DELL Technologies

5 Recommandations pour créer un environnement sécurisé pour l'innovation

1	2	3	4	5
Communiquer tôt et souvent	**Rationaliser et simplifier la pile de sécurité**	**Mettre en place des dispositifs de cybersécurité**	**Rester flexible et faire preuve de créativité**	**Développer une solide culture de la sécurité**
Impliquer les dirigeants et les principales parties prenantes	Réduire la complexité	Définir des règles	Rester ouvert aux nouvelles pratiques de sécurité	Encourager l'implication générale
Comprendre les plans d'innovation	Éliminer la redondance	Mettre en place des contrôles d'accès	Donner la priorité à des méthodes de sécurité ouvertes à l'innovation	Promouvoir la transparence
Donner à l'équipe de sécurité les moyens d'entamer la conversation	Créer une interface unique	Intégrer les systèmes logiques et physiques	Garder à l'esprit que la sécurité n'empêche pas l'innovation	Favoriser la collaboration
	Développer un solide processus d'évaluation des achats			

Créer un environnement sécurisé et propice à l'innovation

Pour optimiser l'innovation dans un monde piloté par la technologie et les données, la cybersécurité doit être conçue pour soutenir l'innovation. Mais comment une entreprise peut-elle créer un environnement qui favorise la croissance, la créativité et l'innovation sans compromettre la sécurité ?

Pour analyser un exemple concret de ce type d'environnement, Sameer Shah, du département Dell Cybersecurity Marketing, a rencontré le Dr Tony Bryson, Responsable de la sécurité des systèmes d'information (RSSI) de la ville de Gilbert, en Arizona. Ensemble, ils ont discuté de l'initiative novatrice City of the Future (en français, Ville du futur) et du rôle qu'y joue la sécurité.

Lisez la suite pour obtenir un résumé des recommandations du Dr Bryson. Vous retrouverez l'intégralité de l'échange sur **dell.com/cybersecuritymonth**.

> « Assurez-vous de connaître les objectifs des parties prenantes et de savoir comment elles sont susceptibles de tirer parti de la technologie et de l'innovation au profit de l'entreprise et du client ».
>
> ***Dr Tony Bryson**, Responsable de la sécurité des systèmes d'information (RSSI) pour la ville de Gilbert*

La ville du futur

L'initiative City of the future de la ville de Gilbert vise à construire une infrastructure durable et résiliente qui utilise les données pour enrichir le quotidien de ses citoyens. La technologie est omniprésente dans la fourniture des services, du paiement des factures à la gestion de la circulation, en passant par la disponibilité et la qualité de l'eau. Elle permet également de collecter des données pour prévoir l'utilisation et les besoins futurs en matière de services. L'initiative n'a pas d'objectif fixe et définitif, mais s'appuie sur un processus itératif qui encourage des progrès sur le long terme.

En tant que premier RSSI, le Dr Bryson avait pour mission d'adopter une approche plus stratégique de la cybersécurité. Pour fournir des services urbains modernes et technologiques, la ville avait besoin de solutions de protection, de classification et de contrôle des données solides, capables de soutenir ses objectifs ambitieux.

Fort du succès de cette mission, le Dr Bryson a dressé une liste de recommandations clés qui ont favorisé la réussite et permis de créer un environnement propice à la croissance et à l'innovation en toute sécurité.

Communiquer tôt et souvent

Le Dr Bryson a souligné la nécessité d'impliquer les dirigeants et les principales parties prenantes dès le début du processus d'innovation. « Assurez-vous de connaître les objectifs des parties prenantes et de savoir comment elles sont susceptibles de tirer parti de la technologie et de l'innovation au profit de l'entreprise et du client », explique-t-il.

Le sujet de la cybersécurité devrait être amené dès les premières étapes du cycle d'innovation, l'équipe de cybersécurité pouvant alors jouer un rôle phare pour faciliter et encourager ces conversations.

