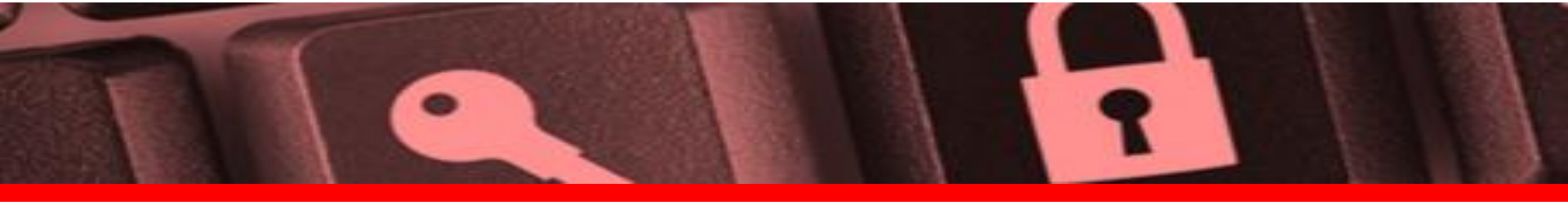
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR

Information Service Center DEFR ISCeco



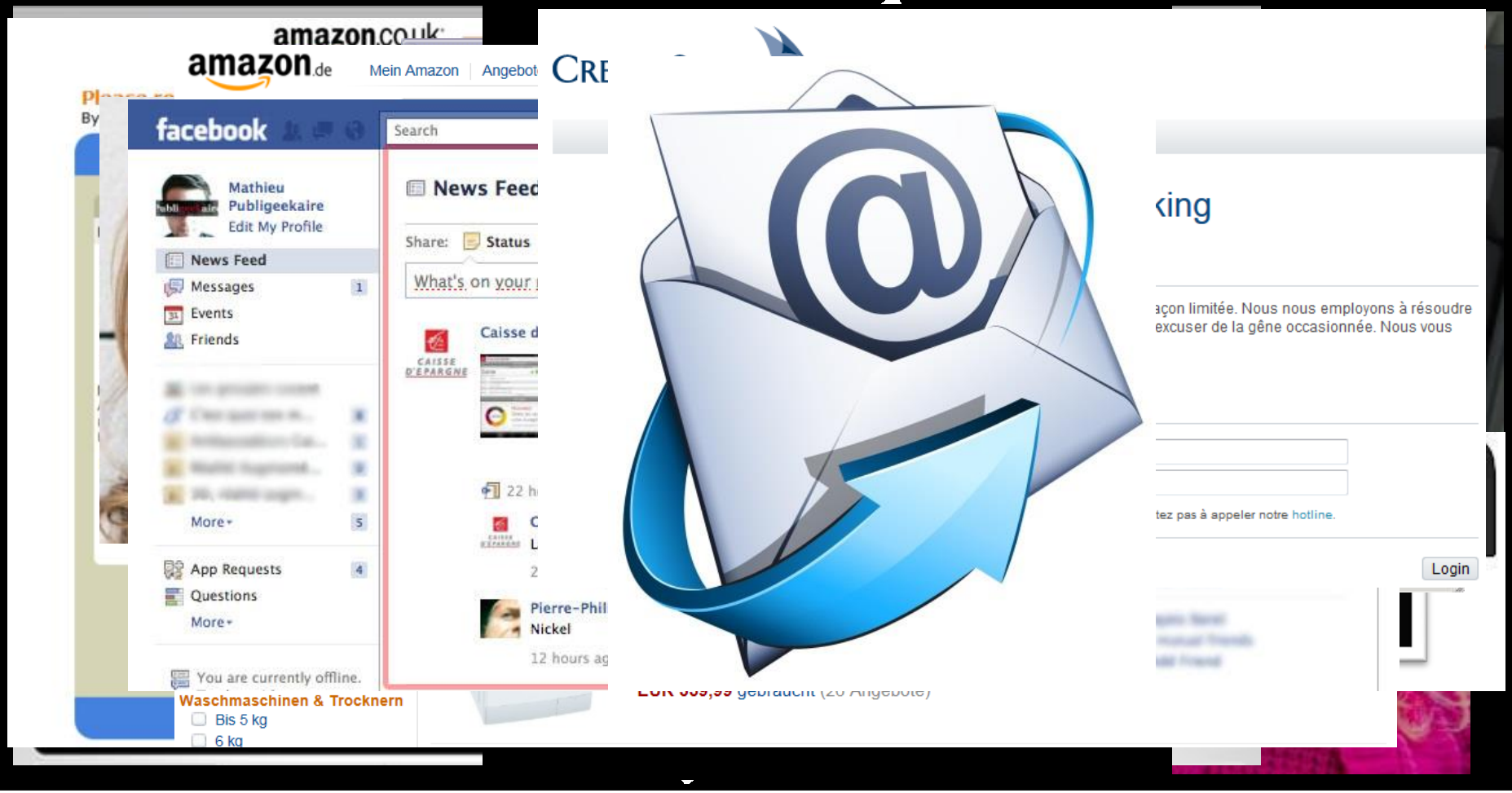
Sécurité de l'Information

Sensibilisation pour managers

INSOMNI'HACK
Swiss security conference and ethical hacking contest

Georges Torti
Responsable de la sécurité de l'information et gestion des risques
Information Service Center DEFR ISCeco

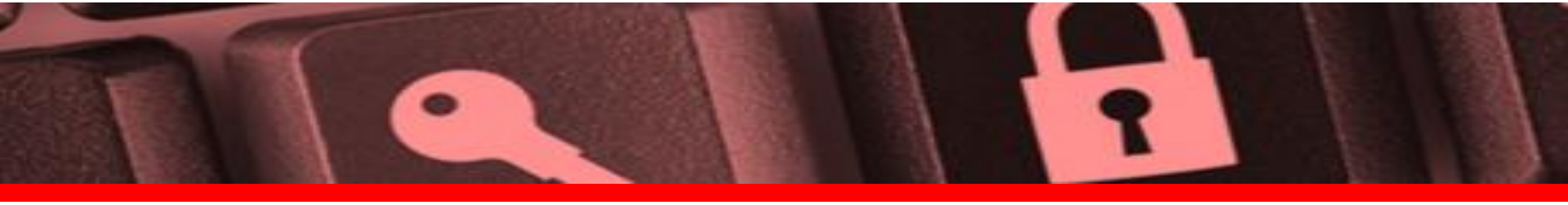
Hacking Story



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de l'économie,
de la formation et de la recherche DEFR

Information Service Center DEFR ISCeco



Sécurité de l'Information

Sensibilisation pour managers

Georges Torti
Responsable de la sécurité de l'information et gestion des risques
Information Service Center DEFR ISCeco

Table des matières

- Introduction
- Pourquoi avons-nous besoin de gérer la sécurité de l’information
- Quelques mythes sur la sécurité de l’information
- Les bases de la sécurité de l’information
- Flashs sur quelques thèmes spécifiques
- Conclusion
- Liens utiles

Introduction

- Il y a dix ans, peu concernés par le sujet
- Aujourd'hui vous ne pouvez plus ignorer la sécurité de l'information
- Pourquoi ?
  - Actives dans le traitement d'informations
  - Dépendantes des informations
  - Accessibles partout et à tout moment

- La sécurité de l'information est aujourd'hui encore trop souvent insuffisamment considérée dans l'entreprise
- Pourquoi ?
  - Quelques mythes concernant la sécurité de l'information

Mythe 1

C’est de l’informatique

- Pas seulement !
- Scénario : un administrateur système désactive l’application principale et supprime les bases de données les plus importantes
- Est-ce un problème informatique ?
- Est-ce que des mesures de sécurité techniques aurait pu éviter ceci ?

