Lettre d'information économique

Sommaire

Editorial

Confirmant la tendance de ces dernières années, le nombre de cyberattaques a continué d'augmenter en 2020. Dans un contexte de crise sanitaire d'ampleur inédite, le passage rapide et massif au télétravail a été source d'opportunités contribuant à une augmentation significative d'atteintes attribuables à des cybercriminels. L'emploi de techniques cybernétiques élaborées associées à des tactiques très sophistiquées d'ingénierie sociale n'épargne aucune entreprise.

Tous les secteurs d'activité sont, à un degré plus ou moins élevé, touchés par cette crise et ses conséquences économiques. En 2021, leur affaiblissement pourrait donner lieu à une multiplication des vulnérabilités au sein des entreprises et les exposer à des ingérences étrangères telles que des tentatives de rachats, de prises de participation capitalistiques ou l'application de dispositifs juridiques extraterritoriaux pour les affaiblir.

Dans ce contexte, plus que jamais la DRSD est à vos côtés pour contribuer à votre protection, par la sensibilisation de vos personnels, le concours à l'entrave de certaines actions ingérentes ou la protection de vos actifs par des audits conseils ou encore l'instauration de dispositifs de protection de type "zone à régime restrictif".

Général de Corps d'Armée Eric Bucquet
Directeur du Renseignement et de la Sécurité de la Défense

SONDAGE

Votre avis nous intéresse !

Afin de vous proposer des contenus toujours en adéquation avec vos attentes, nous vous proposons de répondre à un questionnaire succinct et anonyme. Les réponses seront d'une aide précieuse pour la réalisation des prochains numéros.

Aucune information confidentielle ne vous sera demandée. Les réponses seront traitées dans leur globalité et uniquement à des fins qualitatives et statistiques.

Pour répondre au questionnaire
je clique ICI

La sensibilisation des collaborateurs

La première des contre-mesures efficaces face aux cyber-malveillances

Un adage bien connu en matière de cyber-sécurité prétend que la principale vulnérabilité d'un système d'information se situe entre un ordinateur et un fauteuil.

En effet, afin de contourner les barrières techniques de sécurité mises en place, les cyber-attaquants cherchent tout particulièrement à identifier et exploiter des failles humaines, en recourant à ce qu'il est coutume d'appeler l'ingénierie sociale.

Celle-ci peut être définie comme un ensemble de techniques de ciblage, de manipulation et de persuasion visant à gagner la confiance de collaborateurs de l'entreprise pour obtenir de leur part, à leur insu :

