GUIDE ANSSI

DES BONNES PRATIQUES
POUR L'ACQUISITION ET L'EXPLOITATION
DE NOMS DE DOMAINE

REPONSES DE NAMESHIELD

AGENCE NATIONALE POUR LA SECURITE DES SYSTEMES D'INFORMATION

37 boulevard des Capucines - 75002 Paris | 27 rue des Arènes - 49100 Angers

NAMESHIELD SAS - RCS PARIS B 399 140 961 – SIREN 399 140 961 000 18

Propos introductif : l'ANSSI

L'Agence Nationale de la Sécurité des Systèmes d'Information (**ANSSI**) est un service français créé par décret en juillet 2009. Ce service à compétence nationale est rattaché au Secrétaire général de la défense et de la sécurité nationale (SGDSN), autorité chargée d'assister le Premier ministre dans l'exercice de ses responsabilités en matière de **défense** et de **sécurité nationale**.

L'agence assure la mission d'autorité nationale en matière de **sécurité des systèmes d'information**. À ce titre elle est chargée de proposer les **règles à appliquer** pour la **protection** des systèmes d'information de l'État et de **vérifier l'application** des **mesures** adoptées. Dans le domaine de la défense des systèmes d'information, elle assure un service de veille, de détection, d'alerte et de **réaction** aux **attaques** informatiques, notamment sur les réseaux de l'État.

L'ANSSI apporte son **expertise** et son **assistance technique** aux **administrations** et aux **entreprises** avec une mission renforcée au profit des opérateurs d'importance vitale (**OIV**).

Elle est chargée de la **promotion** des **technologies**, des **produits** et **services de confiance**, des systèmes et des savoir-faire nationaux auprès des experts comme du grand public. Elle contribue ainsi au développement de la confiance dans les usages du numérique.

Son action auprès de différents publics comprend la **veille** et la **réaction**, le **développement** de produits pour la société civile, l'information et le conseil, la formation ainsi que la labellisation de produits et de prestataires de confiance.

L'ANSSI publie chaque année le rapport "**Résilience de l'Internet Français**" dans lequel l'agence étudie les technologies critiques au bon fonctionnement de l'Internet et notamment la **résilience** de **l'infrastructure** de **l'Internet** à travers des protocoles BGP et DNS. Ce rapport amène également un certain nombre de **préconisations** destinées à la robustesse des infrastructures supportant ces protocoles.

Ce document présente les réponses apportées par Nameshield pour se conformer aux recommandations de l'ANSSI en la matière.

Recommandation n° 1 : Utiliser le verrou de niveau registre

Choisir un registre offrant un service de verrou de niveau registre et obtenir des assurances ou des engagements contractuels sur le niveau de service garanti pour cette fonctionnalité.

Solution mise en œuvre par Nameshield

Le **Registry lock**, ou verrou de **niveau registre**, est une **authentification** des **demandes** entre le **Registrar** et le **Registre**. Si le client final fait une **demande** au Registre, celle-ci doit être **confirmée** par une personne désignée chez le Registrar chargée de **déverrouiller** le nom. Le registry lock est disponible chez Nameshield pour toutes les extensions proposant ce système [.com, .net, .tv, .cc, .name, .fr, .eu, .ca, .co.uk, .uk, .cn, etc.] Ces procédés supposent que la demande initiale provienne du titulaire du nom de domaine. Le Registrar ne peut fournir au Registre la validation d'une demande dont il ne connaît pas la légitimité.

Nameshield s'assure systématiquement auprès de son client, titulaire du nom, qu'il est bien le demandeur. Nous utilisons à cette fin des **contacts habilités** préalablement renseignés dans nos bases de données.

Recommandation n° 2 : Choisir un bureau d'enregistrement offrant une authentification renforcée

Choisir un bureau d'enregistrement offrant un mécanisme d'authentification journalisée et renforcée, par exemple grâce à deux facteurs d'authentification et un filtrage des accès à l'interface d'administration.

Solution mise en œuvre par Nameshield

Nameshield assure l'authentification des utilisateurs avec une **gestion** de **mots** de **passe forts**. Les tentatives même infructueuses sont loguées, et le nombre de tentatives d'accès limitées (Capcha avant bannissement).

Ces mesures sont renforcées par une **procédure ACL** (Access Control List) sur **l'adresse IP** des utilisateurs (filtrage IP). Ces procédures sont configurables par les administrateurs, pour les comptes utilisateurs ou les comptes autorisés excluant les tiers non autorisés.

La sécurité de ces accès est également garantie par une **sensibilisation du personnel** et le respect des procédures établies, par exemple pour la communication des accès en ligne. Ces mesures sont une défense efficace contre le phishing et l'ingénierie sociale.