- Des mesures dans la sélection du personnel, la supervision, les règlements internes, et comment cette personne est traitée dans l’entreprise sont à considérer ici

Mythe 2

Le top management n’est pas concerné

- Faux !
- Pas de mesures sans argent et ressources humaines
- Soutien du projet par le top management
- Le top management montre l’exemple
- Un élément primordial dans la sécurité de l’information

Mythe 3

La majorité des investissements seront effectués en technologies

- Faux !
- Technologies en place
- Règles d'utilisation
- Ce que l'on peut et ce que l'on ne peut pas faire
- Investissement
  - le développement de politiques et règlement
  - formations et sensibilisation
  - établissement de processus

Mythe 4

La sécurité de l’information est un projet effectué une fois pour toute

- Faux !
- Processus vivant
- Menaces évoluent
- Procédures adaptées aux modifications dans l’organisation
- Maintenance des logiciels et équipements
- Sensibilisation périodique des collaborateurs
- Travail sans fin

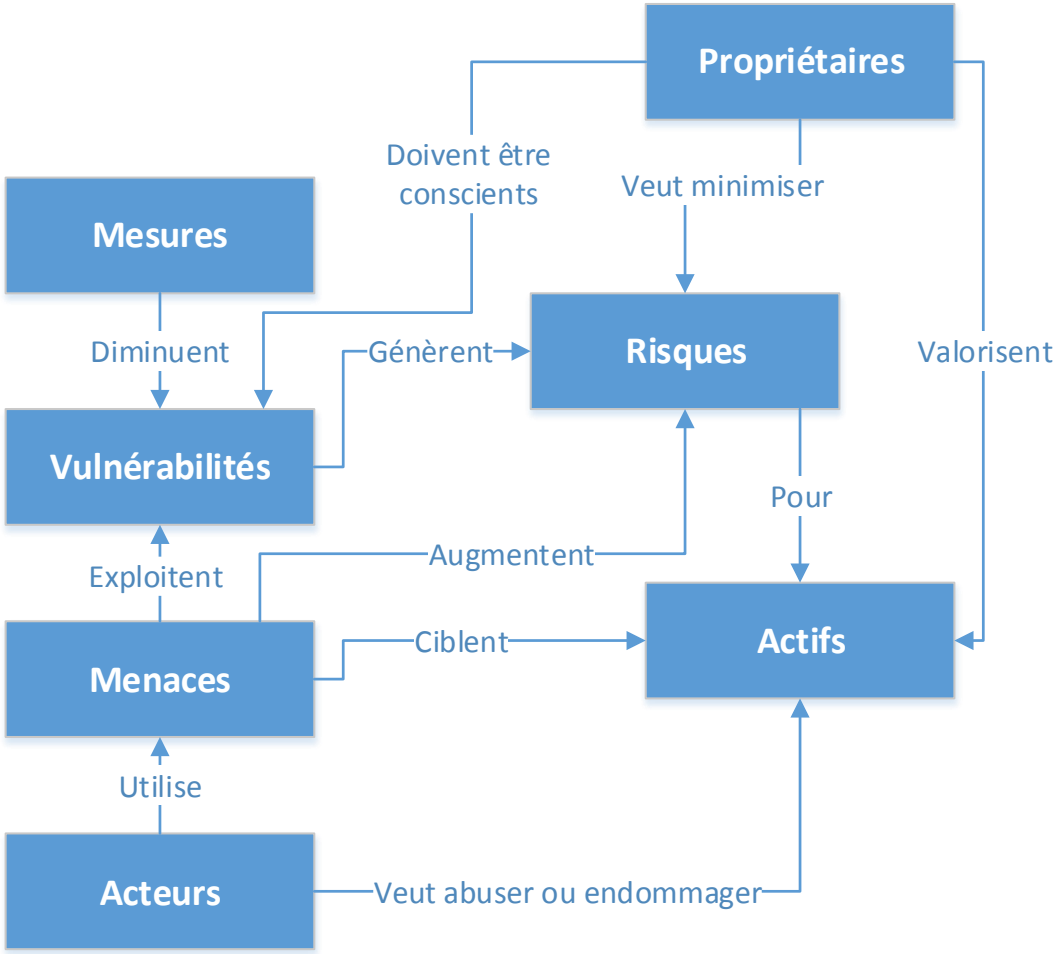
Mythe 5

Cela ne nous concerne pas

- Faux !
- Toute organisation concernée : PME, groupes, états, associations, personnes privées…
- Données sensibles :
  - données personnelles des collaborateurs, des clients, processus métier, brevets, codes d’accès (banque p.ex)
