Vulnérabilités et cybermenaces des SI modernes

CNIS Event, 1er juillet 2014

Frédéric Connes

Frederic.Connes@hsc.fr

Plan

- Caractéristiques des SI modernes
  - Recours de plus en plus fréquent au *cloud computing*
  - Développement de la mobilité
  - Interactions avec la sphère personnelle
  - Ouverture sur les réseaux sociaux

Vulnérabilités et menaces liées au *cloud computing*

- Externalisation d'une partie du SI chez un tiers
  - Perte de contrôle sur la sécurité
- Ou recours à des techniques nouvelles en interne
  - Pas nécessairement bien maîtrisées
- Apparition de logiciels malfaisants spécifiques au *cloud*
  - Bohu, 2011 (cheval de Troie chinois bloquant des anti-virus en *cloud* : Kingsoft, Qihoo, Rising)

Contrôle d'accès

- Erreur du prestataire
  - Dropbox, 21 juin 2011 : mises à jour du code => suppression de la vérification du mot de passe pendant 4 heures
  - Généralisation de l'authentification double facteur chez les prestataires de *cloud*
- Utilisation de logiciels vulnérables
  - *Heartbleed*, 7 avril 2014 : possibilité de récupérer des mots de passe
- Attaques par ingénierie sociale
  - Mat Honan, 3 août 2012 : prise de contrôle de son compte iCloud par des tiers, via les procédures de récupération de mot de passe
  - Développement du *phishing* ciblé sur certaines entreprises

Contrôle d'accès

- Mauvaise politique de mots de passe par le prestataire
  - Notamment sur les comptes d'administration
  - Développement des SSO inter-*cloud* (maillon faible)
- Développement des logiciels de gestion de mots de passe synchronisés en *cloud*
  - Gravissime si faille de sécurité sur le conteneur de mots de passe
- Machines et réseaux virtuels
  - Séparation purement logicielle : canaux cachés inévitables
  - Maillon faible : machine mal sécurisée d'un client quelconque
- Cibles
  - Réseaux d'administration, de supervision et de sauvegarde
  - Administrateurs systèmes et réseaux
    - OVH, mi-juillet 2013 : accès au compte e-mail d'un administrateur => accès au VPN interne d'un autre employé => accès au *backoffice* interne

Confidentialité

- Absence de chiffrement en interne chez le prestataire
  - E. Snowden, octobre 2013 : trafic en clair au sein du *cloud* Google, permet l'espionnage par la NSA
  - Mouvement de chiffrement en interne (Yahoo!, Google, Microsoft…)
- Accès possible par les employés du prestataire
  - Même si données chiffrées par le prestataire
  - Clés SSH du prestataire par défaut sur certains serveurs dédiés
  - Aucun contrôle sur le recrutement des employés
- Seul chiffrement efficace : côté client
  - Mais problème des accès multiterminaux : partage de la clé via l'éditeur de la solution, sinon pas pratique
  - Mises à jour automatiques du code exécutant la partie cryptographique

Intégrité

- Confusion entre réplication des données et sauvegarde
  - Protège uniquement contre les problèmes techniques
  - Effacement d'une donnée sur un périphérique l'efface partout
- Excès de confiance envers les services *cloud*
  - Oubli de faire des sauvegardes
  - Voire choix délibéré de ne pas en faire
- Développement des services de sauvegarde en *cloud*
  - Sauvegardes hors-ligne ne sont plus la norme
  - Tests de restauration plus complexes à organiser hors production
  - Aucune confidentialité

Disponibilité et maîtrisabilité

- Dépendance envers la connexion Internet
  - Stabilité et dimensionnement (saturation)
- Absence de maîtrise des plages de maintenance
- Services *cloud* : cibles de choix pour les dénis de service
  - 8e rapport annuel d'Arbor Networks (*Worldwide Infrastructure Security Report*), 2011-2012 : 14% des entreprises interrogées ont subi un déni de service visant spécifiquement un service *cloud*
- Problème matériel, de maintenance, catastrophe naturelle…
  - Swissdisk, 18 octobre 2009 (avec perte de données)
  - Amazon Web Services, 14 juin 2012 (nombreux services impactés)
- Fermeture du service
  - Iron Mountain, avril 2011 (service de stockage en *cloud*)
- Formats de données variables en fonction des prestataires

