Derrière le pare-feu :

Implémenter des dispositifs de protection du DNS pour réduire les vulnérabilités et les risques en ligne

Derrière le pare-feu : Implémenter des dispositifs de protection du DNS pour réduire les vulnérabilités et les risques en ligne

Depuis plus de 25 ans, les pare-feux constituent la première ligne de défense dans la sécurité des réseaux. Ils agissent comme une barrière entre les réseaux internes sécurisés, fiables et contrôlés, et les réseaux externes non sécurisés, tels qu'Internet.

Et ils sont essentiels, parce que la cybercriminalité est en augmentation et s'infiltre partout. De nombreux responsables de la sécurité informatique réagissent en renforçant les dispositifs de défense au sein du pare-feu de l'entreprise, et en exécutant des simulations et des tests de pénétration.

Mais aujourd'hui, disposer uniquement d'un pare-feu n'est pas suffisant face à l'augmentation exponentielle de la cybercriminalité.

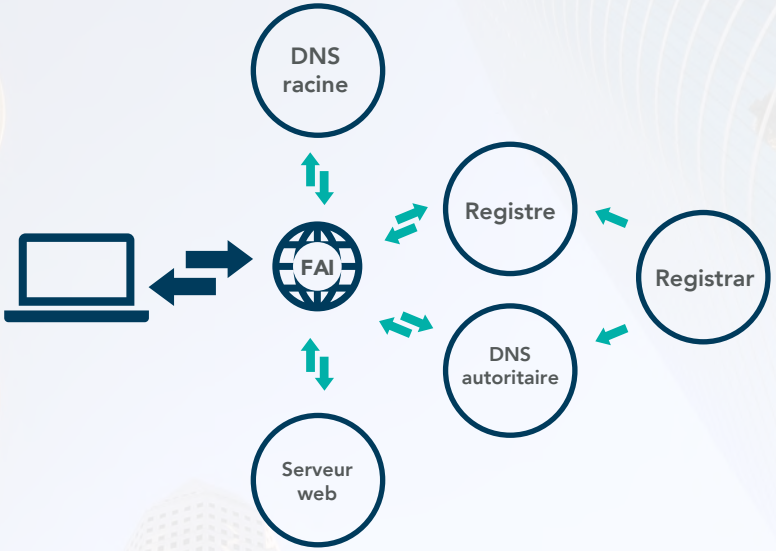
En outre, la sécurité des actifs numériques hors du périmètre du pare-feu – noms de domaine, serveurs DNS et certificats numériques par exemple – est souvent négligée. Une bonne gestion des actifs numériques, et notamment du DNS, est essentielle pour un fonctionnement sans faille des activités de l'entreprise.

Le DNS est l'infrastructure nécessaire au bon fonctionnement d'Internet, en servant de répertoire pour diriger les utilisateurs vers le contenu Web voulu. Lorsque les serveurs DNS tombent en panne, ce sont tous les sites Web qui cessent de fonctionner. Dans ce cas-là, le premier réflexe est de se servir du téléphone et des e-mails pour ne pas interrompre l'activité. Mais une panne des serveurs DNS signifie également une perte de fonctionnalité des messageries et de la téléphonie (VoIP), et l'impossibilité pour les télétravailleurs de se connecter. En outre, le protocole FTP utilisé pour le transfert de fichiers volumineux et les services d'authentification multifacteur (la messagerie, Google® et Microsoft®, par exemple) ne sont plus autorisés.

Tout dysfonctionnement de ces actifs numériques a un impact important, qu'il s'agisse d'une perte de revenus ou de données, ou d'atteinte à la réputation de la marque.

Le DNS est fragile : À MANIPULER AVEC PRÉCAUTION !

DNS : derrière ce simple acronyme se cache la complexité d'un système constitué d'un réseau mondial d'entités distinctes qui interagissent en relayant des échanges d'informations. Cette nature complexe expose le DNS à de multiples failles potentielles, puisque chaque point du système peut être vulnérable face aux attaques qui peuvent affecter votre entreprise.



