REFLETS
Une autre approche de l'actualité

PAYS :France
PAGE(S) :64-65
SURFACE :169 %
PERIODICITE :Mensuel

DIFFUSION :(6000)
JOURNALISTE :Dorothée Decrop

► 1 juin 2022 - N°143

Cybersécurité : savoir penser prévention dans la transformation digitale

Au printemps 2020, 8 millions de salariés ou fonctionnaires ont vu la totalité de leur activité basculer en télétravail. Dans cette situation hors norme, l'impératif de continuité d'activité a parfois relégué la sécurité au second plan. Pourtant, la cybersécurité est un indispensable corollaire à la transformation digitale des organisations. 54 % des entreprises déclarent avoir subi au moins une attaque en 2021[1].

Par Dorothée Decrop >EXEC M 21

REPÈRES

- *Diplômée du programme Management et Gestion des organisations de l'ESSEC*
- *20 ans d'expérience dans le lobbying et la mise en place de politiques publiques*
- *Déléguée générale d'Hexatrust, groupement d'entreprises innovantes, leaders du cloud computing et de la cybersécurité*

Depuis deux ans, les organisations font face à un grand mouvement de réorganisation. Nous connaissons un important phénomène de dépérimétrisation des organisations. L'authentification des collaborateurs ne se fait plus à l'entrée des entreprises. Les entreprises n'ont pas la garantie de qui se trouve derrière l'écran. Les services cloud remplacent peu à peu les serveurs internes. Les collaborateurs utilisent de plus en plus d'applications pour accompagner leur quotidien, que ces applications aient été ou non validées par l'entreprise. Les fichiers s'échangent de plus en plus et sortent de l'entreprise, tandis que le télétravail a éloigné certains collaborateurs du centre névralgique de l'entreprise. En résumé, les frontières physiques de l'entreprise ont été redéfinies.

Le risque cybersécurité est aujourd'hui identifié comme le risque numéro un pour les entreprises au niveau mondial, et comme le deuxième en France[2]. Si le *phishing* (73 %) est le vecteur d'attaques le plus répandu et doit faire l'objet d'une sensibilisation permanente des collaborateurs, l'augmentation des attaques indirectes par rebond via un prestataire (21 % *vs* 16 % en 2019) n'est pas à négliger en raison de l'impact qu'elles ont sur les relations donneurs d'ordre / sous-traitants. Dans ce contexte, préparer sa cyber-résilience nécessite de dépasser cinq idées reçues.

IDÉE REÇUE N° 1 : LES CYBERATTAQUES N'ARRIVENT QU'AUX AUTRES

Parmi les membres du CESIN[3], plus d'une entreprise sur deux (54 %) déclare avoir subi entre une et trois cyberattaques réussies au cours de l'année 2021. Le rapport sur les risques globaux du Forum économique mondial de 2022[4] rappelle que 2020 a connu une hausse des *malwares* de 358 %, tandis que les rançongiciels ont augmenté de 435 %. La question n'est pas de savoir quand une organisation sera attaquée, mais si elle a mis en place un dispositif suffisamment robuste pour en limiter l'impact.

IDÉE REÇUE N° 2 : LA CYBER EST UNE QUESTION D'EXPERTS

Les fonctions de responsable de la sécurité des services informatiques (RSSI) sont indispensables au suivi et à la résolution des vulnérabilités informatiques internes. Néanmoins, avec 73 % des attaques qui passent par le *phishing* ou l'hameçonnage, la protection interne en matière de cybersécurité est non seulement l'affaire de tous, mais aussi celle de chacun. Les questions de formation et de sensibilisation interne doivent devenir incontournables dans les organisations, et régulières.

Pour être efficace, la politique de cybersécurité ne doit plus être vue comme un sous-ensemble de la stratégie informatique. Sa place est désormais au cœur de la gouvernance des entreprises, portée par la direction ou les Comex. En cas d'attaque, ce sont toutes les

REFLETS
Une autre approche de l'actualité

PAYS :France
PAGE(S) :64-65
SURFACE :169 %
PERIODICITE :Mensuel

DIFFUSION :(6000)
JOURNALISTE :Dorothée Decrop

► 1 juin 2022 - N°143

fonctions d'une organisation qui sont impactées. C'est l'actif à la fois matériel et immatériel qui est touché : les ressources humaines pour la gestion des collaborateurs, la communication pour la réputation, la gestion administrative et financière pour la gestion de la rançon ou le compte de résultat en cas de rupture d'activité, la direction juridique pour la gestion de la plainte et le respect du RGPD, les fonctions commerciales pour la rupture d'activité et l'exploitation des données clients – et enfin, évidemment, les fonctions informatiques pour la gestion des projets IT et leur remédiation.