Vulnérabilités et menaces liées à la mobilité

- Mobilité : porte ouverte sur le SI
  - Par commodité (déplacements, télétravail...)
- Flottes non-homogènes => sécurité plus complexe à gérer
  - Souvent, demandes spécifiques des VIP
  - Mises à jour OS/applications très variables suivant le modèle
  - Modèles durcis restent marginaux
- Absence de contrôle sur les applications installées
  - Peuvent être malfaisantes
  - Pas toujours possible de créer des « *stores* » privés
  - Encore pire si un utilisateur « *jailbreak* » ou « *root* » son terminal
- Ingénierie sociale beaucoup plus facile en mobilité

Contrôle d'accès

- Terminaux mobiles souvent mal protégés
  - Codes PIN au lieu de véritables mots de passe (sur les applications, souvent identiques à celui du terminal)
  - Mots de passe de services souvent sauvegardés
  - Donnent accès à des informations très sensibles : e-mails, contacts, agendas, fichiers, CRM, voire accès VPN
- Vol ou perte du terminal
  - Périphériques laissés sans surveillance (hôtel, domicile…)
  - Attaque de la RAM sur un terminal verrouillé en veille
  - Risque majeur si le terminal n'est pas verrouillé
  - Catastrophique si le gestionnaire de mots de passe est ouvert
- Piégeage physique ou logique dans une chambre d'hôtel
  - Ajout de composants, flash du BIOS…

Confidentialité et intégrité

- Disques non-chiffrés dans leur intégralité
  - Contraintes légales dans certains Etats
- Connexions non-chiffrées à partir de Wi-Fi publics
  - Hôtel, restaurant, aéroport, conférence…
- VPN utilisé en même temps qu'une connexion non-sécurisée
- Sensibilisation insuffisante aux filtres écran et au verrouillage du poste
  - Salarié qui laisse son ordinateur portable ouvert non-verrouillé dans le train pendant 10 minutes, pour aller au bar, avec des documents confidentiels à l'écran
- Géolocalisation : donne des indications sur les clients et prospects
- Exploitation malfaisante de la fonctionnalité d'effacement à distance

Vulnérabilités et menaces liées aux interactions avec la sphère personnelle

- *Bring your own device*
  - Propagation de logiciels malfaisants vers le SI
  - Fuite de données depuis le SI
  - Absence de contrôle sur la sécurité du périphérique personnel
  - Nouveaux risques avec les objets connectés
- *Bring your own software/service*
  - Installation de logiciels malfaisants (administrateurs de leur poste)
  - Services *cloud* personnels : risque de confusion
    - Document professionnel déposé par erreur dans la Dropbox personnelle
- Partage de connexion avec l'ordiphone personnel
- Tunnels non-bloqués vers des machines personnelles
- Mots de passe personnels faibles réutilisés en environnement professionnel

Vulnérabilités et menaces liées aux réseaux sociaux

- Facilitent l'usurpation d'identité
  - Création d'un faux compte au nom d'une personnalité
  - Demandes de connexion aux amis connus de la personnalité
  - Effet boule de neige
  - Echanges avec les amis proches de la personnalité permettent de récupérer des informations confidentielles
- Les connexions des salariés peuvent révéler
  - Noms des clients et prospects
  - Structure interne de l'organisme
  - Informations utiles pour l'ingénierie sociale

Vulnérabilités et menaces liées aux réseaux sociaux

- Moindre méfiance des utilisateurs
  - Utilisation d'applications intégrées aux réseaux sociaux, qui peuvent être malfaisantes
  - Mauvaise maîtrise des cercles de publication
    - En interne : informations publiées par mégarde à des cercles plus larges que les collègues concernés
    - Sur des réseaux sociaux grand public : publications accessibles à des relations personnelles
  - CV mentionnant des projets secrets
  - *Phishing* en provenance d'un réseau social plus efficace
    - Fausses demandes de connexion
- Synchronisation entre un réseau social et le CRM
  - Risque de fuite d'information

Conclusion

- Vulnérabilités et cybermenaces le plus souvent
  - Techniques
  - Comportementales (ignorance, mauvais usages, tentation de la facilité…)
- Touchent tous les organismes indépendamment de leur taille
- Pas encore assez de recul sur les nouveaux outils
- Solutions
  - Techniques
  - Organisationnelles
  - Juridiques

Questions