

OFFRE DE SERVICES

SÉCURITÉ DES NOMS DE DOMAINE BASÉE SUR LES PROTOCOLES DMARC, SPF, DKIM ET BIMI



ADAMA BERTE
Consultant Expert Cybersécurité

CEO BerTechs

 <https://app.bertechs.net>

 info@bertechs.net

QUI SOMMES-NOUS ? QUELLES SONT NOS VALEURS ?

BerTechs est une entreprise Malienne spécialisée dans la cybersécurité des réseaux et systèmes d'information. Notre mission principale est d'assurer la protection des entreprises et des services publics contre les cyberattaques de plus en plus répandues et sophistiquées. La menace cyber est globale et nulle n'est épargné. **BerTechs** vous aide alors à les anticiper en renforçant votre cyber-protection.

NOTRE MISSION : VOTRE CYBER-PROTECTION

NOS VALEURS

-  Professionnalisme
-  Expertise technique
-  Ecoute du client
-  Qualité de service fourni

Nous travaillons dur pour offrir des services de qualité et garantir la satisfaction de nos clients. Nous sommes fiers de la réputation que nous avons acquise dans le domaine de la cybersécurité des noms de domaine et nous continuerons à nous améliorer pour répondre aux besoins de nos clients.

Cherchez-vous un partenaire de confiance pour protéger vos noms de domaine? Alors ne cherchez plus, **BerTechs** vous offre des services de cybersécurité de qualité.

Contactez-nous dès maintenant pour en savoir plus : info@bertechs.net

POURQUOI SECURISER LES NOMS DE DOMAINES ?

Saviez-vous que les cyberattaques ont augmenté de plus de 300% depuis le début de la pandémie COVID-19? Il est donc plus important que jamais de protéger votre entreprise contre les menaces en ligne.

La sécurité des noms de domaine est d'une importance cruciale car les noms de domaine constituent la première ligne de défense contre les attaques en ligne. Les noms de domaine sont utilisés pour attribuer des adresses e-mails au personnel et les diriger vers des sites web et des applications. Les cybercriminels utilisent les failles de sécurité des noms de domaine pour lancer des attaques telles que le phishing, l'usurpation d'identité, le vol de données et des attaques par déni de service.

Les entreprises, pour protéger leurs ressources digitales, leur réputation en ligne et prévenir les cyberattaques contre les noms de domaine, doivent implémenter les contrôles de sécurité basés sur les protocoles de sécurité conformes à l'état de l'art en matière de protection des noms de domaine.

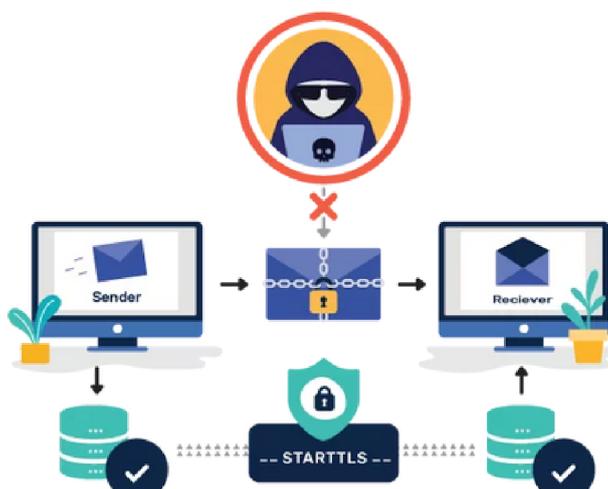
IMPORTANTANCE DE LA CYBER-PROTECTION DES NOMS DE DOMAINE :



POURQUOI SECURISER LES NOMS DE DOMAINES ?

QUELQUES RISQUES CYBER LIÉS AUX NOMS DE DOMAINE :

- **Usurpation de nom (DNS Spoofing)** : également connu sous le nom d'empoisonnement du cache DNS, c'est un type de cyberattaque dans lequel un pirate détourne le processus de traduction DNS et redirige un utilisateur vers un faux site web. L'authentification DNS peut empêcher ces attaques en vérifiant l'authenticité des réponses DNS et en s'assurant qu'elles proviennent d'une source fiable
- **Typosquatting** : Des cybercriminels peuvent acheter des noms de domaine similaires à ceux de entreprises mais contenant des fautes de frappe souvent indétectable à l'oeil. Cela peut être utilisé pour tromper les utilisateurs et les amener à divulguer des informations personnelles ou à effectuer des paiements.
- **Hameçonnage** : Des cybercriminels peuvent utiliser des noms de domaine similaires à ceux d'une marque ou d'une entreprise pour mener des attaques de phishing en envoyant des e-mails ou des messages texte trompeurs pour inciter les utilisateurs à divulguer des informations personnelles ou à effectuer des paiements.
- **Attaques par déni de service (DDoS)** : Les noms de domaine peuvent être la cible d'attaques par déni de service (DDoS) qui visent à rendre un site web ou un service en ligne inaccessible en surchargeant le serveur d'hébergement avec un grand nombre de requêtes simultanées. Cela peut entraîner des temps d'arrêt coûteux pour les entreprises.



