naitways

Special Report

Comment sécuriser une PME : Naitways prône l'approche par les risques

Disposant de moyens financiers et humains contraints, les PME éprouvent des difficultés à mettre en place une véritable stratégie de cybersécurité. Opérateur de services et d'infrastructures, Naitways leur propose une approche pragmatique de sécurité « by design » en priorisant les risques auxquelles elles sont confrontées.

Les statistiques montrent l'extrême vulnérabilité des PME aux cybermenaces alors qu'elles sont essentielles dans le tissu économique français. Selon le rapport du Campus Cyber (octobre 2023), 56% d'entre d'elles ont été confrontées à au moins un incident cyber en 2021. Des incidents qui peuvent avoir des conséquences dramatiques. La moitié des PME qui ont subi une attaque sont susceptibles de faire faillite dans les 18 mois qui suivent !

Si la menace est tangible, une forme de déni persiste. Près de sept dirigeants de PME sur dix pensent qu'elles ne constituent pas une cible potentielle, d'après un sondage mené par l'Ifop pour l'assureur cyber Stoïk. Cette perception est sensiblement la même quel que soit le secteur d'activité considéré. La prise de conscience est, bien sûr, beaucoup plus forte auprès des entreprises ayant subi une attaque informatique. Parmi les PME qui craignent de se faire attaquer, 58 % ont déjà été victimes de cybercriminels.

Ayant des ressources financières et humaines contraintes, les petites structures sont, de fait, perçues comme des proies faciles par ces cybercriminels qui mènent contre elles des campagnes massives de type ransomware, phishing (hameçonnage) ou de déni de service (DDoS).

Les PME présentent, par ailleurs, l'avantage de payer plus facilement les rançons en raison de l'impact que génère une attaque sur une structure de taille humaine mais aussi de leur faible résilience.

Placer le curseur au bon endroit

Arthur Danger, Directeur avant ventes & solutions de Naitways, voit un autre fléau qui menace les petites et moyennes entreprises : le discours des éditeurs et des fournisseurs spécialisés dans la cybersécurité qui entretiennent un climat anxiogène. « *Pour un dirigeant de PME, il est difficile de faire le tri entre ce qui relève du marketing et des risques réellement encourus. Où placer le curseur ?* ».

Selon lui, une politique de cybersécurité est « *un équilibre à trouver entre l'identification des risques et le niveau d'investissement à consentir pour les mettre sous contrôle* ». « *Financièrement et techniquement parlant, il est relativement facile de couvrir 90 % des risques. Cela devient coûteux d'arriver à 95 % et particulièrement dispendieux d'atteindre 100 %.* »

A rebours du discours dominant, Naitways, opérateur de services et d'infrastructures, créé il y a plus de quinze ans, propose une approche pragmatique de la cybersécurité en priorisant les risques et en proposant une réponse graduée. Pour Arthur Danger, il convient également de faire de la pédagogie et surmonter certains a priori. « *Les solutions cyber seraient nécessairement chères et inaccessibles.* »

Une politique de cybersécurité est un équilibre à trouver entre l'identification des risques et le niveau d'investissement à consentir pour les mettre sous contrôle.

Autre idée reçue : la sécurité briderait l'innovation et entraverait la productivité d'une entreprise en imposant des règles contraignantes. « *Non, une politique cyber bien conçue permet à l'informatique de rester un levier à la performance* », estime l'expert. Dans le cadre de ce travail de pédagogie et de partage d'informations pertinentes, Naitways multiplie les retours d'expérience lors d'événements clients. « *Le message passe mieux quand un dirigeant de PME échange avec un autre chef d'entreprise.* »

Évaluer, protéger, détecter, répondre

L'approche par les risques promue par Naitways démarre classiquement par une phase d'audit permettant d'évaluer la maturité cyber d'une organisation. « *Des tests d'intrusion (pentest) permettent notamment*

d'identifier les failles de sécurité sur vos applications, ce qui est souvent oublié, et de mesurer la résistance des infrastructures aux menaces externes, explique **Julien Léger**, directeur opérationnel de Naitways. «*A partir de ce bilan, il est possible de définir un plan d'actions* ».

A la fois opérateur télécom, hébergeur, cloud provider et infogéreur, Naitways présente l'avantage d'avoir une expertise globale du système d'information lui permettant de sécuriser aussi bien les couches réseaux que les serveurs. « *De par notre activité d'opérateur hébergeur, nous avons une connaissance concrète du maintien en conditions opérationnelles (MCO) des infrastructures critiques* », précise **Arthur Danger**.

