Le point de rencontre entre votre stratégie de cybersécurité et la gestion des noms de domaine

Document de réflexion CSC

Sommaire

Les cyberrisques gérés à la vitesse de l'IA

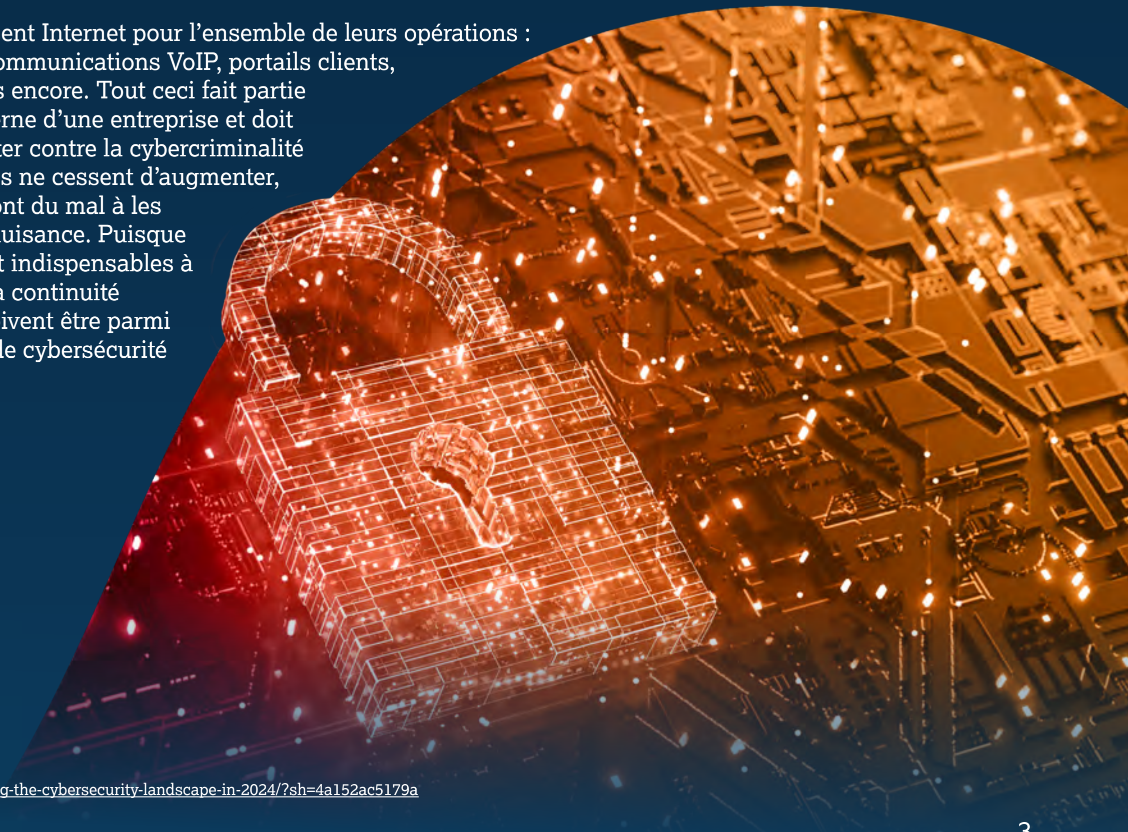
Avec le développement de l'intelligence artificielle (IA) et l'augmentation exponentielle de la complexité des cybermenaces, les entreprises et les particuliers doivent redoubler d'efforts pour se protéger contre les cyberrisques critiques. Ce qui donne aux hackers la possibilité de faire plus de mal en moins de temps est exactement ce qui favorise également de meilleures stratégies de cyberdéfense.[1] Les résultats d'une récente étude de Splunk[2] sur l'IA révèlent que 70 % des cadres supérieurs de la sécurité pensent que l'IA donne des avantages aux attaquants plus qu'aux défenseurs, bien que 35 % l'expérimentent déjà pour la cyberdéfense.

Mais le tableau n'est pas si sombre. Un récent rapport de Goldman Sachs suggère que l'IA générative pourrait augmenter le produit intérieur brut (PIB) de 7 %, un effet vraiment significatif pour une technologie unique. Toutefois, les cybercriminels utilisent également l'IA générative dans le cadre d'attaques ciblées pour sophistiquer leurs attaques et accélérer leur déploiement. L'IA générative permet aussi aux hackers de créer des e-mails de phishing personnalisés et ciblés, exempts d'erreurs d'orthographe et de grammaire, ce qui les rend plus difficiles à détecter. Les outils d'IA actuellement disponibles sur le dark web, tels que FraudGPT, permettent aux hackers de lancer des attaques d'ingénierie sociale par deepfake plus complexes, capables de manipuler les émotions ou la confiance de leurs cibles bien plus rapidement.

Les noms de domaine constituent la base à partir de laquelle les cyberattaques sont lancées

Dans un monde où les attaques de phishing, les attaques de type Business Email Compromise (BEC) et l'ingénierie sociale conduisent à des attaques toujours plus sophistiquées (par des logiciels malveillants et rançongiciels, notamment), il est surprenant que les responsables de la sécurité des systèmes d'information (RSSI) n'accordent pas plus d'attention à leurs noms de domaine et à la surface d'attaque externe qui existe en ligne. Ils consacrent beaucoup de temps à la fortification de leur réseau, mais les périmètres ont changé. De nombreux RSSI ne connaissent pas les registrars de leurs noms de domaine, et ignorent totalement s'ils fournissent le niveau de sécurité adéquat pour l'entreprise.

