Awareness Training

BDO Algeria

May 2016

Amine Benamar
Head of forensics Technology services

Séminaire International sur la Cyber-sécurité Alger

Index

I. Préambule
II. Les enjeux
III. Pourquoi les pirates s'intéressent aux S.I. ?
IV. La nouvelle économie de la cybercriminalité
V. Les impacts sur la vie privée
VI. Les infrastructures critiques
VII. DIC & DICP

Préambule

- Système d'Information (S.I.)

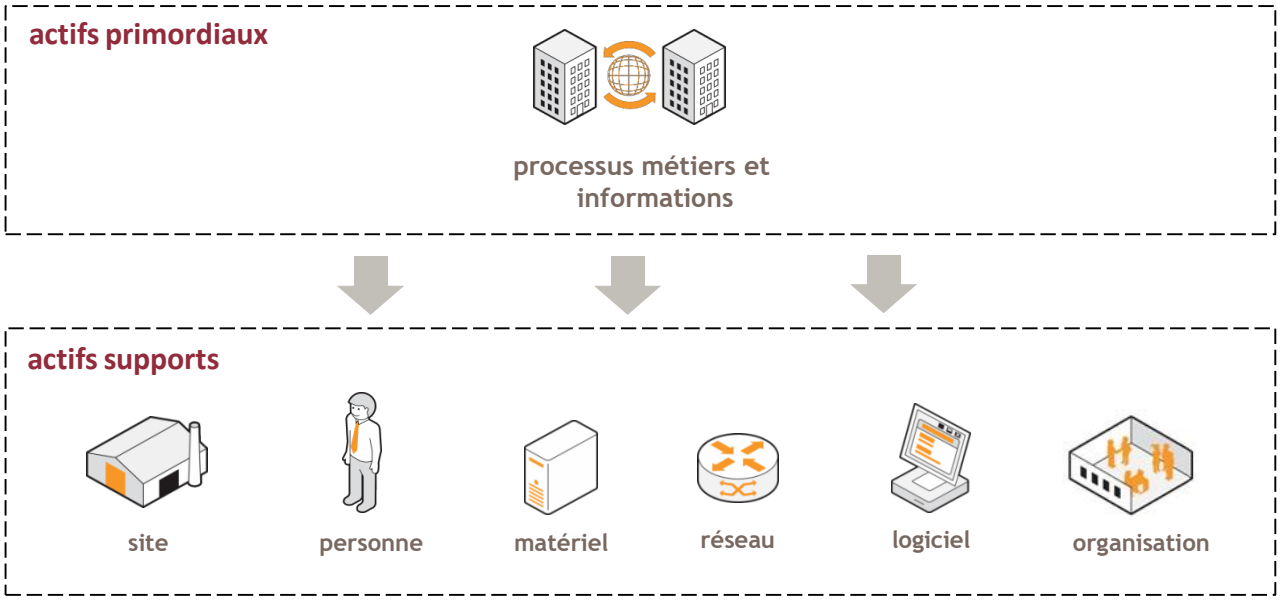
  – Ensemble des ressources destinées **à collecter, classifier, stocker, gérer, diffuser les informations** au sein d'une organisation

  – Mot clé : information, c'est le « nerf de la guerre » pour toutes les entreprises, administrations, organisations, etc.

Le S.I. doit permettre et faciliter la mission de l'organisation

Préambule

- Le système d'information d'une organisation contient un ensemble d'actifs :



La sécurité du S.I. consiste donc à assurer la sécurité de l'ensemble de ces biens

Les enjeux

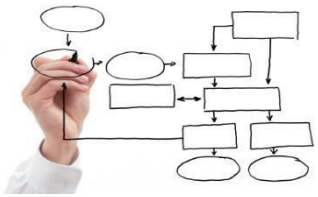
Impacts financiers

Impacts sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires

Impacts organisationnels



Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

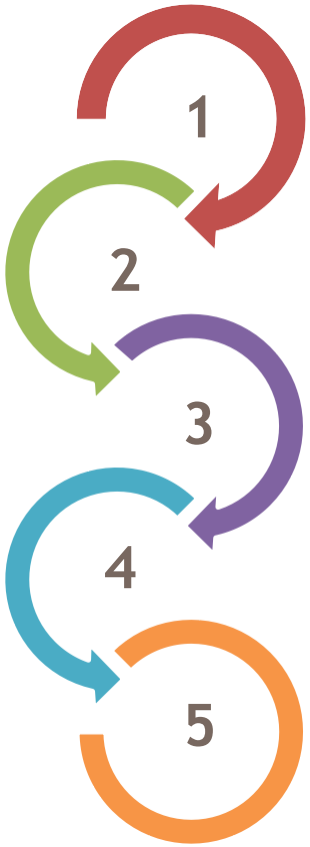
- Les motivations évoluent
  - Années 80 et 90 : beaucoup de bidouilleurs enthousiastes
  - De nos jours : majoritairement des actions organisées et réfléchies
- Cyber délinquance
  - Les individus attirés par l'appât du gain
  - Les « hacktivistes »
  - Motivation politique, religieuse, etc.
  - Les concurrents directs de l'organisation visée
  - Les fonctionnaires au service d'un état
  - Les mercenaires agissant pour le compte de commanditaires
  - …

Pourquoi les pirates s'intéressent-ils aux S.I. des organisations ou au PC d'individus ?

