NumSpot
Cloud. Européen. Citoyen.

Le partenaire cloud souverain et de confiance des secteurs stratégiques et sensibles

Garantir les plus hauts standards de sécurité pour assurer la protection de leurs données et celles des citoyens.

En quoi le recours au cloud souverain et de confiance est-il un accélérateur en matière de cybersécurité ?

Résumé

- Le **coût accru** des risques cyber pour les entreprises les pousse à chercher toujours plus de **garanties de sécurité**.
- Les **facteurs de vulnérabilité** (humain, liés à l'obsolescence des infrastructures, des logiciels...) ne manquent pas.
- Le cloud souverain et **de confiance** qualifié **SecNumCloud** constitue une solution très performante pour répondre aux différentes problématiques des entreprises à risque potentiel, traitant des **données sensibles**.
- Le respect des **plus hauts standards de sécurité** est fondamental pour l'avenir de ces acteurs.

La **cybercriminalité**, c'est-à-dire le vol, le détournement de fonds, le piratage, et la destruction de données, a augmenté de 600 % depuis la pandémie. On estime que le coût pour les entreprises va bondir de 3 000 milliards de dollars en 2015 à environ **10 500 milliards de dollars d'ici à 2025** *(source Cybersecurity Ventures)*. Par an !

Les cybercriminels, toujours plus rapides et à l'affût des vulnérabilités de nos sécurités informatiques, cherchent à accéder aux **informations confidentielles** des entreprises et organisations, telles que les **données personnelles** des clients ou les **secrets commerciaux** pour en faire un usage criminel.

Quels sont les principaux facteurs de vulnérabilité des entreprises face aux cyberattaques ?

1 Une infrastructure informatique obsolète

Des entreprises utilisent des systèmes informatiques obsolètes ou qui ne sont pas à jour des derniers correctifs de sécurité. Elles sont beaucoup plus vulnérables aux cyberattaques.

2 Une mauvaise gestion des mots de passe

Les mots de passe faibles ou partagés entre plusieurs utilisateurs peuvent facilement être compromis, offrant aux cybercriminels un accès facile aux systèmes et aux données sensibles de l'entreprise.

3 Un manque de mise à jour et de patchs de sécurité

Les mises à jour régulières des systèmes informatiques sont essentielles pour remédier aux failles de sécurité connues et limiter les risques d'attaques. Non effectuées, elles augmentent la vulnérabilité aux cyberattaques.

4 L'utilisation de logiciels non autorisés

Non soumis aux mêmes tests de sécurité que les logiciels autorisés, les logiciels non autorisés peuvent introduire des vulnérabilités dans les systèmes informatiques de l'entreprise.

5 Le risque humain

Maillon le plus faible de la chaîne et facteur de risque le plus important : le personnel humain de l'entreprise. Selon un rapport Wavestone, cabinet de conseil européen, 80% des incidents de cybersécurité sont causés par des erreurs humaines.

+

Cette statistique montre que les erreurs humaines et les comportements à risque jouent un rôle significatif dans les failles de cybersécurité, soulignant l'importance de la sensibilisation et de la formation en matière de sécurité pour les employés.

Le **risque humain** se manifeste par un **manque de connaissances**, de l'**inattention** ou de la **négligence**. Il s'agit par exemple de collaborateurs qui ouvrent des liens dangereux, ou communiquent via des logiciels qui ne chiffrent pas les données, ou partagent des informations de manière non sécurisée sur leurs appareils mobiles, ou encore perdent des appareils appartenant à l'entreprise contenant des **données sensibles**.

Si le cloud computing offre de meilleures garanties en matière de cybersécurité et réduit le risque de piratage des données, en revanche, lorsqu'une entreprise utilise un environnement cloud pour exécuter ses applications, elle est responsable de la sécurité de ses applications. Cela signifie qu'elle doit prendre des **mesures de sécurité** pour protéger ses applications contre les cyberattaques. En cas d'infection des applications, c'est tout l'environnement cloud qui peut se trouver infecté et attaqué.

Pourquoi le cloud est-il un meilleur bouclier contre les cyberattaques ?

- **Ressources expertes**
  Les fournisseurs de services cloud disposent d'équipes dédiées de professionnels de la sécurité informatique qui travaillent en permanence pour protéger les données de leurs clients contre les attaques. Ils utilisent des technologies avancées, telles que l'analyse comportementale et l'apprentissage automatique, pour identifier les menaces potentielles et y répondre rapidement.

