Sécurité des actifs numériques : *Revenons aux fondamentaux*

Sécurité des actifs numériques : *Revenons aux fondamentaux*

La multiplication des cyberattaques et des violations des données dans le monde entier impliquent des incidents de plus en plus intenses et fréquents, avec pour conséquence une sécurisation de l'environnement qui devient beaucoup plus complexe. Si les entreprises continuent d'investir dans la technologie, celle qui sert à sécuriser les organisations est mise à l'épreuve quotidiennement.

Nombre des méthodes, outils et techniques de sécurité aujourd'hui utilisés par les entreprises pour sécuriser leur environnement et protéger leur marque se sont montrés efficaces à ce jour, mais les attaques viennent désormais de toute part. Hackers, hacktivistes, cybercriminels, gouvernements étrangers et personnel interne (comme les employés) attaquent continuellement les protocoles de sécurité pour trouver la faille où s'engouffrer.

Sachant que les flux de données utilisent divers points d'entrée, les organisations qui font encore la différence entre la sécurité interne et celle du périmètre devraient de toute urgence reconsidérer leur approche de la sécurité – notamment au niveau des actifs numériques (noms de domaine, système DNS et certificats numériques) – afin de garantir la bonne continuité de leur activité commerciale jour après jour.

Comment passer d'une approche traditionnelle de la cybersécurité à une approche qui permet de limiter les risques actuels ?

Connaître et identifier vos actifs numériques pour mieux les gérer.

Comprendre les implications potentielles d'un incident de sécurité sur votre activité et planifier en conséquence.

Optimiser votre ROI. Vous devez distinguer vos actifs de valeur (vos domaines critiques notamment) des autres.

Protéger les nombreux canaux numériques.

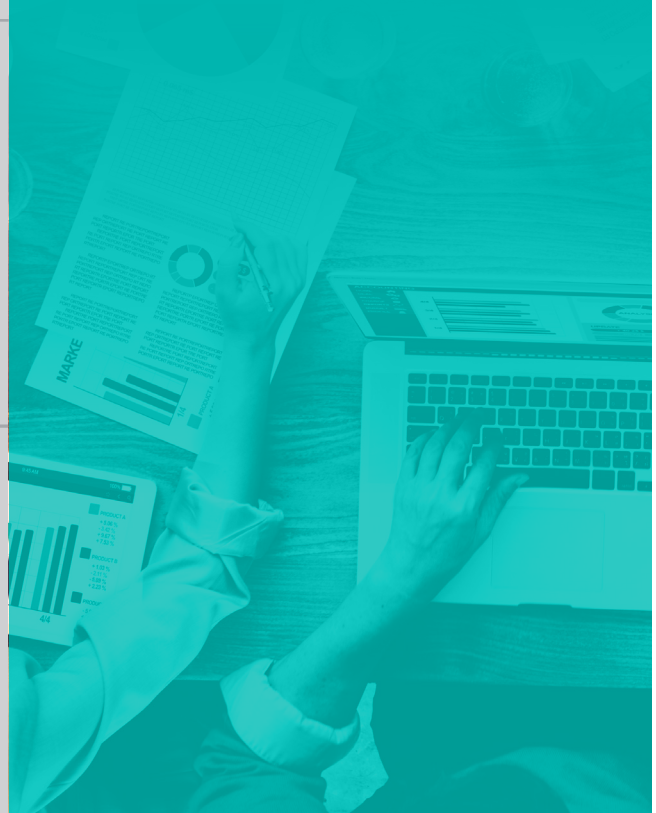
1

2

3

4

Connaître et identifier vos actifs numériques pour mieux les gérer.



Ces 20 dernières années, votre entreprise a accumulé un grand nombre d'actifs immatériels. Ces actifs représentent votre entreprise, lui permettent d'effectuer des transactions, et assurent une communication et des interactions fluides avec vos clients, vos fournisseurs et vos collègues. En résumé, ils ont changé votre façon de communiquer, de fonctionner et de consommer.