De la détection des menaces (scan des vulnérabilités) à la réponse sur incident en passant par les moyens de protection (chiffrement, authentification-MFA, FWaaS), Naitways propose un portefolio cybersécurité complet. Depuis son SOC (Security Operations Center), ses experts alertent dès l'indentification de la menace et proposent un plan d'action pour la contenir et la neutraliser.

Quel que soit le niveau de service souscrit, Naitways propose, par défaut, un service de plan de reprise d'activité. Ce PRA est le seul moyen véritablement éprouvé pour survivre à une attaque par ransomware. A partir d'un système de sauvegarde sain et préalablement testé, il permet à une organisation de restaurer rapidement son système d'information et de poursuivre son activité.

Pour proposer ce service de « Security by design », Naitways dispose de trois datacenters en France – deux en région parisienne, un en région lyonnaise. Avec ces sites géo-redondants, le prestataire répond, suivant l'option retenue, à l'exigence d'un éloignement géographique de plus de 10 kms ou de plus de 400 kms. Naitways est, depuis mai 2022, certifié ISO 27001 (management de la sécurité de l'information) et, plus récemment, hébergeur de données de santé (HDS).

L'homme, le maillon faible

Une politique de sécurité des systèmes d'information (PSSI) ne repose pas que sur des dispositifs techniques. Le volet organisationnel et humain est également essentiel, l'homme restant le maillon faible de toute stratégie cyber. Largement pratiquées par les hackers, les techniques dites d'« ingénierie sociale » exploitent les failles humaines pour subtiliser des informations-clés, comme des identifiants et des mots de passe.

L'approche par les risques promue par Naitways démarre classiquement par une phase d'audit permettant d'évaluer la maturité cyber d'une organisation.

Pour diminuer ce risque, Naitways encourage le rôle de sensibilisation des dirigeants au sein de l'entreprise.« *En effet, les dirigeants*

doivent comprendre les enjeux cyber, intégrer le risque cyber et sensibiliser leurs collaborateurs. Ils deviennent ainsi le premier relais d'une stratégie dédiée, estime **Arthur Danger**. *Il est essentiel que les entreprises appliquent elles-mêmes les règles de sécurité pour les généraliser.* »

Naitways mène des campagnes de faux phishing afin d'éveiller les esprits. Cet apprentissage par l'erreur permet aux collaborateurs qui auront commis l'erreur de cliquer sur un lien frauduleux de mieux prendre conscience des risques cyber.

« *Au-delà du phishing, deux types d'attaques connaissent une grande popularité : l'arnaque au président et la fraude au fournisseur* », complète **Julien Léger**. Il s'agit cette fois de sensibiliser les populations d'utilisateurs concernés par ces menaces, comme le service comptable ou les achats, par des actions ciblées.

Quel que soit le niveau de service souscrit, Naitways propose, par défaut, un service de plan de reprise d'activité.

Naitways, à la fois opérateur, hébergeur, cloud provider et infogéreur

- Créée il y a plus de quinze ans, Naitways présente l'originalité d'être à la fois opérateur télécom, hébergeur, cloud provider et infogéreur. Basée à Paris et à Lyon mais intervenant dans toute la France, la société de services IT, certifiée ISO 27001 et HDS, peut ainsi apporter une approche globale et transverse sur les couches réseaux, cloud, systèmes, et fournit des services managés sur-mesure.
- Naitways emploie une soixantaine collaborateurs pour un portefeuille de 250 clients et plus de 50 000 utilisateurs protégés au quotidien. Si son cœur de cible est constitué d'entreprises françaises de 100 à 500 salariés, elle accompagne aussi quelques grands groupes à l'international, en apportant des réponses sur-mesure avec une expertise de haut niveau sur de nombreux sujets (externalisation du SI de bout en bout, Cloud, cybersécurité, disponibilité et sécurité des données critiques, sauvegarde de données, PRA, connectivité des bâtiments…).
- Parmi ses références, on peut citer Covivio (gestion foncière), Le Palais des Thés, Wojo (coworking), Eurowatt (gestion de parcs éoliens), l'Agence des espaces verts de la région Ile-de-France (AEV), l'association BruitParif ou Sogaris (logistique urbaine du Grand Paris).
- Enfin, l'engagement et la proximité sont des atouts très appréciés des clients.

Conception éditoriale & Réalisation graphique : Groupe IT Procom - www.itprocom.fr - Crédit photos : Shutterstock