MICROTEL 91
Informatique & Multimédia

Pierre De Corbier

Risques numériques

10/02/2023

Introduction

Risque

Définition

Evaluation

Inventaire

Risques techniques

Risques humains

Actions de réduction

Locales

Internet

Qu’est-ce qu’un risque ?

risque

nom masculin

(italien *risco*, du latin populaire *resecum*, ce qui coupe)

LAROUSSE

1. Possibilité, probabilité d'un fait, d'un événement considéré comme un mal ou un dommage : Les risques de guerre augmentent.

2. Danger, inconvénient plus ou moins probable auquel on est exposé : Courir le risque d'un échec. Un pilote qui prend trop de risques.

SYNONYME :
péril

3. Fait de s'engager dans une action qui pourrait apporter un avantage, mais qui comporte l'éventualité d'un danger : Avoir le goût du risque.

4. Préjudice, sinistre éventuel que les compagnies d'assurance garantissent moyennant le paiement d'une prime : Risques naturels, industriels.

Exemple

Danger : virage

Risque : dérapage

Facteurs de risque :

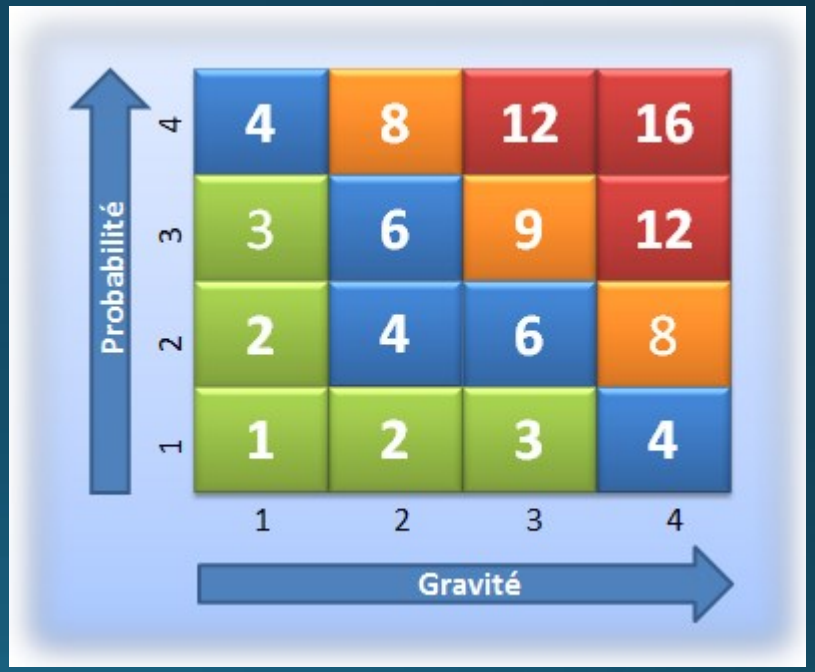
- Vitesse
- Etat de la route
- Etat du véhicule
- Etat du conducteur
- Comportements

Conséquences :

- Passagers abimés
- Véhicule abimé

Evaluation d'un risque

- Identifier les dangers et les facteurs de risque.
- Identifier les conséquences
- Evaluer la probabilité que les conséquences se produisent
- Evaluer la gravité des conséquences
- Identifier les actions de réduction du risque et évaluer leur efficacité et leur coût



Inventaire

- On s'intéresse aux risques numériques pour un utilisateur, ses proches, son matériel et son environnement
- On ne retient que les risques pour lesquels nous pouvons mettre en œuvre des actions de réduction
- Ces risques concernent aussi bien les ordinateurs que les smartphones et les tablettes

- Risques techniques
  - Incidents matériels
  - Incidents logiciels
  - Environnement

- Risques humains
  - Maladresse
  - Méconnaissance
  - Malveillance

Risques techniques

- Défaillance d'un disque dur, d'une clef USB, d'une micro-SD
- Défaillance d'un processeur, d'une mémoire, du clavier, d'un écran etc…
- Occurrence d'un bug

- Coupure réseau de données
- Panne de courant, chute du matériel, inondation…

- Perte de données + coût €
- Indisponibilité + coût €
- Perte de données + Indisponibilité
- Indisponibilité
- Perte de données + Indisponibilité + coût €

Risques humains

- Maladresse
- Méconnaissance
- Malveillance

Maladresse

- Effacer accidentellement des fichiers
- Se prendre les pieds dans les fils
- Renverser son café dans son ordinateur portable
- Se faire dérober un mot de passe