10 menaces et risques associés aux vulnérabilités du DNS

1. Piratage DNS
2. Empoisonnement du cache DNS
3. Domain-shadowing
4. Interruption de services DNS
5. Malware
6. Tunnels DNS
7. Attaques zero-day
8. Attaques par déni de service (DDoS)
9. Noms de domaine expirés, volés ou perdus
10. Certificats numériques expirés, manquants ou mal installés

1

2

3

4

Les 4 étapes d'une approche « défense en profondeur »

Le terme « défense en profondeur » désigne une approche sécurité multicouche, qui protégera vos actifs immatériels situés hors du pare-feu.

ÉTAPE 1 :

Utilisez des fonctionnalités de sécurité avancées.

Pour vos noms de domaine critiques, c'est-à-dire ceux sur lesquels reposent vos opérations commerciales, ajoutez :

- Un Registry Lock pour contrer tout piratage DNS ;
- Le protocole DNSSEC (domain name system security extensions) pour empêcher tout empoisonnement du cache DNS ;
- Des certificats numériques pour chiffrer les données ;
- Le protocole DMARC (domain message authentication reporting and conformance) pour authentifier vos e-mails et réduire les menaces des attaques de phishing qui ciblent votre personnel ;
- Des enregistrements CAA (Certificate Authority Authorization) pour exécuter vos politiques de certificats numériques.

1

2

3

4

Les 4 étapes d'une approche « défense en profondeur »

Le terme « défense en profondeur » désigne une approche sécurité multicouche, qui protégera vos actifs immatériels situés hors du pare-feu.

ÉTAPE 2 :

Contrôlez les autorisations utilisateur.

Assurez-vous de savoir quels utilisateurs ont accès à vos actifs immatériels critiques, et quelles sont les autorisations dont ils disposent, puis gérez activement ces autorisations. Vous devriez être capable d'accéder aux autorisations d'un clic de souris, de recevoir des notifications, mais aussi de surveiller et d'octroyer les autorisations de modification à partir d'une plateforme unique. Une telle centralisation permettra de repérer plus facilement les modifications non autorisées, de type piratage DNS et domain-shadowing.

Les 4 étapes d'une approche « défense en profondeur »

Le terme « défense en profondeur » désigne une approche sécurité multicouche, qui protégera vos actifs immatériels situés hors du pare-feu.

ÉTAPE 3 :

Sécurisez l'accès aux portails.

Vous devriez sécuriser l'accès à tous les portails que vous utilisez. Pour chaque portail, l'accès devrait être soumis à une authentification multifacteur, incluant la validation IP, l'authentification à deux facteurs et une fonctionnalité de type Federated Identity (ou authentification unique). Cette démarche permet de recourir à un nombre réduit de prestataires pour gérer les accès et réduire le risque de modifications non autorisées de vos actifs numériques.

Les 4 étapes d'une approche « défense en profondeur »

Le terme « défense en profondeur » désigne une approche sécurité multicouche, qui protégera vos actifs immatériels situés hors du pare-feu.

ÉTAPE 4 :

Ayez recours à des prestataires de services corporate.

