Capgemini RESEARCH INSTITUTE

AVRIL 2020

Renforcer l'immunité en matière de cybersécurité : faire face aux risques de cybersécurité dans le monde actuel du télétravail

À mesure que la pandémie de COVID-19 resserre son étau, le télétravail devient la nouvelle norme pour de nombreuses entreprises. Selon une enquête récente, 85 % des entreprises déclarent qu'au moins la moitié de leur personnel travaille à domicile en raison du COVID-19[1].

Le passage à un modèle d'exploitation en télétravail a des implications importantes pour la sécurité informatique et la cybersécurité, avec des risques croissants. Par exemple, chez Cisco Systems, le nombre de demandes d'assistance de la part des télétravailleurs pour des problèmes de sécurité a décuplé ces dernières semaines[2]. Il existe également des risques accrus d'attaques cautionnées par des États pour pénétrer des infrastructures critiques telles que celles des soins de santé, des organisations humanitaires et des services financiers[3]. Les infrastructures critiques, notamment les hôpitaux et les services de livraison de nourriture, ont connu une augmentation des attaques. Un établissement médical en Europe a récemment été victime d'une cyberattaque suffisamment grave pour nécessiter le report d'une opération chirurgicale urgente, le transfert de patients dans un état critique dans des établissements voisins et l'arrêt de l'ensemble du réseau informatique[4].

Pendant cette crise, deux facteurs sont importants pour les chefs d'entreprise. Tout d'abord, comprendre pourquoi la cybersécurité doit être un domaine d'action clé pour leur entreprise pendant la crise COVID-19. Et, deuxièmement, comprendre quelles sont les meilleures pratiques qui sont essentielles pour améliorer la sécurité dans le cadre du télétravail.

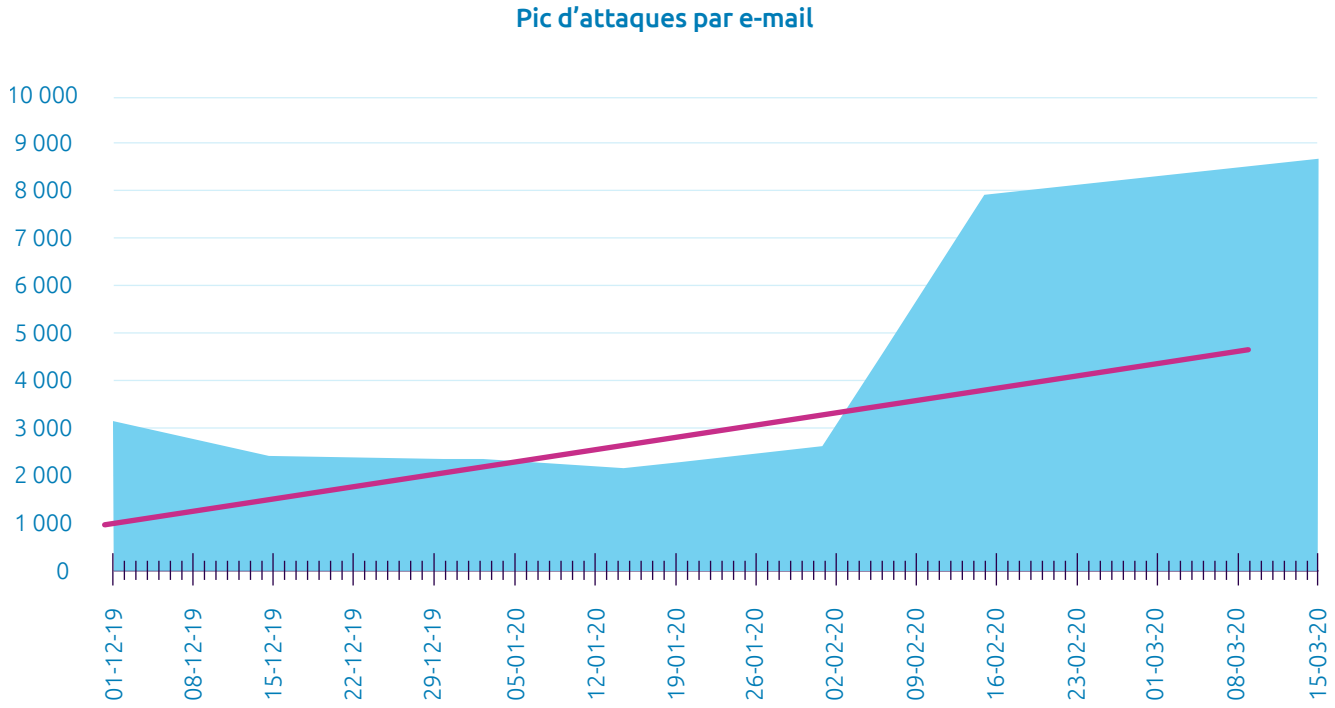
La cybersécurité doit être au centre de la crise COVID-19

