Risques cyber : pourquoi opposer assurance et sensibilisation à la cybersécurité ?

Avec la progression constante et continue des cyberattaques, la question de la survie des entreprises les plus fragilisées devient plus prégnante. La surface des vulnérabilités est devenue si large, notamment du fait des nouveaux modes de travail, du shadow IT, ou tout simplement du manque de moyens alloués à la sécurité informatique qu'il parait indispensable, quand il n'est pas trop tard, de définir ou affiner de véritables stratégies de sécurité.

Parmi les priorités identifiées, en particulier avec l'explosion des ransomwares, le choix d'une assurance adaptée apparait rapidement à l'ordre du jour des directions, surtout dans les grands groupes. Pourtant, celle-ci fait débat, notamment du fait des coûts croissants et des pré-requis fixés par les compagnies d'assurance, toujours plus complexes d'après le dernier baromètre du CESIN.

Pourquoi alors, ne pas changer de paradigme et privilégier une double approche, associant à la fois l'assurance à celle de l'anticipation et la connaissance des risques en amont ? En résumé : anticiper pour agir durablement en plus de « panser » immédiatement…

Former chacun des collaborateurs à la cybersécurité, premier rempart contre les cybermenaces En 2021, 70 % des entreprises membres du CESIN ont déployé des modules de sensibilisation aux risques cyber en télétravail et 40 % ont procédé à des simulations d'attaques. Des chiffres en forte hausse par rapport à 2020.

Depuis 2020, les pires scenario imaginés par les analystes en cybersécurité se sont produits. Alors que la cybercriminalité se professionnalise et gagne en puissance chaque jour, l'enjeu est plus que jamais de former des experts cyber, y compris dans le but d'amener chacun-e à se protéger individuellement. Et cela d'autant plus qu'une récente campagne de simulation de phishing a révélé que près d'1 utilisateur sur 5 avait cliqué sur le lien faussement malveillant et téléchargé le malware associé.

Face aux risques, la crise sanitaire a révélé de nombreux retards en matière de pratiques individuelles en environnement de travail et aussi de préparation en cas de crise. Lors de la mise en place des politiques de confinement et du 100 % télétravail, nombre d'entreprises n'étaient pas prêtes à cette modification des modes de travail ni à encadrer l'usage des nouveaux outils et applicatifs liés à ces nouveaux modes de travail.

Et c'est là que l'on a pu mesurer l'ampleur du phénomène de shadow IT. En 2021, une étude de NinjaOne souligne que 41 % des télétravailleurs européens interrogés enfreignaient, parfois sans le savoir, les règles basiques de sécurité en utilisant des machines et applicatifs complémentaires pour réaliser leurs missions.

Cette fragilité des politiques de sécurité informatique se trouve encore aujourd'hui renforcée par la méconnaissance des techniques des cyberattaquants et leurs méthodes de ciblage, toujours plus

sophistiqués. Rançongiciels, attaques DDos (par déni de service), arnaques au Président ou encore phishing, les attaques se sont beaucoup diversifiées, chaque utilisateur étant considéré comme une porte d'entrée potentielle dans les réseaux de l'entreprise.

Face à ce constat, l'acculturation à la cybersécurité est essentielle pour s'assurer que nul ne reste ignorant face aux risques actuels. Certes, la sensibilisation à la cybersécurité par la pédagogie et les modules de formation, est un premier pilier, mais elle ne sert l'objectif d'acculturation qu'en étant récurrente et à jour face aux menaces changeantes. En complément de cette phase d'éducation, des petits programmes de simulation sont utiles car, comme le disait Bouddha, « La réalisation réside dans la pratique ».

Le rôle prépondérant des directions d'entreprise et des prescripteurs de l'enseignement

Parce que s'assurer contre les risques ne suffit pas et ne saurait limiter ni même réduire les risques de cyberattaques, la généralisation des connaissances en matière des risques cyber s'impose et doit être prise en main, non plus par les DSI seuls mais par les directions d'entreprise.

Les collaborateurs eux-mêmes doivent être engagés dans le processus de déploiement de programmes de sensibilisation, afin de répondre à leurs besoins ; de faire l'état des lieux de leurs connaissances et de participer à l'audit des vulnérabilités complets par les experts. Car le facteur humain peut ne plus être une faille mais bien une force dans la sécurité de l'entreprise face aux cybermenaces.

L'école a également un rôle à jouer puisqu'elle forme les esprits de demain. Serait-il incohérent de voir émerger aux côtés des sciences couramment étudiée des cours de sensibilisation et d'introduction à la cybersécurité ? Outre le fait de former les jeunes générations, cela peut aussi être vecteur de transformation par la transmission de savoirs au sein du noyau familial.

Et enfin, être source de vocations, alors que le secteur de la cybersécurité peine encore à recruter des profils. Pour toutes ces raisons, la démystification de ce qu'est la cybersécurité, auprès de tous les publics est plus que jamais nécessaire.

Le cercle vertueux de la sensibilisation

C'est sûr, les jeunes générations auront bien vite une « conscience cyber » et sauront convaincre le reste de la population des enjeux et opportunités que représente la cybersécurité.

Du côté des institutionnels, de nombreuses initiatives, comme Cybermalveillance.gouv, l'ANSSI en France, le Conseil de Sécurité de l'ONU, l'agence européenne de veille (ENISA) jouent un rôle prépondérant dans l'alerte et la sensibilisation aux nouveaux risques cyber.

Dans son nouveau guide d'hygiène informatique, l'ANSSI inscrit d'ailleurs la sensibilisation et la formation au premier rang de ses dix priorités à prendre en compte par l'entreprise. Dans un tel contexte, il y a fort à parier que la généralisation de la sensibilisation à la cybersécurité dans nos entreprises françaises conduise bientôt à une baisse de leurs primes d'assurance