- **Gains financiers** (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires
- **Utilisation de ressources** (puis revente ou mise à disposition en tant que « service »)
  - Bande passante & espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)
- **Chantage**
  - Déni de service
  - Modifications des données
- **Espionnage**
  - Industriel / concurrentiel
  - Étatique

La nouvelle économie de la cybercriminalité

- **Une majorité des actes de délinquance réalisés sur Internet sont commis par des groupes criminels organisés, professionnels et impliquant de nombreux acteurs**



des groupes spécialisés dans le développement de programmes malveillants et virus informatiques

des groupes en charge de l'exploitation et de la commercialisation de services permettant de réaliser des attaques informatiques

un ou plusieurs hébergeurs qui stockent les contenus malveillants, soit des hébergeurs malhonnêtes soit des hébergeurs victimes eux-mêmes d'une attaque et dont les serveurs sont contrôlés par des pirates

des groupes en charge de la vente des données volées, et principalement des données de carte bancaire

des intermédiaires financiers pour collecter l'argent qui s'appuient généralement sur des réseaux de mules

La nouvelle économie de la cybercriminalité

- Quelques chiffres pour illustrer le marché de la cybercriminalité…

de 2 à 10 $ le prix moyen de commercialisation des numéros de cartes bancaires en fonction du pays et des plafonds

5 $ le tarif moyen de location pour 1 heure d'un botnet, système permettant de saturer un site internet

2.399 $ le prix de commercialisation du malware « Citadel » permettant d'intercepter des numéros de carte bancaire (+ un abonnement mensuel de 125 $)

Les impacts de la cybercriminalité sur la vie privée (quelques exemples)

- **Impact sur l'image / le caractère / la vie privée**
  - Diffamation de caractère
  - Divulgation d'informations personnelles
  - Harcèlement / cyber-bullying
- **Usurpation d'identité**
  - « Vol » et réutilisation de logins/mots de passe pour effectuer des actions au nom de la victime
- **Perte définitive de données**
  - malware récents (rançongiciel) : données chiffrées contre rançon
  - connexion frauduleuse à un compte « cloud » et suppression malveillante de l'ensemble des données
- **Impacts financiers**
  - N° carte bancaire usurpé et réutilisé pour des achats en ligne
  - Chantage (divulgation de photos ou d'informations compromettantes si non paiement d'une rançon)

Les impacts de la cybercriminalité sur les infrastructures critiques

- Infrastructures critiques = un ensemble d'organisations parmi les secteurs d'activité suivants, et que l'État Algérien considère comme étant tellement critiques pour la nation que des mesures de sécurité particulières doivent s'appliquer
  - Secteurs étatiques : civil, justice, militaire…
  - Secteurs de la protection des citoyens : santé, gestion de l'eau, alimentation
  - Secteurs de la vie économique et sociale : énergie, communication, électronique, audiovisuel, information, transports, finances, industrie.

- Ces organisations sont classées comme **Opérateur d'Importance Vitale (OIV).** La liste exacte est classifiée (donc non disponible au public).

Les besoins de sécurité

Introduction aux critères DIC

- Comment définir le niveau de sécurité d'un bien du S.I. ? Comment évaluer si ce bien est correctement sécurisé ?
- 3 critères sont retenus pour répondre à cette problématique, connus sous le nom de D.I.C.

Bien à protéger

Disponibilité

Propriété d'accessibilité au moment voulu des biens par les personnes autorisées (i.e. le bien doit être disponible durant les plages d'utilisation prévues)

Intégrité

Propriété d'exactitude et de complétude des biens et informations (i.e. une modification illégitime d'un bien doit pouvoir être détectée et corrigée)

Confidentialité

Propriété des biens de n'être accessibles qu'aux personnes autorisées

Les besoins de sécurité

Exemple d'évaluation DICP

Disponibilité = Très fort ✓

Un haut niveau de disponibilité du site web est nécessaire, sans quoi l'entreprise ne peut atteindre son objectif de faire connaitre ses services au public

Intégrité = Très fort ✓

Un haut niveau d'intégrité des informations présentées est nécessaire. En effet, l'entreprise ne souhaiterait pas qu'un concurrent modifie frauduleusement le contenu du site web pour y insérer des informations erronées (ce qui serait dommageable)

Confidentialité = Faible ✓

Un faible niveau de confidentialité suffit. En effet, les informations contenues dans ce site web sont publiques par nature!

Preuve = Faible ✓

Un faible niveau de preuve suffit. En effet, ce site web ne permet aucune interaction avec les utilisateurs, il fournit simplement des informations fixes.

Notions de vulnérabilité, menace, attaque

Notion de « Vulnérabilité » :

Faiblesse au niveau d'un bien (au niveau de la conception, de la réalisation, de l'installation, de la configuration ou de l'utilisation du bien).

Notion de « Menace » :

Cause *potentielle* d'un incident, qui pourrait entrainer des dommages sur un bien si cette menace se concrétisait.

Notion d'« Attaque » :

Action malveillante destinée à porter atteinte à la sécurité d'un bien. Une attaque représente la **concrétisation d'une menace**, et nécessite **l'exploitation d'une vulnérabilité.**

Panorama de quelques menaces

Hameçonnage & ingénierie sociale

Fraude interne

Violation d'accès non autorisé

Virus informatique

Déni de service distribué

Questions

CONTACT US

IT & Telecommunication
Amine Benamar
Head of Forensics TS

abenamar@bdo.dz
Mobile: +213 560 999 050

BDO IT & Telecom
Business Center Dar El Madina
Building "C" 8th Floor
16035 Hydra – Algiers, Algeria

Tél: +213 23 53 11 14/15
Fax: +213 23 53 11 16
www.bdo.dz