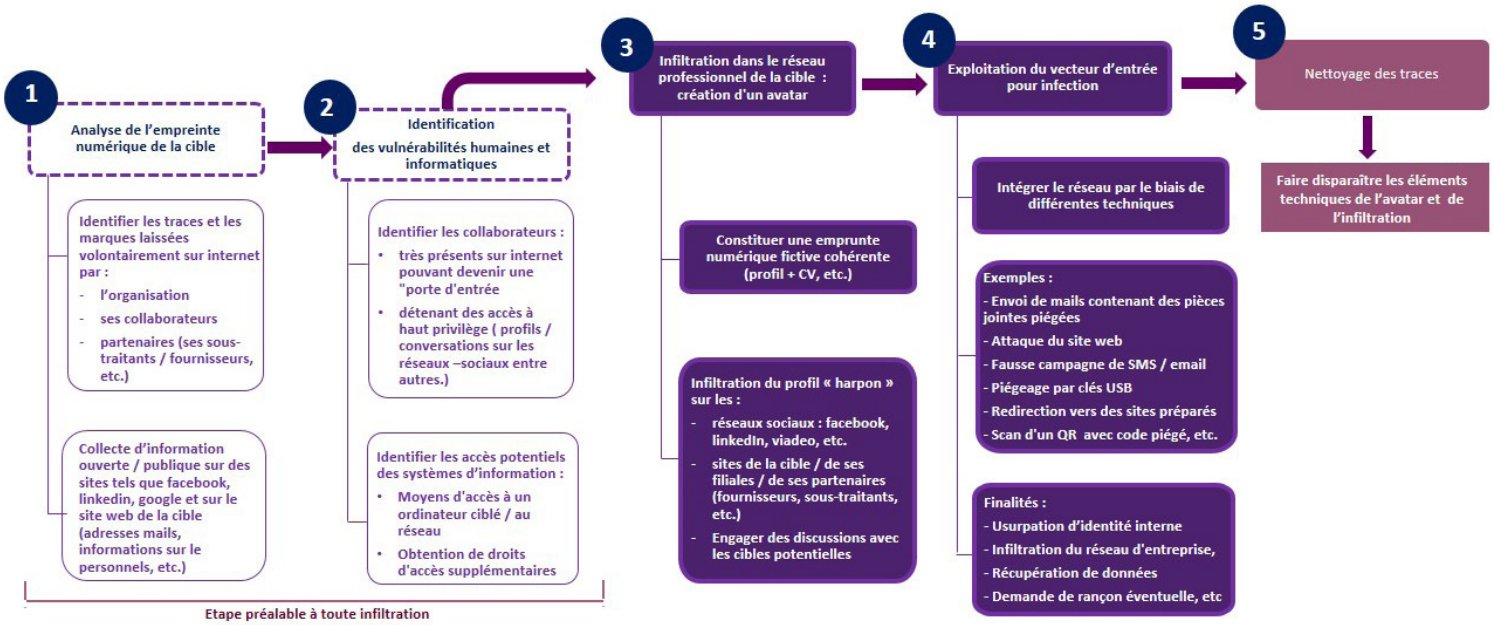
- un accès à un système d'information ;
- la divulgation de données sensibles, d'ordre personnel ou professionnel ;
- voire la réalisation d'une action particulière.

Face à cette menace, la première des contre-mesures efficaces consiste à sensibiliser régulièrement l'ensemble des collaborateurs, en les invitant à :

- ne pas s'exposer sur les réseaux de manière inutile et non maîtrisée, tant professionnellement que personnellement ;
- adopter, en toute circonstance, les bons réflexes comme le fait de vérifier systématiquement la qualité de ses interlocuteurs et de la légitimité des demandes ou de ne pas ouvrir de pièces-jointes suspectes, par exemple.

Dans le cadre de ses actions de sensibilisation au profit de ses partenaires économiques, en complément de celles menées par leurs propres chaînes de sécurité, la DRSD propose des démonstrations techniques concrètes qui permettent à chacun d'expérimenter la réalité des menaces auxquelles il est exposé. Connaissance, vigilance et bon sens suffisent souvent à déjouer un grand nombre de risques.

Anatomie d'une attaque par ingénierie sociale en 5 étapes



drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Cyber sécurité : attention aux affabulateurs !

Dernièrement, la DRSD a eu connaissance des activités d'un escroc mythomane parvenu à tromper la vigilance d'une grande entreprise de services numériques (ESN) en se faisant passer pour un ingénieur en cyber sécurité alors qu'il n'en avait aucunement les qualifications. Engagé et placé dès sa période probatoire sur un programme de défense sensible, il était en attente d'habilitation au secret-défense. L'imposture a été découverte après plusieurs semaines, mettant évidemment un terme au processus et privant définitivement l'individu d'accès à des postes sensibles liés à la défense et nécessitant une habilitation. L'entreprise victime de cette tromperie avait heureusement respecté l'interdiction d'accès aux informations ou supports classifiés (ISC) sans habilitation, limitant ainsi le préjudice subi.

