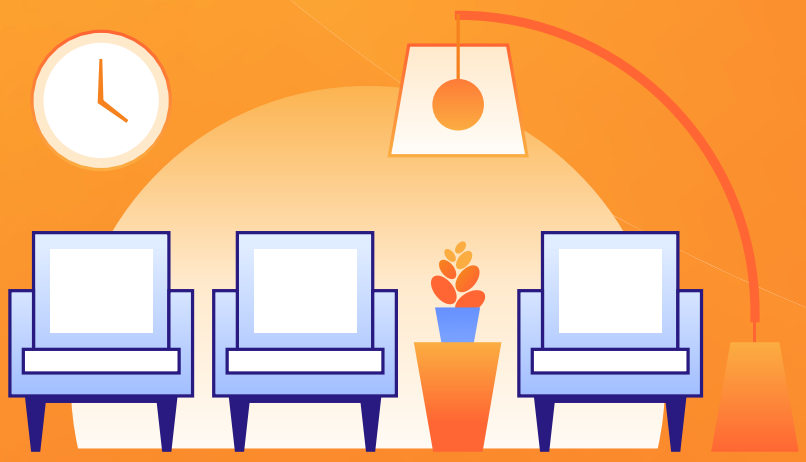
CLOUDFLARE

LIVRE BLANC

La cybersécurité dans le secteur public : déployer une protection dans le cloud pour les autorités publiques



Les longues attentes sur les fauteuils rigides des agences publiques devraient bientôt appartenir au passé. C'est en tout cas ce que souhaitent de nombreux gouvernements dans le monde, ainsi que leurs citoyens. Les administrations publiques aspirent à devenir plus efficaces, plus rapides et plus transparentes.

Pour atteindre ces objectifs, les administrations publiques doivent proposer des services en ligne modernes, reposant sur une infrastructure informatique performante. Les services cloud pourraient être le meilleur moyen pour elles d'assurer ces services ; cependant, la migration vers le cloud est susceptible d'exposer ces organisations à des cybermenaces. Pour faire face à ces menaces, elles devront déployer à la fois des mesures internes et des fonctionnalités de sécurité assurées par des prestataires externes tels que Cloudflare. Le réseau mondial et les services de cybersécurité étendus de Cloudflare peuvent offrir un rempart solide contre les attaques les plus préjudiciables sur Internet.

Les administrations publiques de presque tous les pays sont aujourd'hui engagées dans un processus de numérisation. La pandémie de COVID-19 a contraint les administrations d'État à repenser le rôle de l'État et à développer des solutions numériques permettant d'assurer la continuité des services publics et la stabilité de la société, leur imposant souvent de dépasser le champ d'application des politiques et réglementations existantes.

Différentes initiatives se sont soldées par des succès et des échecs, et le rythme des avancées a été variable d'un pays à l'autre, mais les tendances générales en matière de développement de services d'administration en ligne demeurent positives et encourageantes. À cet égard, un nombre croissant de pays ont renforcé leurs cadres institutionnels et juridiques, et la plupart ont élaboré une stratégie nationale en matière d'administration en ligne ou numérique. Dans le même temps, différents pays ont également adopté une législation englobant la cybersécurité, la protection des données personnelles, la politique nationale relative aux données, l'ouverture des données des administrations d'État et la participation en ligne. Les particuliers et les entreprises ont chaque jour davantage la possibilité d'interagir avec les institutions publiques par l'intermédiaire de plateformes en ligne, d'obtenir des informations sur la législation en matière de liberté d'information et d'accéder à des contenus et des données publics.

(Source : https://desapublications.un.org/sites/default/files/publications/2022-09/Report%20without%20annexes.pdf)

Tout ceci exige une infrastructure informatique puissante, qui nécessite, à son tour, une protection contre les cyberattaques, toujours plus nombreuses et puissantes. La mise en œuvre de cette protection constitue un défi, mais il existe des mesures et des solutions de sécurité qui ont fait leurs preuves.

Protection des données et sécurité de l'information

En plus de développer leur infrastructure informatique, les administrations publiques doivent également assurer la protection des données personnelles, dont certaines sont particulièrement sensibles. Elles doivent se conformer à l'ensemble des réglementations applicables en matière de protection des données, telles que le Règlement général sur la protection des données (RGPD), au sein de l'UE. Dans le même temps, les administrations doivent faciliter encore davantage l'accès des citoyens à l'information via des sites web et des portails. Elles doivent également prendre en charge les communications externes par le biais du courrier électronique, de l'accès à distance des collaborateurs aux ressources informatiques et de l'utilisation croissante des services de cloud.

