

**Cyber-résilience: une base solide pour la reprise économique**

**Casablanca, Septembre 2021 :** Une cyberattaque a lieu toutes les onze secondes dans le monde, comme l’a démontrée une récente étude réalisée par Cybersecurity Ventures. Ces attaques sont aveugles : elles ciblent tout, aussi bien les infrastructures nationales critiques, que les données personnelles sensibles. L'impact économique et social des cyber-attaques est souvent astronomique. Les coûts liés à ce type d'attaques et la vulnérabilité accrue qu’elles génèrent imposent plus que jamais aux gouvernements d'accélérer rapidement leur cyber-résilience, c'est-à-dire leur capacité à prévenir la cybercriminalité, à y répondre et à s'en prémunir, afin de garantir une base solide pour la reprise économique mondiale.

Le travail à distance étant appelé à perdurer, nous sommes devenus plus vulnérables que jamais face aux cyberattaques. McKinsey signale que les attaques de phishing ont été multipliées par sept depuis le début de la pandémie, les criminels profitant des retards de mise à jour des filtres de messagerie et des filtres Web pour s’en prendre massivement aux travailleurs à distance.

**Le lourd bilan des cyberattaques...**

Les rançongiciels et autres cyberattaques sophistiquées sont plus répandus et plus dangereux que jamais; elles visent de plus en plus les infrastructures critiques. Les ramifications financières de la cybercriminalité sont énormes et selon certaines prévisions, la cybercriminalité commencera à coûter au monde pas moins 10 500 milliards de dollars par an à l’horizon 2025, soit exponentiellement plus que les dommages causés par toutes les catastrophes naturelles sur la même période. Cependant, les dommages causés par les cyber-attaques vont bien au-delà des coûts financiers, puisqu’elles provoquent le vol et la destruction de données personnelles et de propriété intellectuelle, en plus des atteintes possibles à la réputation.

Dans des pays d'Afrique émergente comme le Maroc, le Nigeria et d'autres encore, les gouvernements ont déjà élaboré des stratégies nationales de cybersécurité destinées à protéger leurs citoyens, leurs entreprises et leurs infrastructures critiques contre ce type de risque. À l'heure où les entreprises du monde entier envisagent une reprise économique axée sur la technologie, les gouvernements qui concentrent leurs investissements et leurs efforts aux bons endroits seront les mieux outillés pour se prémunir contre les cyberattaques et atténuer ainsi les dégâts grâce à une infrastructure numérique robuste.

Au-delà de la protection : la cyber-résilience et une solide stratégie de récupération des données demeurent des ingrédients essentiels. La cybersécurité est plus qu'une simple police d'assurance contre les attaques. La cyber-résilience, si elle est mise en œuvre efficacement, est capable de puissamment contribuer à mieux asseoir la prospérité économique et l'innovation sur le long terme à travers le Maroc et le reste de l'Afrique émergente.

La transformation numérique, qui est cruciale pour accélérer la reprise économique, nécessite une cyberfondation résiliente qui puisse garantir la sécurité et la confiance. Les nouvelles technologies - IA, Big Data, cloud et edge computing - révolutionnent l'économie, mais les préoccupations en matière de sécurité risquent de ralentir leur adoption. Ces inquiétudes pourraient également faire hésiter les entreprises à lancer des projets numériques, étouffant ainsi leur potentiel d'innovation.

En fait, le rapport africain KnowBe4 2020, qui examine l'état de la cybersécurité dans les pays d'Afrique émergente, a révélé que 52 % du public interrogé ne sait pas ce qu'est un ransomware. Ce constat est troublant, compte tenu des pertes financières que les attaques par ransomware sont connues pour causer tant pour les personnes que pour les entreprises.

Une stratégie de récupération solide est un élément essentiel pour remettre une entreprise sur les rails. Les entreprises doivent donc considérer la récupération comme un élément essentiel de leur stratégie globale de gestion des risques. Les responsables de la sécurité de l'information (CISO) doivent s'intéresser aux technologies et aux services qui sont susceptibles d'améliorer leur position globale en matière de cybersécurité, et de leur permettre ainsi de mieux se remettre d'une cyberattaque qui serait destructrice.

Aujourd'hui, de nombreuses entreprises envisagent de créer des environnements isolés qui soient capables d’héberger leurs données les plus critiques. En fait, des directives réglementaires récentes soulignent que la sauvegarde et la récupération sont des éléments clés d'une bonne stratégie de cybersécurité, de préférence avec une infrastructure de sauvegarde ou de récupération qui soit isolée des autres systèmes.