Aujourd'hui, le monde est plus que jamais connecté : c'est une fantastique opportunité pour les entreprises du monde entier, mais aussi un défi de taille. Le développement de l'économie numérique mondiale accompagne celui des actifs immatériels, comme les noms de domaine, les certificats numériques, les noms d'utilisateurs de réseaux sociaux et les applications mobiles. Il est donc impératif pour les entreprises de savoir quels actifs numériques elles possèdent et utilisent. Sans cela, elles risquent d'être vulnérables aux infractions au droit des marques et aux cyberattaques.

Il est probable que les informations complètes sur les actifs détenus et ceux qui sont réellement utilisés soient dispersées dans plusieurs services, par exemple le service marketing, juridique, informatique, voire les ressources humaines. Il faut donc d'abord dresser une liste de tous vos actifs numériques, puis demander à vos fournisseurs et registrars (bureaux d'enregistrement) de lancer un audit. Chaque entreprise doit avoir une perspective globale, c'est-à-dire que même si vous êtes basé aux États-Unis, vous devez rechercher les actifs numériques au niveau international, dans tous les pays où votre entreprise est présente.

Voici une liste de contrôle. Déterminez :

- ○ **Les noms de domaine que vous possédez, y compris ceux qui sont enregistrés dans un but promotionnel (comme les Vanity URL) et pour des motifs défensifs.**
- ○ **Qui vous fournit les services DNS pour chaque nom de domaine, que ce soit votre registrar, un prestataire de services DNS spécialisé, ou que vous disposiez de votre propre infrastructure DNS.**
- ○ **Le nombre de certificats numériques que vous possédez, y compris le type de validation pour chacun, et la manière dont ils sont gérés.**
- ○ **Le nombre de pseudos (noms d'utilisateur) de réseaux sociaux dont vous disposez sur toutes les plateformes.**
- ○ **Qui a accès aux noms d'utilisateurs et mots de passe de réseaux sociaux, et comment les pseudos sont gérés.**
- ○ **Si vous avez créé et publié des applis mobiles, et si tel est le cas, comment celles-ci sont gérées.**

Au moment de recueillir ces informations, il est essentiel de savoir également quel utilisateur a accès à quelle ressource.

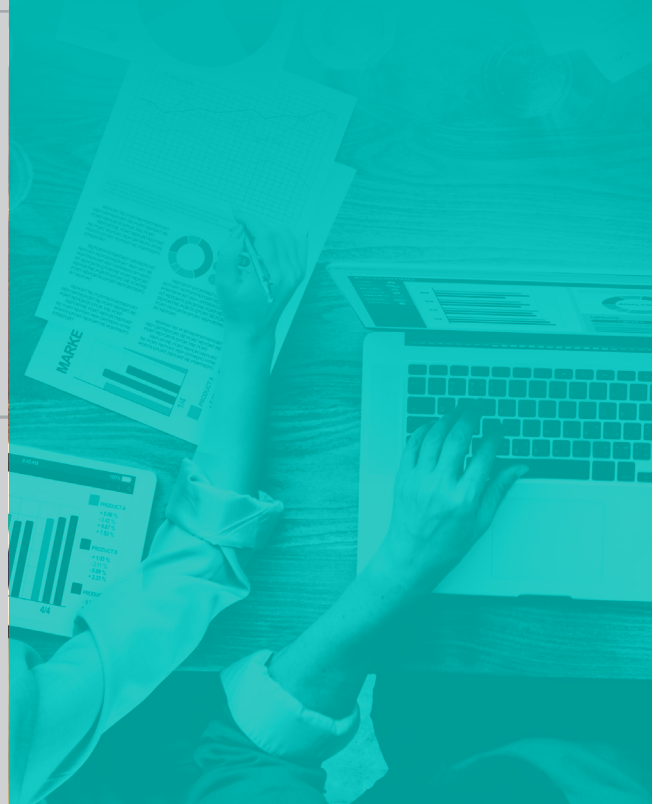
1

2

3

4

Connaître et identifier vos actifs numériques pour mieux les gérer.