IDÉE REÇUE N° 3 : LA CYBER EST UN SUJET TECHNIQUE

Parler de la cybersécurité, c'est évidemment parler d'expertise technique et de maîtrise de systèmes d'informations. Mais, malgré les apparences, la cybersécurité est avant tout une question d'humains. Les attaquants sont des humains motivés par des intentions criminelles ou de cyber-espionnage. Les vecteurs des attaques sont des humains qui aujourd'hui en subissent les conséquences directes sur leur carrière[5]. Les victimes sont des humains qui parfois ne se relèveront ni économiquement, ni techniquement, voire ni moralement d'une attaque. Enfin, les défenseurs qui accompagnent les entreprises lors des attaques et de la phase de remédiation sont des parties prenantes dont le choix est tout sauf neutre.

IDÉE N° 4 : LA CYBER, CE NE SONT QUE DES CONTRAINTES

Définir sa politique de cybersécurité grâce au triptyque formation, processus et outils, c'est l'opportunité de redéfinir des leviers de compétitivité. C'est également s'assurer des conditions de partenariats durables avec son écosystème en permettant de rassurer ses interlocuteurs sur la bonne protection contre des attaques indirectes par rebond d'un sous-traitant/co-traitant. D'ailleurs, pour certaines organisations, la politique cybersécurité devient un choix stratégique et vient renforcer la proposition de valeur, comme l'indique le rachat de Tanker par Doctolib.
Enfin, outre la notation financière, la notation ESG (environnement, société, gouvernance) comporte également une référence à la cybersécurité, qui constitue une dimension essentielle de la gouvernance de l'entreprise mais également de la responsabilité sociétale des entreprises sous l'angle de la protection contre le vol des données.

HEXATRUST

Hexatrust est un groupement d'entreprises innovantes, alliant des leaders du cloud computing et de la cybersécurité. Les solutions labellisées Hexatrust répondent toutes à des exigences techniques de maturité, elles sont reconnues en Europe et à l'international par les plus grandes organisations et s'inscrivent dans des logiques de certification et de souveraineté. Les sociétés membres d'Hexatrust œuvrent ensemble pour promouvoir et construire la confiance dans le cloud et l'excellence cyber.
http://www.hexatrust.com/

IDÉE N° 5 : LA CYBER, C'EST CHER

En France, le budget moyen alloué à la cybersécurité est de 3 à 5 % des dépenses informatiques, tandis qu'il atteint environ 15 % aux États-Unis et 22 % en Israël. Ce qui est exorbitant, c'est surtout le coût d'une interruption d'activité, d'une rançon, d'un vol de données stratégiques, la compromission d'information, la réputation. Aussi, la formation et l'investissement en solutions et accompagnement en cybersécurité doivent être résolument perçus comme un investissement en faveur du développement durable des organisations.
En conclusion, il est plus que jamais temps de développer la culture de la cybersécurité au cœur des organisations grâce à la formation et à la sensibilisation des collaborateurs. La politique de cybersécurité repose sur le triptyque formation, processus et solutions de sécurité. C'est la conjugaison d'une bonne sensibilisation, d'un investissement raisonnable et d'une bonne organisation du travail qui assure une prévention efficace contre les cybermenaces. Dans ce contexte, chaque collaborateur se doit d'être un maillon fort.

1. Sondage OpinionWay pour le CESIN.
2. Baromètre Allianz 2022.
3. Club des experts de la sécurité de l'information et du numérique.
4. « The Global Risks Report 2022 », World Economic Forum, Insight Report 17th Edition, in partnership with Marsh & McLennan, SK Group and Zurich Insurance Group.
5. « Les erreurs humaines en cybersécurité sources de licenciement » Jacques Cheminat, Le Monde informatique, 29 mars 2022.