Les entreprises du monde entier utilisent Internet pour l'ensemble de leurs opérations : sites web, e-mails, authentification, communications VoIP, portails clients, applications fournisseurs, et bien plus encore. Tout ceci fait partie intégrante de la surface d'attaque externe d'une entreprise et doit être surveillé en permanence pour lutter contre la cybercriminalité et la fraude. Alors que les cyberrisques ne cessent d'augmenter, les entreprises et les cyberassureurs ont du mal à les quantifier et à gérer leur capacité de nuisance. Puisque l'Internet et les noms de domaine sont indispensables à l'infrastructure d'une entreprise et à la continuité des activités, les noms de domaine doivent être parmi les éléments centraux de la stratégie de cybersécurité d'une organisation.



1. forbes.com/sites/emilsayegh/2023/12/19/navigating-the-cybersecurity-landscape-in-2024/?sh=4a152ac5179a
2. splunk.com/en_us/form/ciso-report.html

« Les noms de domaine, qui permettent l'exécution de fonctions vitales de l'entreprise, se trouvent dans un écosystème devant être considéré comme faisant partie de la surface d'attaque externe de tout type d'organisation. Les activités s'effectuent dans un environnement où les noms de domaine, ainsi que les sous-domaines, peuvent être soit littéralement compromis (détournés), soit enregistrés de manière malveillante, ce qui signifie que des marques ressemblantes, qui sont en fait de faux sites web, usurpent l'identité d'une marque à des fins malveillantes, par exemple des attaques de type BEC, de phishing et de diffusion de logiciels malveillants. Beaucoup de gens sont surpris par le fait que n'importe qui peut enregistrer un nom de domaine tant que celui-ci est disponible. Par conséquent, si vous n'enregistrez pas les domaines qui utilisent votre marque, ou si vous n'utilisez pas d'homoglyphes ou d'autres stratégies pour protéger votre marque, il y aura toujours des fraudeurs en ligne qui tenteront de se faire de l'argent grâce à votre marque et à la confiance qu'elle inspire. Cela met en péril à la fois vos revenus et votre réputation, sans parler des problèmes de sécurité des consommateurs qui entrent en jeu. »

Ihab Shraim, directeur de la technologie,
Digital Brand Services de CSC dans un entretien avec Safety Detectives

Les organisations et leurs domaines peuvent être attaqués de plusieurs manières :

Domaines compromis ou sous-domaines détournés

Les cybercriminels compromettront tous les domaines non sécurisés. Les entreprises doivent commencer par adopter une approche de Défense en profondeur (DiD) multicouche pour s'en protéger. Tout d'abord, elles doivent sécuriser la présence en ligne de leur marque en sécurisant leur portefeuille de noms de domaine, qui peut contenir diverses marques obtenues via des acquisitions, et leur empreinte DNS (système de noms de domaine) en ligne.

Création de domaines malveillants et frauduleux

Si certains pays limitent les possibilités qu'un individu quelconque enregistre des extensions en exigeant une marque commerciale, un numéro siren/siret ou une présence locale, il est alarmant de constater que n'importe qui peut enregistrer n'importe quel domaine. L'objectif d'enregistrements frauduleux de noms de domaine est de profiter de la confiance des consommateurs dans la marque ciblée pour lancer des attaques de phishing convaincantes, d'autres formes de détournement de marque ou des violations de la propriété intellectuelle (PI). Cela entraîne une perte de revenus, un détournement du trafic et une dégradation de la réputation de la marque pour l'organisation en question, tout en enrichissant les fraudeurs. Il existe d'innombrables tactiques d'usurpation des noms de domaine utilisant des permutations et des homoglyphes facilement exploitables par les fraudeurs et les tiers malveillants.

Domaines de marque récemment expirés et réenregistrés par un tiers

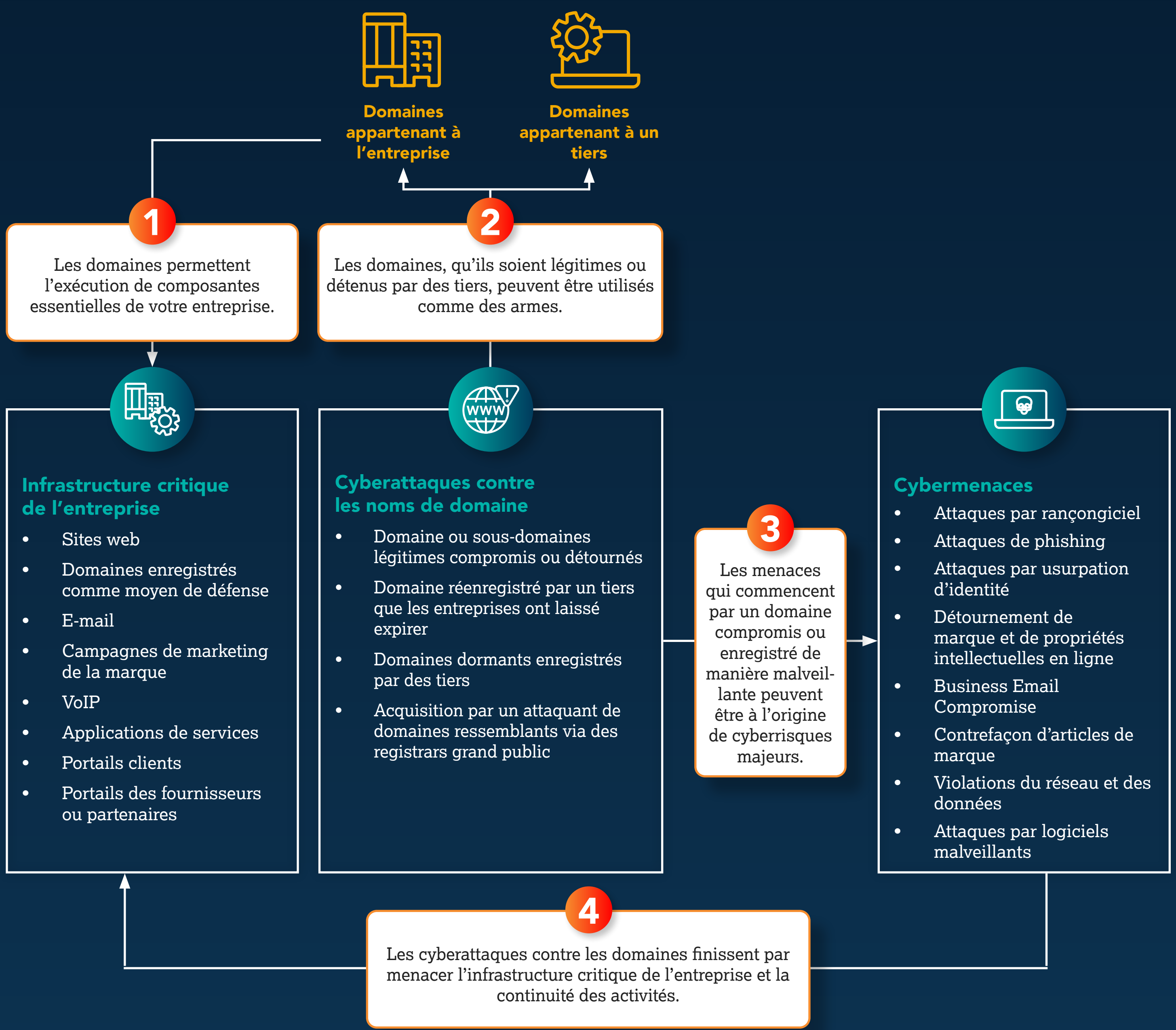
Les entreprises enregistrent leurs noms de domaine vitaux de manière défensive afin de prévenir la fraude en ligne vis-à-vis de leur marque. Toutefois, si elles sont par la suite confrontées à des pressions financières ou au ralentissement d'une marque, elles peuvent ne pas renouveler un domaine lorsqu'il arrive à expiration. Les cybercriminels profitent de cette opportunité pour réenregistrer immédiatement le même nom de domaine à des fins malveillantes. Ils sont constamment à l'affût de domaines de marque disponibles qu'ils pourraient utiliser comme une arme.