La crise COVID-19 présente de nombreux défis en matière de cybersécurité. Une situation où les employés travaillent généralement de chez eux offre davantage de possibilités aux cybercriminels, une conséquence du changement de la surface d'attaque et de l'environnement de travail. Les cybercriminels incitent également les employés et le grand public à accéder à des sites Web frauduleux et à ouvrir des e-mails d'hameçonnage, en misant sur le fait que les gens sont impatients de recevoir des conseils, des consignes et des nouvelles sur le coronavirus. Ces attaques de cybersécurité exploitent la peur et le doute que le coronavirus a créés dans les esprits, incitant les gens à prendre de mauvaises décisions en matière de sécurité. Par exemple, les cybercriminels montent des cyberattaques en demandant aux employés de télécharger les dernières données sur le coronavirus d'un site Web ou de fournir des renseignements sur leur entreprise pour obtenir des aides du gouvernement.

Tom Hale, président de SurveyMonkey, confirme cette tendance : *« Nous avons constaté une augmentation des tentatives d'hameçonnage liées au COVID-19, qui jouent sur l'émotion et se servent de la crise pour créer un sentiment d'urgence. »* [5]

En Italie, l'un des pays les plus touchés par le virus, la première vague de la pandémie s'est accompagnée d'un pic de connexions anormales aux messageries électroniques (voir Figure 1).

Figure 1 : Les incidents de cybersécurité atteignent des sommets en Italie



Source : Données télémétriques sur les menaces mondiales Cynet, mars 2020[6]

Nous observons un phénomène similaire dans d'autres pays ces derniers temps. En France, l'Agence nationale de la sécurité des systèmes d'information a publié une mise en garde contre les attaques de rançongiciels visant les collectivités locales[7]. Les e-mails d'hameçonnage (des e-mails personnalisés envoyés à certains utilisateurs pour les inciter à partager des informations sensibles) ont également augmenté à un rythme effréné au cours des trois derniers mois. Par exemple, les attaques d'hameçonnage par e-mail liées au COVID-19 ont augmenté de 667 % depuis fin février[8]. *« Je n'ai jamais vu un tel volume d'hameçonnage. Je vois littéralement des messages d'hameçonnage dans toutes les langues de la planète »*, ajoute Marc Rogers, vice-président de la stratégie de cybersécurité chez Okta, une société de gestion des identités et des accès, et responsable de la sécurité chez Defcon[9].

Renforcer la sécurité des télétravailleurs

Alors que le monde est confronté à une crise humanitaire majeure liée au COVID-19, les entreprises doivent également s'attaquer d'urgence aux risques de cybersécurité accrus qui accompagnent cette situation. Selon notre expérience, la meilleure stratégie comporte trois phases distinctes :

667 %

D'AUGMENTATION DES ATTAQUES D'HAMEÇONNAGE PAR E-MAIL LIÉES AU COVID-19 DEPUIS FIN FÉVRIER

PHASE 1

- Sensibiliser les employés aux problèmes de cybersécurité liés au COVID-19
- Élaborer des consignes de cybersécurité pour les télétravailleurs

PHASE 2

- Améliorer la surveillance à distance et les capacités de détection des cybermenaces
- Augmenter les capacités de cybersécurité grâce à des outils basés sur l'IA
- Déployer l'orchestration, l'automatisation et la réponse aux incidents de sécurité
- Collaborer en externe pour échanger sur les cyberattaques liées à la crise du COVID-19

PHASE 3

- planifier un retour échelonné au réseau d'entreprise
- Identifier les points de défaillance potentiels des systèmes et revoir les protocoles de sécurité