 <https://app.bertechs.net>

 info@bertechs.net

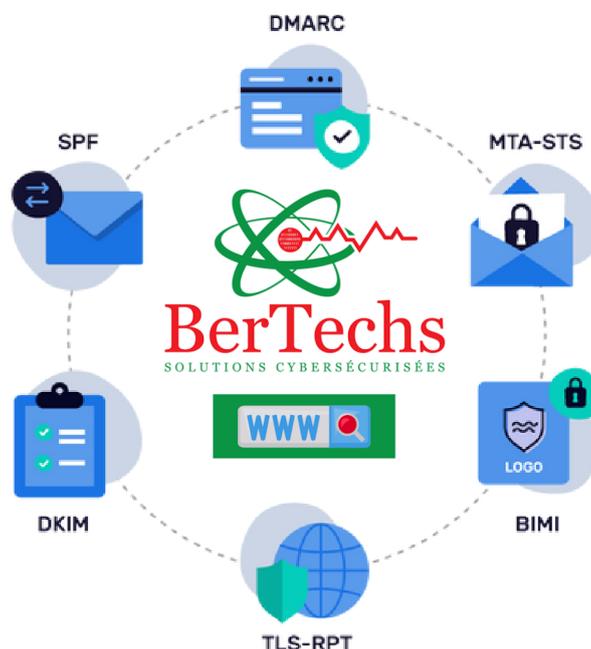
OFFRE DE SERVICES DE SÉCURITÉ DES DOMAINES

Nos offres de service vous aideront à renforcer la sécurité de vos noms de domaines en minimisant les risques liés aux cyberattaques telles que le phishing, les usurpations d'identité, la compromission des e-mails professionnels et d'autres menaces potentielles à travers les protocoles de sécurité conformes à l'état de l'art actuel

Nous disposons d'une [plateforme web http://app.bertechs.net](http://app.bertechs.net) développée pour garantir la cyber-protection de vos noms de domaine. Elle regroupe un ensemble d'outils de cybersécurité des noms de domaine basés sur les protocoles de sécurité conforme à l'état de l'art.

NOS SERVICES DE SÉCURITÉ DES NOMS DE DOMAINE INCLUENT :

- L'audit de sécurité des noms de domaine
- La configuration et l'implémentation des protocoles DMARC, SPF, DKIM, BIMI et MTA STS,
- La surveillance continue du domaine et la maintenance
- La rédaction des rapports de violation de sécurité
- La formation des employés sur les bonnes pratiques de sécurité



