La souveraineté numérique existe par défaut aux États-Unis.

Zeina Zakhour est vice-President, Global CTO Cybersecurity chez Atos. Cet entretien a été publié le 11 mars 2022.

1/ Comment devient-on Global CTO Digital Security d'Atos ?

Il faut surtout être passionné. La cybersécurité est une industrie en plein changement où les innovations technologiques émergent chaque trimestre et où **le panorama des cybermenaces évolue également rapidement. Donc, cœurs sensibles, s'abstenir !**

Le CTO est un agent de changement clé dans l'entreprise et le rôle de CTO Digital Security est axé sur l'innovation technologique pour transformer et optimiser la sécurité des produits et les services numériques. Donc, Cela nécessite une compréhension approfondie de la technologie et des innovations technologiques cyber, et une capacité à définir et porter une stratégie et une vision métier pour anticiper les changements numériques et accélérer la sécurisation par défaut de la société numérique de demain.

2/ Quelle est la réalité du hacking par rapport à l'image que peuvent s'en faire les cinéphiles ? (Vous avez écrit un article à ce sujet)

En effet, j'avais analysé dans un entretien la pertinence et la représentation de la cybersécurité, dont particulièrement le hacking dans les films et c'est vrai que le constat était très loin de la réalité. Mais il faut aussi dire que le profil d'un cybercriminel a beaucoup changé ces dernières années. Cela fait 20 ans que je travaille dans la cybersécurité et **les cybercriminels auxquels on faisait face il y a deux décennies ne sont plus les mêmes aujourd'hui.**

Aujourd'hui nous faisons face à du crime organisé avec des organisations de cyber-crimes ayant des objectives et méthodes différentes, à des cybercriminels activistes (hacktivistes) et à des cybercriminels liés à des états.

Certains cybercriminels perpétuent les méthodes classiques et se focalisent sur des attaques paralysant une entreprise.

D’autres adoptent des méthodes furtives pour pouvoir compromettre l’environnement de leurs cibles sans se faire détecter, qu’elles soient des organisations étatiques, des organisations publiques ou privées.
Quelle que soit la méthode adoptée, les cybercriminels aujourd’hui sont bien organisés, et procèdent à un profilage de l’environnement technologique mais aussi des personnes pour identifier et exploiter le maillon faible, qu’il soit technologique ou humain.
Il ne faut surtout pas oublier que la cybercriminalité, hélas, est prolifique et c’est bien cette motivation qui pousse des cybercriminels à innover et adopter les dernières technologies pour développer des cyberattaques pointues, furtives et destructives.

3) Même s’il nous semble que la personne en tant que telle demeure le critère le plus légitime, une femme a-t-elle selon vous une perception différente de la sécurité au sens large ?

Je pense que chacun d’entre nous est différent, notre personnalité, notre caractère, notre façon de raisonner, de s’exprimer… Une équipe gagnante est une équipe diverse, que ce soit la diversité homme-femme, la diversité culturelle ou même diversité neurologique. L’innovation ce n’est pas avoir des gens qui pensent de la même façon. Nous ne pouvons pas créer des technologies couvrant les besoins de tous, avec des équipes sans diversité.

4) De nombreuses entreprises du CAC40 se reposent sur vos “solutions”. Parvenez-vous à déconnecter votre cerveau quand vous vous endormez ?

J’ai confiance dans les solutions que nous déployons et nos équipes qui veillent avec vigilance. Une équipe bien structurée et bien organisée, permet à chacun de se déconnecter quand il le faut. Nous ne sommes pas seuls face aux cyber-menaces…
C’est vrai que notre métier de cybersécurité, c’est une grande responsabilité car nous protégeons les environnements numériques de nos clients et l’impact d’une cyber-attaque peut paralyser l’accès à ces services pour toute une population surtout dans le monde hyper-connecté d’aujourd’hui. Mais cela donne à notre travail un sens profond. Nous protégeons le monde numérique mais aussi par conséquent le monde physique car de nos jours les mondes numériques et physique sont

interconnectés. Oui, c'est une responsabilité mais on le fait parce que nous sentons qu'à notre petite échelle nous contribuons à protéger notre monde.

5) Notre précédent invité, Sébastien Garnault, évoquait le fait que pour les Américains, souveraineté équivaut souvent à "sécurité nationale". Comment réagissez-vous à ce parallèle ?

Oui la souveraineté pour les Américains équivaut à « sécurité nationale ». Mais c'est surtout car **la souveraineté numérique est presque acquise aux Etats-Unis. La souveraineté numérique existe par défaut aux États-Unis** où l'innovation technologique bat son plein. Les startups en cybersécurité ont levé des fonds à hauteur de 29,5 milliards de dollars en capital risque en 2021 au niveau mondial et les majorités des fonds étaient investis sur les startups américaines. Le continent américain est un vivier d'innovation de nouvelles technologies ce qui fait que la souveraineté numérique, qui comprend la souveraineté technologique et également la souveraineté des données, est assurée par défaut.

