L'ECONOMISTE

Le Cercle des Experts

Cyber-résilience: Un impératif stratégique pour les dirigeants

Par Taïeb DEBBAGH | Edition N°:6976 Le 24/03/2025 | Partager

Taieb Debbagh est expert en cybersécurité et protection des données personnelles. Ancien secrétaire général du département ministériel en charge du Digital, il a contribué à l'élaboration de la stratégie Maroc Numeric 2013. Il a été président de la commission «Structures organisationnelles» de la Global Cybersecurity Agenda (UIT-Genève). Il est également auteur du livre «15 ans de cybersécurité au Maroc» et co-auteur de «Système de management de la Cybersécurité nationale» (Amazon-avril 2024)

À l'ère du digital, la cybersécurité n'est plus une question technique réservée aux experts mais un enjeu stratégique qui concerne directement le haut management. Les cyberattaques se multiplient et gagnent en sophistication, menaçant non seulement les infrastructures informatiques, mais aussi la stabilité financière, la réputation et même la pérennité des organisations.

Dans ce contexte, la cyber-résilience devient une nécessité absolue. Il ne s'agit plus seulement de prévenir les attaques, mais d'adopter une posture qui permet à l'entreprise d'anticiper, de détecter et de se remettre rapidement d'un cyber-incident, tout en garantissant la continuité de ses activités. Cette approche globale implique une gouvernance forte, une gestion des risques intégrée et une culture de la cybersécurité partagée à tous les niveaux de l'organisation.

■ Des menaces en forte augmentation

La cybersécurité s'impose désormais comme une priorité mondiale face à l'escalade sans précédent des cyberattaques. En 2024, leur fréquence a bondi de 30% par rapport à l'année précédente, portant le coût global des cybercrimes à plus de 10 milliards de dollars (Proginov). Aucune entreprise n'est épargnée, quelle que soit sa taille, tandis que les attaques gagnent en complexité. L'intelligence artificielle (IA) joue un rôle majeur dans cette évolution, en automatisant et en perfectionnant les techniques utilisées par les cybercriminels.

L'enquête de 2024, réalisée par PwC et l'AUSIN a fait ressortir les constats suivants:

- Les principales menaces identifiées par les entreprises sont la demande de rançon (84%), les fuites de données (61%) et la compromission de la messagerie (45%);

- Les conséquences redoutées sont la perte des données clients, employés ou des transactions (84%), l'atteinte à l'image de l'entreprise (65%) et l'indisponibilité de service (58%);

- Les pertes financières générées par les fuites de données ont représenté des pertes supérieures à 500.000 dirhams pour 32% des entreprises.

Malgré ces constats, PwC indique que 58% des dirigeants ne considèrent toujours pas la cybersécurité comme une priorité absolue. Ce retard dans la prise de conscience fragilise les organisations et les expose à des crises majeures.

La cyber-résilience devient une nécessité absolue. Il ne s'agit plus seulement de prévenir les attaques, mais d'adopter une posture qui permet à l'entreprise d'anticiper, de détecter et de se remettre rapidement d'un cyber incident, tout en garantissant la continuité de ses ctivités (Ph. Privée)

■ Faire partie d'un cadre stratégique global et transverse

Face à cette menace permanente, la cyber-résilience doit devenir une priorité du conseil d'administration et du Comité de direction. La cybersécurité ne peut plus être réduite à un simple ensemble de solutions techniques. Elle doit faire partie d'un cadre stratégique global et transverse.

La première étape consiste à établir une gouvernance claire.

Un comité cybersécurité, rattaché directement au conseil d'administration, doit piloter les décisions stratégiques et assurer un suivi régulier de la posture de sécurité de l'organisation. Ensuite, la cybersécurité doit être intégrée aux mécanismes de gestion des risques. Cela implique des audits réguliers, des tests d'intrusion et une cartographie précise des cybermenaces.

Aujourd'hui, le phishing et l'ingénierie sociale sont la première cybermenace pour votre organisation, selon KnowBe4 «68% de toutes les violations de données sont causées par une erreur humaine». La sensibilisation des collaborateurs et des dirigeants aux bonnes pratiques est essentiel pour limiter ces risques.

Les 5 tendances clés pour 2025

■ **Manipulation des données privées:** L'essor des agents IA dans les entreprises ouvrira de nouvelles failles de sécurité.

■**Équilibre entre IA et gestion des risques:** L'IA deviendra incontournable en entreprise, malgré les risques qu'elle pose. Il faudrait surveiller les fuites involontaires d'informations sensibles.

■ **Géopolitique et cyber espionnage:** Les tensions internationales intensifieront les cyberattaques qui cibleront des infrastructures critiques, servant à la fois des objectifs politiques, économiques et de propagande.

■ **Explosion des attaques mobiles:** Les cybercriminels imiteront des entités légitimes pour inciter les victimes à divulguer leurs données, en cliquant sur des liens malveillants.

■ **Transformation du rôle du RSSI:** L'importance des RSSI au sein des conseils d'administration augmentera, renforçant leur rôle stratégique dans la gestion des cyber-risques.