La France, considérée comme performante et compétitive par rapport à de nombreux autres pays, a pris des mesures pour renforcer le secteur de la cybersécurité, notamment via des politiques de régulations, en investissant dans la recherche et le développement, et en encourageant la formation et l'éducation dans ce domaine.

- **Gestion des accès**
  Les fournisseurs de services cloud proposent également des outils de gestion des identités et des accès pour garantir que seules les personnes autorisées ont accès aux données. Ces outils permettent aussi de suivre les activités des utilisateurs, de détecter les comportements suspects, et de réagir rapidement aux menaces potentielles.

- **Chiffrement et authentification**
  Le chiffrement convertit les données en un code illisible pour les personnes non autorisées. Il est utilisé par les fournisseurs de services cloud pour protéger les données stockées dans le cloud. Les systèmes d'authentification incluent des mots de passe, des codes PIN, des clés de sécurité ou des systèmes de reconnaissance biométrique. Combinés, ils rendent beaucoup plus difficilement accessibles les données à qui n'est pas autorisé.

- **Résilience**
  Les fournisseurs de services cloud disposent de technologies de sauvegarde et de récupération pour garantir la protection des données en cas de perte ou de corruption des systèmes. Ils disposent également de centres de données redondants pour stocker les données dans des emplacements géographiques différents, et ainsi garantir leur disponibilité en cas de panne ou de catastrophe naturelle.

Pourquoi le cloud est-il un meilleur bouclier contre les cyberattaques ?

- **La qualification SecNumCloud, atout majeur de cybersécurité**

SecNumCloud

Ce standard délivré par l'ANSSI (Agence Nationale des Systèmes de Sécurité Informatiques), autorité émanant du gouvernement impose de répondre à des exigences très élevées garantissant le plus haut niveau de sécurité en matière d'hébergement et de gestion des données.

Ce standard très exigeant a également la particularité de ne pouvoir être décerné qu'à des acteurs réputés comme souverain. A ce titre, les prestataires agréés doivent garantir que les données qu'ils traitent ne peuvent pas être soumises à des lois non européennes, telles que le Cloud Act américain. C'est le principe d'«Immunité au droit non communautaire ». Ainsi, le siège social du prestataire de services doit être établi dans un État membre de l'UE et des règles précises en matière d'actionnariat y sont énoncées.

> La qualification SecNumCloud, atout majeur de cybersécurité

Le choix d'un cloud souverain et de confiance se révèle également être un plus par rapport à des exigences règlementaires sectorielles telles que :

> **La règlementation NIS2**
Les Elle a pour but de renforcer la cybersécurité des réseaux et des systèmes d'information au sein de l'Union européenne. Elle impose notamment des obligations en matière de cybersécurité et de déclaration d'incidents aux opérateurs de services essentiels (OSE) ainsi qu'aux fournisseurs de services numériques (FSN)

La conformité des organisations est attendues pour **octobre 2024**.

> **La règlementation DORA**
Elle tient compte des risques toujours plus importants de cyberattaques, et matérialise la décision de l'Union Européenne de renforcer la sécurité informatique des entités financières (banques, compagnies d'assurance, entreprises d'investissement).

La conformité à cette règlementation est attendue pour **janvier 2025**.

Le cloud propose donc de réelles garanties en matière de cybersécurité, mais la sécurité dans le cloud **reste une responsabilité partagée entre le fournisseur de services cloud et son utilisateur.**

Si l'utilisateur intègre des éléments corrompus ou de mauvaises pratiques là où il a la responsabilité du contrôle, il n'est pas exempt de risques.

À propos de NumSpot

NumSpot est un acteur du cloud souverain et de confiance. Né de la volonté de 4 entreprises françaises de premier plan des secteurs public et privé (Banque des Territoires, Docaposte, Dassault Systèmes et Bouygues Télécom), NumSpot propose une offre de cloud indépendant, souverain et robuste adossé au IaaS d'OUTSCALE qualifié SecNumCloud. NumSpot est un cloud réversible et transparent, basé principalement sur l'open source et des solutions européennes. L'offre NumSpot s'adresse prioritairement aux secteurs confrontés à une forte sensibilité des données (secteur public, santé, services financiers et assurance, OIV et OSE) en France et en Europe, et à la recherche d'une solution souveraine et de confiance en accord avec les règlementations RGPD et européennes. NumSpot fait ainsi le choix d'œuvrer pour l'intérêt général en proposant un véritable pacte de confiance entre un fournisseur de cloud, ses clients et les citoyens européens.

Suivez-nous @NumSpot
@NumSpotCloud