Nous **sensibilisons** également nos clients à la **gestion** de la **sortie** de **salariés** et à l'importance du rôle de l'administrateur désigné chez eux à autoriser les accès. Ces précautions nous ont conduits à spécifier dans nos relations contractuelles la responsabilité du Client dans l'usage des moyens d'authentification qui sont mis à sa disposition ainsi que l'usage des **filtrages IP.**

Nameshield augmente également la sécurité d'accès à sa plateforme dédiée et propose **l'identification double facteurs**. Dans le domaine de la sécurité informatique, le principe de la double authentification est efficace et simple. Cette procédure permet de renforcer la sécurité en proposant aux utilisateurs de se connecter à leur compte en saisissant un code chiffré de validation envoyé sur un téléphone portable en complément de leur nom d'utilisateur et de leur mot de passe. Cette validation en deux étapes contribue à protéger le compte utilisateur contre les accès non autorisés au cas où un tiers parviendrait à obtenir son mot de passe.

Recommandation n° 3+ : Utiliser le verrou niveau bureau d'enregistrement lorsque disponible

Choisir un bureau d'enregistrement offrant un mécanisme de verrou de niveau bureau d'enregistrement afin de prévenir les transferts frauduleux de gestion de domaines.

Solution mise en œuvre par Nameshield

Nameshield complète le dispositif registry lock avec un **Registrar lock** établi entre notre client et nous, pour les nombreux registres n'ayant pas implémenté cette mesure de sécurité. Il interdit les modifications (DNS ou transfert) et est levé sur procédure manuelle à l'initiative de Nameshield auprès des contacts habilités de notre client.

Recommandation n° 4 : Choisir un bureau d'enregistrement prenant en charge DNSSEC

Sélectionner un bureau d'enregistrement qui permette de publier les informations nécessaires à l'utilisation de DNSSEC.

Solution mise en œuvre par Nameshield

Nameshield encourage cette approche et l'anticipe par sa propre démarche de **certification ISO/IEC 27001**[1] dont le périmètre englobe les biens informationnels que nous gérons pour nos clients, notamment les portefeuilles de noms de domaine et de marques.

La certification elle-même repose sur une analyse des risques et sur la constante amélioration des mesures de sécurité qui les concernent, aussi bien les procédures métiers que les Systèmes d'information. Cette approche ISO/IEC 27001 encourage l'implication des tiers dans sa démarche.

Recommandation n° 5 : Evaluer les risques associés au recours à un revendeur

Lorsqu'un titulaire a recours à un prestataire, comme un revendeur, il doit entamer une démarche d'évaluation et de maîtrise des risques, notamment en suivant les recommandations du guide d'externalisation de l'ANSSI.

Solution mise en œuvre par Nameshield

Nameshield n'est pas concerné par ce point.

[1] L'ISO/CEI 27001 est une norme internationale de système de gestion de la sécurité de l'information

Recommandation n° 6 : Utiliser au moins deux serveurs faisant autorité

Servir les noms de domaine depuis au moins deux serveurs faisant autorité distincts.

Recommandation n° 7 + : Répartir les serveurs dans plusieurs préfixes réseau

Répartir les serveurs de noms faisant autorité dans plusieurs préfixes (blocs d'adresses IP) ou utiliser la technique de routage anycast.

Recommandation n° 8 + : Répartir géographiquement les serveurs

Éloigner les serveurs de noms, par exemple, en les plaçant dans différents centres de données, afin de mieux résister aux aléas naturels et aux incidents techniques.

Solution mise en œuvre par Nameshield

Nameshield sert les noms de domaine depuis **cinq clusters de serveurs faisant autorité**. Le réseau Nameshield est bâti sur une **architecture réseau** en **anycast** pour répondre à cette problématique, répartie dans 3 réseaux différents et 3 sous-réseaux IP sur 10 points géographiques différents.

L'infrastructure de Nameshield est bâtie sur notre **cœur de réseau** (hébergé en cluster de performance au sein de **deux data centers** situés en France dans des villes différentes, sur **différentes installations** (réseaux électriques et fibres optiques).

Cette infrastructure est associée à **15 points de présence dans le monde** : Paris (x2), Amsterdam, Francfort, Londres, New York, Washington DC, Miami, San José, Seattle, Los Angeles, Dallas, Sydney, Tokyo, Singapour.

Il s'agit d'un **ensemble de serveurs dans une infrastructure propre**, associant plusieurs réseaux de différents prestataires (donc des préfixes différents comme le préconise l'ANSSI) hébergent des architectures systèmes en **cluster** et des **DNS hidden bastions**. Ce DNS hidden est situé derrière un **pare feu** que seuls nos DNS sont habilités à franchir. Il est bâti sur le **modèle de Cluster** de disponibilité et permet de garantir l'intégrité des zones DNS.