Une sécurité de l'information insuffisante peut avoir des conséquences graves, parmi lesquelles les suivantes :

- **Perte de disponibilité :** les informations de base ne sont pas accessibles ou sont uniquement accessibles dans une mesure limitée. Cela peut, par exemple, signifier que la capacité d'une institution à accomplir des tâches spécialisées est limitée, voire suspendue.
- **Perte de confidentialité :** des données personnelles ou confidentielles sont accidentellement divulguées.
- **Perte d'intégrité (exactitude de l'information) :** des données sont falsifiées ou manipulées, perdent leur authenticité (authenticité et vérifiabilité) et sont attribuées à la mauvaise personne (falsification de l'identité numérique), par exemple.[1]

[1] Définie, par exemple, par l'Office fédéral de la sécurité de l'information du gouvernement allemand.

Directives relatives à la sécurité de l'information

Comment les administrations publiques devraient-elles renforcer la protection des données et la sécurité de l'information ?

La norme internationale ISO-27001 propose une méthodologie globale permettant aux entreprises et organisations d'améliorer la sécurité de leurs informations, et constitue la fondation de certifications correspondantes, largement reconnues dans le monde entier.

Les opérateurs d'infrastructures critiques sont également tenus, conformément aux législations telles que la directive NIS2 de l'UE, de prendre des précautions organisationnelles et techniques afin de prévenir les perturbations affectant leur infrastructure informatique. S'ils ont recours à des services cloud, ils peuvent être amenés à se conformer à des exigences spécifiques en matière de protection des données et de cybersécurité, à l'image du catalogue des critères de conformité cloud (C5) en Allemagne, du référentiel SecNumCloud en France ou de la politique Cloud Security Principles au Royaume-Uni.

Principes de sécurisation de l'infrastructure informatique

Outre ces directives, procédures et législations complètes, les principes suivants se sont avérés efficaces pour aider les entreprises et organisations des secteurs privé et public à renforcer la sécurité de l'information :

- La sécurité de l'information est une problématique qui concerne la direction des entreprises, et doit relever de la compétence du personnel dirigeant.
- Des ressources humaines et financières suffisantes doivent être consacrées à la sécurité de l'information. On considère que l'allocation de 15 à 20 % du volume total des dépenses informatiques est un montant raisonnable.
- Des entreprises externes spécialisées doivent réaliser des tests de sécurité.
- Des directives et des procédures de sécurité doivent être élaborées, mises en œuvre et déclarées contraignantes. Elles doivent notamment englober la sauvegarde régulière des données et la création de sauvegardes tenues à jour, l'introduction de règles concernant les mots de passe sécurisés et la désignation de personnes responsables de la mise en œuvre des mesures respectives.
- Les applications et les logiciels de tous les appareils, ainsi que leurs systèmes d'exploitation respectifs, doivent toujours être mis à jour dès la publication des mises à jour correspondantes, afin que l'application de correctifs permette l'élimination immédiate des failles de sécurité.
- Un plan d'urgence doit être mis en place afin de réagir à d'éventuels incidents affectant la sécurité informatique. Ce plan doit faire l'objet d'examens et de révisions à intervalles réguliers.
- En fin de compte, les utilisateurs d'appareils commettront toujours des erreurs, mais ils peuvent aussi détecter les dangers ; tous les collaborateurs doivent donc être familiarisés et formés à la sécurité informatique.

Augmentation des cybermenaces suite à l'invasion de l'Ukraine par la Russie

Selon le rapport 2023 Internet Organised Crime Threat Assessment (IOCTA) publié par le Centre européen de lutte contre la cybercriminalité (European Cybercrime Centre, EC3) d'Europol, l'évolution de la situation géopolitique à la suite de l'invasion de l'Ukraine par la Russie a suscité un « barrage de cyberattaques perturbatrices contre des cibles ukrainiennes et russes, mais également dans le monde entier, en particulier dans l'Union européenne. L'augmentation de ces activités malveillantes visant les États membres de l'UE est principalement imputable à un nombre important d'attaques par déni de service distribué (DDoS, Distributed Denial of Service) ciblant les institutions publiques nationales et régionales ».

La vague de cyberattaques lancées par des acteurs pro-russes contre des gouvernements s'est poursuivie pendant l'année 2024 :

- Janvier 2024 : des pirates informatiques russes lancent une attaque par rançongiciel contre l'unique fournisseur de services numériques pour les services gouvernementaux de Suède. L'attaque a affecté les opérations de 120 agences gouvernementales et a été lancée alors que la Suède se préparait à rejoindre l'OTAN, entraînant des perturbations qui ont duré plusieurs semaines.

- Mai 2024 : l'Allemagne accuse des pirates informatiques russes de s'être introduits dans les comptes de messagerie du parti social-démocrate allemand, principal parti de la coalition gouvernementale du pays. La campagne a débuté en mars 2022, lorsque des pirates ont exploité des vulnérabilités dans Microsoft Outlook pour cibler le comité exécutif du parti, ainsi que des entreprises allemandes du secteur de la défense et de l'aérospatiale.