L'utilisation de l'IA par la ville de Gilbert en est un excellent exemple. Le Bureau de la sécurité a mis le sujet sur la table il y a deux ans et a joué un rôle de leader en posant des questions essentielles : comment faire confiance aux données générées par l'IA, comment les stocker et comment s'assurer que les citoyens comprennent réellement comment est utilisée l'IA ? Cela a conduit à la création d'un comité interfonctionnel, puis à l'embauche dans la ville de Gilbert du premier directeur de l'intelligence artificielle officiant à temps plein dans l'Ouest des États-Unis.

« Rien de tout cela n'aurait pu se produire si nous avions mis en place une barrière de sécurité qui empêchait cette innovation particulière de se produire », explique le Dr Bryson. « Pour innover et essayer de faire les choses bien, il faut déjà commencer par en parler. »

Rationaliser et simplifier la pile de sécurité

L'une des premières tâches du Dr. Bryson a été de faire l'inventaire des solutions de sécurité afin de comprendre l'utilisation de chaque produit et service. Ce travail a mis en évidence une redondance importante. La réduction et la rationalisation permettraient d'économiser de l'argent, mais plus important encore, elles doteraient la petite équipe de sécurité d'une interface unique et d'une source unique de vérité pour gérer les mesures de cybersécurité et résoudre les problèmes.

Le Dr. Bryson a fait écho à l'idée reçue selon laquelle la complexité serait l'ennemie de la cybersécurité en déclarant : « Je ne veux pas que les gens soient obligés de passer d'un système à l'autre pour comprendre ce qui se passe ».

Mettre en place des dispositifs de cybersécurité adaptés

Les innovateurs de l'entreprise doivent comprendre et respecter les mesures de protection qui garantissent la sécurité des systèmes et des données. Ces règles peuvent être des stratégies, des contrôles d'accès ou d'autres principes qui aident les innovateurs à mieux visualiser le terrain de jeu à leur disposition. Ce terrain de jeu représente un environnement sécurisé pour l'innovation, né d'un partenariat efficace entre l'équipe en charge de la sécurité et celle en charge de l'innovation.

DELL Technologies

Rester flexible et faire preuve de créativité

Pour le Dr Bryson, bien qu'il soit important d'avoir et d'appliquer des normes de cybersécurité, l'innovation requiert parfois de la fluidité et de la créativité. Il a ainsi ajouté : « L'innovation ne se limite pas à une unité commerciale. Elle s'exprime souvent dans les technologies de l'information et même au cœur des stratégies de sécurité. Dans ce contexte d'innovation, vous devrez peut-être trouver de nouvelles façons créatives et originales d'assurer la sécurité de vos systèmes et de vos données. Vous devez vous y préparer. »

Développer une solide culture de la cybersécurité

Le Dr Bryson a souligné l'importance de développer une solide culture de la sécurité. « La culture suffit presque à elle seule à assurer la cybersécurité. Sans culture pour sensibiliser les gens à la cybersécurité, la menace est étendue. »

Une solide culture de la cybersécurité repose sur de nombreux éléments déjà abordés : un dialogue ouvert et transparent, une implication à l'échelle de l'entreprise, des normes clairement définies et un esprit de collaboration entre l'équipe de sécurité et ses clients, internes et externes.

À mesure que la croissance s'accélère, la cybersécurité doit délaisser l'approche réactive axée sur la défense au profit d'une approche proactive et positive qui offre de meilleurs résultats.

Les entreprises doivent adopter une vision moderne de la sécurité qui protège et favorise l'innovation.

Pour ce faire, elles peuvent miser sur une communication et une collaboration qui intègrent des mesures de sécurité dès la phase de développement. L'objectif est de créer un environnement où la créativité peut s'exprimer sans compromettre la sécurité.

Découvrez comment relever certains des défis actuels majeurs en matière de cybersécurité sur **dell.com/cybersecuritymonth**

DELL Technologies