Cycle numérique

Cyber-défense : quelles sont les menaces concrètes pour le cabinet et comment bâtir un plan d'action pour se protéger ?

MERCI D'ÉTEINDRE VOS PORTABLES & PC

…Pour leurs sécurités !

Objectifs du cycle

- Parfaire sa connaissance des différentes menaces existantes
- Mesurer l'impact potentiel d'une attaque sur le cabinet
- Faire un diagnostic de son propre cabinet face aux menaces
- Bâtir son propre plan d'actions pour protéger son cabinet

Enquête DENJEAN&ASSOCIES / GAN ASSURANCES

- « 52% des entreprises ont déjà subi une ou plusieurs tentatives d'attaques visant leur réseau informatique et 93% des entreprises ayant déjà vécu des cyberattaques ont pâti de ces agressions »
- « A l'exception des grands groupes, toutes les entreprises sous-estiment les risques de cyberattaque »
- « Une méconnaissance de l'ampleur et des cibles du piratage informatique en France »
- « 58% des TPE, environ 75% des PME et des ETI, et 100% des grands groupes se jugent bien protégés contre la cyberfraude »
- « 75% des sociétés disposent aujourd'hui de process de cybersécurité »
- « 60% des entreprises sont prêtes à consacrer à la lutte contre la cyberfraude un budget annuel supérieur ou égal à 1% de leur chiffre d'affaires »

Source : Magazine Données partagées, numéro 133 Septembre/Octobre/Novembre 2017, page 23

Quelques questions

- Votre cabinet a-t-il été victime d'une attaque ?
- Un de vos clients a-t-il été victime d'une attaque ?
- Un de vos confrères/consœurs a-t-il été victime d'une attaque ?
- Quelle a été la réaction (du cabinet/du client/du confrère) ?
- Non, alors pourquoi pas vous ?

Quelques questions

- Vous connaissez tous l'ANSSI ?

A = Agence

N = Nationale de la

S = Sécurité des

S = Systèmes d'

I = Information

- Mais que fait l'ANSSI ?

Précautions élémentaires

- Vous connaissez tous le guide des bonnes pratiques…

www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/

- Vous connaissez tous le guide d'hygiène informatique…

http://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/

Petites démonstrations…

- Usurpation du nom de réseau WIFI – SSID de ECF
- Explication de la menace :
  - L'attaquant va usurper le nom de votre réseau wifi et d'un réseau de confiance (ECF, Gare TGV, Restaurant, Hôtel, etc…)
  - Les périphériques (smartphone/pc) vont se connecter automatiquement et prioritairement dessus car le signal est plus fort
  - L'attaquant va « capter » tous les flux qui transitent sur le réseau (dont les mots de passe)

Petites démonstrations…

- Accès non autorisé aux données via une simple clé USB

- Explication de la menace :
  - Vous laissez votre pc sans surveillance
  - Un attaquant connecte une clé USB avec une distribution « live » Linux
  - Un autre système d'exploitation se lance et donne accès à tous les documents disponibles sur le disque dur du pc

Panorama des menaces

- Les classiques sur votre SI : Virus, Chevaux de Troie, malware, phishing
- Les classiques sur votre site internet : vandalisme, attaque DDoS
- Les plus récentes : ransomware/cryptoware, attaque de vos données stockées dans le cloud
- Les plus sournoises : l'exfiltration de données, le sabotage, le chantage, la fraude au commutateur téléphonique
- La liste est malheureusement sans fin…

Panorama des menaces

- Il y a plusieurs types de menaces :
  - Les menaces que l'on détecte
  - Les menaces que l'on connait
  - Les menaces que l'on ne connaît pas
  - Les menaces que l'on ne peut pas imaginer

Aucun système n'est invulnérable. Protéger aujourd'hui, peut signifier vulnérable demain !