- Perte de données (photos, vidéos, courriers…)
- Blessures + Indisponibilité + coût €
- Perte de donnée + Indisponibilité + coût €
- Multiples

Méconnaissance (1)

- Surestimer la sécurité des sites web
  - https://
  - Sauvegardes inexistantes ou non fiables
  - Accès administrateur non sécurisé
  - Mots de passe stockés
  - Failles de sécurité non résolues
  - Objectifs cachés
- Multiples

Méconnaissance (2)

- Exposer les enfants aux dangers
  - Contenu inapproprié
  - Cyber harcèlement
  - Mauvaises rencontres
  - Infos privées publiées ad vitam
  - Tentatives d'escroquerie
  - Dépense d'argent involontaire
  - Téléchargements de malwares
  - Addiction, problèmes de sommeil, de concentration
- Multiples

Méconnaissance (3)

- Être manipulé
  - Ingénierie sociale : attaques basées sur la peur, l'ambition, la curiosité, l'urgence, la bienveillance, la culpabilité…
- Tomber dans le piège de l'addiction
- Faire des achats en ligne frustrants
  - Escroqueries, engagements non tenus (délais, qualité, quantité)
- Ne pas respecter la législation
  - Vie privée
  - Patrimoine numérique
  - Signature numérique

- Multiples

- Santé
- Insatisfaction, Coûts €

- Poursuites

Malveillance (1)

- Vol ou destruction de matériel
- Vol, substitution, transformation des données
  - Bancaires
  - Identité
  - Données médicales
  - Photos, vidéos
  - Créations
  - Courriels
  - Agenda
  - Projets
  - Opinions

- Perte de donnée + Indisponibilité + coût €
- Multiples
  - Coût €
  - Usurpation
  - Exploitation préjudiciable
  - Usurpation, harcèlement
  - Spoliation
  - Exploitation préjudiciable
  - Exploitation préjudiciable
  - Spoliation, sabotage
  - Harcèlement, condamnations

Malveillance (2)

- Être victime de harcèlement sur les réseaux sociaux
- Attaques par les courriels
  - Pourriels
  - Hameçonnage
  - Canulars

- Infection par logiciels malveillants
  - Virus
  - Chevaux de Troie
  - Logiciels espions
  - Rançongiciels

- Santé, réputation

- Multiples
  - Perte de temps
  - Escroquerie
  - Réputation, diffusion de malware
- Tout peut arriver

  Usurpation d'identité, chantage, perte de données, de temps, d'argent, de réputation, de relations, de travail

Actions de réduction du risque

Rappels

- La réduction du risque peut diminuer
  - Sa probabilité
  - La gravité de ses conséquences
  - Les deux
- On ne met en œuvre que les actions de réduction dont les conséquences sont moins contraignantes que celles du risque

- Ces actions sont
  - Locales
    - Sur le matériel
    - Sur le logiciel
    - Sur les données
    - Sur le réseau local
    - Sur les habitudes
  - Sur l'utilisation d'internet
    - Sites visités
    - Diffusion de données
    - Communication avec des tiers

Actions de réduction locales

- Sur le matériel
- Sur le logiciel
- Sur les données
- Sur le réseau local
- Sur les habitudes

Réduction des risques sur le matériel

- Entretien
  - Garder les aérations dégagées
  - Éviter les miettes et les boissons dans les claviers
  - Ranger et attacher les câbles
  - Installer le matériel de façon stable
  - Le tenir à distance de l'eau, des radiateurs et de l'exposition directe au soleil
  - Remplacer les disques, clefs USB et cartes mémoires avant qu'ils ne lâchent. Ils ont une durée de vie limitée
  - Toujours arrêter son ordinateur proprement et éteindre l'écran en dernier
  - En cas de pannes de courant fréquentes, installer un onduleur
  - Retirer les CD, DVD et toutes les prises avant de déplacer l'ordinateur

Réduction des risques sur le logiciel

- Applications
  - N'installez que ce dont vous avez réellement besoin
  - Utilisez systématiquement les procédures de désinstallation
  - Ne téléchargez que sur les sites officiels
  - Méfiez-vous des TOP-x
  - Open source et logiciels libres ?
    Il est possible de vérifier/modifier ce que fait le logiciel…
- Mises à jour
  - Système d'exploitation
  - Antivirus
  - Logiciels installés
  - Ne mettez pas tout à jour en même temps