Phase 1 : sensibiliser les employés aux défis de cybersécurité liés au COVID-19

Des consignes complètes en matière de cybersécurité doivent être élaborées pour les télétravailleurs, puis mises à jour et partagées en temps réel. Matt Petrosky, vice-président de l'expérience client chez GreatHorn, une société spécialisée dans la sécurité des e-mails dans le cloud, explique : *« Les entreprises devraient... mettre en place des mécanismes pour renforcer ces politiques au moment où elles ont le plus besoin d'être appliquées (par exemple dans le contexte d'un e-mail demandant une action financière ou des informations confidentielles), afin que les utilisateurs puissent prendre des décisions éclairées avant d'interagir avec des e-mails suspects. En rappelant aux employés les politiques en vigueur au bon moment, les entreprises peuvent réduire considérablement les risques associés au télétravail. »* [10]

D'autres exemples d'initiatives de sensibilisation essentielles :

- Mener des campagnes de sensibilisation à la sécurité dans toute l'entreprise afin d'informer les employés des problèmes de cybersécurité auxquels ils peuvent être confrontés lorsqu'ils travaillent de chez eux.
- Comme les employés travaillent de chez eux, ils ne sont pas forcément en mesure d'accéder aux canaux de communication internes via des VPN sécurisés, et les pages Web internes de l'entreprise ne sont peut-être pas la bonne solution pour sensibiliser les employés. La mise en place d'autres canaux de communication ne nécessitant pas de VPN est essentielle pour garantir que tous les employés reçoivent des informations régulières en matière de cybersécurité.
- Informer les employés sur les fraudes par e-mail et les programmes malveillants qui profitent de la pandémie. Il s'agit par exemple de

faux e-mails prétendant provenir de sources authentiques telles que le Centre de contrôle et de prévention des maladies (CDC), l'Organisation mondiale de la santé (OMS), le gouvernement ou les mutuelles. Les e-mails professionnels devraient être une source d'information vitale pour les employés et il sera important de les sensibiliser aux questions de sécurité liées aux e-mails.

- Veiller à ce que les employés soient vigilants face aux e-mails qui leur demandent de partager des données personnelles afin de bénéficier d'aides du gouvernement pour acheter des remèdes, des vaccins et des kits de dépistage.

- Informer les employés des risques potentiels liés à l'utilisation de systèmes de stockage non approuvés, y compris le risque de vol de données.

- Sensibiliser les employés aux risques associés aux fuites de données ou aux violations de la confidentialité des données personnelles, conformément aux lois comme le RGPD, car les employés peuvent utiliser des appareils personnels qu'ils partagent avec d'autres membres de leur famille.

- Partager une liste d'outils de collaboration tiers approuvés pour les employés. Certains outils de collaboration peuvent en effet présenter des failles de sécurité dont les employés n'ont pas conscience.

Phase 2 : améliorer la surveillance et la détection à distance des cybermenaces

Même si de nombreux télétravailleurs utiliseront des appareils fournis par l'entreprise, par exemple des ordinateurs portables, l'utilisation d'appareils personnels sera également répandue. L'utilisation accrue des appareils personnels impose un certain nombre de mesures essentielles :

- Veiller à ce que les applications qui contiennent des données sensibles soient accessibles par le biais d'une application de bureau à distance.

- Veiller à ce que les dispositifs fournis par l'entreprise puissent être effacés à distance en cas de violation.

- Mettre en place une surveillance continue de tous les dispositifs utilisés pour accéder à des données confidentielles et les partager.

Avant le COVID-19, 30 % du personnel de la First Horizon Bank, basée aux États-Unis, était en mesure de travailler à domicile, un chiffre qui est maintenant passé à 50 %. La banque disposait déjà d'un système VPN, mais elle ajoute aujourd'hui divers outils (des bureaux virtuels, par exemple) pour élargir les possibilités de télétravail. La banque a également abordé de front la cybersécurité en ajoutant de nombreux mécanismes de protection et en surveillant étroitement ses réseaux. *« . . . puisque nous avons de plus en plus d'employés en télétravail, [nous] essayons de maintenir notre environnement contrôlé »*, explique Bruce Livesay, DSI de First Horizon. *Il ne fait aucun doute que les cybercriminels cherchent à en tirer profit. »* [12]

Il est essentiel d'améliorer la gestion des identités et des accès (IAM), car les cybercriminels munis d'identifiants volés tenteront d'accéder à des données importantes. Pour les secteurs très réglementés, comme les services financiers et la santé, ce sera un domaine important à prendre en compte pendant cette crise. Privilégier l'authentification multifactorielle à l'authentification unique pour les applications critiques contribuera à améliorer la sécurité. Par exemple, l'entreprise de logiciels « Autodesk » développe l'utilisation de l'authentification à deux facteurs, pour surveiller les risques dans la supply chain technologique de l'entreprise pendant la pandémie[13].

