Risque de cyberattaques pour les entreprises : de la nécessité d'anticiper pour mieux se protéger

Le contexte géopolitique incertain actuel peut s'accompagner de conséquences numériques néfastes pour les entreprises. En effet, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) a constaté l'usage de cyberattaques dans le cadre du conflit et appelle à la vigilance des entités françaises face au risque de propagation des menaces. Dans ces circonstances inédites, le défi est d'anticiper et de se protéger sans toutefois céder à la panique.

Opérateur de Services Hébergés spécialiste des services informatiques et télécoms destinés aux entreprises et aux collectivités, Adista accompagne les organisations dans la construction de leur politique de cybersécurité pour protéger au maximum leurs données, leurs systèmes d'information et leur activité.

Le site du gouvernement cybermalveillance.gouv.fr précise qu'aucune *« cyberattaque directe ayant pu avoir des impacts significatifs sur la population française n'a été recensée »* sur son périmètre. Il précise toutefois que cette situation peut être susceptible d'évoluer dans la durée et que le risque, s'il reste pour l'instant faible, n'exclut pas de possibles perturbations sur les services numériques français.

Au-delà du contexte exceptionnel que nous vivons, les cyberattaques ont augmenté fortement ces dernières années. Ainsi, l'ANSSI constate sur le territoire une **augmentation de 65%** des faits de cybercriminalité par rapport à 2020, lesquels ont généré **plus de 173 000 demandes** d'assistance en ligne sur le dispositif **cybermalveillance.gouv.fr**. Dans son dernier rapport d'activité annuel, ce dernier révèle d'ailleurs que les menaces rencontrées par les Français concernent particulièrement trois formes de cybermalveillance : **l'hameçonnage, les rançongiciels et le piratage de compte (de messagerie, bancaire, etc)**.

La vigilance doit donc être accrue, puisque les conséquences des cyberattaques sont bien souvent importantes pour les organisations : paralysie partielle voire totale des systèmes d'information, vol ou perte de données sensibles, chantage à la diffusion de données, etc...
Dans la majorité des cas, ce sont les petites et moyennes entreprises qui sont victimes de ces actes informatiques malveillants, notamment parce qu'elles manquent de ressources dédiées afin de sécuriser efficacement leur environnement numérique. Mais les plus grands groupes sont autant concernés. Dans tous les cas, les défis à relever sont nombreux pour les *DSI*.

Des actions clés et de l'anticipation pour maintenir l'activité en cas d'urgence

Près d'une entreprise sur deux se dit inquiète quant à sa capacité à faire face efficacement aux cyber-risques. Pour celles-ci, la cybersécurité doit garantir la disponibilité d'un environnement numérique de confiance indispensable dans leur relation avec leurs partenaires et leurs clients, mais aussi avec leurs collaborateurs.

Hyper-dépendantes de leur système d'information, les organisations présentent d'inévitables faiblesses qu'elles doivent être en capacité de connaître et de comprendre pour améliorer leur cyber-résilience face à une crise. La capacité d'un système ou d'un réseau à continuer de fonctionner, cela en dépit d'un incident, est indispensable pour limiter l'indisponibilité des services.
Afin que les entreprises puissent assurer la continuité de leur activité en cas d'urgence et pour limiter au maximum l'impact d'un incident majeur, Adista a établi cinq grandes recommandations :

1. **Réduire la surface d'attaque** en mettant en place des dispositifs efficaces de contrôle et de filtrage des accès, mais aussi en appliquant et en faisant appliquer régulièrement les mises à jour de sécurité.

2. **Privilégier une protection dynamique** en recourant à des technologies avancées comme EDR ou des IDS/IS pour réduire significativement les risques.

3. **Engager les collaborateurs** en développant une culture cyber dans l'organisation et en favorisant l'adoption de bons comportements pour lutter contre les menaces mais aussi lorsqu'un événement est détecté.

4. **Se préparer au pire** en sauvegardant et vérifiant les capacités de restauration et en identifiant des partenaires fiables en cas d'incident et, si possible, en transférant les risques résiduels à un assureur.

Afin de dépasser la cybersécurité et atteindre la cyber-résilience, il est nécessaire de se concentrer sur le comportement de toutes les parties prenantes internes et pas seulement celui des équipes de sécurité. Une approche plus globale **qui place l'humain au cœur de la cybersécurité.**

C'est dans cette optique qu'Adista a lancé **une campagne de sensibilisation à destination des salariés inédite et originale**, composée d'un roman-photo et d'affiches web et print. Le roman-photo, initiative sans équivalent dans le secteur, présente trois situations de cyberattaques au quotidien et la meilleure réponse à y apporter. Les affiches rappellent quant à elles de manière décalée l'importance de la vigilance au quotidien face à des attaques toujours plus sophistiquées.

Adista : plus de 30 ans d'expertise au service de la cyber-résilience des organisations

En sa qualité d'opérateur télécoms et de fournisseur de services d'infogérance comme d'hébergement informatique, Adista intègre depuis longtemps la question de la cybersécurité comme une brique essentielle dans la construction de systèmes d'information résilients.

L'offre Cybersécurité et Cyber Résilience d'Adista s'appuie sur un centre de compétences dédié, formé pour assurer la sécurité des SI de plusieurs centaines de clients, collectivités, PME, ETI ou grandes entreprises. Quelle que soit la taille ou le secteur d'activité des organisations auprès desquelles elle intervient, Adista agit et conseille sur un périmètre très large. Ses experts en sécurité informatique définissent les stratégies de sécurité et les plans de continuité et reprise d'activité. Cette stratégie est personnalisée au contexte et à l'exigence définie par les dirigeants des organisations. Plus encore que la simple protection des réseaux, infrastructures et terminaux, Adista a fait le choix d'un positionnement incluant les aspects organisationnels et le facteur humain.

« Nous accompagnons les organisations dans le développement d'une véritable culture de la cybersécurité, en formant les collaborateurs aux bonnes pratiques à adopter face aux risques informatiques. Une manière efficiente de mieux anticiper les menaces et de réduire les risques. »
David Boucher, Responsable du Pôle d'Expertise Cybersécurité Adista

Actuellement, Adista intervient sur la sécurisation de plusieurs centaines d'organisations, **en protégeant notamment plus de 17 000 postes de travail et plusieurs dizaines de milliers de boîtes mails.**

À propos d'Adista

Opérateur de Services Hébergés, Adista se positionne en France comme le premier opérateur cloud et télécoms alternatif B2B et le spécialiste des services informatiques et voix. La force d'Adista réside dans sa capacité à associer les savoir-faire d'hébergeur, d'opérateur de télécommunications, de spécialiste de l'informatique d'entreprise et du développement applicatif. Maîtrise de bout en bout de la qualité des services, vision hybride du système d'information, capacité à livrer les services IT et les technologies THD partout en France font la réussite de l'entreprise. Après l'acquisition de Fingerprint en 2020 et de Waycom en 2021, Adista s'est rapprochée cette même année d'unyc, acteur majeur de la vente indirecte de services télécom. L'entreprise annonce un chiffre d'affaires de 222 millions d'euros pour 2021 et compte 900 collaborateurs répartis dans une quarantaine d'agences. Elle ambitionne de réaliser un chiffre d'affaires de 500 millions d'euros en 2026 et de devenir le 3ème opérateur télécoms B2B en France dans dix ans. www.adista.fr

CONTACT PRESSE - WORDCOM Consulting
Tél. 01 45 44 82 65
Eglantine de Cossé Brissac eglantine@wordcom.fr
Ellora Possenti rp@wordcom.fr