 <https://app.bertechs.net>

 info@bertechs.net

OFFRE DE SERVICES DE SÉCURITÉ DES DOMAINES

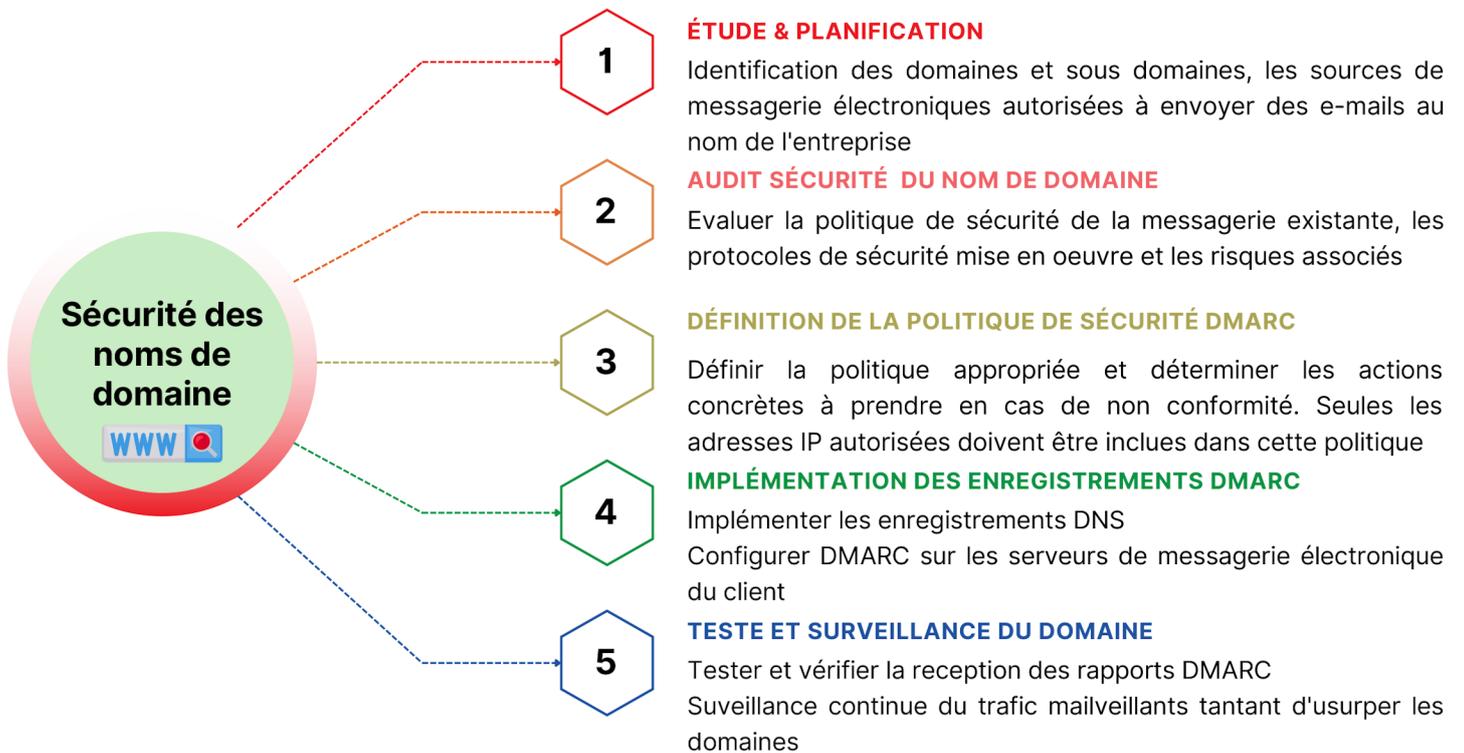
VOICI COMMENT CHACUN DE CES PROTOCOLES AIDE À GARANTIR LA SÉCURITÉ DES NOM DE DOMAINE :

- **DMARC** : Domain-based Message Authentication, Reporting & Conformance, permet aux propriétaires de domaines d'indiquer aux fournisseurs de services de messagerie comment gérer les e-mails qui ne sont pas authentiques. DMARC permet de spécifier comment les **e-mails non authentiques doivent être traités**, tels que le marquage comme spam ou le rejet pur et simple.
- **SPF** : Sender Policy Framework, permet aux propriétaires de domaines d'indiquer quels sont les serveurs de messagerie autorisés à envoyer des e-mails en leur nom. SPF utilise une liste de serveurs de messagerie autorisés pour **déterminer si un e-mail est authentique ou non**.
- **DKIM** : DomainKeys Identified Mail, permet de **signer les e-mails sortants** en utilisant une clé de cryptage spécifique au domaine. Cette signature est vérifiée par les fournisseurs de services de messagerie pour s'assurer que **l'e-mail provient bien du domaine indiqué**.
- **BIMI** : Brand Indicators for Message Identification, permet aux propriétaires de domaines d'afficher leur **logo dans les boîtes de réception des destinataires** qui utilisent des fournisseurs de services de messagerie qui prennent en charge BIMI. Cela renforce la **reconnaissance de la marque** et offre une preuve supplémentaire que l'e-mail est authentique.
- **MTA STS** : Mail Transfer Agent Strict Transport Security, est un protocole qui permet de sécuriser la transmission des e-mails entre les serveurs de messagerie. MTA STS utilise HTTPS pour garantir que la communication entre les serveurs de messagerie est **cryptée et sécurisée**.



PHASES D'IMPLEMENTATION

L'implémentation de la cyber-protection des noms de domaine nécessite une planification et une excellente communication avec le client



L'implémentation de DMARC nécessite des investigations approfondies côté clients pour s'assurer que tous les domaines qui envoient des emails au nom de l'entreprise sont pris en compte et que leurs configurations sont sécurisées. Les clients doivent collaborer avec les parties prenantes de leur entreprise pour identifier ces domaines et analyser les rapports SPF et DKIM afin de s'assurer que les protocoles sont configurés correctement. Les clients doivent également vérifier les adresses IP autorisées, les enregistrements DNS et la réception des rapports pour s'assurer du bon fonctionnement des configurations DMARC implémentées