- Utilisation de l’infrastructure (responsabilité juridique)

Pourquoi gérer la sécurité de l'information ?

- Des acteurs
- Des motivations
- Des menaces
- Des vulnérabilités
- Des conséquences



Des acteurs

- Les activistes
- Les états
- Les organisations criminelles
- Les terroristes
- Les «Script Kiddies»
- Les «Insiders»
  - Employés
  - Ex-employés
  - Employés de fournisseurs ou prestataires de services

Des motivations

- Finances
- Militaire – espionnage
- Idéologie
- Politique
- Prestige / Challenge / Ego
- Revanche
- Destruction / Terrorisme
- Amusement

Des menaces

- Accès au réseau / aux locaux non autorisé
- Virus / codes malicieux
- Brèche d’informations confidentielles
- Falsification d’information
- Ecoute / Espionage
- Erreur de programmation
- Feux (volontaire/accident)
- Erreur de manipulation
- Perte d’électricité / climatisation
- Vol / Perte d’appareils
- Attentat / Vandalisme
- Désastre naturel

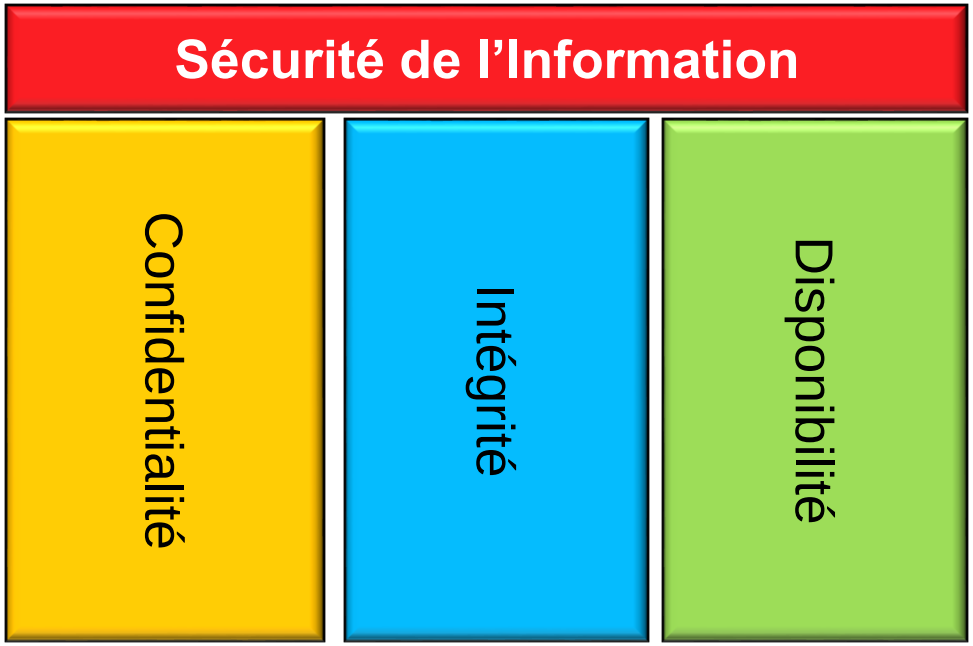
Des vulnérabilités

- Mise à jour des logiciels
- Mots de passe standards ou faible
- Accès pas contrôlés
- Complexité pour l’utilisateur
- Mise au rebus non contrôlé
- Manque de documentation
- Fins de contrat
- Pas de sauvegardes
- Tests insuffisants
- Sensibilisation des utilisateurs