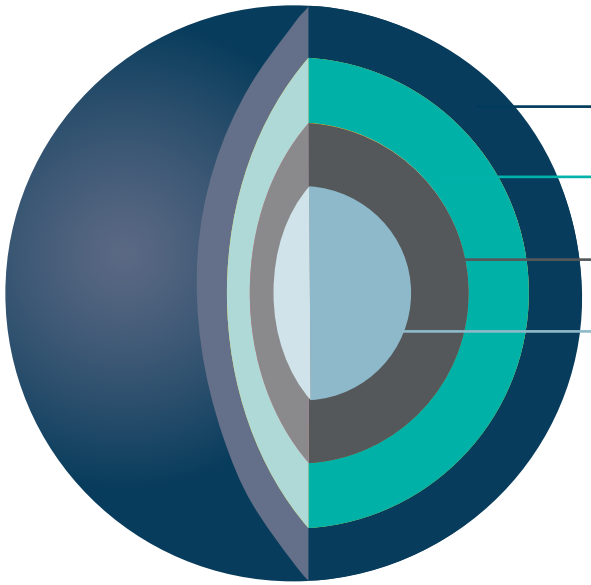
Dernier conseil : choisissez bien vos partenaires. En plus de limiter le nombre de prestataires et de portails que vous utilisez pour contrôler votre exposition au risque, vous ne devez faire aucune concession sur la qualité de la gestion de vos noms de domaine, de votre DNS ou de vos certificats numériques. Les meilleurs prestataires de niveau professionnel vous permettront de consolider la gestion de tous vos actifs, avec des systèmes sécurisés et des processus pour vous aider à atténuer les risques et les menaces. Les prestataires de niveau professionnel s'appuient sur l'expertise de leurs analystes internes, et mettent à votre disposition la connaissance et le support de leurs responsables grand compte pour vous aider à identifier les risques et à choisir les bonnes solutions.

Comment gagner en visibilité sur des menaces de sécurité hors du pare-feu

Chez CSC, nous avons remarqué qu'actuellement aucune solution n'aidait les entreprises, et en particulier les responsables de la sécurité informatique, à surveiller les actifs situés hors du pare-feu. Les tableaux de bord existants se concentrent sur les failles dans les réseaux internes et les pare-feux, mais proposent peu d'outils pour identifier les risques majeurs qui peuvent atteindre vos actifs hors du périmètre du pare-feu.

CSC Security Center℠ a été conçu pour aider les professionnels de la sécurité informatique à réduire les risques pour les actifs numériques non protégés. Notre solution utilise notre algorithme propriétaire pour identifier les noms de domaines critiques de votre portefeuille en analysant les multiples caractéristiques du nom de domaine. Une inspection plus poussée de chaque domaine identifie les risques probables et propose des recommandations en vue d'atténuer les menaces.

La visibilité permet la mise en œuvre de contrôles et de politiques flexibles



Avec le développement de CSC Security Center, les entreprises peuvent désormais identifier leurs noms de domaine critiques et les failles de sécurité, et identifier les risques, y compris l'empoisonnement du cache DNS, le piratage de noms de domaine et le piratage DNS, les attaques DDoS, et bien plus encore. Nous recommandons d'aller plus loin et d'implémenter des politiques visant à définir le bon cadre pour renforcer la sécurité de l'entreprise.

PRESTATAIRE DE SERVICES AUX ENTREPRISES

- Data Centers certifiés ISO 27001
- Conformité SOC 2®
- Tests de sécurité, de vulnérabilité et de pénétration
- Accréditation ICANN
- Des partenariats de haut niveau pour la technologie DNS et les certificats numériques
- Formation à la sécurité des actifs, à la détection des tentatives de phishing et d'ingénierie sociale
- Politique du bureau dégagé obligatoire
- Demandes écrites obligatoires (jamais par téléphone)
- Respect des exigences de conformité des données et de la réglementation RGPD (pratiques WHOIS)
- Politique de renouvellement automatique
- Politique de verrouillage des transferts au niveau registre

ACCÈS SÉCURISÉ AU PORTAIL

- Politique d'authentification à deux facteurs obligatoire
- Validation IP facultative
- Fonctionnalité Federated Identity facultative

CONTRÔLE DES AUTORISATIONS UTILISATEUR

- Visibilité sur les autorisations élevées avec notifications
- Politique de gestion des contacts autorisés

FONCTIONNALITÉS DE SÉCURITÉ AVANCÉES

- Identification des noms de domaine critiques
- Détection des failles de sécurité
- Politique de verrouillage automatique

Les piratages DNS prennent de l'importance dans le domaine de la cybersécurité, avec des attaques quotidiennes pour une année 2019 marquante.

