RAPPORT DE CYBERSÉCURITÉ

Octobre 2019

Vincent D'Angelo *Directeur mondial, Développement corporate et Alliances stratégiques*

Quinn Taggart *Responsable produits senior, Noms de domaine*

Ken Linscott *Directeur produits, Noms de domaine et sécurité*

Letitia Thian *Responsable marketing*

Recherche et éditorial par CSC

Ce rapport de cybersécurité CSC regroupe dans un document qui se veut exhaustif les données les plus importantes et les plus récentes en matière de cybercriminalité et de cybersécurité. Il propose un aperçu détaillé des informations essentielles pour vous et votre marque. Dans cette édition spéciale, nous allons nous intéresser à l'adoption de mécanismes de sécurité des noms de domaine par l'industrie de défense au niveau mondial.

Sécurité du nom de domaine

CSC collabore avec plus de 65%

des PLUS GRANDES marques mondiales

CSC assiste plus de 65 % des plus grandes marques mondiales dans la gestion de leur présence en ligne (Interbrand®). À l'aide de nos outils brevetés, nous aidons les entreprises à identifier les failles de sécurité et les opportunités stratégiques au sein de leur portefeuille de noms de domaine. Nous nous appuyons sur cette même méthodologie pour analyser les principaux noms de domaine des entreprises du monde entier afin de vérifier l'efficacité de leur sécurité.

Cette édition est consacrée aux sous-traitants des acteurs publics de l'industrie de défense au niveau mondial. Les agences gouvernementales et leurs sous-traitants sont en effet la cible d'attaques régulières, qui créent des failles de sécurité [1] pouvant affecter la sécurité nationale et le bien-être des citoyens. Nous pensons donc qu'il est impératif de diffuser ces informations. Les noms de domaine, le DNS (domain name system) et les certificats numériques sont les piliers qui soutiennent l'infrastructure Internet. De ce fait, les applications, les outils, les systèmes et les données sensibles qui reposent sur cette infrastructure peuvent tomber dans de mauvaises mains s'ils ne sont pas sécurisés par des mécanismes adéquats de contrôle du DNS[2].

Nous avons analysé certains des plus grands sous-traitants de l'industrie de défense issus de 24 pays, afin de découvrir dans quelle mesure cette industrie a adopté les contrôles de sécurité des noms de domaine.

Sécurité du nom de domaine et tendances observées

Étude basée sur 100 sous-traitants de l'industrie de défense au niveau mondial

Les dernières attaques DNS

L'année 2019 a commencé avec une alerte de la CISA (Cybersecurity and Infrastructure Agency) américaine concernant des attaques DNS. Depuis, d'autres alertes ont été émises par des experts du secteur, comme Brian Krebs et des agences gouvernementales comme le NSCS, le centre de cybersécurité du Royaume-Uni . Ces efforts ont donné lieu à une prise de conscience des risques constants liés aux piratages des noms de domaine et du DNS. Cependant, de nombreux secteurs présentent une grande surface d'attaque, comme le montrent les Rapports de cybersécurité CSC sur le secteur financier et les médias . Il faut ajouter que ces attaques ciblent tout type d'entreprise quel que soit son secteur d'activité, sa taille ou son implantation géographique. Ainsi, un hôpital californien s'est récemment fait voler son nom de domaine et a perdu l'accès à son site Web, sa messagerie, ses applications et toutes les données associées.

Enregistrement des noms de domaine

29 % REGISTRAR PROFESSIONNEL

71 % REGISTRAR COMMERCIAL

RISQUE

Traditionnellement, ce sont les registrars (bureaux d'enregistrement) de noms de domaine commerciaux qui sont les plus visés par les cyberattaques. Les entreprises devraient s'associer à un registrar de niveau professionnel qui investit lourdement au niveau technologique, mais également dans la formation à la sécurité de ses employés – y compris en instaurant un devoir de vigilance – pour pouvoir identifier les attaques malveillantes, notamment sur les noms de domaine stratégiques.

OBSERVATIONS

29 % des acteurs de l'industrie de défense ont recours à des registrar professionnels.

Les attaques malveillantes contre les noms de domaine, les messageries, le DNS et les certificats numériques ont augmenté. La gestion du portefeuille de noms de domaine global par un registrar professionnel reconnu rendra l'adoption de normes de sécurité des noms de domaine bien plus facile à implémenter et à surveiller que s'il s'agissait d'un registrar commercial. En outre, l'évaluation régulière des mécanismes de contrôle et de sécurité, des processus et des outils d'un registrar de noms de domaine deviendra une composante essentielle du positionnement d'une organisation en matière de cybersécurité.