Consolidez vos actifs en ligne avec des prestataires de niveau professionnel

En comprenant les besoins globaux de votre entreprise relatifs aux noms de domaine, aux services DNS et aux certificats numériques, vous vous assurez que chacun de vos prestataires répond à vos critères d'exigence. Pour chaque spécialité, il existe de multiples prestataires : du modèle à bas coût « self-service » au modèle avec services limités, en passant par les prestations avec paiement par carte, aux prestataires spécialistes de l'entreprise qui proposent un service haut de gamme, accompagné des accords de niveau de service (SLA), des clauses de responsabilité et des modèles tarifaires dont vous avez besoin en tant qu'entreprise internationale. Un autre élément dont vous devez tenir compte est l'approche de la sécurité que propose votre partenaire.

En plus d'analyser avec soin la qualité des prestations de vos fournisseurs, une des meilleures pratiques consiste à consolider vos actifs numériques afin de garantir leur bonne gestion et la continuité de vos activités. Disposer d'une seule équipe dédiée à la gestion de tous vos actifs numériques, idéalement depuis une plateforme unique, vous offrira davantage de flexibilité pour contrôler leur évolution, qu'il s'agisse de l'enregistrement ou de l'expiration de noms de domaine, de la modification d'identifiants de réseaux sociaux, ou du renouvellement de certificats numériques. Et surtout, vous aurez une vision claire de vos vulnérabilités.

Demandez à vos prestataires existants – ou potentiels – de réaliser un audit de vos actifs immatériels. Si ce n'est pas déjà le cas, choisissez un prestataire de niveau professionnel. Il sera plus à même de vous proposer ce qu'il y a de mieux en gestion des certificats numériques, des noms de domaine et des services DNS. Il devrait également être capable de surveiller tous les noms de domaine qu'il gère pour appliquer l'ensemble de vos politiques de DNS et de certificats numériques. Vous aurez notamment besoin de réponses claires aux questions suivantes : quels noms de domaine ne sont pas actifs en ligne ou ne résolvent pas correctement ? Quels noms de domaine critiques n'utilisent pas le protocole DNSSEC ? Le protocole AOSSL est-il toujours activé sur vos domaines stratégiques ?

Ce type d'audit devrait au moins s'inscrire dans une maintenance régulière afin d'administrer vos systèmes conformément à votre politique et d'identifier les domaines enregistrés en dehors de celle-ci. Avec le meilleur prestataire, l'analyse sera aussi proche du temps réel que possible, avec des notifications pour vous alerter de problèmes potentiels ou de cas de non-conformité. Cela signifie qu'une fois votre politique définie, vous avez également besoin de former votre personnel à la respecter.

En savoir plus au point 4.