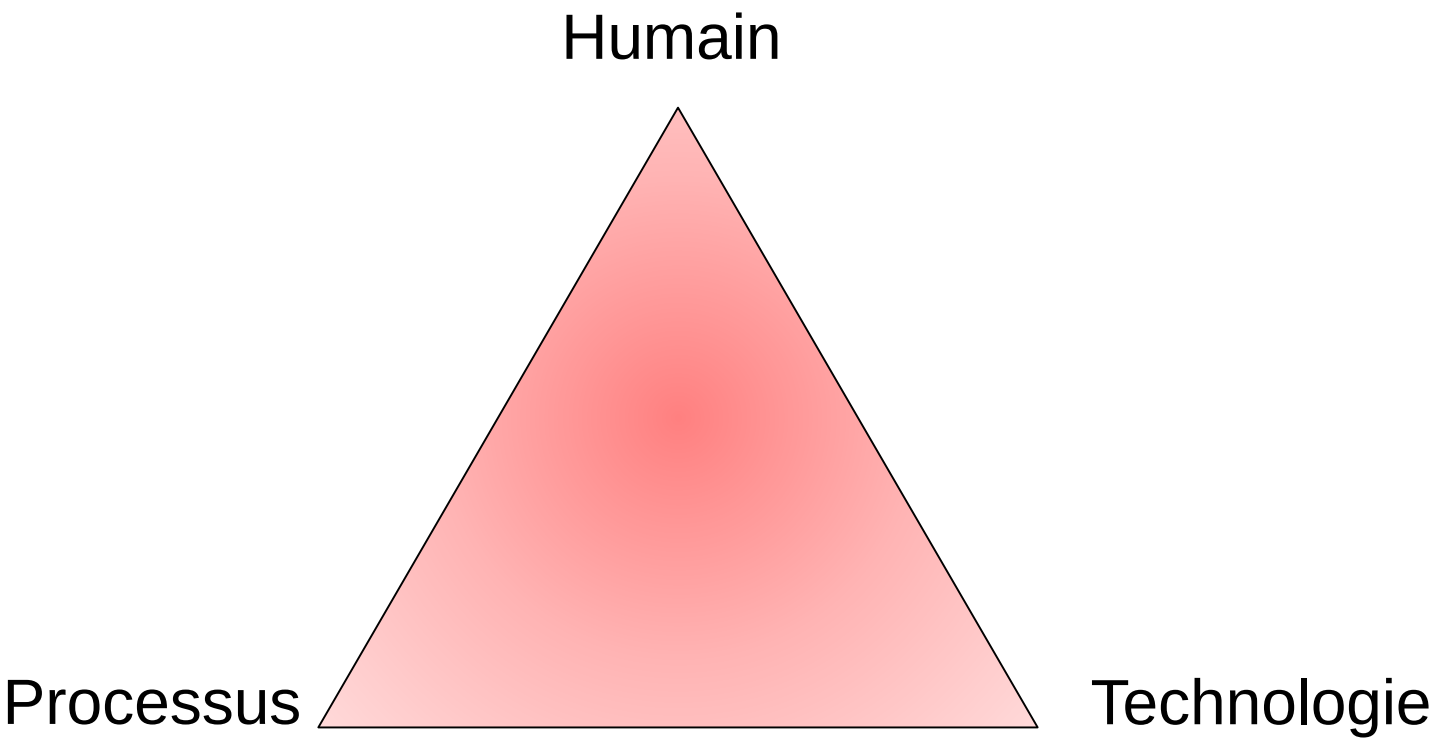
Des conséquences

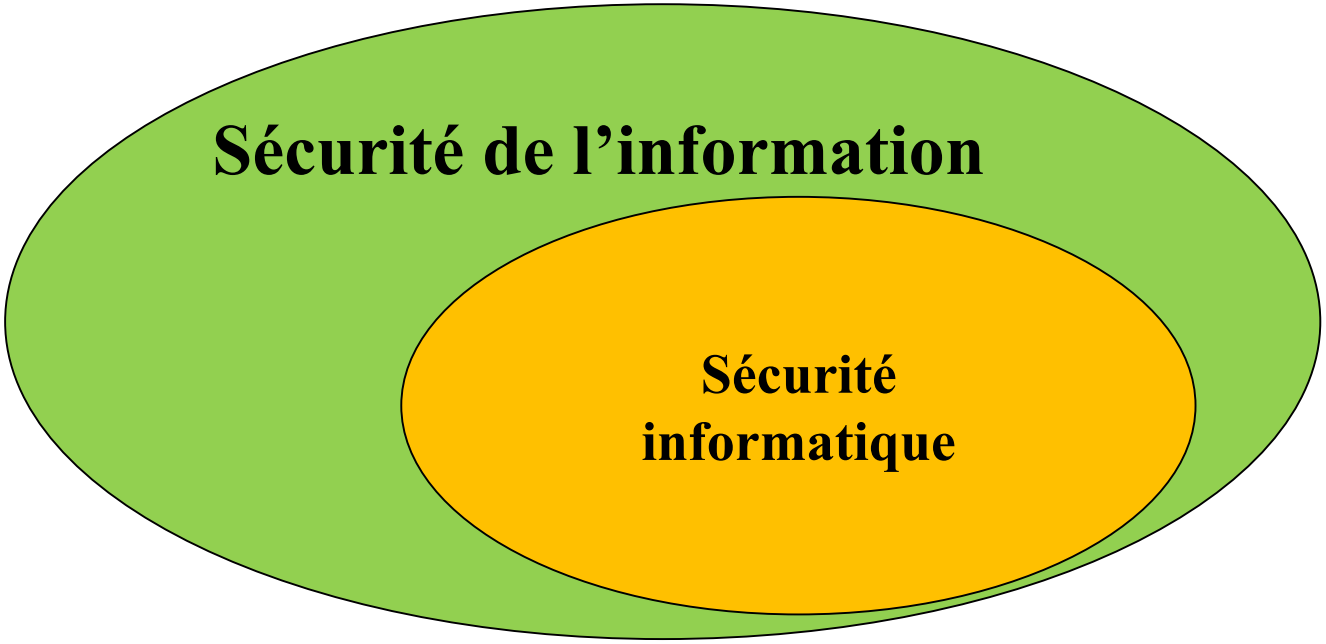
- Réputation
- Disponibilité
- Confiance (données sensibles, données personnelles)
- Financier (Transfert d’argent, services non payés)
- Chantage
- Juridiques

Bases de la sécurité de l’information



Bases de la sécurité de l’information




Sécurité de l'information
Sécurité informatique

F L A S H

Flash 1 | Protection des données personnelles

- Les données personnelles constituent un bien précieux
- Données personnelles : toutes les informations qui se rapportent à une personne identifiée ou identifiable
- Utilité des données personnelles:
  - Comportement d’achat, profil de personnalité, profil de déplacement, intérêts personnels, état de santé, moyens financiers…
- Loi sur la protection des données
  - vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données

Flash 1 | Protection des données personnelles

“ Puis-je accéder sans restrictions à mon dossier du personnel ? ”

“ Peut-on conserver les CV des candidats refusés ? ”

“ Peut-on collecter les coordonnées personnelles des collaborateurs et collaboratrices pour un annuaire intranet ? ”

GESTION RH

Quelles informations dois-je garder dans le dossier personnel d'un collaborateur ?