Réduction des risques sur les données

- Faire des sauvegardes
  - Etendue : complète / données seules / changements
  - Périodicité : changement / jour / semaine / mois
  - Localisation : autre disque ou DVD-rw / autre pièce / cloud
  - Méthode : copie / compression / chiffrement

- Gérer les données sensibles
  - Identifier : plusieurs niveaux de sensibilité possibles
  - Regrouper : les informations sensibles dispersées sont difficiles à protéger
  - Protéger : chiffrement avec un algorithme sûr (ex: AES, AES-CBC)
  - Métadonnées : fichiers bureautiques, photos, vidéos

- Effacer les données de façon définitive
  - Avant de jeter, donner ou vendre un objet qui contient des informations

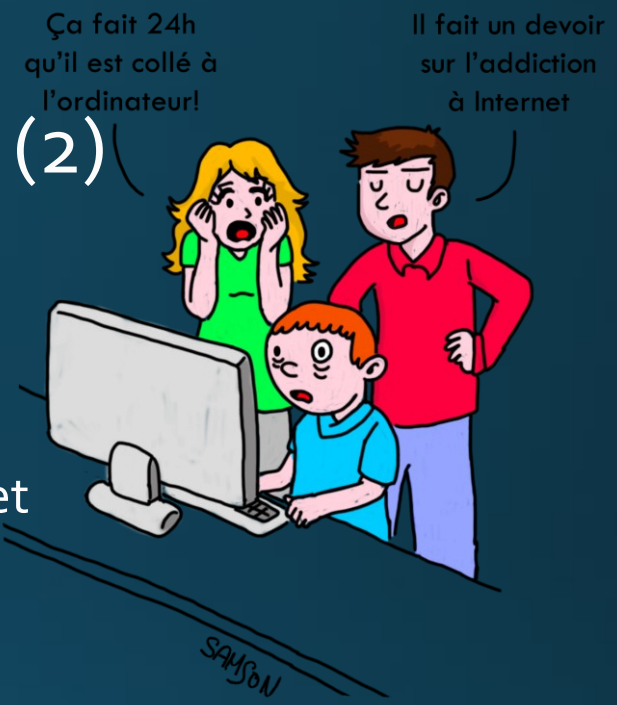
Réduction des risques sur le réseau local

- Sécuriser la box
  - modifiez le nom d'utilisateur et le mot de passe par défaut (généralement «admin» et «oooo») de votre page de configuration accessible via votre navigateur Internet
- Sécuriser son Wi-Fi
  - protocole de chiffrement WPA2 ou au pire WPA-AES (n'utilisez jamais le chiffrement WEP cassable en quelques minutes)
  - modifiez la clé de connexion par défaut avec un mot de passe robuste
  - ne divulguez la clé qu'à des tiers de confiance et changez-la régulièrement
  - Utilisez l'assistance technique de votre fournisseur d'accès

Réduction des risques sur les habitudes (1)

- Séparer les usages
  - ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles
  - ne stockez pas de données professionnelles sur vos équipements communicants personnels
  - Attention au BYOD
- Lors des déplacements
  - Sauvegarde sur un support amovible
  - Gardez vos appareils avec vous

Réduction des risques sur les habitudes (2)



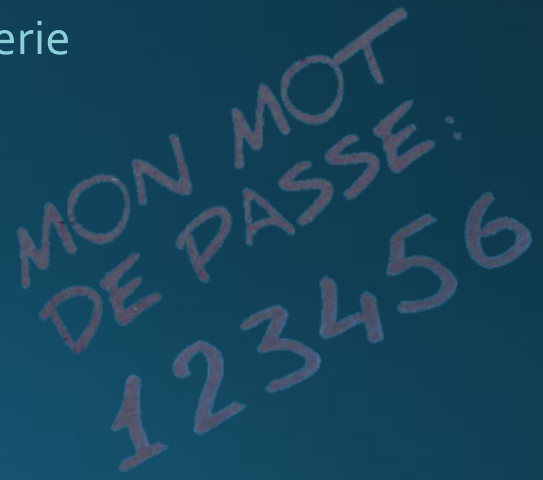
- Protéger les enfants
  - Mettre une limite d'âge. Réseaux sociaux à partir de 13 voire 15 ans
  - Donner des règles claires sur le temps qu'ils peuvent passer sur Internet
  - Activer le contrôle parental pour limiter les risques d'exposition à des contenus choquants
  - Mettre l'ordinateur et la tablette dans une pièce commune
  - Les sensibiliser aux dangers des réseaux sociaux… (cyber harcèlement, usurpation d'identité, personnes mal intentionnées, jeux pervers…)
  - Les accompagner dans la protection de leurs données personnelles, les informations et photos mises en ligne leur échapperont pour toujours
  - Adapter les contenus. Pour les jeux, se fier à la norme PEGI
  - Être vigilant vis-à-vis des «challenges» qui se propagent très rapidement
  - Contacter Net Ecoute, le numéro vert national **3018** en cas de cyber harcèlement