Domaines dormants

Certains cybercriminels peuvent enregistrer et conserver des domaines de marque, peut-être en hébergeant des pages d'attente ou parking, ou en affichant des messages de type « site en construction », dans l'intention de les revendre à l'organisation ciblée. Ils peuvent également préparer une activité encore plus malveillante, telle qu'une attaque de phishing ou par logiciel malveillant. Un nom de domaine dormant qui est utilisé comme arme plus de six mois après sa date d'enregistrement initiale est appelé « domaine sous-marin » (« submarine domain »). Les domaines dormants échappent souvent à toute détection initiale, car ils ne présentent pas immédiatement les caractéristiques d'un domaine enregistré pour lancer une attaque (par exemple, un enregistrement MX actif), qui déclenchent généralement un signal d'alarme. Les cybercriminels disposent ainsi d'une grande marge de manœuvre pour élaborer des campagnes d'attaque plus complexes et plus personnalisées, aux conséquences plus dévastatrices.

Outre l'ancienneté du domaine, il est également important de surveiller activement la proximité des enregistrements de nom de domaine avec les menaces précédemment identifiées et de déterminer s'il existe un schéma d'enregistrement. Les schémas d'enregistrement ne sont pas faciles à repérer en un seul endroit, mais si votre registrar de noms de domaine fournit une technologie d'IA et de machine learning sur ses données propriétaires et sur divers noms de domaine de premier niveau (TLD), des modèles peuvent être identifiés sur l'ensemble des adresses IP. Il est également essentiel de surveiller les comportements imitateurs dans l'activité de votre domaine. En d'autres termes, lorsque votre marque enregistre une série de nouveaux domaines pour un nouveau produit ou service, des tiers font-ils de même ?

Surface d’attaque externe d’un domaine



La plupart des risques liés à la cybersécurité sont bien connus des dirigeants d’entreprise. Ils savent à quel point il est important de se protéger contre les violations des données, d’assurer la gestion des identités et des vulnérabilités, les contrôles d’accès et la protection des données. Ils sont conscients du risque de vol d’identifiants et de la nécessité de rester vigilants face aux tactiques d’ingénierie sociale. Cependant, lorsqu’il s’agit de la cybersécurité quotidienne, il apparaît évident que de nombreuses équipes ignorent qui est responsable de la sécurité des noms domaine de leur organisation. Les noms de domaine sont souvent utilisés pour des initiatives marketing ou pour la protection de la marque, ce qui peut amener les équipes de sécurité à penser que la protection des noms de domaine en ligne relève du service Marketing ou Juridique. Si les organisations ne savent pas qui sont leurs registrars de noms de domaine, il y a de fortes chances qu’elles ne connaissent pas les politiques utilisées par ceux-ci ni les mesures de sécurité mises en place pour les domaines.

Malheureusement, informés du développement de la présence en ligne des entreprises, leurs adversaires s’intéressent tout particulièrement aux noms de domaine d’entreprises laissés sans protection. Si elle ne renforce pas sa stratégie de sécurité, une organisation se retrouvera dans l’œil du cyclone, naviguant sur un chemin semé d’attaques de domaine et de DNS, au risque d’une dévastation financière et d’une atteinte à sa réputation. Le *Rapport sur la sécurité des noms de domaine*, récemment publié par CSC, analyse les entreprises figurant dans la liste Forbes Global 2000 et révèle que près des trois quarts d’entre elles ont mis en œuvre moins de 50 % de toutes les mesures de sécurité des noms de domaine. Cette constatation, associée à la méconnaissance générale de leurs registrars de noms de domaine par de nombreuses organisations, suggère que la sécurité des noms de domaine a tendance à être reléguée au second plan, peut-être en partie à cause d’un manque d’appropriation interne.