S’exprimant à ce sujet, Nawfal Saoud, directeur régional des ventes - Solutions de protection des données, Maroc et Afrique émergente, Dell Technologies, a déclaré : " En tant que fournisseur de confiance de solutions de protection des données pour des dizaines de milliers d'entreprises dans le monde, Dell Technologies a été, une fois de plus, consacré par le Magic Quadrant de Gartner 2021 en tant que leader pour les solutions logicielles de sauvegarde et de restauration d'entreprise. Chez Dell Technologies, nous sommes fermement engagés à aider nos clients au Maroc et en Afrique émergente, à naviguer dans ces eaux incertaines, en leur fournissant des solutions innovantes de protection des données et de cyber-résilience qui leur permettront de protéger leurs charges de travail et leurs données critiques ".

À l'ère du numérique, toutes les entreprises s'inquiètent aujourd’hui de l'impact paralysant qu'une cyberattaque malveillante pourrait générer sur leur activité. Selon le 2021 Global Data Thales Threat Report, les logiciels malveillants sont répertoriés comme étant l’une des principales sources d'attaques de sécurité, suivis par le phishing par ransomware.

Depuis le déclenchement de la pandémie, il est devenu essentiel pour les entreprises comme pour les gouvernements, de mieux se prémunir contre les cybermenaces croissantes susceptibles de paralyser les systèmes financiers mondiaux. À cet égard, la Sheltered Harbor Alliance, qui est une norme industrielle pour la protection, la portabilité et la récupération des données ainsi que la continuité des services essentiels pour les institutions financières américaines, joue un rôle clé dans cette dynamique de protection contre les cybermenaces. Dell Technologies est non seulement le premier fournisseur de solutions technologiques du programme de partenariat Sheltered Harbor Alliance, mais aussi un partenaire engagé auprès des acteurs financiers du monde entier.

Les cyberattaques génèrent des répercussions funestes sur les emplois, mais aussi sur la cyber-réputation, tout en coûtant des millions de dollars aux entreprises. La réponse face à l'évolution rapide de ces menaces consiste à disposer d'une solution de récupération très efficace des données, mais aussi de systèmes de protection innovant contre les logiciels malveillants dormants, l'effacement et le verrouillage des données, la corruption de la data, les attaques d'initiés et la destruction des actifs de sauvegarde et de stockage.

Les RSSI doivent donc envisager des stratégies de récupération qui puissent combiner les avantages de l'isolation et ceux de la continuité des activités, car elles minimisent l'impact d'une cyberattaque et permettent de récupérer plus rapidement toutes les données sensibles nécessaires à la bonne marche d’une entreprise. Il s'agit d'un moyen à la fois efficace et infaillible, notamment lorsque toutes les autres stratégies échouent.

**Un nouveau laboratoire de télécommunications pour stimuler l’innovation de la 5G**

Dell explore également les technologies et les applications futures dans le nouveau **Dell Technologies Open Telecom Ecosystem Lab** à Round Rock, Texas, en collaborant notamment avec ses partenaires et clients. Grâce à un environnement de test « carrier-grade », les CSPs peuvent reproduire les sites clients et tester des solutions et services multifournisseurs en situation réelle. Les nouvelles solutions peuvent être incubées en laboratoire, puis rapidement mises sur le marché, ce qui permet aux CSPs de créer de nouveaux services et applications d’entreprise à la périphérie. Le programme de partenariat technologique de Dell fournit des ressources d’ingénierie et une assistance à la gestion de projet pour concevoir, développer, commercialiser et vendre des solutions et des services réseau.

**Ressources complémentaires**

* Retrouvez Dell sur [Twitter](https://twitter.com/delltech), [Facebook](https://www.facebook.com/DellTechnologies/), [YouTube](https://www.youtube.com/delltechnologies) et [LinkedIn](https://www.linkedin.com/company/delltechnologies/)
* Pour consulter les ressources approuvées de Dell Technologies, consultez notre [Bibliothèque multimédia](https://corporate.delltechnologies.com/en-us/newsroom/media-library.htm)

**A propos de Dell Technologies**

[Dell Technologies](http://www.delltechnologies.com/) (NYSE:DELL) aide les entreprises et les particuliers à mieux ériger leur avenir numérique et à transformer leur manière de travailler, de vivre et de se divertir. La société propose à ses clients le portefeuille de technologies et de services le plus vaste et le plus large qui existe à l’ère de la data.