DOSSIER PERSONNEL

Puis-je contacter un précédent employeur dont le nom figure dans un CV ?

Quelles informations dois-je garder dans le dossier personnel d'un collaborateur ?

- **i** Lors de ses entretiens d'évaluation annuels, un collaborateur se plaint systématiquement d'un collègue au moyen d'une feuille annexe.
- **d** La direction des ressources humaines (DRH) met le document d'évaluation au dossier du collaborateur en supprimant à chaque fois l'annexe.
- **p** Le collaborateur demande son transfert dans un autre service. Lors de l'entretien qui a lieu à ce sujet, la DRH n'a pas trace des récriminations du collaborateur qui justifient sa demande de transfert.
- **r** Si le collaborateur a des copies de ses commentaires, la DRH peut en tenir compte. Sinon, elle ne pourra pas donner foi aux propos du collaborateur.
- **c** La DRH doit garder toutes les informations pertinentes dans le dossier du collaborateur. Les commentaires du collaborateur à une évaluation en font partie.

Think Data

http://www.thinkdata.ch

Flash 2 | Mise au rebus

- Procéder à une mise au rebus sécurisée des supports qui ne servent plus
- Eviter ainsi une fuite d’informations confidentielles
- Incinération – déchiquetage – effacement certifié

Flash 3 | Sauvegarde / Restauration

- Réaliser des copies de sauvegarde des informations, des logiciels et des configurations
- Définir l’étendue des sauvegardes
  - Fréquence (Heures / Jours / Mois / Année)
  - Méthode de sauvegarde (totale / différentielle)
  - Exigences en matière de conservation (durée de rétention)
  - Emplacement pour le stockage des médias (distance / sécurité)
- Tests réguliers de restauration

Flash 4 | Continuité des activités

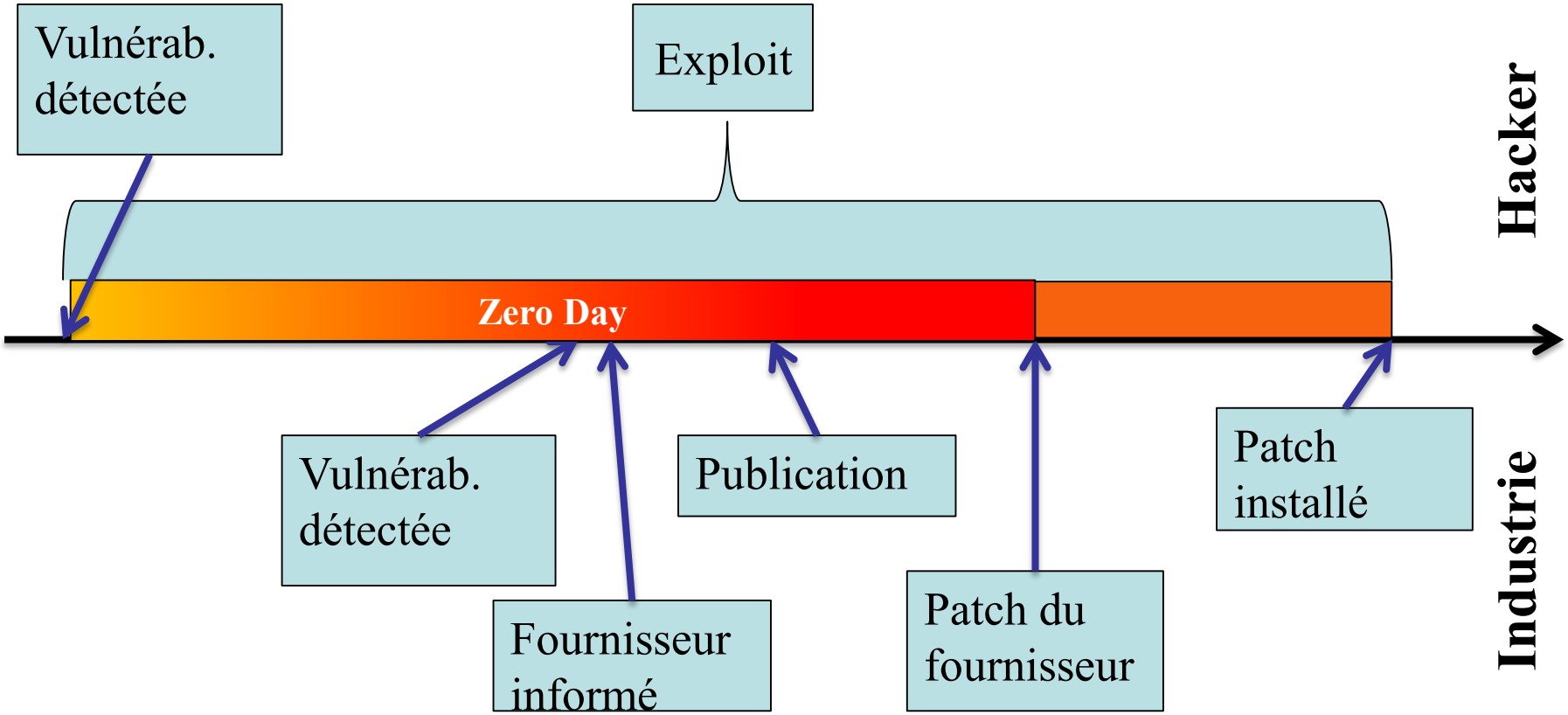
- Etre préparé pour affronter un événement perturbant
- Ne pas uniquement considérer l'informatique, mais l'ensemble du métier
- Créer un plan de restauration pour garantir la continuité (documenté)
- Avoir ce plan et les informations sous format non électronique, hors entreprise
- Tester le plan et corriger
- Mettre à jour périodiquement et lors de changements importants