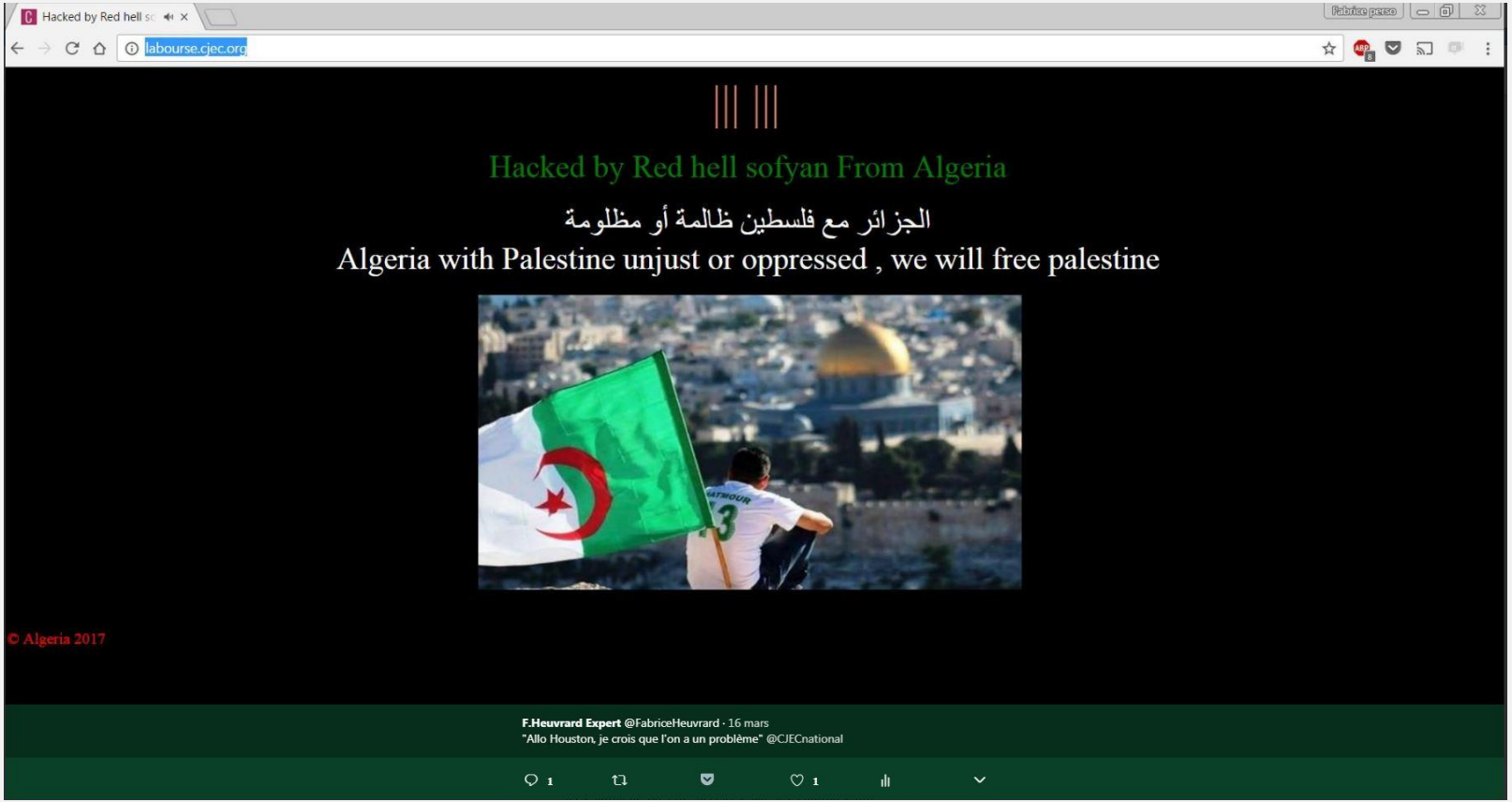
Qui sont les attaquants et leurs motivations ?

- Des profils divers :
  - salarié(e) mécontent(e) => d'où l'importance de désactiver le profil du salarié lors de son départ
  - concurrent(s)
  - « hacker »
- Des motivations diverses :
  - pécuniaire
  - Technique (l'attaquant veut démontrer sa compétence technique)
  - concurrentielle

Les impacts pour le cabinet

- Perte de productivité : X heures * taux horaire
- Perte de confiance des clients si le piratage est rendu public
- Démotivation des collaborateurs
- Difficulté de recruter de nouveaux collaborateurs
- Perte de confiance entre les collaborateurs et l'expert-comptable