Augmenter les capacités des analystes en cybersécurité grâce à des outils de cybersécurité basés sur l'IA

Les analystes en sécurité ont un immense travail à accomplir. Étant donné que les employés se connectent à partir de plusieurs appareils depuis quelques semaines, il sera difficile de distinguer les véritables menaces des faux positifs. Mais même avant le COVID-19, 56 % des entreprises déclaraient que leurs analystes en sécurité des réseaux étaient « dépassés », en raison du vaste éventail de points de données et de terminaux qu'ils devaient contrôler[14]. Dans cet environnement aux ressources limitées, l'agilité sera donc essentielle. Chez Siemens, l'utilisation de l'IA a permis à l'entreprise de renforcer la sécurité sans augmentation massive des ressources. Le Siemens Cyber Defense Center (CDC) a utilisé AWS (Amazon Web Services) pour créer une plateforme d'intelligence artificielle à haut débit entièrement automatisée et hautement évolutive pour évaluer 60 000 menaces

> « NOUS AVONS CONSTATÉ UNE AUGMENTATION DES TENTATIVES D'HAMEÇONNAGE LIÉES AU COVID-19, QUI JOUENT SUR L'ÉMOTION ET SE SERVENT DE LA CRISE POUR CRÉER UN SENTIMENT D'URGENCE. »
>
> **Tom Hale,**
> Président, SurveyMonkey

potentiellement critiques par seconde. L'IA leur a permis d'atteindre cette capacité avec une équipe de moins d'une dizaine de personnes[15]. **Nos recherches** ont montré qu'avec l'IA, le temps global nécessaire pour détecter les menaces et les violations pouvait diminuer de 12 %[16].

Déployer l'orchestration, l'automatisation et la réponse aux incidents de sécurité pour améliorer la gestion de la sécurité

L'orchestration, l'automatisation et la réponse aux incidents de sécurité (SOAR)[17] désignent des technologies qui permettent aux entreprises de collecter des données et des alertes de sécurité provenant de différentes sources, en exploitant la puissance humaine et la puissance des machines pour l'analyse des incidents. Cette stratégie permet de définir, de hiérarchiser et de piloter des activités normalisées de réponse aux incidents avec des mesures et des rapports améliorés et un temps de réaction plus court. Cependant, nos recherches ont montré que seules 36 % des entreprises l'ont déployé à ce jour[18].

Collaborer en externe pour échanger sur les cyberattaques liées au COVID-19

Les plateformes permettant de collaborer avec d'autres entreprises et de partager les dernières données sur les menaces sont toujours importantes, mais elles le sont particulièrement dans l'environnement de travail virtualisé actuel :

- les grandes entreprises financières européennes (dont Mastercard Europe, la Banque de France, SWIFT, De Nederlandsche Bank et Euroclear) se sont associées à la Banque centrale européenne pour partager des renseignements sur les menaces pour la cybersécurité dans le cadre de l'Initiative de partage d'informations et de renseignements sur la cybercriminalité (CIISI-EU). Les informations seront partagées en ligne et permettront de contrer efficacement les nouvelles cybermenaces[19].
- La X-Force d'IBM, une plateforme propriétaire pour le partage de renseignements sur les menaces, a mis au jour l'attaque Emotet. Il s'agit d'un logiciel malveillant conçu pour tirer parti du COVID-19 au Japon, grâce à des e-mails d'hameçonnage censés provenir d'un organisme d'aide aux personnes handicapées. Une fois ouvert, le document contenu dans l'e-mail télécharge et installe Emotet[20].

Cependant, malgré les avantages évidents de cette démarche, de nombreuses entreprises ne travaillent pas ensemble. Selon les recherches que nous avons menées sur l'IA dans le domaine de la cybersécurité, seul un cadre sur deux déclare partager des renseignements sur les menaces en dehors de son entreprise par le biais de plateformes de crowdsourcing[21].