Failing to plan is planning to fail

Flash 5 | Cloud

- Cible intéressante pour la cybercriminalité – concentration de données
- Emplacement géographique des données difficile à maîtriser
- Aspects juridiques à analyser (accès aux informations / législations / CG)
- Cryptage (clé de cryptage) –Accès et stockage – Isolation
- Disponibilité de la solution cloud / d’internet
- Support et contact
- Réaliser ses propres sauvegardes
- Assurer la «sortie» du cloud / changement de prestataire

Flash 6 | Gestion des vulnérabilités



Flash 7 | Règles d’hygiène

- Sensibiliser et former les utilisateurs à la sécurité
- Maintenir ses systèmes à jour
- Protéger l’information
- Sécuriser les appareils mobiles
- Restreindre les accès aux besoins nécessaires (moindre privilège)
- Utiliser des comptes personnels, non génériques
- Appliquer des règles de sécurité pour la navigation sur internet
- Adopter des mots de passe forts, et les stocker en sécurité
- Sauvegarder ses données, et contrôler les sauvegardes
- Lutter à différents niveaux contre les virus et autres programmes malveillants

Conclusion

- Le management doit s’occuper de la sécurité de l’information
- Ce n’est pas une affaire du service informatique
- C’est un processus sans fin
- Il faut une bonne combinaison entre
  - Les hommes
  - Les processus
  - Les technologies

Liens

- MELANI : www.melani.admin.ch
- Loi sur la Protection des Données : www.leprepose.ch
- Thinkdata : www.thinkdata.ch
- ANSSI : www.ssi.gouv.fr/entreprise
- Guide belge de la cybersécurité : http://vbo-feb.be/Global/Publicaties/Gratis%20downloads/CybersecurityFR.pdf
- Règlement informatique (EN): http://www.sans.org/security-resources/policies/general/pdf/acceptable-use-policy
- Guide d'hygiène informatique : http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Aide mémoire pour les PME: https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

La sécurité de l’information est un processus, pas un produit

Merci pour votre engagement !