Les économies face au changement : Il est grand temps d'adopter une "culture de la sécurité technologique"

Mohamed El Nemr - Milieu de travail moderne et sécurité - Microsoft Moyen Orient, Afrique et Marchés Emergents

Depuis le début de la pandémie liée à la COVID-19, les failles en matière de cybersécurité n'ont pas cessé de se multiplier et de faire les gros titres des médias. Les cybercriminels ont trouvé dans la crise sanitaire actuelle une belle occasion pour s'en prendre, de manière ciblée et massive, aux entreprises sans défense.

On estime que plus d'un milliard d'Africains auront accès à Internet à l'horizon 2022. Les statistiques actuelles démontrent que la cybercriminalité coûte chaque année à l'Afrique plus de 4 billion USD. Le plus problématique cependant, c'est que la vulnérabilité du continent ne fait que s'accroître à cause des mesures de sécurité qui sont adoptées et qui demeurent à la fois faibles et dépassées.

Aujourd'hui, la tendance est que le monde de l'entreprise commence à adopter un mode de travail de plus en plus "hybride" (certains employés ont choisi de retourner au bureau, d'autres préfèrent travailler depuis leur domicile). Face à cet état de fait, de nouveaux défis commencent à se présenter, notamment pour les entreprises qui n'ont toujours pas choisi de placer la sécurité au centre de leur modèle de gestion. Aujourd'hui, et plus que jamais, les employés qui travaillent à distance devraient commencer à être outillés et préparés à faire face aux "cyberfraudes" de tout acabit.

Les entreprises, tous secteurs confondus, commencent désormais à faire face à une toute nouvelle normalité. Leurs stratégies de sécurité interne se doivent à présent d'être basées sur deux volets importants. Tout d'abord, la sensibilisation : celle-ci doit être réalisée du sommet à la base et doit s'articuler sur l'importance de la sécurité et sur son impact sur l'entreprise. Le second volet doit se rapporter à la nécessité d'investir dans des technologies correctes et sûres, qui restent accessibles à chacun des membres du personnel. Ces deux éléments sont les ingrédients mêmes de l'"intensité technologique" d'une entreprise. Ils conditionnent la manière avec laquelle une entreprise réussit à adopter les toutes dernières technologies et les intègre à son mode de gestion. Ils conditionnent également la manière avec laquelle toute entreprise parvient à construire sa propre capacité numérique.

Vue la pandémie actuelle, les enjeux pourraient même devenir beaucoup plus importants qu'auparavant. Si certaines entreprises sont incapables de surmonter la crise actuelle, d'autres sont en revanche parfaitement outillées pour faire face aux événements les plus imprévisibles.

En matière de cybersécurité, vos employés sont la source de vos plus grands risques

Une enquête menée par Gallagher en 2020 a révélé qu'environ 60 % des violations de données sont causées suite à une erreur humaine (de nombreux employés sont victimes d'e-mails de phishing potentiellement dangereux car ils les consultent sans la moindre protection). La raison est que de nombreuses entreprises n'ont pas jugé important de communiquer avec les membres de leur personnel afin d'expliquer à ces derniers de quelle manière ils pourraient éviter certaines actions dangereuses.

Pour toute entreprise, la formation continue de ses employés devient donc un sujet crucial. Dorénavant, ce genre de formation devrait faire partie intégrante de la stratégie de sécurité durable à adopter par toutes les entreprises. La meilleure manière d'y parvenir c'est de disposer d'un programme et d'un budget qui soit consacrés à la formation et à la sensibilisation. Investir dans les ressources humaine et dispenser, de manière proactive et cohérente, des formations et des actions de sensibilisation suffisantes en matière de cybersécurité, demeurent les moyens les plus puissants qui soient pour se protéger contre les vulnérabilités susceptibles de nuire aux entreprises. Les gestionnaires devraient commencer par définir un plan qui garantirait l'intégration de la formation et de la sensibilisation à sécurité dès le début du cycle de vie opérationnel d'une entreprise. Ils devraient par la suite envisager un budget bien précis qui permettrait de promouvoir la sécurité au sein de l'entreprise.

Une autre manière de s'assurer qu'une entreprise est suffisamment prémunie contre les attaques c'est d'instaurer un environnement "sans honte". Ainsi, et au delà de la sensibilisation et de la formation, il est important de créer un environnement où les employés pourraient facilement partager et parler des vulnérabilités potentielles qu'ils seront susceptibles de rencontrer. Personne ne voudrait perdre son emploi après que l'entreprise au sein de laquelle il travaille soit détruite par une cyberattaque. C'est pourquoi tous les employés ont intérêt à mutualiser leurs efforts afin de prendre position, de manière efficace, contre les cybercriminels.

Investir dans les bonnes technologies

Chez Microsoft, nous sommes depuis toujours engagés en faveur de la sécurité. Nous créons ainsi des technologies qui permettent de protéger nos clients lorsqu'ils utilisent des logiciels ou des services sur le cloud. Notre priorité en matière de sécurité est de pouvoir répondre 24 heures sur 24 et 7 jours sur 7 aux exigences du cycle économique. Nous travaillons en permanence à garantir à nos clients qu'ils ne subiront que très rarement des interruptions de service suite à des événements liés à la sécurité. Afin de réaliser tous ces objectifs, nous investissons plus d'un milliard de dollars par an dans la sécurité. Nous employons également plus de 3 500 professionnels de la sécurité. Nous avons enfin établi de nombreux partenariats avec des écosystèmes de toutes sortes. A l'heure où le monde du travail moderne devient de plus en plus complexe, notre objectif primordial consiste à continuer à développer et à améliorer nos capacités en matière de cybersécurité afin d'aider nos clients à garder en permanence une longueur d'avance vis à vis des menaces qui s'accentuent de jour en jour.

Des solutions de protection, telles que Microsofts 365, aident à atténuer de manière sensible les risques potentiels, tout en fournissant une solution globale de bout en bout qui permet de sécuriser toute la surface d'attaque d'une entreprise. Les entreprises qui optent pour cette solution bénéficient en outre de dispositifs de protection très avancés contre des menaces telles que l'hameçonnage ciblé, ou encore les logiciels de rançon. Cette solution permet aussi de détecter les brèches éventuelles pouvant survenir au sein des dispositifs de protection, de même qu'elle permet d'améliorer les capacités de réaction face à une attaque et de ramener l'entreprise à son état initial de non menace.

Se basant sur le fait qu'il n'existe aucune solution unique pouvant répondre aux besoins spécifiques de toutes les entreprises à la fois, la solution Azure Stack permet de créer et d'exécuter de manière personnalisée des applications hybrides qui s'adaptent à différents types de sites, mais aussi aux bureaux distants et aux clouds.

Aujourd'hui, nous prenons plus que jamais conscience du fait que nous ayons beaucoup de choses encore à accomplir pour permettre d'utiliser les technologies existantes sans encourir le moindre risque. Nous sommes également persuadés que nous ne pourrons jamais avancer si nous ne développons pas une manière de pouvoir collaborer plus efficacement ensemble, mais aussi d'apprendre.