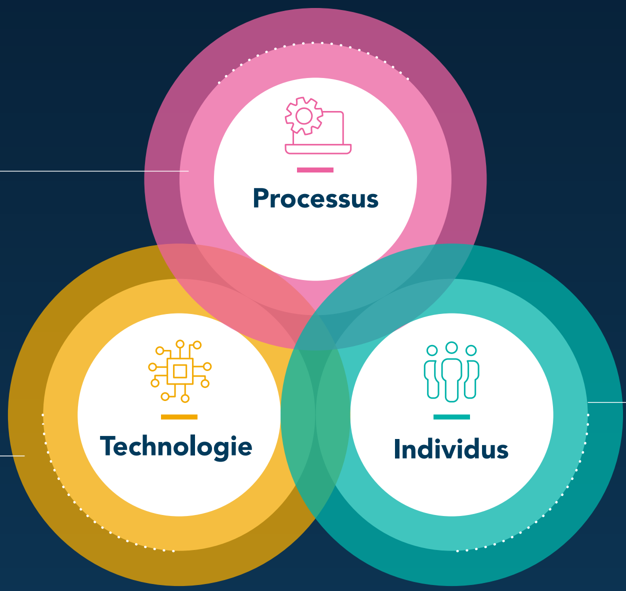
L'intérêt de faire appel à un registrar corporate

Il existe deux catégories générales de registrars de noms de domaine : grand public et corporate. Les registrars grand public représentent plus de 99 % de l'ensemble des registrars dans le monde et s'adressent aux services de domaines, aux sites web, aux messageries personnelles, aux indépendants et aux start-ups en phase de démarrage. Les registrars corporate se spécialisent dans la prestation de services aux entreprises et aux propriétaires de marques qui ont besoin de niveaux avancés de capacités métiers, d'expertise et de personnel d'assistance en matière de gestion de domaine et de DNS, ainsi qu'en termes de sécurité, de protection de la marque et de lutte contre la fraude, de gouvernance des données et de cybersécurité.

Grand public vs. corporate

Les registrars corporate sont intransigeants sur la sécurité

- Accrédités par l'ICANN et les registres
- Comptabilité complète de tous vos fournisseurs de domaines, fournisseurs de DNS et de certificats numériques
- Mandat de demande par écrit (jamais par téléphone)
- Conformité aux règlementations sur les données et au Règlement général sur la protection des données (RGPD)
- Politique de verrouillage au niveau du registre



- Vérification de l'identité des clients de type Know Your Customer (KYC)
- Contrôle de l'Office of Foreign Assets Control (OFAC)
- Assistance interne mondiale 24 h/24, 7 j/7 et 365 j/an dans les langues locales
- Formation régulière du personnel à la cybersécurité

- Centres de données accrédités ISO 27001
- Conformité SOC 2®
- Tests de pénétration et de vulnérabilité effectués par des tiers
- Tests de sécurité réguliers, incluant injection SQL et XSS

La bonne pratique consiste à faire appel à un fournisseur corporate qui a investi dans les individus, les processus et les technologies intégrés dans une optique de sécurité. Si n'importe qui peut prétendre offrir des services qui répondent aux besoins des entreprises mondiales d'aujourd'hui, il incombe aux entreprises de comprendre les différences entre les différents fournisseurs tiers. Elles doivent comprendre comment le choix d'un fournisseur s'inscrit dans les décisions prises concernant la stratégie de sécurité globale de leur organisation, ainsi que les préoccupations en matière de conformité et de risque.

Sept mesures à prendre par un registrar corporate pour sécuriser votre portefeuille de noms de domaine

Tout comme la gestion d'un portefeuille de certificats numériques, la gestion des noms de domaine peut s'avérer complexe. En appliquant ces mesures, vous prendrez le contrôle des actifs critiques de votre entreprise et réduirez les menaces de sécurité qui pèsent sur votre marque.

1 Centralisation

À l'instar de la gestion des certificats numériques avec une infrastructure à clés publiques (PKI), la gestion d'un portefeuille global de noms de domaine dans un même système de gestion permet de mettre en place des processus cohérents et de sécuriser les actifs sur lesquels compte votre entreprise.

2 Automatisation

- Une fois que tous les actifs de votre domaine sont centralisés, vous pouvez bénéficier de l'automatisation grâce à un certain nombre d'interfaces de programmation d'application (API), comme pour la gestion des certificats numériques. Les API de portefeuilles de noms de domaine doivent inclure notamment les fonctionnalités suivantes :
- Rapports sur le portefeuille de domaines
- Vérifications de la disponibilité des domaines pour de nouveaux enregistrements
- Enregistrement de domaine avec modèle de commande pour enregistrer un grand nombre d'extensions
- Mises à jour des serveurs de noms de domaine et des contacts WHOIS
- Récupération des enregistrements DNS et modification des zones
- Gestion de la redirection d'URL
- Rapports sur 10 types d'évènements liés à la sécurité sur vos domaines à des fins d'audit ou d'intégration chez les fournisseurs de services SIEM (gestion des informations et des événements de sécurité)
- Gestion de certificats numériques, y compris la commande, le renouvellement, la récupération, la réémission et la révocation des certificats ; la vérification de l'état est disponible pour toutes les commandes et les mises à jour

3 Conformité

Vous gagnez du temps en faisant appel à un fournisseur qui comprend les différentes juridictions pour chaque nom de domaine et qui veille à ce que vos données soient tenues à jour et respectent les lois du pays ou de la région.

4 Intégration

Il est très important que vos noms de domaine et DNS soient intégrés afin de pouvoir effectuer des changements rapidement et en toute sécurité.