La souveraineté numérique européenne, qui est un sujet phare de la présidence française de l'Union Européenne, est différente et repose sur les piliers innovation et sécurité certes, mais aussi valeurs et ouvertures.

Et il est essentiel de soutenir cette souveraineté européenne. Le savoir-faire européen est reconnu au niveau mondial. Il faut juste qu'on soit moins conservateurs sur notre continent en termes d'investissement et plus agiles pour aider les start-ups à grandir. La souveraineté numérique européenne va nous permettre de positionner l'Europe comme une puissance d'innovation, pour attirer les investissements et les talents et faire émerger des entreprises européennes développant les technologies de demain. **J'ai grand espoir dans l'initiative « Scale up Europe » qui a pour but d'aider et financer les entreprises européennes innovantes pour en faire des références mondiales dans le secteur numérique.**

L'innovation d'aujourd'hui est celle qui nous permettra de proprement sécuriser les technologies émergeantes qui transforment la façon dont nous travaillons et la façon dont nous consommons le numérique. Investir dans des startups, implémenter leurs technos n'est pas un risque mais au contraire nous permet de créer ce pôle d'innovation essentiel pour la souveraineté cybersécurité européennes et française.

6) Est-ce que la créativité vous semble une qualité requise pour être un bon CTO ?

La créativité est essentielle pour un CTO et est une source continue en idées inédites et innovantes. Le CTO est le garant de l'innovation technologique. Pour pouvoir innover il faut sortir des sentiers battus, il faut pouvoir trouver de nouveaux moyens pour plus d'excellence opérationnelle, ou améliorer les solutions et technologiques existantes dans une approche d'innovation incrémentale. Il faut aussi pouvoir créer de nouvelles technologies qui vont perturber et créer une rupture dans le panorama technologique existant. Or, Innover sans créativité me semble impossible.

7) Quel est à vos yeux le domaine où la France aurait intérêt à conjuguer ses efforts avec un autre pays européen pour peser sur le marché global ?

L'innovation en France a amené des avancées dans le quantique, les super-calculateurs, la cybersécurité, l'intelligence artificielle, la 5G et bien d'autres domaines numériques. Collaborer au niveau européen nous permet d'accélérer nos cycles d'innovation, d'étendre notre marché cible et de mettre le savoir-faire européen en premier plan. Les entreprises françaises et européennes le font très bien grâce au support fourni par l'union européenne qui a reconnu ces technologies comme priorité d'investissement stratégique dans le plan de relance pour l'Europe et le programme pour la « décennie numérique ».

8) Beaucoup de proies "faciles" sont prises pour cible lors de cyberattaques. Que dit le fait que cette criminalité puisse s'en prendre à des hôpitaux, par exemple ? Et quel type de réponse informatique, mais aussi pénale cela appelle-t-il ?

Il y a bien le mot « crime » dans cybercrime, et malheureusement les cybercriminels choisissent leurs proies méticuleusement sans regard pour les vies humaines. Ils vont s'attaquer aux entreprises qui ont le moins de maturité et aux secteurs d'activité où la donnée a le plus de valeur. Et malheureusement certains hôpitaux couvrent les deux cas d'usage.

Aujourd'hui une cyberattaque ne va pas seulement avoir un impact financier ou provoquer une interruption d'activité pour une entreprise mais aussi cela peut impacter la vie humaine. Une cyberattaque sur une stations de traitement d'eau ou une

station de production d’électricité impacte tout un pays. Une attaque sur un hôpital peut tuer des malades. L’année dernière des personnes sont décédées à cause de cyberattaques qui avaient paralysé le système informatique de l’hôpital.
Comme le risque cyber est maintenant un risque économique majeur, il faut que les entreprises implémentent les bonnes solutions de protection et de détection et réponse à incident. Il faut que les pays renforcent leurs capacités à traiter des données de cybercrime et le rapport du club des juristes publié l’année dernière montre des pistes intéressantes pour la France. Il est essentiel qu’on puisse coopérer au-delà des frontières pour pouvoir arrêter les cybercriminels qui sont hébergés dans des pays « sanctuaires » pour eux. Il y a beaucoup d’avancée sur ce volet ces dernières années où nous avons vu des opérations menées sur plusieurs continents pour démanteler des réseaux cybercriminels grâce à une coopération internationale.

9) Vous arrive t-il d’échanger entre pairs sur la meilleure manière de prévenir ou de contrer une attaque ?

Oui bien sûr et c’est même essentiel de nos jours. Nous avons face à nous des cybercriminels qui sont très bien organisés avec des membres partout dans le monde, une approche collaborative et une vitesse d’innovation importante. Donc pour faire face, il faut travailler main dans la main et partager l’intelligence recueillie sur les techniques et méthodes d’attaques utilisées. A titre d’exemple, Atos est membre de la Charter of Trust qui rassemble des industriels souhaitant travailler ensemble pour améliorer le niveau de maturité de sécurité du secteur d’activité mais aussi pour pouvoir échanger sur les meilleures pratiques pour prévenir et contrer les cyberattaques.