - Assureurs cyber au courant de la situation mais aucun en France n'a soulevé ce point à ce jour a notre connaissance

Quel impact sur la cyber assurance

- Télétravail avec le BYOD
  - Scénario 1: attaque du SI Corporate via le BYOD
    - Couvert par la plupart des polices du marchés
  - Scénario 2: attaque du seul BYOD
    - Adaptation de la police peut être nécessaire pour certains cas
    - Cas de la fuite de données personnelles: couvert par la plupart des polices du marchés

Un vrai challenge : La sortie de crise

- la réintégration de tous ces outils potentiellement infectés sur le reseau des entreprises est un défi

- Comment maintenir les niveaux de securité avec des budgets sous tension du fait de la crise economique?

Les renouvellements en cyber assurance (1/3)

Evolution des taux de prime:

- Fin des baisses en Europe au T4 2019 (qui est un marché beaucoup plus compétitif que US et UK)
- T1 2020:
  - Grands comptes: généralement +0 a +10% sur les renouvellements (contre 5-25% au US & UK)
  - PME: marché stable/légère baisse
- Covid amplifiera cette hausse … si la sinistralité augmente

Les renouvellements en cyber assurance (2/3)

Question de renouvellement

- Tendance: de plus en plus de questions « risques » plutôt que « risques IT »
- Focus spécifiques:
  - Ransomware
    - Back up (offline) / PCA – Gestion de crise /
  - Télétravail (COVID)
    - VPN, accès sécurisé à distance, MFA
    - Sensibilisation des employées au risque et à l'utilisation du VPN…
    - Politique BYOD dans PSSI

Les renouvellements en cyber assurance (3/3)

Exclusion COVID en Cyber?

- A aujourd'hui, pas de demande des assureurs
- 2 tentatives en Europe, toutes refusées par Marsh car :
  - Pas un bon message envoyé aux clients
  - Pas pertinent

Conclusion
L’approche par les risques

- Promouvoir la prise de conscience des mesures de securité pour les risques actuels
- Planifier les scénarios de risques pour la sortie de crise
- Anticiper les changements à long terme sur les nouvelles habitudes de travail

Votre Guide