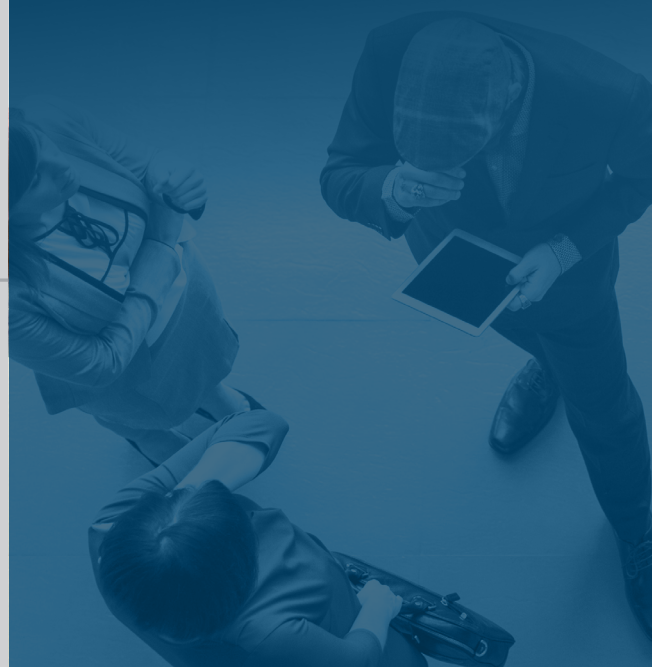
1

2

3

4

Comprendre les implications potentielles d'un incident de sécurité sur votre activité et planifier en conséquence.



Ce dispositif de prévention vous permet d'analyser en détail tout incident potentiel, et d'assurer la continuité de votre activité. C'est donc une question essentielle qui doit être traitée au plus haut niveau de l'entreprise.

Le rapport Horizon Scan Report 2018 du Business Continuity Institute a identifié les 10 premiers risques pesant sur la continuité d'activité en interrogeant 657 personnes dans 76 pays. Cette information en surprendra plus d'un, mais les actifs numériques constituent l'un des facteurs actifs de ces risques :

Cyberattaques. Le DNS est vulnérable à de nombreux types de cyberattaques : empoisonnement du cache DNS, piratage DNS, domain-shadowing, logiciels malveillants, tunnelisation DNS, attaques DDoS et attaques de phishing, sans compter l'exploitation frauduleuse de certificats numériques expirés.

Atteinte des données. Les cyberattaques contre les actifs numériques sont de plus en plus utilisées pour voler des données, que ce soit en dissimulant un autre vecteur d'attaque ou en profitant directement d'une sécurité et d'une gestion déficientes des

Interruptions des réseaux IT et télécoms. Dès lors que les noms de domaine ou les services DNS d'une entreprise subissent des dysfonctionnements, tous les moyens de communication via Internet peuvent être interrompus. Dans ce cas-là, comment une entreprise peut-elle communiquer avec ses clients et ses collaborateurs ?

Perturbation de la chaîne logistique. Puisqu'un dysfonctionnement des noms de domaine et des services DNS implique une rupture des communications, comment une entreprise pourrait-elle continuer ses opérations et maintenir sa chaîne logistique ?

Il est clair que les implications sont énormes, et qu'appliquer des mesures de sécurité de base sur vos actifs en ligne est crucial. Dans le monde entier, les cyberattaques augmentent en intensité. Peu importe que vous soyez visé par des hacktivistes ou des cybercriminels, en cas d'attaque, les conséquences risquent d'être importantes pour votre entreprise.

Posez-vous les questions suivantes

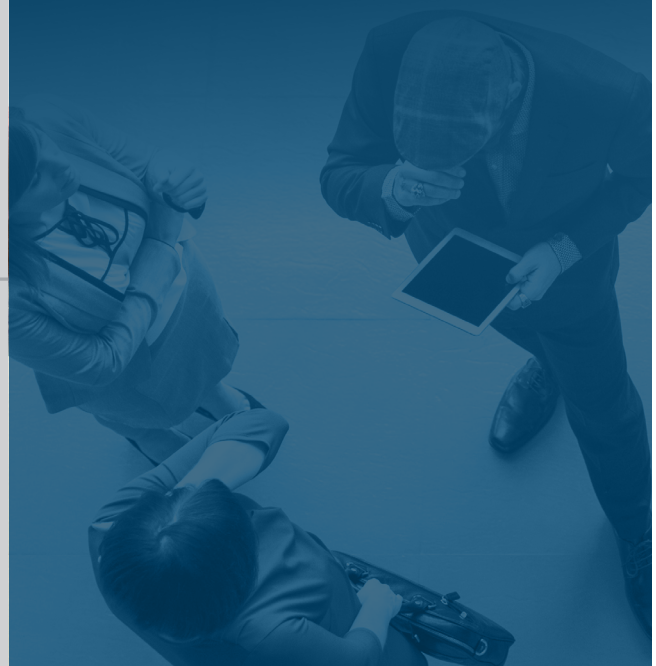
1

2

3

4

Comprendre les implications potentielles d'un incident de sécurité sur votre activité et planifier en conséquence.



