Explications et sources des modules de l'outil de quantification du risque cyber

Numérotation et explications/sources du schéma global de l'outil.

Sélection choix attaque : 3 attaques parmi les plus fréquentes (DDoS, Phishing, Ransomware)

Source : https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/#:~:text=Les%2010%20types%20de%20cyberattaques%20les%20plus%20courants,8%208.%20Attaque%20par%20%C3%A9coute%20illicite%20%C3%89l%C3%A9ments%20suppl%C3%A9mentaires

Bloc « fréquence » :

BLOC PROBA SURVENANCE D'UNE ATTAQUE A_i POUR LA GARANTIE PERTES D'EXPLOITATION.

- 1ere sous branche :

  - 5 : Score lié aux caractéristiques de l'entreprise [0,1], S_c

    - 1 : **Taille de l'entreprise C**

      4 choix (<10, 10-49, 50-250, >250) donnés par l'OCDE.

      Source : OCDE : Entreprises selon leur taille, https://data.oecd.org/fr/entrepreneur/entreprises-selon-leur-taille.htm, 2019
      Puis pourcentage de prévalence attaques cyber selon taille d'entreprises
      Source : ANSSI, Panorama de la menace 2022

    - 3 : **Pays de l'entreprise C**

      5 choix (Afrique du Sud, Namibie, Tanzanie, Liberia, Mozambique) basés sur rapport de la CNUCED

      Source : CNUCED, La contribution potentielle de la zone de libre-échange continentale africaine à une croissance inclusive.

      Puis utilisation du score créé par la Global Security Index pour mesurer l'engagement cyber des pays.

      Source : Global Cybersecurity Index : Classement des pays Africains en 2020

    - 2 : **Secteur d'activité de l'entreprise C**

      4 choix (Industrie, Agriculture, Services de santé, banque/assurance). Utilisation des pourcentages pour les secteurs d'entreprise d'une attaque cyber.

Source : Statista, https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/#:~:text=Distribution%20of%20cyber%20attacks%20across%20worldwide%20industries%20in,telecom%200%25%205%25%2010%25%2015%25%2020%25%2025%25%2030%25

- 4 : **Score** = Moyenne des caractéristiques

➢ 6 : **$P(A_i, G)$** = probabilité qu'une attaque Ai déclenche la garantie G, peu importe les caractéristiques de l'entreprise
Source :
Pour Phishing : the government's Cyber Security Breaches Survey 2022
Pour DDoS : On récupère 16% sur le [Rapport sur les menaces DDoS] de CloudFlare pour DDoS avec demande de rançons qui est le plus courant, on majore cette donnée (+3%) pour prendre en compte l'ensemble des attaque DDoS
Pour Ransomware : SonicWall, [Tendances en matière de cybercriminalité]

➢ 7 : **$P(A_i,G)*S_c$** = 8 : **$P_c(Ai,G)$**, simple multiplication

- 2ème sous branche :

➢ 9 : **Scan de vulnérabilités de l'entreprise C**
Récupère la liste des CVE à l'instant t d'une entreprise C. Dans le code, ensemble de CVE aléatoires dans la base de données de MITRE, taille de l'échantillon en fonction du nombre de machines de l'entreprise.
Cette liste forme le sous ensemble CVE1
Source : CVE - Download CVE List (mitre.org)

➢ 11 : **Liste de CVE exploitables KEV**
Cette liste forme le sous ensemble CVE2
Source : https://www.cisa.gov/known-exploited-vulnerabilities-catalog

➢ 10 : **Liste de CVE à l'origine d'une attaque A_i :** pour chaque attaque, on réalise une liste qui recense toutes les CVE (forcément exploitables) déclenchant cette attaque.
Cette liste (pour l'attaque Ai sélectionnée) forme le sous ensemble CVE3
Quelques sources :
Phishing : Comprehensive analysis of initial attack samples exploiting CVE-2023-23397 vulnerability | Securelist
DDoS : https://www.akaoma.com/ressources/cve/dos-denial-of-service?start=8.
Ransomware : https://www.cybersecuritydive.com/news/CISA-CVE-most-common-vulnerability-2020-2021-ransomware/604426/
Divers : aa23-215a_joint_csa_2022_top_routinely_exploited_vulnerabilities.pdf

➢ 12 : **Intersection des 3 sous-ensembles**
Intersection de CVE1 CVE2 et CVE3 pour obtenir l'ensemble CVE_c.

➢ 13, 14, 15 et 16 : **Calcul score EPSS pour chaque CVE de CVE_c.**
Le score EPSS calcule la probabilité que la CVE soit exploitée dans les 30 jours. Score dynamique.
Source : Exploit Prediction Scoring System (EPSS) (first.org)

- 17 : **Moyenne pondérée des scores EPSS** de chaque CVE pour obtenir une moyenne globale
- 18 : **Obtention de P_c(CVE à l'instant t entraînent A_i ,G)**.

- 3ème sous branche :
  - 20 : **Imaginer des données historiques** de l'entreprise de type sondage :
    - Avez-vous déjà reçu des mails suspects ? Si oui,
    - Combien ?
    - Avez-vous cliqué ?

- 4ème sous branche :
  - 19 : **Imaginer des modules** pour les autres vecteurs d'attaque (CVE, ingénierie sociale, etc.)

22 : **P_c(A_i,G survienne)**

- 20 : **Produit ou moyenne pondérée**, hypothèse d'indépendance des probabilités
- 21 : Si non indépendance des probabilités, alors prendre en compte des **coefficients de corrélation**.

BLOC POUR LA REUSSITE D'UNE ATTAQUE A_i

Dans ce bloc, le manque de données est fort mais contournable.