Actions de réduction sur Internet

- Sites visités
- Diffusion de données
- Communication avec des tiers

Réduction des risques sur les sites visités (1)

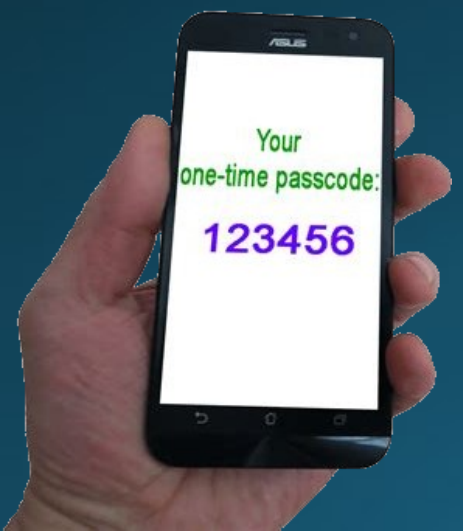
- Avant toute saisie ou connexion
  - https:// pour sécuriser la connexion et vérifier chaque caractère de l'adresse du site
- Utiliser des mots de passe efficaces
  1. Suffisamment longs (au minimum 12 caractères)
  2. Impossibles à deviner (aucun lien avec vous) , surtout pour la messagerie
  3. Faciles à mémoriser (ou utiliser un gestionnaire de MDP sécurisé)
     - Méthode des 1ères lettres : 1tvmQ2tl'A
     - Méthode phonétique : ght8CD%€7am
     - Mots aléatoires du dictionnaire : vacherosehelicopterepoilu
     - Ou votre propre méthode



- Gérer ses mots de passe
  - Les modifier au moindre soupçon et changer ceux mis par défaut
  - Utiliser un mot de passe différent pour chaque service
  - Ne jamais donner ses mots de passe ou les utiliser sur du matériel en libre accès
  - Attention aux questions secrètes qui permettent de réinitialiser le mot de passe
  - Certains sites ont des exigences sur les caractères

Réduction des risques sur les sites visités (2)

- Activer l'authentification à deux facteurs lorsqu'elle est disponible
  - 2 facteurs différents parmi ce qu'on sait, ce qu'on possède, ce qu'on est
  - En général en plus du mot de passe on utilise un code fourni par son téléphone
    - Le code est un mot de passe à usage unique (OTP)
    - Envoyé par SMS ou par courriel
    - Ou fourni par une application (TOTP basé sur le temps)
      - FreeOTP
      - Google Authenticator
      - Authy
      - Microsoft Authenticator
      - Sophos Authenticator
      - …



Réduction des risques sur les sites visités (3)

- Eviter les sites douteux ou illicites
- Faites vos achats en ligne et téléchargements avec prudence
  - Fuyez les offres trop alléchantes
  - Vérifier les mentions légales, les CGV, l'identité du vendeur
  - Contacter le vendeur (téléphone, courriel) pour vérifier qu'il est sérieux
  - Rechercher des avis sur le vendeur avec le mot « arnaque » ou « escroquerie »
  - Renoncer si le moindre doute subsiste

- Prudence aussi avec les moteurs de recherche
  - Les premières réponses sont souvent « sponsorisées »
  - Vos recherches sont exploitées à d'autres fins que de vous rendre service
  - Il existe des moteurs qui n'ont pas ces inconvénients : DuckDuckGo, Qwant…
- Ordinateur partagé : utilisez le mode de navigation privée

Réduction des risques sur la diffusion des données

- Identifier les informations sensibles
  - Tout ce qui permet d'usurper votre identité, de vous faire du chantage et de vous nuire directement ou indirectement
- Ne confier que ce qui est nécessaire
  - Uniquement à des sites ou des tiers dans lesquels vous avez confiance
  - Dont vous savez qu'ils ont la capacité à sécuriser les informations confiées