  La Pologne et la République tchèque ont accusé des cyber-espions russes de cibler leurs réseaux gouvernementaux et d'infrastructure. Les pirates informatiques sont parvenus à accéder à leurs systèmes en exploitant une vulnérabilité dans Microsoft Outlook.

(Source : https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents)

Les pierres d'achoppement sur la voie de la sécurité de l'information

Pour mettre en œuvre, puis garantir la sécurité de l'information, les autorités, les municipalités et les institutions publiques doivent agir de manière aussi professionnelle que les acteurs malveillants potentiels dont ils sont la cible. Cependant, les autorités, les municipalités et les institutions publiques manquent souvent de spécialistes qualifiés, capables de mettre en œuvre une approche globale de la sécurité de l'information. Une infrastructure informatique fragmentée comporte également un certain nombre de problèmes : la diversité des équipements et des logiciels, parfois obsolètes, entraîne des lacunes en matière de sécurité. Il est difficile d'assurer une protection suffisante dans le cadre d'opérations sur site, hybrides et à distance, et les municipalités et autres institutions publiques ont tout intérêt à solliciter l'aide de prestataires externes spécialisés.

Renforcer la sécurité de l'information et améliorer les performances avec Cloudflare

Le cloud de connectivité de Cloudflare peut aider les administrations publiques à relever les défis complexes inhérents à la préservation de la sécurité de l'information. Cette plateforme unifiée de services cloud-native aide les entreprises et organisations à reprendre le contrôle et la visibilité des environnements informatiques complexes, tout en améliorant également les performances.

Contrôle et visibilité

Le cloud de connectivité de Cloudflare propose un réseau sécurisé permettant de bloquer les cyberattaques. Les sites web et les portails bénéficient d'un bouclier protecteur impénétrable par les logiciels malveillants, les attaques par phishing (hameçonnage) multicanal ainsi que les attaques de type kill chain ou HTTP/2 Rapid Reset (qui figure parmi les attaques DDoS les plus dévastatrices de tous les temps). Cloudflare bloque chaque jour plus de 209 milliards de cyberattaques dans le monde.

Afin d'améliorer la visibilité des menaces, Cloudflare analyse continuellement le trafic mondial de données transitant sur son réseau. Cloudflare, l'un des plus grands bots d'indexation du monde, juste derrière Google, utilise l'intelligence artificielle pour analyser l'ensemble du web à la recherche de modèles identifiables sur les pages d'accueil, entre autres paramètres. Cloudflare peut ainsi prévoir les menaces plusieurs semaines à l'avance et déjouer les attaques potentielles à un stade précoce.

Performances

Cloudflare est l'un des plus vastes réseaux du monde, présent dans plus de 320 villes dans plus de 120 pays. Il traite plus de 57 millions de requêtes HTTP par seconde et sert des millions de pages web chaque jour. Afin d'éviter les goulets d'étranglement, un algorithme achemine intelligemment le trafic de données par les chemins réseau les plus rapides et les plus fiables. En outre, le routage géolocalisé garantit que les contenus sont fournis par les serveurs les plus proches géographiquement des utilisateurs.

Pour améliorer la vitesse et la connectivité, les serveurs sont situés aux points d'échange entre différents réseaux. Ces points d'échange Internet (Internet Exchange Point, IXP) assurent l'interconnexion des réseaux des différents fournisseurs d'accès Internet. Le réseau de Cloudflare dispose de connexions directes avec pratiquement tous les fournisseurs d'accès Internet et de cloud, lui permettant ainsi d'atteindre 95 % des personnes disposant d'une connexion Internet, partout dans le monde, dans un délai d'environ 50 millisecondes. Dans l'ensemble, Cloudflare est connecté à environ 13 000 réseaux de fournisseurs de services, de fournisseurs de cloud et de grandes entreprises.

Cloudflare accélère l'acheminement des données et réduit la latence en mettant le contenu en cache sur des serveurs périphériques. Différents outils et services d'optimisation permettent également d'améliorer les performances, par exemple, en ajustant et en optimisant les images et en minimisant les fichiers HTML, CSS et JavaScript.