5 Flexibilité

- Chaque entreprise est différente et peut avoir besoin d'une configuration spécifique. Vous pouvez avoir, par exemple, une utilisation très décentralisée des domaines, ou ceux-ci peuvent être segmentés en unités commerciales. Disposer d'un système susceptible d'être géré par un groupe diversifié nécessite un certain niveau d'adaptation afin que les bons utilisateurs accèdent aux bonnes informations. En outre, les entreprises doivent pouvoir explorer et comprendre les données complexes de leur portefeuille de noms de domaine. Les entreprises doivent pouvoir accéder rapidement aux données au sein d'un environnement sécurisé, fiable et riche en fonctionnalités, ce qui leur permet d'analyser de grandes quantités d'informations et de prendre des décisions éclairées. Les rapports qu'il est nécessaire d'examiner régulièrement comprennent notamment :
- Statut des sites actifs : visibilité permettant de savoir si un domaine publie du contenu.
- Total de noms par marque : informations sur la façon dont les différentes marques sont représentées au sein du portefeuille.
- Pays : compréhension de la manière dont la présence internationale d'une marque est exploitée.

6 Paysage en mutation

- Chaque année, de plus en plus de nouveaux noms de domaine sont lancés, et vous devez vous assurer que votre entreprise prend les bonnes décisions quant aux noms à enregistrer en fonction des menaces potentielles. Il est utile de disposer d'une équipe de conseillers stratégiques pour protéger votre marque. Ces derniers peuvent vous aider à répondre à des questions importantes telles que :
- Ai-je le bon nombre de domaines ou dois-je envisager d'étendre mes enregistrements défensifs pour atténuer davantage les risques ?
- Un flux de travail de bout en bout a-t-il été mis en place pour atténuer les attaques de domaine à l'aide de renseignements sur les menaces ?
- Comment savoir où enregistrer un domaine ?
- Quels sont les risques si je ne l'enregistre pas ?
- Comment communiquer au sein de mon organisation et enregistrer des domaines de manière centralisée ?

7 Surveillance

Aucune entreprise ne peut enregistrer toutes les variantes des noms de domaine. C'est pourquoi une solution efficace de surveillance des noms de domaine permet de repérer les cas où des tiers profitent du nom de votre marque.

Faites appel à un registrar corporate pour évaluer l'impact sur vos domaines et DNS de la directive européenne NIS2 sur la cybersécurité

De quoi s'agit-il ?

« D'ici au 17 octobre 2024, la Commission adoptera des actes d'exécution établissant les exigences techniques et méthodologiques applicables aux mesures concernant les fournisseurs de services DNS, les registres de noms de domaine, les fournisseurs de services informatiques cloud, les fournisseurs de services de centre de données, les fournisseurs de réseaux de diffusion de contenu, les fournisseurs de services gérés, les fournisseurs de services de sécurité gérés, les fournisseurs de places de marché en ligne, de moteurs de recherche en ligne, de plateformes de services de réseaux sociaux et de services de confiance. »[3]

Dans quel but ?

« Les règles européennes en matière de cybersécurité introduites en 2016 ont été mises à jour par la directive NIS2 entrée en vigueur en 2023. Cette directive modernise le cadre juridique existant afin de suivre l'essor de la numérisation et l'évolution du paysage des menaces de cybersécurité. En étendant le champ d'application des règles de cybersécurité à de nouveaux secteurs et entités, elle améliore encore la résilience et les capacités de réaction aux incidents des entités publiques et privées, des autorités compétentes et de l'UE dans son ensemble. »[4]

3. nis-2-directive.com/NIS_2_Directive_Article_21.html#:~:text=By%2017%20October%202024%2C%20the,service%20providers%2C%20content%20delivery%20network
4. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Les risques liés au choix d'un registrar grand public

Lorsque les entreprises cherchent à réduire leurs coûts, l'abandon d'une partie du portefeuille de noms de domaine peut être considérée comme un moyen facile d'y parvenir. Cette solution à court terme peut entraîner le risque à long-terme que les domaines soient attaqués par des hackers et que les revenus soient détournés de la marque authentique, entre autres.

De nombreuses entreprises considèrent que tous les registrars se valent.

Afin de protéger les marques en ligne, la sécurité des noms de domaine doit constituer une branche essentielle de la cybersécurité, or, elle n'est pas toujours la priorité absolue des registrars de noms de domaine grand public.[5] La confiance accordée aux registrars grand public est souvent injustifiée, car ceux-ci n'ont pas été conçus pour faire de la sécurité des noms de domaine une priorité. Cette confiance injustifiée est susceptible de nuire à la stratégie de sécurité globale d'une entreprise.

Les registrars de noms de domaine grand public ont une relation transactionnelle avec leurs clients et n'offrent pas le même degré de minutie et d'analyse que les fournisseurs corporate. Leurs solutions ne permettent pas d'atténuer les risques en ligne liés au spoofing de domaine, aux attaques par détournement de nom de domaine et de DNS, aux prises de contrôle de sous-domaine et aux attaques de phishing. Certains registrars grand public ont des pratiques commerciales qui peuvent involontairement nuire aux marques. Certains exploitent des places de marché de domaines qui capturent, vendent aux enchères et cèdent au plus offrant des noms de domaine de marques ou de marques commerciales, ou se livrent à la location de noms de domaine et préconisent l'enregistrement de noms de domaine de marque commerciale, ce qui favorise le typosquatting. Bien que ces pratiques ne compromettent pas directement les entreprises, elles encouragent le détournement de marque ou l'enregistrement de noms de domaine similaires prêtant à confusion, qui pourraient être utilisés à des fins malveillantes.