En effet, la cybersécurité, en plein essor, est parfois sujette à certaines méconnaissances ou exagérations, voire à certains phantasmes, quant aux opportunités et capacités techniques réellement offertes. En conséquence, le secteur attire aujourd'hui des escrocs et des affabulateurs qui tirent profit de l'actuelle pénurie en ressources humaines et peuvent dissimuler leurs impostures derrière la technicité du domaine. De plus, de façon opportuniste, ces individus malveillants peuvent tenter d'approcher des entreprises en s'appuyant sur des dispositifs particuliers d'aides financières, mis en place pour faciliter l'accès des PME et TPE aux prestations en cybersécurité. En effet, si de tels outils contribuent à diminuer le coût de la cyber sécurité pour les entreprises, ils constituent également un effet d'aubaine pour les escrocs qui usent des faibles coûts affichés comme d'un levier pour convaincre des entreprises d'avoir recours à leurs services.

Au-delà des pertes de temps et d'argent causées par ces impostures, les entreprises peuvent se voir dérober des données sensibles et mettre à mal leurs systèmes d'information ainsi que leurs réputations par des individus malveillants ou parfois simplement déséquilibrés. Capables de produire de faux documents et doués pour la manipulation, ces derniers représentent une menace avérée.

Afin de se préserver de ces situations, la DRSD recommande aux entreprises de vérifier de façon approfondie les qualifications des candidats à l'embauche ou susceptibles de réaliser des prestations, en particulier lorsque, dans le contexte actuel de pénurie de ressources humaines, les opportunités qui se présentent semblent au-delà des attentes légitimes et raisonnables.

Formation en sécurité économique

L'institut des hautes études de défense nationale (IHEDN) renforce sa promotion d'une culture sur les enjeux de sécurité de défense et propose une nouvelle session nationale : « Majeure Défense et Sécurité Economique »

Objectifs et apports de la nouvelle majeure "défense et sécurité économique"

1. Favoriser **la diffusion d'une véritable culture de sécurité et d'intelligence économique ;**
2. Explorer à travers **huit modules** les principales questions soulevées par ce nouvel impératif de défense et de sécurité :

- Les nouvelles frontières technologiques sont-elles le nouvel horizon de la souveraineté économique française et européenne ?
- Dans quelle mesure l'autonomie stratégique implique-t-elle désormais la sécurité économique ?
- Comment assurer la souveraineté numérique à l'heure des grands oligopoles USA-Chine ?
- Quels enjeux juridiques soulèvent la défense et la sécurité économique ?
- Quelles sont les spécificités de la base industrielle et technologique de défense (BITD) dans le paysage international ?
- Quelles sont les sources de déstabilisation aujourd'hui ? Que seront-elles demain ?
- Comment assurer le déploiement territorial de la politique de sécurité économique ?
- Comment traduire en actions le renseignement d'intérêt économique ?

MAJEURE "DÉFENSE ET SÉCURITÉ ÉCONOMIQUE"

Période de formation **septembre 2021 à juin 2022**
Formation dispensée en **38 jours environ**
Nombre d'auditeurs : **40 auditeurs**

LIEUX DE FORMATION

Paris et missions d'étude en France et à l'étranger

Apport de la majeure pour les auditeurs

- Forger une communauté de compétences et d'engagement conjoint au service de la défense et de la sécurité économique.
- Engager une réflexion partagée sur les enjeux interministériels et intersectoriels de la politique de défense et sécurité économique.
- Élaborer des propositions d'actions innovantes visant à identifier les sujets clés de demain.
- Acquérir des méthodes d'analyse prospective.
- Dépasser sa sphère d'expertise spécifique pour appréhender les enjeux stratégiques dans leur globalité et leur complexité.

DATES A RETENIR

Recueil des candidatures en ligne

- A compter du 23 novembre 2020

Clôture des candidatures

- 28 mars 2021

Entretiens avec les jurys de sélection

- du 1er mars au 31 mai 2021

Publication au Journal officiel de la liste des auditeurs de la session nationale 2021-2022

- 1er - 15 juillet 2021

CONTACTS

Pour toutes questions relatives au contenu de la majeure : dse@ihedn.fr
Pour toutes questions relatives au processus de recrutement :
01 44 42 47 06 - recrutement.auditeurs@ihedn.fr

Gardons contact

Restons en contact

Direction zonale Sud Ouest

drsd-bordeaux-cie.contact.fct@intradef.gouv.fr