actifs numériques CHECKLIST DE SÉCURITÉ

ACTIFS NUMÉRIQUES
gestion des fournisseurs

- ☐ Vous tenez une comptabilité complète de tous vos fournisseurs de noms de domaine, systèmes de noms de domaine (DNS) et certificats SSL.
- ☐ Tous vos fournisseurs d'avoirs en ligne fournissent une assistance de qualité professionnelle, 7j/7, 24h/24, 365j/an.
- ☐ Tous vos fournisseurs d'actifs numériques ont investi solidement dans la protection de leurs systèmes (en ayant par exemple des centres de données certifiés ISO 27001, conformes à la norme SOC 2®) contre la pénétration par des tiers, en faisant des tests de vulnérabilité et de sécurité contre les injections SQL, les failles XSS, etc.
- ☐ Tous vos fournisseurs d'actifs numériques ont investi intensément dans la formation de leur personnel, par exemple dans leur formation à la sécurité, la sensibilisation au phishing (avec des envois réguliers d'e-mails-tests de phishing), l'authentification à deux facteurs pour les accès extérieurs au réseau, etc.
- ☐ Tous vos fournisseurs d'actifs numériques ont investi puissamment dans la protection de leurs clients, par exemple dans la validation des IP, l'authentification à deux facteurs, une procédure concernant les contacts autorisés, le tout-écrit-et-jamais-par-téléphone pour les commandes et les requêtes, l'identité fédérée, etc.
- ☐ Aucun de vos fournisseurs n'a pour antécédents d'avoir été victime de phishing, d'ingénierie sociale, de détournement de DNS ni d'attaques DDoS.
- ☐ Tous vos fournisseurs de biens numériques utilisent leurs propres accréditations de premier rang, sans intermédiaires. Ce qui veut dire que votre fournisseur de noms de domaine est accrédité directement auprès des registres et que votre fournisseur de certificats SSL est une autorité de certification accréditée à part entière.

NOMS DE DOMAINE
gestion

- ☐ Vous tenez un inventaire exhaustif de tout votre portefeuille de noms de domaine.
- ☐ Vous avez mis en place une procédure d'auto-renouvellement avec vos fournisseurs, alimentée par un crédit sur votre compte.
- ☐ Tous les membres de votre personnel ont reçu la formation et adhèrent au processus centralisé d'enregistrement de nouveaux noms de domaine.
- ☐ Concernant le WHOIS, vous avez établi des instructions claires sur la trame et les champs définis par l'utilisateur qui doivent être fournis au point d'enregistrement.
- ☐ Vous suivez une procédure pour identifier les enregistrements de l'entreprise qui se font en dehors de votre gestion centralisée.

DNS
gestion

- ☐ Vous tenez un répertoire complet de la totalité de votre portefeuille de fournisseurs DNS.
- ☐ Vous suivez un protocole pour identifier les noms de domaine dont les DNS ne sont pas de niveau professionnel, avec une garantie de 100% de disponibilité.
- ☐ Tous les membres du personnel ont reçu la formation et adhèrent à l'obligation de coupler tous les nouveaux noms de domaine vitaux avec des DNS de niveau professionnel.

CERTIFICATS SSL
gestion

- ☐ Vous maîtrisez parfaitement la liste de vos fournisseurs de certificats SSL.
- ☐ Tous les membres du personnel ont reçu la formation et adhèrent au processus centralisé d'achat des nouveaux certificats et de remplacement des anciens.
- ☐ Vous suivez un protocole pour identifier tous les certificats SSL acquis en dehors de vos procédures centralisées.

NOMS DE DOMAINE "VITAUX" (Stratégiques)
gestion

- ☐ Vous avez la capacité d'identifier immédiatement tous vos noms de domaine "vitaux" et de démontrer qu'ils sont sécurisés.
- ☐ Tous les fournisseurs de DNS pour vos noms de domaine "vitaux" présentent une garantie vérifiable de disponibilité à 100%, et des antécédents concordants.
- ☐ Tous vos noms de domaine "vitaux" utilisent des certificats SSL appropriés et de niveau professionnel.
- ☐ Tous vos noms de domaine "vitaux" utilisent le protocole DNSSEC (domain name system security extensions) pour les protéger contre "l'empoisonnement" du cache DNS.
- ☐ Tous vos noms de domaine "vitaux" utilisent le protocole "Multilock" pour les protéger contre le détournement de DNS.
- ☐ Tous vos noms de domaine "vitaux" utilisent les services d'authentification d'e-mail.

RÉDUCTION DES MENACES
permanente

- ☐ Vous utilisez des services supplémentaires pour réduire la menace d'attaque DDoS, afin de protéger d'autres serveurs au-delà du DNS.
- ☐ Vous utilisez des services d'authentification par e-mail, combinés avec la surveillance du phishing, et des services de neutralisation pour réduire la menace venant des attaques de phishing.

+33 (0)1 40 41 65 30 cscdigitalbrand.services/fr