Verrouillage du registre

13 % VERROUILLAGE DU REGISTRE ACTIVÉ

65 % VERROUILLAGE DU REGISTRE DÉSACTIVÉ

22 % *VERROUILLAGE DU REGISTRE NON DISPONIBLE

RISQUE

Les noms de domaine non verrouillés sont vulnérables aux tactiques d'ingénierie sociale, qui peuvent conduire à des modifications non autorisées du DNS et à des piratages de nom de domaine. Il arrive toutefois que certains noms de domaine demeurent non verrouillés, tous les registres du monde ne disposant pas de services de verrouillage.*

OBSERVATIONS

13 % ont mis en place un verrouillage du registre.

Ces verrous empêchent tout piratage du nom de domaine et toute modification non autorisée du DNS, qui pourraient mettre le site hors ligne ou rediriger ses utilisateurs vers du contenu malveillant. Vu les risques constants d'attaques DNS pesant sur les agences gouvernementales et d'autres acteurs de secteurs sensibles, peu de sous-traitants de l'industrie de défense ont adopté ces mécanismes de contrôle.

Plus inquiétant encore, 69 % des entreprises qui utilisent le même nom de domaine pour leur site Web principal, leur messagerie et leurs serveurs DNS – et qui auraient donc dû utiliser verrouiller le registre – ne l'ont pas fait.

Sécurité du nom de domaine et tendances observées

Prestataire de services DNS

32% DNS INTERNE

13% DNS D'ENTREPRISE / PROFESSIONNEL

55% AUTRES (DNS D'HÉBERGEMENT / COMMERCIAL)

RISQUE

Les prestataires de services DNS non destinés aux entreprises présentent des risques de sécurité potentiels, avec la possibilité d'attaques DDoS (Distributed Denial of Service), d'interruption des services et de perte de revenus.

DNSSEC

3% DNSSEC ACTIVÉ

97% DNSSEC DÉSACTIVÉ

RISQUE

L'absence de déploiement DNSSEC – l'un des protocoles de sécurité les plus rentables à mettre en place – crée des vulnérabilités au niveau du DNS et peut favoriser, par exemple, le détournement par un hacker de n'importe quelle étape du processus de recherche DNS. Les pirates sont alors en mesure de prendre le contrôle d'une session de navigation Internet pour rediriger les utilisateurs vers de faux sites Web.

HTTPS everywhere

77% HTTPS EVERYWHERE DÉPLOYÉ

23% HTTPS EVERYWHERE NON DÉPLOYÉ

RISQUE

Le chiffrement associé aux certificats numériques pour toutes les activités transactionnelles en ligne limite le risque de piratage de sessions Web par des cybercriminels en vue de commettre des usurpations d'identité ou d'installer des logiciels malveillants sur les appareils des utilisateurs. Il permet aussi de lutter contre le piratage des communications Web pouvant générer une violation ou un vol des données clients, une attaque DDoS ou la dégradation d'un site Web.

OBSERVATIONS

13 % des entreprises utilisent un prestataire de services DNS professionnel ; 3 % déploient DNSSEC.

La préférence accordée aux registrars commerciaux par les sous-traitants de l'industrie de défense est amplifiée par l'hébergement sur des serveurs DNS non destinés aux entreprises, ce qui augmente l'exposition aux attaques DDoS et aux vecteurs de risque similaires. Notre étude montre que 13 % de ces sous-traitants privilégient des prestataires de services DNS destinés aux entreprises. Environ 32 % utilisent leur propre architecture DNS, tandis que 55 % ont recours à des prestataires commerciaux. DNSSEC est une autre méthode pour protéger la communication globale entre les utilisateurs et les propriétés d'un site Web. Les taux d'adoption de la technologie DNSSEC ne dépassent toutefois pas les 3 %.

Sécurité du nom de domaine et tendances observées

Type de certificat numérique

4% EV

84% OV

12% DV

RISQUE

Les certificats numériques qui exigent un niveau d'authentification plus élevé, tels que les certificats à validation d'organisation (OV) et à validation étendue (EV), sont moins susceptibles d'être compromis que les certificats à validation de domaine (DV).