Les impacts pour le cabinet – un exemple de vandalisme



Diagnostic du cabinet

- Etablir la liste des applications vitales pour le cabinet, par exemple :
  - La messagerie
  - Les logiciels métiers (paie, compta, etc…)
  - Le site internet, s'il est utilisé activement par les clients
  - Les réseaux sociaux si votre cabinet les utilisent
- Etablir la liste des matériels prioritaires à sécuriser
  - Smartphone(s)
  - PC
  - Imprimante(s)
  - Réseau(x) wifi interne
- Hiérarchiser les différentes menaces par rapport à son propre SI

Bâtir un plan d'action pour protéger son cabinet

- Garder à l'esprit que le cabinet est le dépositaire d'un capital informationnel stratégique : les données de ses clients

- Il faut repenser le cabinet sous un angle sécuritaire
- Tout en restant pragmatique…
- La meilleure défense restera la veille sur l'émergence des nouvelles menaces et leur prévention au sein du cabinet

Bâtir un plan d'action pour protéger son cabinet

- Le facteur humain
  - Formation des salariés (inutile si absence de mise en pratique)
  - Désignation d'un « Monsieur Informatique »
  - Limiter le BYOD et gérer les périphériques en mode « télétravail » - Connaissez-votre numéro IMEI *#06# ?
- Le facteur économique
  - Budget financier
    - intervention prestataire externe
    - upgrade des licences
    - Renouvellement du matériel informatique
  - Budget de temps

Bâtir un plan d'action pour protéger son cabinet

- Le facteur organisationnel
  - Bâtir un process en cas d'attaque
  - Réaliser une charte informatique sur les points importants

- La sécurité : c'est partout et c'est tout le temps !

Vers une opportunité de mission ?

- Après avoir mise en place (avec succès) un plan d'action au sein du cabinet, pourquoi ne pas le proposer à vos clients ?
- Votre cabinet connaît l'infrastructure de ses clients !
- Votre client vous fait confiance
- Une mission à valeur ajoutée pour votre client et vos collaborateurs

Focus sur le règlement RGPD

- Le règlement UE sur la protection des données (RGPD ou GDPR en anglais) est applicable le 25 mai 2018
- Les experts-comptables, sociétés d'expertise comptable et AGC sont concernés en tant que prestataires de services pour leurs clients UE
- Et selon le cas : nos clients

Focus sur le règlement RGPD

- Définition du traitement
  - Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction

- La simple collecte et conservation de données personnelles suffit donc à caractériser un traitement

- Toute donnée personnelle conservée dans les dossiers clients de l'expert-comptable est donc considérée comme un traitement relevant de la règlementation !

Focus sur le règlement RGPD

- Définition des données à caractère personnel
  - Toute information se rapportant à une personne physique identifiée ou identifiable
    - Est réputée être « une personne physique identifiable », une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale (RGPD art 4,1)

- Le nom, prénom, adresse courrier ou mail (même professionnel) d'une personne physique suffit à caractériser une donnée personnelle !

Focus sur le règlement RGPD – Qui est concerné ?

- Les données personnelles visées par la règlementation incluent celles relatives aux personnes physiques, notamment :
  - Les dirigeants et chef d'entreprise
  - Actionnaires
  - Salariés
  - Fournisseurs des clients de l'expert-comptable même s'ils interviennent à titre professionnel (avocat, traducteur, etc…)
  - Clients des clients de l'expert-comptable même s'ils interviennent à titre professionnel

Focus sur le règlement RGPD – localisation

- Où trouver des données personnelles ?
- Notamment dans tous les dossiers clients informatisés des experts-comptables
  - La comptabilité d'un client de l'expert-comptable
  - Les déclarations fiscales
  - Le secrétariat juridique
  - Et naturellement la paie
- Nous sommes concernés :
  - Comme entreprise (notamment vis-à-vis des salariés)
  - Comme prestataire de services

Focus sur le règlement RGPD – Obligations

- Tenue d'un registre des traitements
- Mise en place de procédures prévues dans le règlement
- Notification des failles de sécurité
  - Le niveau des obligations dépend du rôle joué par l'entité
  - Ceci devra donc estimé pour les principales missions de l'expert-comptable
- Nomination d'un Délégué à la Protection des Données dans certains cas