Nous avons tous entendu l'expression « une chaîne n'a que la résistance de son maillon le plus faible ». Chaque entreprise dépend de divers fournisseurs et prestataires, et avec une série complexe de fournisseurs et de processus vient un risque accru d'attaques de la chaîne logistique. Une attaque de la chaîne logistique est une cyberattaque qui se produit lorsqu'un acteur malveillant compromet le système d'une marque par l'intermédiaire d'un partenaire tiers ayant accès à vos systèmes et données. Le fournisseur dont la stratégie de cybersécurité est la plus faible est généralement ciblé.

Une attaque contre votre fournisseur vous affecte également. Les deux dernières années ont été marquées par quelques attaques notables de la chaîne logistique. Il est important de s'assurer que le registrar de noms de domaine de toute entreprise est sécurisé et ne risque pas d'être compromis. Les registrars de noms de domaine doivent être contrôlés par une équipe qui comprend parfaitement le rôle de ces acteurs dans la stratégie de sécurité globale d'une entreprise. Il est important de surveiller les antécédents d'un fournisseur en matière d'atteintes à la sécurité. Les registrars de noms de domaine axés sur la sécurité peuvent en fin de compte alléger le poids qui repose sur les équipes de sécurité et permettre aux entreprises de détecter les menaces dans leurs domaines avant même que leur marque ne subisse des dommages importants.

« Comme décrit dans son rapport 10K pour 2022, publié le 16 février, la société a été victime d'une intrusion une fois par an depuis 2020 par le même groupe de cyberattaquants, la dernière datant de décembre dernier. Il convient également de mentionner que l'entreprise avait déjà précédemment fait l'objet de cyberincursions. Les conséquences pour GoDaddy® sont une chose, mais, plus important encore, les intrusions ont conduit à la compromission de données de plus d'un million d'utilisateurs de l'entreprise. »[6]

-- Dark Reading, « What GoDaddy's Years-Long Breach Means for Millions of Clients »

5. cpomagazine.com/cyber-security/the-glaring-gap-in-your-cybersecurity-posture-domain-security/
6. darkreading.com/cyber-risk/what-godaddy-years-long-breach-means-millions-clients

L'atténuation du risque de compromission des domaines légitimes grâce à une stratégie de défense en profondeur à plusieurs niveaux

Pour atténuer le risque de cyberattaques, les principes de la défense en profondeur peuvent être appliqués à la sécurité des noms de domaine. La défense en profondeur est une approche qui a vu le jour en tant que stratégie militaire visant à protéger un bien ciblé. Pour la sécurité des noms de domaine, elle prévoit l'utilisation coordonnée de contre-mesures de sécurité à plusieurs niveaux.

Si n'importe qui peut prétendre offrir des services qui répondent aux besoins des entreprises mondiales d'aujourd'hui, chaque entreprise doit prendre le temps de comprendre les différences entre les différents fournisseurs tiers. Les entreprises doivent comprendre comment le choix d'un fournisseur s'inscrit dans les décisions prises concernant la stratégie de sécurité globale de leur organisation, ainsi que les préoccupations relatives à la violation de la propriété intellectuelle et au droit des marques commerciales.

1

Assurez-vous que le registrar de vos noms de domaine est de niveau corporate

En ce qui concerne l'écosystème des noms de domaine, le choix d'un registrar de noms de domaine peut avoir un impact sur les collaborateurs responsables de la cybersécurité et de l'informatique, du juridique (conseiller général), du risque, de la conformité (directeur général des risques), ainsi que sur les attaques de phishing, la fraude en ligne et le détournement de marque. Pour gérer le portefeuille de noms de domaine d'une entreprise, vous devez travailler avec un fournisseur qui a investi dans la protection de ses propres systèmes.

2

Travaillez exclusivement avec un registrar qui fournit un accès sécurisé à votre plateforme de gestion des noms de domaine

Le deuxième niveau d'une approche de défense en profondeur pour la sécurité des noms de domaine consiste à s'assurer que votre registrar impose un accès sécurisé au système de gestion des noms de domaines et des DNS. Les registrars doivent exiger une authentification à deux facteurs pour tous leurs clients. Ils doivent également proposer la validation IP et l'identité fédérée (SSO - « Single Sign ON ») afin que leurs clients puissent se connecter à leur réseau en sachant qu'ils disposent d'une authentification sécurisée pour leur plateforme de gestion des noms de domaine.Netzwerk anmelden können.

3

Assurez-vous que toutes les autorisations des utilisateurs sont contrôlées et gérées

Lorsque vous travaillez avec un registrar, il est essentiel qu'il offre des niveaux granulaires d'autorisations. Le registrar doit vous permettre de gérer l'accès et les autorisations des utilisateurs. Il doit fournir une visibilité sur les autorisations élevées, notamment des notifications en cas de changement. Cela est particulièrement important en cas de cyberattaque. Si un attaquant parvient à accéder à un système d'enregistrement, il créera un nouvel utilisateur ou modifiera les autorisations d'un utilisateur existant afin de pouvoir causer des dommages.

4

Utilisez des fonctions avancées de sécurité du nom de domaine

Le quatrième niveau de l'approche de défense en profondeur consiste à appliquer des fonctions avancées de sécurité au niveau de chaque domaine. Une fois que vous avez identifié les noms de domaine pertinents, il est temps d'y appliquer les contrôles appropriés. Tout d'abord, le Registry Lock, c'est-à-dire le verrouillage du nom de domaine au niveau du registre, qui désactive l'automatisation entre un registrar et un registre. Cela signifie que le DNS ne peut être modifié sans un mot de passe manuel qui doit être confirmé par un contact autorisé pour déverrouiller le nom de domaine. Il s'agit d'un moyen hautement sécurisé et efficace de s'assurer que le DNS d'un nom de domaine important ne peut être modifié sans l'autorisation appropriée. C'est par ailleurs la première recommandation de l'ANSSI (l'Agence Nationale de la Sécurité des Systèmes d'Information).

