IA, Cybersécurité et Télétravail : la tri-force de l'année 2021

L'année 2020 aura été source de profonds changements à plusieurs niveaux. Il a fallu adapter notre façon de vivre, d'échanger ou encore de travailler au rythme des mesures sanitaires. La pandémie a forcé les entreprises à repenser l'environnement de travail et à équiper les collaborateurs pour qu'ils poursuivent leurs activités à distance. Mais la démocratisation du télétravail a malheureusement offert de nouvelles opportunités aux hackers qui profitent de la confusion et de l'incertitude ambiantes pour sévir. Si le télétravail a permis de sauvegarder des emplois et à certaines entreprises de se maintenir à flot, il n'est pas pour autant sans danger, notamment en matière de cybersécurité.

Disposer de solutions de cybersécurité avancées est désormais essentiel pour faire face à la recrudescence d'attaques et d'escroqueries en ligne à travers le monde. Les récents incidents de sécurité liés au lancement du vaccin contre la COVID-19 ont montré que les hackers n'ont pas d'états d'âme et qu'ils n'hésitent pas à s'attaquer directement à la santé publique. Personne n'est donc à l'abri.

Le monde a changé et les pratiques de cybersécurité doivent évoluer en conséquence. Comment ? Voici quelques pistes détaillées par Charles Eagan, CTO chez BlackBerry

Le syndrome « Netflix » obligera les fournisseurs à se différencier avec des solutions de sécurité basées sur l'IA et le Machine Learning

Il existe aujourd'hui près de 6 000 fournisseurs de solutions de sécurité différents. Alors que les entreprises cherchent à renforcer leurs défenses, elles peinent à choisir les solutions adaptées en raison du nombre de fournisseurs et de technologies et beaucoup d'entre elles sont noyées dans le brouhaha constant de la cybersécurité.

Avant même de mettre en place des solutions de sécurité, les entreprises doivent déjà faire face au syndrome « Netflix ». En clair, lorsque vous vous connectez à l'application Netflix, un très grand nombre de suggestions en tous genres se présente à vous si bien que vous ne savez plus vraiment quoi regarder. Votre moment de détente étant quasiment chronométré, vous ne voulez pas faire le mauvais choix. Côté entreprises, ce n'est pas tellement le temps mais bien le budget qui est limité. Elles veulent alors être sûres d'en avoir pour leur argent et surtout de faire le bon choix en matière de sécurité. S'il est facile de « zapper » sur Netflix, il est bien plus difficile de changer de fournisseur de solution de sécurité, surtout s'il a mis en place une solution globale.

Le principal enjeu pour les fournisseurs de solutions de sécurité est de tenir les promesses formulées tout en se différenciant de leurs concurrents. C'est pourquoi 2021 sera une année où le résultat fera foi. Plutôt que de parler du fonctionnement de leurs solutions, les fournisseurs doivent surtout prouver leur efficacité et leur engagement à respecter les standards de performance.

Ce n'est pas un secret, de nombreuses entreprises et industries ont dû lutter pour subsister en 2020 et beaucoup d'entre elles vont participer à la construction d'une « meilleure normalité ». Malheureusement, la menace pèse sur leurs têtes : il existe plus d'un milliard de logiciels malveillants dans le monde qui exploitent d'innombrables vecteurs d'attaque, le tout dans un contexte pandémique particulièrement tendu. Grâce à une démarche holistique basée sur l'IA/Machine Learning (ML) et soutenue par une stratégie de données, les fournisseurs pourront aider les entreprises à faire face et/ou à se reconstruire.

Une IA efficace destinée à soutenir l'intelligence humaine sans la remplacer

De plus en plus présente dans tous les aspects de notre vie connectée, l'IA modifie peu à peu notre façon de travailler et de communiquer. Si les changements ne sont pas toujours aussi rapides que prévu, le phénomène prend de l'ampleur. Beaucoup de bruits parasites autour de l'IA ont fait écran au potentiel de cette technologie dans la sécurité et aux quelques fournisseurs qui l'exploite véritablement.

D'une certaine façon, l'IA est devenue victime de son propre succès. C'est une notion à la mode apposée tel un slogan sur les produits et les outils marketing. Or, dans le domaine de la cybersécurité, l'IA et le ML ne sont pas des remèdes miracles. Mais lorsque ces technologies sont utilisées de façon appropriée et en combinaison avec de la Data Science pour concevoir des modèles et examiner les erreurs, elles dévoilent un potentiel sans égal.

Cependant, lorsqu'une simple automatisation de tâches manuelles est qualifiée d'IA, cela affecte négativement la perception que les entreprises en ont, en particulier dans le domaine de la cybersécurité. La plupart des problèmes prétendument résolus par l'IA ne sont pas aussi complexes que les problématiques à résoudre dans le secteur de la cybersécurité. Par conséquent, se tourner vers l'IA est une bonne chose, mais il vaut mieux utiliser celle qui se veut authentique et qui, en association avec la Data Science, se révèle être un véritable outil stratégique.

