Cnam Ile-de-France – Formation Ouverte à Distance
Année 2021/2022 – 2nd semestre

CONSERVATOIRE NATIONAL DES ARTS ET METIERS

Correction Examen SEC101 – FOAD IDF

Session 2
Septembre 2022

Durée	3 heures
Document (s) autorisé(s) :	tout document papier
Calculatrice :	x
Téléphone portable :	**Interdit**

Le sujet comporte 3 pages (dont celle-ci).
Barème d'évaluation : voir ci-dessous

Les 8 questions à développement court représentent respectivement 2 pts chacune, sauf la dernière à 3 pts.

1pt pour la présentation et l'orthographe si et seulement si toutes les questions sont traitées

Votre note sur 20.

Courage, la première fois ne fut pas la bonne

« Qu'importe le flacon, tant qu'on a l'ivresse »
Proverbe de fin d'UV

NE SERONT NOTEES SEULEMENT CELLES DONT LES REPONSES SERONT ARGUMENTEES.

Enseignant : Pierre LENOIR

Cnam Ile-de-France – Formation Ouverte à Distance
Année 2021 / 2022 – 1er semestre

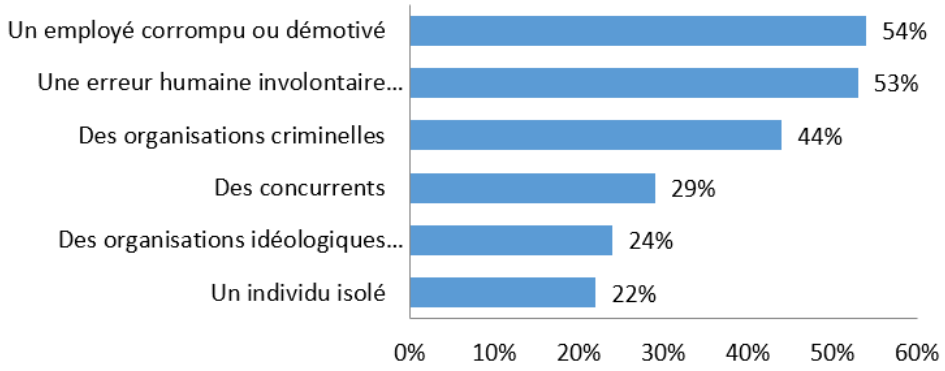
Questions à développement court

1/

Les cybermenaces profitent non pas tant des failles technologiques qu'humaines

La cybercriminalité ne s'appuie pas vraiment sur les failles de sécurité technologiques pour se développer. Elle prolifère surtout à partir des failles de sécurité humaines. C'est ainsi que 99 % des cyberattaques s'alimentent de failles résultant de l'action humaine. On peut voir dans la figure ci-dessous quelles sont les principales sources de failles humaines.

Répartition des principales sources de failles humaines



Source : Le baromètre cybersécurité 2019 par Sylob, L'Usine Nouvelle et Hub One
« *En 2019, 51 % des attaques ont eu recours à des techniques dépourvues de logiciels malveillants, contre 40 % en 2018, ce qui souligne la nécessité d'aller au-delà des solutions antivirus classiques* »10.
La fréquence des « arnaques au Président » (escroquerie aux faux ordres de virement - FOVI) qui n'est pas une cyberattaque à proprement parler - montre à quel point l'humain est au cœur des failles, même les plus évidentes. Ainsi, « *plus de 23 milliards d'euros ont été volés par des cybercriminels depuis 2016, suite à la compromission d'emails centrés sur les individus* »11, que ce soit via l'arnaque au Président, l'usurpation d'identité ou par rançonnage. C'est parce que les hackers en sont pleinement conscients que s'est développée l'ingénierie sociale, forme de cybercriminalité qui consiste à exploiter la nature humaine pour mieux la rançonner.
Parfois, ces failles sont occasionnées par des tiers appartenant au cercle intime des collaborateurs ou des dirigeants d'entreprise. Ainsi, des systèmes ont été pénétrés et ont perdu leur intégrité via les proches de dirigeants ou directeurs qui possédaient des droits étendus sur les systèmes d'information de l'entreprise. Un exemple connu est celui de la compromission d'un système par l'intégration d'un *malware* téléchargé par l'enfant d'un dirigeant : ce dernier cherchait à télécharger illégalement un film, via Bit Torrent, le logiciel légal de pair à pair *(peer-to-peer)12*.

A la lecture de cet extrait :

En tant que RSSI, quel serait vos propositions organisationnelles et techniques afin de se prémunir de ce risque ?

Correction 1 :
On peut noter dans l'extrait de l'article que la plupart des origines des sources humaines sont internes sans que des sources extérieures à l'organisation soit impliquées.
Afin de réaliser un ROSI important, des solutions de sécurisation et contrôle des actions des collaborateurs permettent de couvrir partir

Solutions organisationnelles :

- **Assurer des droits au justes besoins suivant le profil des utilisateurs. On évitera que les dirigeants et responsables supérieurs aient des droits sur tout le SI.**
- **Sensibiliser aux risques**
- **Au recrutement, s'assurer de la probité des personnes**
- **Faire signer une charte d'utilisation des ressources informatiques**
- **Vérifier le niveau de satisfaction des collaborateurs sur la condition de carrière et permettre l'évolution ou le départ de façon saine.**

Solutions techniques :

- **Mettre en place une politique d'audit, de journalisation et d'alertique**
- **Mettre en place une solution de tracage des documents**
- **Mettre une sauvegarde régulière et la rester tout autent**
- **Mettre en place un FW nouvelle génération avec analyse de flux et interdire les flux exotique même initier depuis les zones de confiance (politique de zero trust)**