Comment des sous-domaines légitimes sont détournés sans pour autant être piratés

Il n'est pas rare que les grandes entreprises avec des portefeuilles de marque variés et opérant à l'international n'aient pas conscience de l'ampleur de leur empreinte numérique globale. Au fil du temps, les enregistrements numériques s'accumulent, compliquant les bonnes habitudes en matière de sécurité informatique. Si les entreprises ont fait appel à des fournisseurs cloud pour accéder à de nouvelles technologies, la multiplication associée des enregistrements DNS, en plus d'environnements de plus en plus complexes, les expose à des niveaux de risque plus élevés. Sans un suivi quotidien approprié des enregistrements numériques, les entreprises accumulent du « bruit » qui complique l'application d'une bonne hygiène cybernétique, ouvrant des failles faciles à exploiter pour les cybercriminels.

« Les enregistrements numériques s'accumulent au fil du temps, et les administrateurs qui ne connaissent pas l'historique de chaque domaine hésitent à supprimer les anciens enregistrements, craignant qu'ils ne soient liés à des infrastructures essentielles. Cette accumulation d'enregistrements de zone DNS inactifs qui ne pointent vers aucun contenu est connue sous le nom de « DNS flottants » (« dangling DNS ») et présente un risque de détournement de sous-domaine, où un attaquant prend le contrôle d'un sous-domaine légitime qui n'est plus utilisé pour héberger son propre contenu frauduleux ou malveillant. »

Mark Flegg, directeur mondial des services de sécurité chez SC Media, « Comment empêcher que les enregistrements DNS portent atteinte à la sécurité »

En effet, les cybercriminels scrutent les infrastructures, notamment le cloud et les services mis à la disposition du public. Ils recherchent en particulier les enregistrements de zone DNS qui renvoient vers des services web qui ne sont plus utilisés par une marque. En hébergeant leur contenu chez des fournisseurs de service cloud qui n'opèrent pas de vérification, les criminels peuvent récupérer une zone de destination précédemment utilisée. Ils peuvent ainsi rediriger les internautes vers des sous-domaines sur lesquels ils ont chargé leur propre contenu illégitime, sans avoir à infiltrer l'infrastructure d'une entreprise ou le compte d'un service tiers. Par exemple, ZDNet a rapporté qu'une société informatique internationale avait été victime d'un détournement mené par des hackers afin de présenter des cercles de poker sur leurs sous-domaines.

Le fait de tirer parti d'enregistrements DNS flottants ouvre une passerelle pour d'autres cyberattaques, notamment le phishing et les programmes malveillants, ce qui peut entraîner des pertes de revenus, l'exfiltration de données, la perte de la confiance des consommateurs et une atteinte à la réputation d'une entreprise induite par des failles de sécurité. Une étude réalisée par la société autrichienne de conseil en sécurité informatique Certitude Consulting et récemment publiée sur *Security Week* tire la sonnette d'alarme : des milliers d'entités sont vulnérables à de telles attaques. Il est impératif d'intégrer la gestion des enregistrements DNS aux bonnes pratiques informatiques. Depuis plus de 20 ans, les entreprises s'exposent à un risque de mauvaise gestion en s'appuyant sur une multiplicité de propriétaires, de stratégies et de fournisseurs pour assurer la gestion de leur DNS. De surcroît, la tâche se complique encore en cas de fusions et d'acquisitions, car les propriétaires en proie au doute ont profondément peur de supprimer des éléments à tort.

Le [rapport sur les vulnérabilités au détournement de sous-domaine] de CSC examine plus de 440 000 enregistrements DNS et constate que plus de 21 % des enregistrements DNS pointent vers un contenu non résolu, ce qui rend de nombreuses entreprises vulnérables au détournement de sous-domaine. En outre, plus de 277 000 enregistrements (63 %) affichent des codes d'erreur tels que « 404 not found » ou « 502 bad gateway ». La maintenance des enregistrements DNS est historiquement l'une des tâches les plus fréquemment négligées du fait de la diversité des donneurs d'ordre, des politiques et des fournisseurs. Les enregistrements numériques s'accumulent au fil du temps, et les administrateurs qui peuvent ne pas connaître l'historique de chaque domaine hésitent à supprimer les anciens enregistrements, craignant qu'ils ne soient liés à des infrastructures essentielles. Les DNS flottants présentent un risque de détournement de sous-domaine. Le détournement de sous-domaine consiste pour un pirate à prendre le contrôle d'un sous-domaine légitime qui n'est plus utilisé afin d'y héberger son propre contenu frauduleux ou malveillant. Cela ouvre une passerelle pour d'autres cyberattaques, notamment le phishing, les logiciels malveillants et les rançongiciels.

21%

des enregistrements DNS de sous-domaine actifs pointent vers un contenu non résolu, ce qui rend les entreprises vulnérables au détournement de sous-domaine.

La protection des marques en ligne est une nécessité en matière de cybersécurité

Les noms de domaine enregistrés de manière malveillante sont souvent le précurseur de campagnes de phishing ou de BEC ciblées de grande envergure qui peuvent être accompagnées de logiciels malveillants téléchargeables fatals. Pour prévenir ces premières exploitations, les organisations doivent évaluer l'état de leur écosystème de domaines et restaurer le lien entre les équipes responsables de la gestion de cet aspect et celle responsable de ces initiatives marketings en ligne. Les équipes de sécurité doivent surveiller activement leurs domaines et leurs marques en ligne afin de réduire le risque que des domaines web utilisent le nom de leur marque, ou une variante de celui-ci, pour des activités frauduleuses.

La sécurisation de vos domaines constitue le point de départ de la lutte contre le phishing.

Les entreprises doivent obtenir davantage d'informations sur les hackers qui enregistrent ou réenregistrent des domaines similaires en tentant de se faire passer pour leur marque en ligne. Ces informations peuvent les aider à détecter les incidents de sécurité dès leur apparition et à intervenir.