OBSERVATIONS

84 % utilisent des certificats à validation d'organisation (OV), mais 12 % utilisent des certificats à validation de domaine (DV).
Si le DNS est la porte de la maison, le certificat numérique en est la serrure. Peu importe que la porte soit solide dès lors que la serrure est peu fiable. Un facteur de risque majeur réside dans le mode de validation des certificats numériques. Les certificats à validation de domaine (DV), qui requièrent un niveau plus faible d'authentification, sont utilisés par 12 % des sous-traitants de l'industrie de défense. Cela signifie que si un hacker parvient à accéder à la messagerie interne, il peut facilement valider des certificats numériques via les noms de domaine d'une entreprise dans un but malveillant.

Authentification des e-mails

25% DMARC

85% SPF

3% DKIM

RISQUE

L'authentification du canal de messagerie par le protocole DMARC (Domain-based Message Authentication, Reporting and Conformance), SPF (Sender Policy Framework) ou DKIM (DomainKeys Identified Mail) réduit le risque de spoofing d'e-mail et de phishing.

OBSERVATIONS

27 % utilisent DMARC
La technologie DMARC est un système d'authentification des e-mails conçu pour protéger le nom de domaine de messagerie d'une entreprise contre les tentatives de spoofing, de phishing et autres cyberattaques. Depuis que l'authentification DMARC a été rendue obligatoire par certains gouvernements , l'adoption de ce mécanisme de contrôle par les sous-traitants est recommandée et peut permettre de contrer certaines menaces pesant sur les communications par e-mail.

Enregistrements CAA

4% ENREGISTREMENTS CAA UTILISÉS

96% ENREGISTREMENTS CAA NON UTILISÉS

RISQUE

Un enregistrement CAA (certificate authority authorization) est un enregistrement de ressource conservé dans un fichier de zone, qui permet au propriétaire du domaine d'indiquer quelles Autorités de certification (AC) sont habilitées à émettre un certificat pour un nom de domaine donné. En ajoutant des enregistrements CAA, vous êtes à même de contrôler les AC auxquelles a recours votre entreprise. Cela permet d'assurer que seul votre prestataire peut émettre un certificat pour vos noms de domaine. En outre, c'est un dispositif technique de contrôle essentiel pour l'application de votre politique et la réduction des cyber-risques comme le phishing HTTPS ou le piratage de sous-domaines.

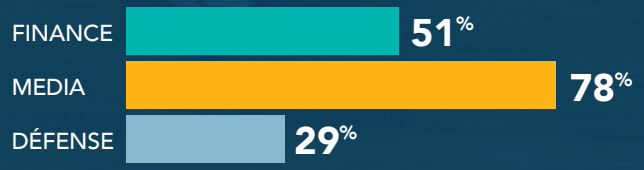
OBSERVATIONS

4 % utilisent des enregistrements CAA.
Lorsque nous avons examiné le taux d'adoption des enregistrements CAA dans l'industrie de défense, nous avons constaté que seules 4 % des entreprises les utilisaient. Et parmi celles-ci, la moitié permettait l'émission de certificats par des prestataires de type commerciaux, non spécialisés dans les services aux entreprises. Ce chiffre est à rapprocher de l'utilisation des enregistrements CAA par 3 % des entreprises publiques dans le monde entier.

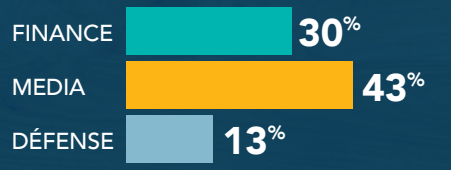
Mécanismes de contrôle des noms de domaine : la défense / les médias / le secteur financier

Le dernier rapport de CSC était consacré aux secteurs de la finance et des médias. Concernant les sous-traitants dans l'industrie de défense, il semble qu'ils aient été plus lents à adopter diverses composantes de sécurisation des noms de domaine (verrouillage du registre, registrar de noms de domaine d'entreprise, prestataires de services DNS professionnels et DMARC notamment). La plupart de ces mécanismes de contrôle sont pourtant recommandés par les leaders du secteur, comme CSC le mentionnait précédemment.