Aujourd'hui, les entreprises créent des communautés axées sur les cyberattaques liées au COVID-19. Yousuf Khan, DSI d'Automation Anywhere, une entreprise de logiciels d'automatisation des processus robotiques, explique : *« Nous assurons une excellente communication avec les employés, les partenaires et les clients pour identifier et résoudre les problèmes en temps réel. Une crise telle que le COVID-19 peut rassembler une communauté mondiale, et la technologie peut être un vecteur important pour résoudre d'immenses problèmes. »* [22]
La Ligue COVID-19 CTI (cyber-threat intelligence) regroupe quant à elle plus de 800 experts en cybersécurité dans 40 pays. Cette communauté est gérée par des cadres techniques de Microsoft, Okta, Amazon et Clearsky Cyber Security et donne la priorité à la défense des ressources médicales de première ligne et des infrastructures critiques[23].

12 %

DE RÉDUCTION GLOBALE DU TEMPS NÉCESSAIRE POUR DÉTECTER LES MENACES ET LES VIOLATIONS AVEC L'IA

Phase 3 : planifier un retour échelonné au réseau d'entreprise

Si les contrôles de sécurité peuvent fonctionner efficacement dans le réseau de l'entreprise, ils ne sont pas nécessairement aussi efficaces pour l'environnement de télétravail. Par exemple, un VPN n'est pas forcément en mesure de maintenir le trafic élevé généré lorsqu'un grand nombre d'employés travaillent de chez eux. Et comme les employés travaillent pendant de longues périodes sans se connecter au VPN de l'entreprise, leurs ordinateurs portables ou de bureau peuvent être en retard sur les mises à jour et les correctifs. *« Comme de nombreux contrôles et outils de sécurité utilisés par les entreprises dont les employés travaillent sur site dépendent du réseau local, ils ne peuvent pas faire beaucoup de choses à distance »*, explique Lisa Davies, responsable de la sécurité d'entreprise chez Redox, une société de technologie médicale. « *Ces entreprises éprouvent plus de difficultés à*

faire les mises à jour, à surveiller les journaux, etc., si les appareils ne sont pas sur le réseau local, si bien que lorsque les employés les emportent chez eux, elles sont démunies.[24] »

Lorsque la situation reviendra à la normale, il est possible que les ordinateurs portables des employés aient été compromis pendant la crise. Il sera essentiel de veiller à ce que les derniers correctifs antivirus soient mis à jour et de contrôler les appareils de manière échelonnée avant de les connecter au réseau de l'entreprise.

Chaque crise, aussi sombre soit-elle, offre de nouvelles occasions d'apprendre. Ce constat est particulièrement vrai pour les entreprises qui n'ont pas mis en place des dispositifs de télétravail éprouvés. Les capacités de cybersécurité seront mises à l'épreuve en raison de l'augmentation du volume des applications à distance. En surveillant de près ce phénomène et en repérant les failles dans les pratiques de cybersécurité, les entreprises peuvent identifier les points de défaillance de leurs systèmes et revoir les protocoles de sécurité, par exemple pour l'accès aux données et leur transfert.

Wayne Sadin, directeur du numérique de la société de services marketing Affinitas Life, explique : « *Même si vous n'avez pas mis en place un plan de télétravail pleinement opérationnel, c'est le bon moment pour tester et optimiser ce que vous avez.*[25] »

Conclusion

La crise du COVID-19 est particulièrement éprouvante pour la société et l'économie mondiale, qu'il s'agisse de l'intégrité de nos systèmes de santé ou de l'efficacité des supply chains mondiales. Elle teste également nos défenses en matière de cybersécurité. Toutefois, les investissements et l'attention que les entreprises consacrent actuellement à cette question leur permettront d'être encore plus fortes à l'avenir, armées pour exploiter les nouvelles avancées technologiques et fonctionner dans un monde où le télétravail deviendra de plus en plus fréquent.

Ce document fait partie de la série spéciale de notes de recherche du Capgemini Research Institute sur les conseils pratiques pour aider les entreprises à faire face à la pandémie de COVID-19. Vous trouverez d'autres notes de recherche et d'autres conseils et analyses à l'adresse suivante : ***https://www.capgemini.com/fr-fr/notre-groupe/covid-19/***

Auteurs

Thierry Daumas, Head of Projects & Consulting, CIS and Global Offer Lead (GOL), Cybersecurity ; **Steve Wanklin**, Capgemini, Group Chief Cybersecurity Officer ; **Geert van der Linden**, Cybersecurity Business Lead ; **Sandeep Kumar**, Vice President, Capgemini Invent, UK ; **Jerome Buvat**, Global Head of Research and Head of Capgemini Research Institute ; **Subrahmanyam KVJ**, Director, Capgemini Research Institute ; **Sumit Cherian**, Manager, Capgemini Research Institute ; **Gaurav Aggarwal**, Manager, Capgemini Research Institute et **Shahul Nath**, Consultant, Capgemini Research Institute, ont contribué à cette note de recherche.