Source: Inforisque

■ **Adopter une posture proactive**

Pour construire une cyber-résilience efficace, les dirigeants doivent adopter une posture proactive. La première mesure est de nommer un Responsable de la Sécurité de Système d'Information (RSSI) rattaché directement à la direction générale, garantissant ainsi un suivi stratégique des risques cyber.

Un reporting régulier sur les menaces et incidents doit être instauré pour assurer une transparence et une réactivité optimales.

L'organisation doit également renforcer sa capacité de détection et de réponse aux cyberattaques. L'utilisation de technologies avancées, comme l'intelligence artificielle et les systèmes de détection des intrusions, permet d'identifier plus rapidement les menaces et de limiter les dommages. Mais la technologie seule ne suffit pas: des exercices de simulation doivent être réalisés régulièrement pour tester la capacité de l'organisation à réagir efficacement en cas d'attaque.

Enfin, la cybersécurité est un enjeu collectif: Collaborer avec des experts indépendants, échanger avec d'autres organisations et s'informer en continu sur l'évolution des menaces sont autant d'actions essentielles pour anticiper les nouvelles formes d'attaques.

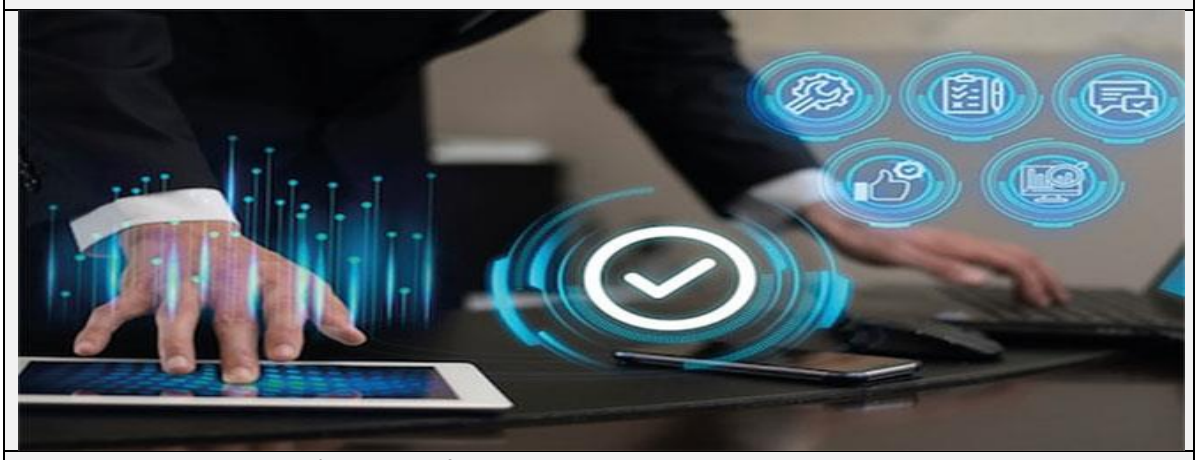
Aujourd'hui, le phishing et l'ingénierie sociale sont la première cybermenace pour une organisation, selon KnowBe4 «68% de toutes les violations de données sont causées par une erreur humaine». La sensibilisation des collaborateurs et des dirigeants aux bonnes pratiques est essentiel pour limiter ces risques (Ph. Privée)

■ **Un enjeu de premier ordre**

La cybersécurité n'est plus une question optionnelle pour les dirigeants. Elle doit être considérée comme un enjeu stratégique de premier ordre et intégrée à la gouvernance globale. Les cyberattaques sont devenues inévitables, mais la capacité à y résister et à en minimiser les impacts dépend directement des décisions prises en amont par le haut management.

Investir dans la cyber-résilience aujourd'hui, c'est protéger non seulement les actifs de l'organisation, mais aussi sa réputation, sa stabilité et la confiance de ses parties prenantes. Dans un monde où les menaces numériques évoluent sans cesse, seule une approche stratégique et proactive permettra aux organisations de garantir leur pérennité.

Principales recommandations



Pour assurer une cyber-résilience efficace, les dirigeants devraient tenir compte des recommandations suivantes :

■ **Intégrer la cybersécurité dans la gouvernance d'entreprise:** Désigner un responsable cybersécurité au niveau exécutif et intégrer la cybersécurité aux discussions stratégiques;

■ **Inclure la conformité est essentiel:** En alignant les pratiques de sécurité sur les exigences réglementaires (05-20, 09-08, RGDP, NIS2, DORA …);

■ Investir dans la prévention et la détection : Utiliser des outils de surveillance avancés et des solutions basées sur l'intelligence artificielle pour détecter les menaces en temps réel;

■ **Mettre en place une gestion de crise efficace:** Élaborer des plans de continuité et de réponse aux incidents afin de minimiser l'impact des cyberattaques;

■ **Adopter une approche proactive**: Tester régulièrement les systèmes, simuler des attaques et s'assurer que les procédures de sauvegarde sont efficaces;

■ Collaborer avec des experts indépendants : Travailler avec des spécialistes en cybersécurité pour bénéficier des meilleures pratiques et solutions adaptées.

Source: T.Debbagh