Contrairement aux croyances populaires, l'IA authentique vient renforcer l'intelligence humaine et n'a pas vocation à la remplacer. Le discours incessant sur l'automatisation et l'essor des robots est tout à fait hors de propos, et 2020 nous a rappelé à quel point la dimension humaine est importante. L'IA ne peut pas remplacer l'intelligence humaine là où elle est indispensable, c'est-à-dire dans la priorisation des problèmes à résoudre et la définition de stratégies de conduite du changement adéquates pour faire face à une pandémie par exemple. En utilisant l'IA pour effectuer les tâches redondantes et à faible valeur ajoutée, les entreprises pourront dégager du temps aux employés pour faire ce qu'ils font le mieux : être créatifs, résoudre les problèmes, gérer le business et mener à bien leurs objectifs de vie.

Télétravail : l'histoire est loin d'être terminée

Les acteurs du secteur tertiaire occupent une part conséquente dans notre économie et ils sont plus susceptibles de mettre en place des infrastructures hybrides pour garder le rythme et continuer à travailler. Ces entreprises réalisent d'importantes économies notamment sur le plan immobilier (loyers, etc.). Si la pandémie a donné un véritable essor au télétravail, rien n'empêche aux

entreprises de le maintenir sur le long terme pour conserver ces mêmes avantages économiques.

Toutefois, le télétravail peut rendre les entreprises et les employés plus vulnérables aux problèmes de cybersécurité, qu'ils découlent d'erreurs humaines involontaires ou fassent suite à des attaques malveillantes. Les fournisseurs ont ici l'opportunité de prouver qu'ils peuvent rendre le télétravail plus sûr, d'autant plus que le nombre de terminaux connectés croit de façon exponentielle.

La cybersécurité doit être intégrée dès la création des dispositifs intelligents

Au cours du développement des dispositifs dits intelligents, la cybersécurité est généralement reléguée au second plan. Prenons l'exemple des véhicules connectés. Les constructeurs utilisent de plus en plus de capteurs (et donc de données) qui permettent de développer de nouvelles fonctionnalités de sécurité au conducteur et d'améliorer son expérience de conduite. En matière de cybersécurité, il existe autant de vecteurs d'attaque que de fonctionnalités. C'est pourquoi, il est indispensable pour les constructeurs d'impliquer la notion de sécurité dès la conception des plateformes utilisées dans les dispositifs intelligents. Dans de nombreux cas, les données en provenance des capteurs ne sont utiles - et sûres - que si elles ne peuvent pas être compromises. La cybersécurité doit devenir un pilier du développement des produits et des plateformes dès le premier jour, au lieu d'être un simple composant annexé à l'architecture.

La cybercriminalité et la COVID-19 continueront de faire des vagues

Les recherches scientifiques autour de la COVID-19 sont de plus en plus ciblées par les hackers, qu'ils agissent au nom d'un État ou pour leur propre compte. Alors que la pandémie sévit dans le monde entier, cette tendance ne risque pas de s'inverser. Pour que la recherche se poursuive sans entrave, les menaces inhérentes ne peuvent tout simplement pas être ignorées. Les institutions et entreprises du domaine de la santé ont toujours été des cibles privilégiées par les hackers, et la cybersécurité doit pouvoir les protéger comme le ferait le vaccin avec le virus.

De nombreux rapports indiquent que des acteurs malveillants ont tenté de subtiliser des données sur le vaccin à de multiples entreprises et institutions au Canada, aux États-Unis et au Royaume-Uni. Les récentes annonces des groupes Pfizer et Moderna participent à décupler le risque, d'autant plus que les vaccins candidats ont démontré un taux d'efficacité de plus de 90 %.

Pour les fabricants de vaccins, les aspects logistiques et de sécurité sont de véritables casse-têtes. De plus, la propriété intellectuelle autour de ces recherches a une valeur inestimable, et nombreux sont les acteurs malveillants qui ne reculeraient devant rien pour obtenir ces informations et prendre en otage la santé publique. Tous les yeux sont tournés aujourd'hui vers l'industrie pharmaceutique et les différentes entreprises qui comptent commercialiser leurs vaccins. La cybersécurité a, par conséquent, un rôle essentiel à jouer au cours de l'année qui vient.

Vers 2021 et au-delà

2020 nous aura prouvé que l'Humanité sait faire preuve d'une fabuleuse capacité d'adaptation, mais elle reste néanmoins vulnérable aux changements soudains et à l'incertitude. Même si un retour à la

normale est souhaité dans bien des domaines, certaines nouvelles normes comme le télétravail vont indéniablement s'inscrire dans la durée. Les progrès technologiques et l'adoption de l'IA permettront aux entreprises d'évoluer et/ou de se reconstruire dans ce nouveau monde. Globalement, le secteur des technologies et de la cybersécurité doit continuer à innover pour soutenir la création d'entreprises et de services publics solides et bien préparés.