Développer des environnements de travail favorables à l'accroissement des compétences cyber des individus

Ayoub Bourhim, Laurent Guillet, Julie Lassalle, Christine Petr

Développer des environnements de travail favorables à l'accroissement des compétences cyber des individus

Ayoub Bourhim, Laurent Guillet, Julie Lassalle, Christine Petr

Contexte et Enjeux

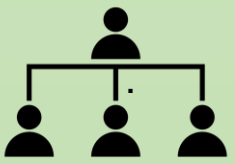
- Coût des cyberattaques entre 2018 et 2020 estimé à **1 billion de dollars** (Smith et al., 2020)
- **45 % des entreprises en France** ont subit au moins **une cyberattaque** en 2022 (CESIN).
- Une urgence pour un monde industriel actuellement en transition vers un modèle connecté avec « **L'industrie 4.0** ».
- Des investissements centrés sur les solutions techniques et peu dans **les acteurs humains**.

Facteurs Individuels

- Des individus souvent perçu comme le «**maillon faible** » de la chaine de la cybersécurité.
- Le postulat de « **l'erreur humaine** » met en cause **les facteurs individuels** comme source des failles de sécurité.
- Des facteurs comme le niveau de compétences ou les biais cognitives,
- Ex. Le biais d'optimisme qui amène à une sous-estimation du risque d'être victime d'une attaque (Moustafa et al., 2021)
- Le rôle des biais cognitifs est d'alléger la **charge mentale.**
- **Perception négative** de l'humain.

Facteurs Contextuels

- **L'organisation du travail** a un poids important sur la perception et les réponses en cas d'attaque cyber (De La Garza et al., 2022).
- **L'organisation du travail** peut entraîner une **surcharge mentale** et **baisser le niveau de vigilance** face à des tentatives d'attaques
- Ex. La **pression temporelle** qui entraine des émotions négatives et du stress chez les individus.



Pour exploiter favorablement les facteurs individuels et contextuels, il faut concevoir des :

Environnements Capacitants

- Considérer l'utilisateur comme un **acteur** de son environnement.
- Co-construire **des environnements de travail permettant le développement des compétences** des utilisateurs en matière de cybersécurité.
- Remise en cause du postulat de « **l'erreur humaine** ».
- **Perception positive** de l'humain.

- Promouvoir une démarche impliquant **l'ensemble des parties prenantes** de l'organisation.
- Envisager la cybersécurité selon **une approche systémique.**

De La Garza, C., Stoessel, C., & Oufi, N. (2022). *Prise en compte des Facteurs Organisationnels Humains en cybersécurité : Aller au-delà de l'erreur humaine*. 42ème Congrès Lambda Mu de l'IMdR, EDF Lab Paris Saclay.
Dejours, C. (2022). Introduction: Vol. 8 éd. (p. 6-22). Presses Universitaires de France.
Lezzi, M., Lazoi, M., & Corallo, A. (2018). Cybersecurity for Industry 4.0 in the current literature : A reference framework. Computers in Industry, 103, 97-110.
Mouchoux, R. (2021, septembre 17). The H-Factor : Turning Human Into The Strongest Link Of Your Cybersecurity Strategy. Conquer Your Risk. https://www.conquer-your-risk.com/2021/09/17/the-h-factor-turning-human-into-the-strongest-link-of-your-cybersecurity-strategy/
Falzon, P. (2010). À propos des environnements capacitants : Pour une ergonomie constructive. In C. Roux (Éd.), Actes du séminaire Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). The Hidden Costs of Cybercrime. 38.
Smith, Z. M., Lostri, E., & Lewis, J. A. (2020). The Hidden Costs of Cybercrime. 38.
Wang, Z., Zhu, H., & Sun, L. (2021). Social Engineering in Cybersecurity : Effect Mechanisms, Human Vulnerabilities and Attack Methods. IEEE Access, 9, 11895-11910.
organisé par le réseau ANACT (p. 60-67).