Savoir quels sont vos actifs critiques

Il est absolument essentiel que vous sachiez identifier vos actifs numériques critiques. Au premier abord, cela peut sembler facile, mais en réalité, vous avez besoin de comprendre comment vos noms de domaine sont utilisés par différentes fonctions à l'échelle de votre activité globale.

Nous vous recommandons de vous associer à un partenaire qui a créé un algorithme ou utilise le machine learning afin d'identifier vos noms de domaine stratégiques

Adopter une approche « défense en profondeur »

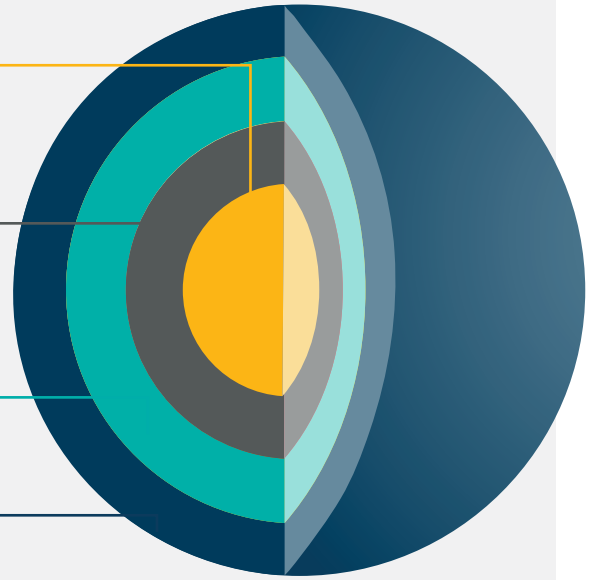
Le terme « défense en profondeur » désigne une approche sécurité multicouche, qui protégera vos actifs immatériels contre les nombreuses menaces impliquant un risque de continuité de vos activités comme mentionné plus haut.

DES FONCTIONNALITÉS DE SÉCURITÉ AVANCÉES POUR LES NOMS DE DOMAINE CRITIQUES DE L'ENTREPRISE
MultiLock, DNSSEC, HTTPS, DMARC et enregistrements CAA

CONTRÔLER LES AUTORISATIONS UTILISATEUR
Visibilité sur les autorisations élevées et les notifications

ACCÈS SÉCURISÉ AU PORTAIL
Validation IP, authentification à deux facteurs et Federated Identity

PRESTATAIRE DE SERVICES AUX ENTREPRISES
Systèmes, personnel, politiques et processus



1

2

3

4

Optimiser votre ROI. Vous devez distinguer vos actifs de valeur (vos domaines critiques notamment) des autres.

Par nature les actifs numériques – et les noms de domaine en particulier – sont peu coûteux, ce qui a engendré des portefeuilles d'actifs hypertrophiés avec un faible ROI. Il est cependant possible de démontrer la rentabilité d'un actif, ce qui est particulièrement important étant donné l'importance des budgets que les entreprises sont prêtes à consacrer aux fonctionnalités de sécurité avancées pour les domaines critiques. L'idée est simple : faites expirer et supprimez les actifs qui n'apportent aucune valeur ajoutée à votre marque pour vous aider à financer les investissements supplémentaires en sécurité requis.

Vous devez vérifier que votre IP numérique renvoie bien vers le contenu adéquat. Vous pouvez également mesurer le trafic Web – un indicateur clé du ROI. Il se peut que vous conserviez des noms de domaine attachés à des campagnes particulières qui ne sont plus actives ou ont été redirigées vers un domaine principal. Vous devriez également passer en revue les noms de domaine qui ont été enregistrés dans un but défensif.