Pour en savoir plus, n'hésitez pas à nous contacter :

Monde

Thierry Daumas
Head of Projects & Consulting, CIS and Global Offer Lead (GOL), Cybersecurity
thierry.daumas@capgemini.com

Geert van der Linden
Cybersecurity Business Lead
geert.vander.linden@capgemini.com

France

Yves Le Floch
Directeur commercial cybersécurité France, Sogeti
yves.le-floch@sogeti.com

Quentin Gaumer
Global head of Cloud Security Services
quentin.gaumer@capgemini.com

Solutions de télétravail et de collaboration sécurisées

Services de cybersécurité

Références

1. CNBC, "Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems", March 2020
2. Reuters, "Mass move to work from home in coronavirus crisis creates opening for hackers: cyber experts, March 2020
3. ZDNet, "FBI re-sends alert about supply chain attacks for the third time in three months," March 2020
4. ZDNeT, "Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak", March 2020
5. CNBC, "Phishing scams, spam spike as hackers use coronavirus to prey on remote workers, stressed IT systems", March 2020
6. Cynet, "Recent Escalations in Cyberattacks in Italy Prove the Coronavirus Impact on Cybersecurity - Acting as a Warning for CISOs Worldwide", March 2020
7. Wired, "Hackers are targeting hospitals crippled by coronavirus", March 2020
8. TechRepublic, "667% spike in email phishing attacks due to coronavirus fears, March 2020
9. CISOMAG, "International Cybersecurity Experts Come Together to Fight COVID-19 Related Cyberthreats", March 2020
10. SC Magazine, "COVID-19 exposes gaps in cybersecurity safety net as millions work from home", March 2020
11. US Federal Bureau of Investigation's public service announcement, "FBI sees rise in fraud schemes related to the coronavirus (COVID-19) pandemic", March 2020
12. American Banker, "Bank CIOs confront challenge of so many employees working at home", March 2020
13. Forbes, "CIOs Vs. COVID-19: Tech Leaders Are Key To Companies' Emergency Plans," March 2020
14. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
15. AWS, "Siemens Handles 60,000 Cyber Threats per Second Using AWS Machine Learning," April 2019.
16. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
17. Gartner, "Preparing Your Security Operations for Orchestration and Automation Tools," February 2018
18. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
19. The Daily Swig, "Europol joins forces with European financial giants to tackle rise in organized cybercrime," March 2020
20. Capgemini Research Institute, "Reinventing Cybersecurity with Artificial Intelligence", July 2019 report
21. Barracuda, "Threat Spotlight: Coronavirus-Related Phishing", March 2020
22. Cmwire, "CIOs Share Business Continuity Plans Amid COVID-19 Pandemic, March 2020
23. GCN, "Cyber experts line up to defend medical community, critical infrastructure", March 2020
24. SC Magazine, "COVID-19 exposes gaps in cybersecurity safety net as millions work from home", March 2020
25. CIO, "COVID-19's impact on the enterprise and remote work," March 2020

À propos de Capgemini

Capgemini est un leader mondial du conseil, de la transformation numérique, des services technologiques et d'ingénierie. A la pointe de l'innovation, le Groupe aide ses clients à saisir l'ensemble des opportunités que présentent le cloud, le digital et les plateformes. Fort de plus de 50 ans d'expérience et d'une grande expertise des différents secteurs d'activité, il accompagne les entreprises et organisations dans la réalisation de leurs ambitions, de la définition de leur stratégie à la mise en œuvre de leurs opérations. Pour Capgemini, ce sont les hommes et les femmes qui donnent toute sa valeur à la technologie. Résolument multiculturel, le Groupe compte aujourd'hui 270 000 collaborateurs présents dans près de 50 pays.
Avec Altran, le Groupe a réalisé un chiffre d'affaires combiné de 17 milliards d'euros en 2019.

Veuillez vous rendre à l'adresse

https://www.capgemini.com/fr-fr/

People matter, results count.

MACS_CS_20200401_AP