Certifications et validations externes de Cloudflare

Cloudflare dispose d'un certain nombre de certifications et de validations externes fondées sur des normes internationales de protection des données et de sécurité de l'information :

- Les solutions de Cloudflare sont conformes aux exigences de la réglementation RGPD de l'UE. Cloudflare garantit, pour les transferts de données vers les États-Unis, un niveau équivalent de protection des données personnelles, conformément au RGPD, fondé à la fois sur ses clauses contractuelles standard avec des mesures de mise en œuvre et par sa certification conformément au cadre de protection des données UE-États-Unis.
- Les autres certifications incluent notamment les normes ISO/IEC 27001:2023 et ISO/IEC 27701:2019 pour la mise en œuvre de systèmes de sécurité de l'information, ainsi que la norme ISO/IEC 27018:2019 pour la protection des données à caractère personnel traitées dans un cloud public.
- Les exigences du catalogue des critères de conformité cloud (« Cloud Computing Compliance Criteria Catalogue », C5), une norme d'essai élaborée par l'agence allemande de cybersécurité BSI, garantissent que les fournisseurs de services cloud satisfont aux critères en matière de sécurité de l'information.
- Les services de Cloudflare sont également conformes au Code de conduite cloud de l'UE (« EU Cloud CoC »). Cloudflare s'engage donc à mettre en œuvre des directives de protection des données et des mesures de sécurité conformes à la réglementation RGPD.
- L'Office fédéral de la sécurité de l'information du gouvernement allemand (BSI) a reconnu Cloudflare comme « fournisseur qualifié de services d'atténuation des attaques DDoS ».

Solutions de Cloudflare pour le secteur public

Cloudflare propose une suite de services modulaire et configurable pour le secteur public, comprenant une vaste gamme de services destinés à protéger les sites web, les applications et les réseaux. Par exemple, Cloudflare réunit une protection contre les attaques DDoS, un pare-feu d'application web (WAF) dans le cloud, la localisation des données, la gestion des certificats, des contrôles d'intégrité et des fonctionnalités de sécurité Zero Trust. Le modèle Zero Trust met en œuvre une vérification stricte de l'identité de tous les utilisateurs et appareils qui tentent d'accéder aux ressources d'un réseau privé, qu'ils se trouvent à l'intérieur ou à l'extérieur du périmètre du réseau. Les services Cloudflare Zero Trust incluent également une assistance à la mise en œuvre, à l'intégration et à la gestion de la configuration.

Le département français de Seine-et-Marne a déployé les solutions Cloudflare Zero Trust afin de renforcer la sécurité et la performance du réseau WiFi public dans les collèges et lycées. Les 129 établissements scolaires du département ont besoin d'une connectivité Internet sécurisée et fiable pour soutenir les objectifs académiques, tout en empêchant les élèves d'accéder à des contenus indésirables. Les administrateurs ont déployé Cloudflare Gateway, une passerelle web sécurisée doté de fonctionnalités de filtrage DNS, dans l'ensemble du département. La solution accélère la connectivité pour les élèves et les enseignants, tout en sécurisant la navigation sur le web et en protégeant les établissements contre les cyberattaques.

À Aalen, en Allemagne, la compagnie d'électricité Stadtwerke Aalen GmbH a adopté les services de Cloudflare afin de résoudre les problèmes de performance du VPN et les difficultés auxquelles se heurtait son service d'assistance. La municipalité a mis en œuvre une solution VPN plus puissante et plus légère, basée sur le protocole WireGuard, et a opté pour le déploiement de Cloudflare One. Les principaux composants de la solution incluent une solution VPN avec des clients utilisateurs WARP, Cloud Access pour sécuriser l'accès aux applications internes, Cloudflare Gateway pour sécuriser l'utilisation d'Internet et Cloudflare Browser Isolation pour déployer une protection contre les attaques par phishing (hameçonnage).

Les prestataires de services externes représentent une solution efficace pour la sécurité de l'information

La numérisation de l'administration publique progresse, et la sécurité de l'information est un aspect essentiel de cette transformation. Cependant, de nombreuses organisations ne disposent pas de ressources et de compétences suffisantes pour satisfaire aux exigences et aux réglementations en matière de sécurité de l'information. Néanmoins, les organismes publics ont la possibilité de faire appel à des prestataires de services externes pour assurer la protection de leurs informations.

Cloudflare peut offrir aux organisations du secteur public une protection efficace contre les cyberattaques. Les organisations peuvent faire leur choix parmi le vaste portefeuille de services de Cloudflare, afin d'adapter les fonctionnalités de sécurité choisies à leurs besoins particuliers.

Plus d'informations et contact

À propos de Cloudflare

Cloudflare, Inc. (NYSE : NET) est le leader dans le domaine du cloud de connectivité. L'entreprise permet aux sociétés d'améliorer la rapidité et la sécurité de leurs collaborateurs, leurs applications et leurs réseaux, partout dans le monde, tout en réduisant la complexité et les coûts. Reposant sur l'un des réseaux les plus vastes et les plus interconnectés du monde, Cloudflare bloque chaque jour pour ses clients des milliards de menaces en ligne.

Contact :

Cloudflare LTD
Riverside Building, 6th Floor,
County Hall/The, Belvedere Rd
London SE1 7PB, United Kingdom
Téléphone : 01 73 01 52 44
Email: enterprise@cloudflare.com
https://www.cloudflare.com/fr-fr/