Cyber-virus : l'autre pandémie qui nous menace

Penser qu'un programme de cyber-sécurité implique uniquement le ou la DSI et ne touche qu'à la dimension technique est une erreur majeure. Cela reviendrait à considérer que la crise du coronavirus ne concerne que les médecins et professionnels de santé.
En réalité, venir à bout du Covid-19 aura nécessité un effort collectif : en première ligne les services hospitaliers, à la baguette la classe politique, et à la manœuvre la société dans son ensemble. Il en va de même pour la cyber-criminalité, une menace à laquelle il n'est possible de faire front que collectivement.

Le déploiement interne d'un programme de cyber-sécurité est un projet politique et humain d'autant que 2021 a vu une explosion des cyber-attaques, dont l'ampleur ne cesse de croître.

DSI et épidémiologistes : même combat ?

Peu d'utilisateurs quotidiens le savent, mais en télétravail, le risque de hacking est accru. Pire, ils sont encore moins nombreux à savoir comment s'en protéger.
Face à ce risque grandissant, un programme de sensibilisation devient capital. Il permet d'expliquer les dangers de cette pandémie à l'ensemble des collaborateurs, et de les faire adhérer aux gestes barrières, pour l'enrayer.
Un programme de sensibilisation peut prendre plusieurs formes : vidéos, campagne d'emailing, gamification, quizz…

Néanmoins, dans un souci d'évangélisation et d'adhésion du plus grand nombre, le registre doit être à la fois pédagogique et ludique, et surtout à la portée de tous. Pour être véritablement efficace et s'ancrer durablement dans les consciences, un tel programme doit également s'inscrire dans le long terme.

Sensibiliser, diagnostiquer, traiter : cela ne vous dit rien ? Le DSI pourrait presque endosser la blouse blanche de l'épidémiologiste.

Pas de remède miracle : mais trois gestes barrières

Mobiliser la classe politique…

L'enjeu principal d'une campagne de cyber-sécurité est de faire comprendre à l'ensemble des collaborateurs les enjeux et les techniques de hacking. Il ne s'agit pas d'un projet informatique au sens restreint du terme. Il s'agit d'un programme d'entreprise où, pour susciter une adhésion globale, les directions des Ressources Humaines et de la Communication, doivent être mobilisées dès le début.

La clé de cette adhésion est avant tout humaine, et fonctionne en cascade : du top management à l'ensemble des collaborateurs, en passant par des relais de transmission tels que les comités de

direction. Sans prise de conscience profonde et généralisée, un programme de sensibilisation ne modifiera pas durablement les comportements, sera voué à l'échec, et l'épidémie ne pourra être endiguée.

… pour sensibiliser la population…

La mise en place de moyens techniques ne suffit pas. Pour combattre les cyber-attaques, il faut que les collaborateurs prennent toute la mesure du danger. L'immunisation ne peut s'obtenir que par la sensibilisation.

De son côté, le programme est un outil qui fait office de vaccin. Il s'ancre profondément dans les esprits pour stimuler une réponse immunitaire presque automatique, des réflexes de protection. Afin de gagner en efficacité et en adhésion, une campagne de sensibilisation doit être adaptée à sa cible.

Ainsi, la première étape du programme, certainement la plus cruciale, consiste à évaluer le niveau de familiarisation des équipes avec le sujet. Cette étape prend souvent la forme d'un questionnaire de connaissances.

La campagne peut alors être mise en place et, de préférence, polymorphe. Elle peut notamment prendre la forme de sessions de formations adaptées au groupe de collaborateurs concerné, en se focalisant sur les risques auxquels ils sont particulièrement exposés dans le cadre de leurs fonctions. Tous les collaborateurs peuvent également être impliqués dans une campagne au format vidéo qui présente, épisode après épisode, les différents risques (WAP, hameçonnage, DDoS, cookies…). Le support visuel fait percevoir le poids de cette menace invisible et immatérielle de façon ludique, pédagogique, mais aussi intuitive.

Enfin, dans le cadre d'une organisation internationale, cette campagne de sensibilisation peut aussi prendre la forme d'une compétition entre les pays, pour stimuler l'enthousiasme des équipes grâce à la gamification. Ce challenge permet aussi de mesurer l'adhésion des équipes et de voir si le programme est véritablement pris au sérieux.

… et mettre en place un plan d'action sur le long terme

Une campagne de cyber-sécurité efficace doit être déployée sur le long terme. Le programme doit donc être actualisé de façon régulière, s'adapter au rythme de l'apprentissage des collaborateurs et des évolutions technologiques. Ce plan d'amélioration continue s'appuie sur une évaluation du taux d'atteinte des objectifs du programme. Ainsi, les équipes en charge de la campagne peuvent continuer à distiller l'information auprès des collaborateurs. Définir un taux d'atteinte des objectifs d'une année sur l'autre permet de créer un cercle vertueux, capable d'endiguer l'épidémie sur le long terme.

Vers l'immunité collective ?

L'objectif d'une campagne de sensibilisation à la cyber-sécurité est donc double : réussir à fédérer l'ensemble des collaborateurs sur le long terme, et obtenir un taux d'adhésion élevé. Il s'agit ni plus ni moins d'une conduite du changement qui doit mobiliser l'ensemble des collaborateurs d'une

entreprise et impliquer les parties prenantes pour atteindre le Graal : l'immunité collective.

A l'image de l'épidémie de coronavirus, il faudra cependant faire face aux variants. En matière de hacking, il est impossible de couvrir le champ des possibles, d'autant que les hackers auront toujours une longueur d'avance.

La seule façon de ne pas être trop atteint par cette situation est d'envisager ce défi technologique permanent comme une occasion supplémentaire de repousser les frontières de l'innovation.