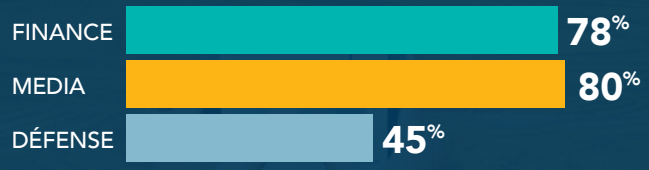
REGISTRAR PROFESSIONNEL



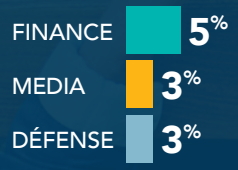
VERROUILLAGE DU REGISTRE ACTIVÉ



DNS D'ENTREPRISE OU INTERNE



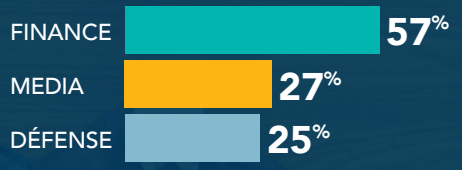
DNSSEC ACTIVÉ



HTTPS EVERYWHERE

TYPE DE CERTIFICAT NUMÉRIQUE (EV OU OV)

DMARC ACTIVÉ



En outre, toutes les mesures de sécurité ne sont pas forcément onéreuses, notamment par rapport aux coûts que peut impliquer une simple faille. Pourtant, on constate que ces composantes de sécurité fondamentales n'ont pas atteint le niveau d'adoption auquel on pourrait s'attendre de la part de l'industrie de défense, vu l'augmentation des cybermenaces année après année. Le plus inquiétant est que les techniques les plus simples, permettant de garantir la sécurité globale du nom de domaine et la confiance des utilisateurs, semblent être les moins susceptibles d'être mises en œuvre par les entreprises.

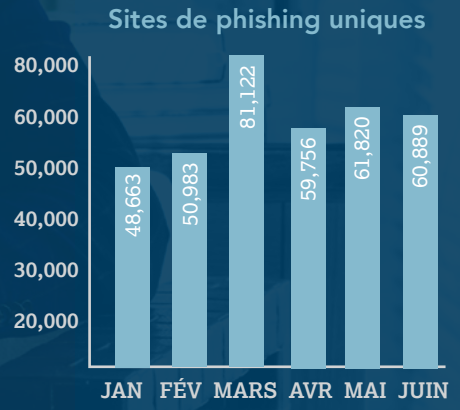
Phishing et fraude par e-mail

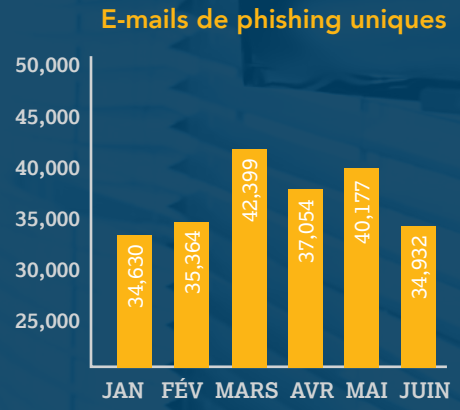
Augmentation importante des sites Web de phishing durant l'année

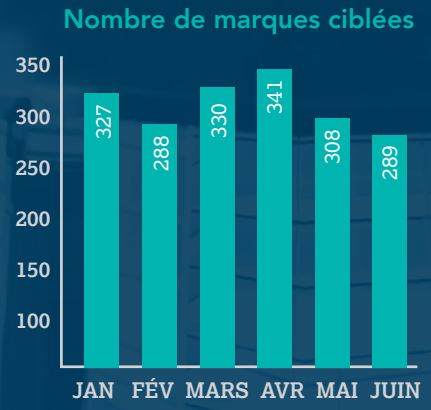
Au deuxième trimestre 2019, plus de 55 % des sites Web de phishing possédaient des certificats numériques, rendant inutiles les avertissements préventifs aux utilisateurs concernant la sécurité des sites Web. Ces sites pirates ont une apparence plus légitime grâce à la mention « HTTPS » dans la barre d'adresse. Ils parviennent donc à tromper les utilisateurs en détournant une fonctionnalité de sécurité d'Internet et permettent aux acteurs malintentionnés de voler les données d'identité ainsi que les identifiants de compte.

Attaques de phishing

Au deuxième trimestre 2019, on a dénombré 182 465 sites Web de phishing, soit une faible augmentation par rapport au trimestre précédent. Toutefois, le total agrégé des attaques au premier semestre 2019 était en augmentation de 25 % par rapport au second semestre 2018.