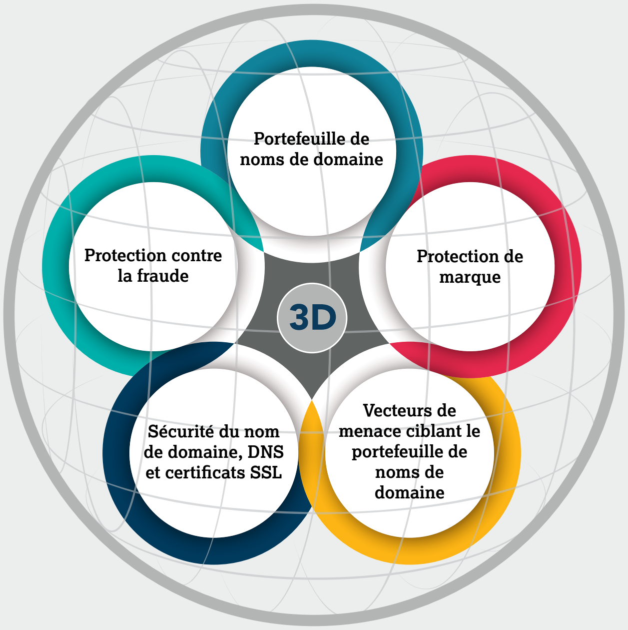
De nombreuses entreprises n'ont jamais compris l'ampleur de ces défis et l'augmentation du nombre de canaux sur lesquels des activités illicites ont lieu en ligne. Elles investissent du temps et de l'argent dans la création de nouvelles marques de confiance, mais tout cela pourrait ne servir à rien si celles-ci deviennent victimes de la criminalité en ligne. La meilleure façon pour les entreprises de protéger leur marque est de mettre en œuvre un programme de protection des marques en ligne qui combine des activités de surveillance en ligne et des moyens d'intervention pour supprimer les contenus frauduleux. Des solutions complémentaires peuvent également contribuer à créer une approche plus complète, comme l'utilisation de réseaux de blocage, qui peuvent intégrer des partenariats avec des fournisseurs de navigateurs, des fournisseurs d'accès Internet (FAI) et d'autres SIEM, pour empêcher les utilisateurs d'Internet d'accéder à des sites web frauduleux. L'utilisation de ces méthodes pour repérer les activités des fraudeurs et y remédier doit également s'accompagner d'un programme de gestion sécurisée des noms de domaine, permettant au propriétaire d'une marque d'administrer et de protéger son propre portefeuille de noms de domaine officiels.

Révolutionner la façon dont vous réduisez votre exposition aux cyberrisques

En tant que premier registrar corporate au monde de noms de domaine pour les plus grandes marques, CSC révolutionne l'écosystème des noms de domaine. Chez CSC, nous pensons que l'intelligence en matière de sécurité des noms de domaine est synonyme de puissance.

Plateforme DomainSec

DomainSec℠ est la première approche holistique du secteur en matière de sécurisation et de défense des écosystèmes de domaine des marques. Il s'agit de la solution de gestion et de sécurité des noms de domaine corporate la plus innovante du marché, associée à des fonctions de protection des marques et de lutte contre la fraude en ligne de nouvelle génération. En combinant les données de ces solutions au sein d'une même plateforme, CSC peut offrir une protection de cybersécurité extrêmement performante pour renforcer la stratégie de sécurité de l'entreprise. Nous pouvons aider les marques à affiner leur modèle de sécurité Zero Trust en allant au-delà de la simple défense des périmètres. Cette plateforme, la première du genre, utilise une technologie propriétaire, combinant le machine learning, l'intelligence artificielle et la technologie de clustering pour produire les renseignements de sécurité d'une intelligence inégalée à l'aide d'indicateurs clés.



Consultez la liste des mesures de sécurité défensives et proactives proposée par CSC pour protéger vos noms de domaine et vos marques grâce à une approche de défense multicouche en profondeur de la sécurité des noms de domaine.

Télécharger notre checklist concernant la sécurité des noms de domaine.

CSC

À PROPOS DE CSC

CSC est le partenaire de confiance des entreprises du classement Forbes Global 2000 (Interbrand®) et 100 Best Global Brands en matière de sécurité et de veille sur les menaces, et propose des solutions de gestion de la sécurité des noms de domaine et de protection des marques en ligne et contre la fraude. Les entreprises internationales investissent considérablement dans leur stratégie de sécurité. C'est la raison pour laquelle notre plateforme DomainSecSM peut les aider à identifier leurs failles en matière de cybersécurité et leur permettre de protéger leurs actifs numériques et leur marque en ligne. En s'appuyant sur la technologie exclusive de CSC, les entreprises peuvent consolider leur stratégie de sécurité pour se protéger contre les vecteurs de cybermenaces qui pèsent sur leur patrimoine numérique, et éviter les pertes de revenus catastrophiques et les atteintes à la réputation de leur marque. Nous fournissons également des services de protection des marques en ligne, qui combinent la surveillance de marque et des interventions ciblées, avec une vue multidimensionnelle sur plusieurs menaces situées à l'extérieur du pare-feu et ciblant des domaines précis. Des services de protection contre la fraude, qui contrent les tentatives de phishing dès les premières phases des attaques, complètent nos solutions. Basée à Wilmington (Delaware) aux États-Unis depuis 1899, CSC possède des bureaux sur tout le territoire des États-Unis, mais également au Canada, en Europe et dans la région Asie-Pacifique. CSC est une entreprise d'envergure mondiale, ce qui nous permet d'intervenir là où sont nos clients en mettant à leur disposition nos équipes d'experts dans chacune de nos activités. Consultez notre site à l'adresse suivante : cscdbs.com/fr.

Contactez-nous

cscdbs.com/fr