Un **second ensemble de serveurs secondaires** plus largement distribué géographiquement complète le dispositif au niveau national et international, et de façon mondiale dans un **ensemble anycasté** destiné à apporter une **réponse** à la menace des Dénis de Service (**Ddos**). Cette architecture est conforme aux recommandations complémentaires ANSSI, dans la triple mesure où les réseaux, les programmes et les serveurs sont séparés et cloisonnés.

Recommandation n° 9 : Prendre en charge TCP comme protocole de transport DNS

Configurer les infrastructures dans leur ensemble, notamment les serveurs, les répartiteurs de charge et les équipements de filtrage, pour prendre en charge TCP, en complément d'UDP, comme protocole de transport pour le DNS.

Solution mise en œuvre par Nameshield

Nameshield prend en charge **TCP** comme **protocole de transport du DNS**. Nous avons configuré nos infrastructures, dans leur ensemble, pour prendre en charge TCP, en complément d'UDP, comme protocole de transport pour le DNS.

Nameshield vise à déployer des moyens de protection qui ne pénalisent pas les requêtes « légitimes » :

Tout d'abord, un **filtrage** à **deux niveaux** sur les **Burst** des requêtes des **gros requêteurs**. Le premier filtrage est effectué sur les couches réseau et n'affecte donc pas la performance des applications DNS et se déroule en paliers pour respecter les demandes légitimes.

Recommandation n° 9 : Prendre en charge l'extension DNS EDNSO

Configurer les infrastructures, notamment les serveurs DNS, les répartiteurs de charge, les systèmes de détection d'intrusion et les pare-feu, afin de prendre en charge EDNS0.

Solution mise en œuvre par Nameshield

Nameshield respecte les **standards** de **EDNS** et a configuré ses infrastructures afin de prendre en charge EDNS. EDNS chez Nameshield est notamment utilisé dans le cadre de :

-La mise en place de **DNSSEC** pour les noms de domaine des extensions automatisées sur cette extension du protocole DNS. Nameshield prend en charge la gestion complète des clés associées et de la relation avec les différents registres ;

-La mise en place de la **géolocalisation** du trafic au travers du service **GeoIP**.

Nameshield a pris en compte le maximum d'aspects de la sécurité du DNS pour déployer des mesures de sécurité avec des configurations adaptées (conformité aux RFC4 et notamment la RFC 4641).

[4]Request For Comment, documents officiels issus de l'IETF décrivant les aspects techniques d'Internet.

Recommandation n° 11 : Définir des valeurs de TTL élevées en mode nominal

Configurer des valeurs de TTL relativement élevées, dans le cadre normal des opérations.

Solution mise en œuvre par Nameshield

Le service DNS Premium proposé par Nameshield permet un **réglage fin des TTL de 30 secondes à l'infini**. De par notre métier, il appartient à nos clients de définir la durée de leurs TTL. Nous avons un rôle de **conseil** sur le sujet et **préconisons** de ne pas mettre toute une zone avec des TTL courts mais uniquement les RR associés aux services qui en ont besoin ; de même sur les services standards (**Web, Mail, VOIP**) un **TTL** idéal de **4 heures** est recommandé.

Pour autant, nous recommandons un **TTL plus court** pour nos clients souhaitant utiliser notre service de **failover**, auquel cas un TTL de **3 minutes** couplé à l'activation du protocole **DNSSEC** pour éviter les attaques par empoisonnement du cache.

Notre interface de gestion technique des DNS permet de changer le TTL standard, qui est de 12 heures sur l'offre standard, au profit d'une valeur au choix de 5 minutes à plusieurs jours afin de permettre des transferts ou des migrations. Les TTL repassent automatiquement à 12 heures au bout de 24 heures pour assurer la persistance des données en cas d'incident.

Recommandation n° 12 : Effectuer des sauvegardes du contenu des zones

Mettre en place une procédure de sauvegardes régulières des données contenues dans les zones DNS

Solution mise en œuvre par Nameshield

Nameshield est certifiée **ISO 27001** sur l'ensemble du **périmètre** de son activité de **registrar**, ce qui englobe le service **DNS Premium**, et implique un ensemble de **mesures** de **protection** et de **sauvegarde** du **Système** d'Information.

Nous disposons d'une **politique de sauvegarde avancée** pour l'ensemble des zones présentes sur notre infrastructure DNS Premium avec notamment la possibilité d'effectuer des **rollbacks** vers différentes versions de zone directement depuis notre interface de gestion DNS Premium.

Nameshield préconise l'utilisation d'une **IHM sécurisée** avec des **saisies contrôlées** sur le plan syntaxique et fonctionnel. Elle propose notamment la **journalisation de la saisie des modifications** dans les fichiers de zones à partir des enregistrements successifs des saisies en base de données vieux de moins d'un an.