- Création d'un $score_c$ de réussite/échec d'une attaque A_i pour garantie G [0,1]
  Ce score a pour but d'atténuer/aggraver la réussite d'une attaque cyber lorsqu'elle survient.
  - 25 : **Formation des employés**
    Création d'un sous score formation :
    - Si pas de formation, score = 1
    - Si formation, score dégressif.

    La formation des employés joue un rôle crucial dans la réussite d'une attaque cyber puisque 90% des attaques proviennent d'une erreur d'un employé.
    - 23 : **Type de formation**

      4 choix (Aucune, Risque phishing, Risque cyber généraliste, Risque phishing et cyber généraliste)

    - 24 : **Fréquence des formations**

      3 choix (ponctuelles, occasionnelles, régulières)

      Sources :

      Phishing formation et données chiffrées : Formation de sensibilisation au phishing : 8 infos que vos employés doivent connaître (vadesecure.com)

Sans formation de sensibilisation à la sécurité, un utilisateur sur trois risque de tomber dans le piège du phishing, et mettre son entreprise en danger, selon une nouvelle étude de KnowBe4 (developpez.com)

Cyber généraliste : 12 sujets essentiels de formation à la sensibilisation à la sécurité pour 2021 (usecure.io) Ici compliqué de trouver de réelles données chiffrées puisqu'en général les formations sont découpées en plusieurs sous catégories comme Phishing.

- 26 : **Protections SI**

  Création d'un sous score protections SI :
  - Si pas de protections, score = 1
  - Si protections, score dégressif.

  8 choix de protections SI : mots de passe robustes, authentification à 2 facteurs, navigation sécurisée, firewall, antivirus, chiffrage des données, sauvegardes régulières, mises à jour régulières.

  Le choix de ces protections est combinatoire. Des protections n'auront pas d'effet sur certaines attaques A_i.

  De la même façon, il est compliqué de trouver de réelles données chiffrées sur l'influence d'une protection sur la réussite d'une attaque mais il est possible de savoir quelles protections seront plus efficaces qu'une autre.

  Source : Les 10 mesures essentielles pour assurer votre cybersécurité - Assistance aux victimes de cybermalveillance

- 27 : **Caractéristiques de l'entreprise C**

  Création d'un sous score caractéristiques :
  - Si pas de rotation, pas de mobilité des employés et âge moyen bas, score = 1
  - Sinon, score dégressif.

  Certains facteurs concernant les employés peuvent directement influer sur la réussite d'une attaque cyber.
  - Age moyen des salaries : on peut imaginer que des salariés de +45 ans sont moins alertes sur les dangers du risque cyber, mais manque de données chiffrées.
  - Rotation des salariés : contrebalance les effets des formations. Idem.
  - Mobilité des salariés : utilisation de réseaux non sécurisés par ex.

- 28 : **Données récupérables attaque A_i réussie** (ex : sondage)

  Création d'un sous score lié à la probabilité de réussite d'une attaque Ai dans l'entreprise C. Voir schéma sondage.

- 30 : **Score de réussite/échec d'une attaque**

  29 : **Moyenne pondérée** des 3 sous scores.

31 : **AGREGATION DES 2 BLOCS PAR SIMPLE PRODUIT** → 32 : **OBTENTION DE P_c(G activée par A_i)**

Bloc « coûts » :

- 46, 47 : **Calcul du taux de marge brute : (**revenus N-1 - charges) / revenus N-1
  - 37 : **Calcul des revenus N-1 en fonction des saisons (RM)**
    - 33 : **CA N-1**, donnée entrée par l'utilisateur
    - 34 : **Facteur de saisonnalité**, intervient en fonction du secteur d'activité de l'entreprise C
    - 35 : **Facteur utilisation réseau SI**, représente l'impact du SI sur la production de l'entreprise.
    - 36 : **Simple multiplication** CA * facteur de saisonnalité * utilisation SI pour obtenir les revenus mensuels de l'entreprise C pour une utilisation SI.
  - 45 : **Calcul des charges**
    - 43 : **Masse salariale annuelle**
      - 39 : **Salaire mensuel**, fonction du secteur et du pays d'activité de l'entreprise C

        Source : Salaires des ingénieurs en Libéria | BDEX France (bdeex.com) (à utiliser pour tous les pays)
      - 38 : **Nombre de salariés**, donnée entrée par l'utilisateur parmi les choix disponibles
      - 40 : **Masse salariale mensuelle**
      - 41 : **Multiplication** * 12
    - 42 : **Autres charges** à ajouter, location des locaux, etc…
    - 44 : **Somme** des charges

- 54 : **Durée de l'attaque** (en jours), donnée entrante de l'utilisateur
- 53 : **Revenus prev/jour, N en fonction des saisons**
  - 51 : **CA , N prev** : **multiplication** (50) du **CA N-1** de l'entreprise (48) et de la **tendance du CA** pour l'année N (49)
  - 52 : **Saison de l'attaque**

55, 56 : **LES COUTS POUR LA DUREE D'ATTAQUE CYBER SONT OBTENUS : marge brute * nombre de jours de durée de l'attaque cyber * Revenus prev/jour,N**

Source : MAAF_Conditions_generales_Multirisque_pro_11031.pdf

Calcul du risque

57 : Simple multiplication des blocs : fréquence * coûts , 58 : **OBTENTION DES PERTES POUR GARANTIE PERTES D'EXPLOITATION POUR UNE ATTAQUE CYBER A_i**

Source : Méthode d'analyse FAIR : une révolution pour l'analyse du risque cyber ? (c-risk.com)