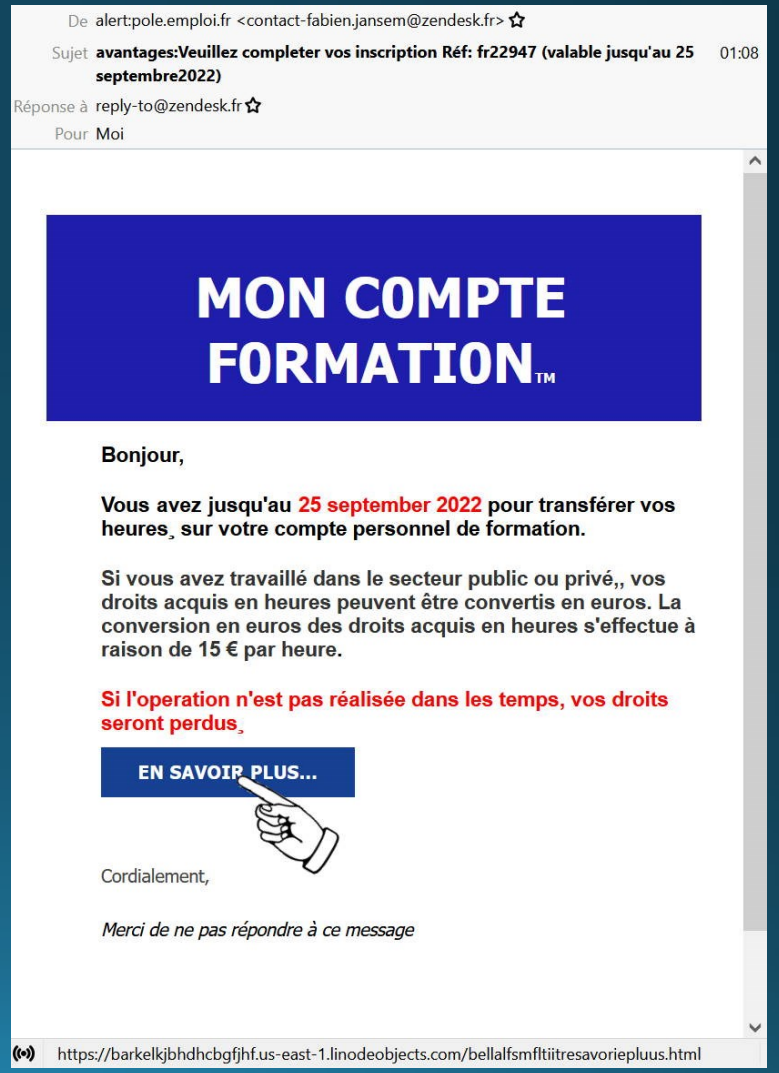
L'art de recouper les données

Selon Arvind Narayanan, professeur américain à Princeton et spécialiste de la recherche sur le recoupement des données :

- 95% des possesseurs de smartphones peuvent être ré-identifiés par le croisement d'au moins quatre de leurs positions géographiques, telles que celles contenues dans les métadonnées des photos prises sur mobile.
- En se basant sur deux localisations, comme le trajet récurrent domicile-travail, 50% des gens seraient identifiables.

Réduction des risques sur la communication (1)

- Courriels
  - l'identité d'un expéditeur n'est jamais garantie : vérifier la cohérence avec le contenu du message
  - n'ouvrez pas les pièces jointes d'un mail non attendu ou provenant d'un expéditeur inconnu
  - n'ouvrez pas les pièces jointes dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts
  - vérifiez l'adresse du site en passant votre souris sur chaque lien avant de cliquer. Si vous avez un doute sur l'adresse affichée en bas, ne cliquez pas.
  - ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles
  - n'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc.
  - L'affichage des images peut donner des informations à l'expéditeur



Réduction des risques sur la communication (2)

- Réseaux sociaux
  - Faites très attention aux posts, photos et vidéos qui vous échapperont dès que publiées. Il est impossible d'effacer ce qu'on ne sait pas localiser
  - Paramétrez vos comptes sociaux pour ne laisser l'accès qu'aux personnes choisies
  - Limitez vos informations personnelles au strict nécessaire
  - N'acceptez pas des inconnus comme amis
  - Soyez respectueux des autres. Ne publiez une information que si vous en avez vérifié la véracité et obtenu l'autorisation des intéressés. Pas de fake-news
  - Expliquez les risques à vos enfants et surveillez, sans vous immiscer, leurs comportements sur le web-social.

Liens

- https://www.cybermalveillance.gouv.fr
- https://www.gouvernement.fr/risques/cybercriminalite
- https://www.interpol.int/fr/Infractions/Cybercriminalite
- https://fr.wikipedia.org/wiki/Gestion_des_risques

Merci de votre attention