Même s'ils n'attirent pas un haut volume de trafic, ils peuvent défendre votre marque de commerce face aux infractions. Conservez les enregistrements défensifs s'ils sont nécessaires, et, le cas échéant, séparez-vous des noms de domaine superflus pour optimiser votre portefeuille. Agir ainsi vous offre plus de latitude pour identifier les failles liées aux noms de domaine disponibles, y compris ceux qui correspondent aux marques, et enregistrer ceux qui doivent l'être.

Il faut cependant savoir qu'un nom de domaine d'entreprise abandonné inclut souvent un relevé d'activité qui peut être exploité en tant que vecteur d'attaque. Toute rationalisation ou initiative de suppression doit donc être entreprise avec précaution par un prestataire de niveau professionnel. Ceux qui disposent des outils pour identifier les domaines critiques seront les mieux à même de garantir que vous ne désinvestissez ou ne supprimez que les domaines qui sont réellement sans valeur pour vous.

1

2

3

4

Protéger les nombreux canaux numériques.

Une fois que vous contrôlez vos propres actifs immatériels, il est temps d'examiner les actifs qui appartiennent à des tiers qui exploitent votre marque ou se font – peut-être – passer pour vous.

Des services de surveillance en ligne constituent un actif important, quel que soit le secteur d'activité. Le niveau de surveillance dont vous avez besoin dépend de votre propre stratégie de marque numérique. Il est important, là encore, de consulter les services juridique et marketing de votre entreprise pour définir ensemble les éléments qui exigent ou non une surveillance étroite.

En effet, si vous vous intéressez plus particulièrement à prévenir les risques de sécurité, les services juridique et marketing souhaiteront avant tout empêcher toute infraction au droit de votre marque. Quelles que soient les motivations, votre objectif commun est le même : protéger votre entreprise !

Lorsque les activités de surveillance de votre marque numérique reflètent vos priorités, elles sont plus rentables et davantage susceptibles de repérer les menaces les plus sérieuses. Vous serez ainsi en mesure de contrer les cybercriminels avant qu'ils ne s'approchent de vos biens. Lorsqu'une solution de surveillance adéquate de votre marque est en place, vous pouvez identifier les alertes qui doivent être traitées immédiatement et ignorer éventuellement celles qui n'auront pas d'incidence. Mais sachez que le filtrage des résultats de la surveillance est un travail constant.

La surveillance vous permet également d'administrer vos politiques et vos contrôles de sécurité. Il s'agit tout d'abord de s'assurer que tous les membres de votre personnel enregistrent les noms de domaine via votre partenaire unique pour la gestion des noms de domaine. Ensuite, il est important de passer en revue les serveurs DNS et certificats numériques associés, d'identifier les noms de domaine stratégiques, et de vérifier si toutes les fonctionnalités de sécurité adaptées ont été mises en œuvre en fonction de l'importance des noms de domaine pour votre marque.

Un bon fournisseur de solutions de surveillance de marque peut vous aider à gérer cette sécurité en continu. Un excellent fournisseur filtrera les alertes et vous communiquera uniquement les infractions qui requièrent votre attention.

CSC Security Center

CSC Security Center répond à des besoins qui n'étaient pas pris en compte précédemment, à savoir la surveillance complète des noms de domaine critique d'une entreprise. Cette solution unique de sécurisation de noms de domaine, créée à partir des algorithmes avancés de CSC, a été conçue pour être la plus complète sur le marché. Elle identifie les noms de domaine critiques, les surveille pour identifier toute menace, envoie des notifications en cas de changement et simplifie la prévention des menaces. Nous vous encourageons à vous renseigner davantage sur CSC Security Center, et notamment comment il peut transformer la gestion de vos actifs numériques tout en limitant les cybermenaces.

cscdigitalbrand.services/fr