RECOMMANDATIONS DE SÉCURITÉ POUR PROTÉGER VOS NOMS DE DOMAINES ET VOS MARQUES CONTRE LES ABUS ET LES FRAUDES EN LIGNE

Adopter une approche Défense en profondeur (DiD) pour la gestion et la sécurité des noms de domaine

- ☐ Éliminez vos risques externes en évaluant la sécurité, la technologie et les processus de votre registrar de noms de domaine et de votre fournisseur de gestion DNS (système de noms de domaine).
- ☐ Sécurisez vos noms de domaine critiques, votre infrastructure DNS et vos certificats numériques en :
  - ☐ Mettant en place une authentification à deux facteurs.
  - ☐ Réglementant les permissions (normales et élevées) et en surveillant tout changement, ainsi qu'en ajoutant une politique de gestion des contacts autorisés.
  - ☐ Surveillant l'activité DNS et en déployant une protection DDoS (déni de service distribué).
  - ☐ Adoptant des mesures de sécurité, telles que le verrouillage du registre de noms de domaine, les extensions de sécurité DNS (DNSSEC), la norme d'authentification Domain-based Message Authentication Reporting and Conformance (DMARC), les enregistrements certificate authority authorization (CAA) et la redondance de l'hébergement DNS.

Surveiller en permanence l'espace de nom de domaine et les principaux canaux numériques

tels que les places de marché, les applications, les réseaux sociaux et les e-mails afin de repérer les détournements de marque, les infractions, les attaques de phishing et la fraude

- ☐ Identifiez les tactiques de spoofing de noms de domaine et de DNS, telles que les homoglyphes (correspondances floues et noms de domaine internationalisés), les noms de domaines similaires, les correspondances par mots-clés et les homophones.
- ☐ Enregistrez les noms de domaine qui pourraient constituer des cibles de grande valeur liées à vos marques (c'est-à-dire les homoglyphes ou les noms de domaine nationaux) afin d'atténuer le risque que des hackers les utilisent.
- ☐ Identifiez les infractions sur les marques commerciales et les atteintes aux droits d'auteur sur les contenus web, les places de marché en ligne, les réseaux sociaux et les applications.

Demandez une consultation gratuite et l'un de nos experts vous contactera.

cscdbs.com/fr

RECOMMANDATIONS DE SÉCURITÉ POUR PROTÉGER VOS NOMS DE DOMAINES ET VOS MARQUES CONTRE LES ABUS ET LES FRAUDES EN LIGNE

Mener des interventions au niveau mondial, y compris en appliquant des techniques avancées de désactivation et de blocage de contenu Internet

- ☐ Généralisez la surveillance du phishing et utilisez un réseau de navigateurs, de partenaires, de fournisseurs de services Internet (FAI) et de systèmes de gestion des informations et des événements de sécurité (SIEM) protégé contre la fraude.
- ☐ Utilisez une série d'approches techniques et juridiques pour protéger vos droits, en choisissant l'approche la plus appropriée au cas par cas.
- ☐ Combinez diverses mesures d'intervention pour lutter contre les atteintes à la propriété intellectuelle et la fraude :

  Les mesures d'intervention de premier niveau le déréférencement de la place de marché, la suspension des pages de réseaux sociaux, le retrait des applications mobiles, les lettres de mise en demeure, la suppression du contenu frauduleux et la limitation complète du vecteur d'attaque.

  Les mesures d'intervention de second niveau la suspension du nom de domaine au niveau du registrar, la suspension du nom de domaine non valide dans la base de données WHOIS et les alertes avec notification de fraude.

  Les mesures d'intervention de troisième niveau le lancement de procédures UDRP/URS, les acquisitions de noms de domaine, les enquêtes approfondies et les achats-tests.

Vérifier que les pratiques commerciales de votre registrar ne contribuent pas à la fraude ni aux infractions sur les marques

Les problèmes suivants apparaissent souvent chez les registrars grand public :

- ☐ L'exploitation de plateformes de vente de noms de domaine, qui capturent, mettent aux enchères et vendent au plus offrant des noms de domaines contenant des noms de marques commerciales.
- ☐ Le spinning de noms de domaine et la promotion de l'enregistrement de noms de domaine contenant des noms de marques commerciales.
- ☐ La monétisation, à l'aide de sites sponsorisés, de noms de domaine contenant des noms de marques commerciales.
- ☐ Des failles de sécurité fréquentes facilitant les attaques DNS, de phishing et Business Email Compromise.

Demandez une consultation gratuite et l'un de nos experts vous contactera.

cscdbs.com/fr