Recommandation n° 13 : Surveiller la santé des serveurs faisant autorité

Mettre en place un système automatisé de surveillance des données fournies par ses serveurs faisant autorité et par ceux des zones parentes

Solution mise en œuvre par Nameshield

Nameshield a mis en place de nombreux **systèmes automatisés de surveillance des données** fournies par ses serveurs faisant autorité et par ceux des zones parentes. **L'ensemble** des **zones critiques** (entendu des zones dont le nombre mensuel de requêtes excède 500 000) est **monitoré**.

Monitoring actuellement en place :
- Surveillance du fonctionnement des logiciels effectuée toutes les 3mn
- Surveillance de l'état général des programmes sur une machine
- Equipe d'astreinte, à laquelle sont remontées les erreurs faisant état d'une coupure ou dégradation de service
- Monitoring externe effectué par un prestataire fournissant des sondes présentes sur 25 points géographiques, dans des réseaux différents
- Mise en place de tableaux de bord avec l'ensemble des métriques systèmes et du monitoring externe ;
- Contrôle de l'intégrité des zones
- Monitoring Failover (optionnel selon le choix de nos clients) automatisé ;
- Monitoring des zones DNSSEC.

Recommandation n° 14 + : Utiliser des piles logicielles variées

Employer au minimum deux logiciels de serveurs DNS différents sur l'ensemble des serveurs faisant autorité sur un nom de domaine.

Solution mise en œuvre par Nameshield

Nameshield n'a pas fait le choix d'une utilisation de multiples briques logicielles et a **construit** son **service** sur un **logiciel** totalement **compatible** avec l'ensemble des RFC **DNS**.
Nameshield suit une **politique de mise à jour dédiée** (veille particulière, procédure d'upgrade, non régression) afin de se **prémunir** d'éventuelles failles de sécurité.

Recommandation n° 15 : Utiliser des composants distincts pour l'interrogation et le service de zones

Le service d'interrogation DNS devrait être rendu par un serveur ou un processus cloisonné distinct de celui rendant le service DNS faisant autorité sur des noms de domaine.

Solution mise en œuvre par Nameshield

Le **service DNS** de Nameshield est **uniquement autoritaire**. Nous ne faisons jamais de récursivité.
Nameshield opère un réseau de DNS autoritaires (SOA et secondaires) qui ne gère pas de données internes, et dont la résolution de nom récursive est désactivée. Ce sont d'autres machines qui servent de forwarder (cache) pour un usage en local.

Recommandation n° 16 : Eviter l'emploi des vues dans l'objectif de cloisonner l'information

Répartir les données internes d'une part, et les données externes d'autre part sur des machines ou des processus distincts et cloisonnés.

Recommandation n° 17 : Utiliser le mécanisme RRL lorsqu'il est disponible

Employer le mécanisme anti-déni de service distribué RRL sur les implantations le proposant.

Solution mise en œuvre par Nameshield

Nameshield utilise bien la fonctionnalité **Response Rate Limiting** sur son infrastructure DNS Premium.

En matière de protection contre les attaques de type DDoS, Nameshield s'appuie sur différentes mesures :

- Notre cœur de réseau est bâti en cluster de performance et notre réseau anycast basé sur de multiples points de présence dans le monde
- Par ailleurs notre solution s'appuie sur la solution Arbor pour la mitigation d'attaques DNS
- A laquelle s'ajoutent nos règles heuristiques de filtrage du trafic

Recommandation n° 18 : ne jamais sciemment décider de ne pas répondre à une requête DNS

Si RRL est mis en œuvre, utiliser une valeur de « slipping » de 1, afin de toujours répondre aux requêtes DNS.

Solution mise en œuvre par Nameshield

Nameshield n'envoie **pas de réponses DNS tronquées**.

Recommandation n° 19 : Préférer l'emploi de délégations avec colle

Privilégier les délégations avec colle lorsque l'usage de délégation sans colle introduit de nouvelles dépendances tierces.

Solution mise en œuvre par Nameshield

Nameshield privilégie les **délégations avec colle** lorsque l'usage de délégation sans colle introduit de nouvelles dépendances tierces. Ceci s'applique à l'ensemble des DNS du service DNS Premium.

Nameshield permet de gérer les **glue records*** dans les zones directement depuis son interface, permettant ainsi de ne pas dépendre d'un tiers. Nameshield permet également de gérer la délégation de zone à partir de ses interfaces de configuration, en respectant des droits d'accès qui vous permettent d'organiser la délégation en fonction de vos filiales ou de vos besoins géographiques.

Recommandation n° 20 : Renforcer la configuration de la plateforme d'hébergement

Durcir le système d'exploitation hébergeant les logiciels DNS.

Solution mise en œuvre par Nameshield

Nameshield **durcit** ses **systèmes conformément** à ses **politiques** et procédures crées dans le cadre de la certification **ISO 27001** ; de plus nous utilisons des **machines dédiées à l'usage exclusif du DNS**.