- CSC Alerts Companies to Increased DNS Hijacking (CSC alerte les entreprises sur la recrudescence des piratages DNS)
- DNS Hijacking Abuses Trust in Core Internet Service (Les piratages DNS sapent la confiance envers Internet)
- Alert Regarding Published Reports of Attacks on the Domain Name System (Alerte : publication de rapports sur des attaques DNS)
- Emergency Directive 19-01 Mitigate DNS Infrastructure Tampering (Directive d'urgence 19-01 Limiter les modifications frauduleuses au sein de l'infrastructure DNS)

Les organisations de sécurité gouvernementales, les ministères des affaires étrangères et de grandes organisations du secteur de l'énergie ont été la cible d'une campagne d'attaques internationale visant à modifier les enregistrements des noms de serveurs DNS pour rediriger les utilisateurs vers des serveurs contrôlés par les attaquants. Cette vague d'attaques a d'abord visé les entités tierces telles que les bureaux d'enregistrement de DNS, les sociétés de télécommunication et les fournisseurs de services Internet, et a notamment servi à dérober des certificats numériques légitimes de ces organisations pour les utiliser sur les serveurs contrôlés.

« Les attaques DNS sont lancées par des criminels qui redirigent le trafic Web d'un site légitime vers un site malveillant et font courir un grand risque aux clients et aux entreprises », déclare Mark Flegg, responsable produit de la division Security Services de CSC. « Les attaques récentes sont complexes et vicieuses, elles exploitent les faiblesses des infrastructures DNS que de nombreuses entreprises mettent en place, puis négligent. Nous conseillons fortement à nos clients d'utiliser les outils et les recommandations disponibles pour sécuriser leur infrastructure numérique. »

La sévérité des attaques a incité plusieurs gouvernements et organisations internationales à réagir en lançant des directives et des alertes, un dispositif sans précédent dans la sécurité des noms de domaine.

« Le piratage des noms de domaine et des serveurs DNS n'est pas une menace nouvelle, c'est pourquoi nous avons développé CSC Security Center. La bonne nouvelle, c'est que des centaines de grandes entreprises du monde entier l'utilisent pour les aider à protéger leurs éléments numériques critiques qui leur permet de fonctionner », ajoute Mark Calandra, directeur général de la division Digital Brand Services de CSC. « La sophistication et l'impact des récentes vagues d'attaques est un avertissement : une gestion efficace des noms de domaine, des serveurs DNS et des certificats numériques doit s'intégrer au cœur de la stratégie de sécurité de toute entreprise qui dispose d'une présence en ligne. »

Pour en savoir plus sur les risques de piratage DNS et sur les solutions qui existent, lisez notre billet de blog (en anglais) *Confused About Domain Locks? Understand the Intricacies and Security Effectiveness.*

Quatre politiques clés que chaque entreprise devrait adopter pour ses domaines critiques :

Authentification multifacteur obligatoire pour contrôler l'accès utilisateur

Politique de renouvellement automatique pour empêcher l'expiration et/ou la perte de noms de domaine

Politique de verrouillage automatique pour empêcher les modifications non autorisées de noms de domaine

Politique de gestion des certificats numériques pour définir les autorités de certifications autorisées

La gestion des actifs numériques implique bien plus que de gérer le renouvellement, la modification et le remplacement des certificats numériques. Nous souhaitons aider activement nos clients à implémenter et à ajuster leurs politiques avec des technologies innovantes couplées aux meilleurs services du secteur. Notre mission est d'aider nos clients à protéger leur activité face aux menaces situées hors du pare-feu.

Pour en savoir plus sur les fondamentaux de la sécurité des noms de domaine, veuillez consulter notre livre blanc, **Sécurité des actifs numériques : Revenons aux fondamentaux !**

cscdigitalbrand.services/fr