Secteurs d'activité les plus touchés

Le SaaS et la messagerie, les services de paiement en ligne, ainsi que les banques et institutions financières sont les trois secteurs les plus touchés par les attaques de phishing au T2 2019.

SOURCE : Rapport de l'APWG « Phishing Activity Trends Report », 2e trimestre 2019

Noms de domaine de premier niveau (TLD) les plus utilisés pour les sites Web de phishing

Sans surprise, les TLD hérités – c'est-à-dire les TLD établis il y a très longtemps et qui comptent un grand nombre de sites Web – sont ceux qui hébergent le plus de hameçonneurs. Toutefois, les TLD de code pays (ccTLD) qui ont été redéfinis, ainsi qu'un petit nombre de TLD génériques souvent proposés à bas prix, hébergent une quantité notable d'opérations de phishing par rapport aux autres noms de domaine dans le monde.

Types de TLD:

TLD hérités | ccTLD | Nouveaux gTLD

↑ / ↓ Changement de classement + / - Changement de volume

.com +714 →	.net +33 Était n° 3 ↑	.br +64 Était n° 8 ↑	.org -9 →
N° 1 • 2,812 noms de domaine	N° 2 • 208 noms de domaine	N° 3 • 146 noms de domaine	N° 4 • 145 noms de domaine
.uk +16 →	.top	.info +36 →	.in +47 Était n° 11 ↑
N° 5 • 137 noms de domaine	N° 6 • 120 noms de domaine	N° 7 • 119 noms de domaine	N° 8 • 105 noms de domaine
.au	.xyz +26 Était n° 17 ↑	.icu	.cl
N° 9 • 80 noms de domaine	N° 10 • 63 noms de domaine	N° 11 • 59 noms de domaine	N° 12 • 47 noms de domaine
.ga -21 Était n° 10 ↓	.ml -35 Était n° 9 ↓	.cf -43 Était n° 6 ↓	.co
N° 13 • 47 noms de domaine	N° 14 • 43 noms de domaine	N° 15 • 41 noms de domaine	N° 16 • 41 noms de domaine
.ru -6 Était n° 13 ↓	.pl +9 Était n° 19 ↑	.id	.it -1 Était n° 16 ↓
N° 17 • 38 noms de domaine	N° 18 • 37 noms de domaine	N° 19 • 36 noms de domaine	N° 20 • 36 noms de domaine

SOURCE : Rapport de l'APWG « Phishing Activity Trends Report », 2e trimestre 2019

Toutes les organisations sont concernées :

Exemples issus des actualités

AMÉRIQUE

Limiter les modifications frauduleuses au sein de l'infrastructure DNS

La CISA (Cybersecurity and Infrastructure Security Agency) du Département américain de la sécurité intérieure a identifié une vague d'attaques visant à modifier les enregistrements des noms de serveurs DNS et a publié une directive destinée aux agences fédérales pour qu'elles adoptent les mesures requises telles que l'audit des enregistrements DNS et la sécurisation de l'accès aux portails afin de réduire l'exposition aux piratages DNS.

cyber.dhs.gov/ed/19-01/

Alerte : publication de rapports sur des attaques DNS

L'ICANN (Internet Corporation for Assigned Names and Numbers) a envoyé une notification d'alerte aux organisations afin qu'elles mettent en œuvre les meilleures pratiques et les mesures requises telles que le déploiement DNSSEC et le verrouillage de registre afin de protéger leurs systèmes contre les activités malveillantes ciblant les serveurs DNS.

icann.org/news/announcement-2019-02-15-en

Plongée dans la récente vague de piratages DNS

KrebsOnSecurity a analysé la vague de piratages DNS complexes afin d'en comprendre l'origine et l'étendue, et constaté que de nombreux gouvernements du monde entier ont été affectés en raison des failles de sécurité chez d'importants fournisseurs d'infrastructures Internet.

krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-dns-hijacking-attacks/

Les services secrets enquêtent sur une faille de sécurité chez un sous-traitant IT du Gouvernement américain

Un sous-traitant IT travaillant avec plus de 20 agences fédérales a subi une violation des données à cause d'un malware dissimulé dans la pièce jointe d'un e-mail. L'attaque a compromis les communications par e-mail et les identifiants de connexion aux bases de données des agences affectées.

krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/

ROYAUME-UNI

Campagne de piratages DNS et conseils pour limiter les risques

Le NCSC (National Cyber Security Centre) britannique a publié un bulletin consultatif indiquant que la vaste campagne mondiale d'attaques DNS continue d'être active dans de nombreuses régions et secteurs, et fournit des conseils d'atténuation des risques concernant la sécurité des registrars, des serveurs DNS et des applications Web.

ncsc.gov.uk/news/ongoing-dns-hijacking-and-mitigation-advice

BULGARIE

Une nation toute entière vient d'être piratée

Les autorités fiscales de Bulgarie ont subi une attaque qui a entraîné une violation des données personnelles et financières de 5 millions de citoyens sur les 7 millions d'habitants que compte le pays.

edition.cnn.com/2019/07/21/europe/bulgaria-hack-tax-intl/

ÉQUATEUR

Presque tout le monde en Équateur est victime de violation des données

Les informations détaillées de près de 20 millions d'Équatoriens, parmi lesquels le Président lui-même, ont été dérobées sur le serveur d'un sous-traitant local, de même que les données des registres gouvernementaux et d'autres organisations.

engadget.com/2019/09/17/ecuador-data-breach-20-million-citizens/

AUSTRALIE

L'ACSC souhaite déployer un service DNS de sécurisation pour les infrastructures critiques et gouvernementales

L'ACSC (Australian Cyber Security Centre) australien pilote un projet de service DNS de protection qui devrait être adopté par les agences gouvernementales et les gestionnaires d'infrastructures sensibles.

itnews.com.au/news/acsc-to-deploy-protective-dns-service-for-govt-critical-infrastructure-520138

Recommendations

Adopter une approche « défense en profondeur »

UTILISER 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

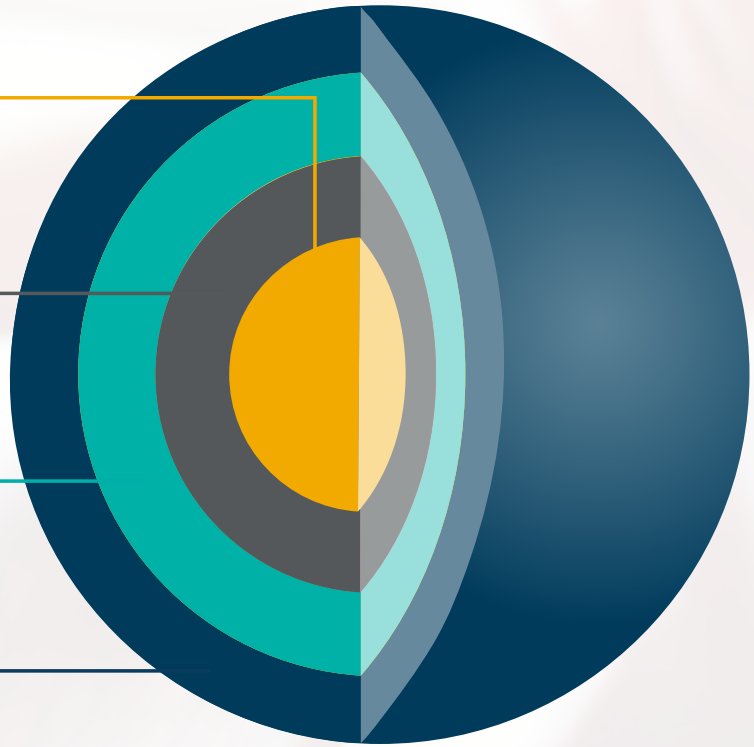
Visibilité sur les niveaux d'autorisation élevés et les notifications

ACCÈS SÉCURISÉ AU PORTAIL

Validation IP, authentification à deux facteurs et Federated Identity

PRESTATAIRE DE SERVICES AUX ENTREPRISES

Systèmes, personnel, politiques et processus



CSC soutient les entreprises qui font d'importants investissements dans la sécurité en identifiant les failles de sécurité dans leurs actifs immatériels tels que les noms de domaine, le DNS et les certificats numériques. Les solutions de sécurité CSC protègent les entreprises des cybermenaces qui pèsent sur leurs actifs numériques, et les aident à éviter les pertes de revenus, les atteintes à la réputation de leur marque ou les pénalités financières pouvant résulter d'une non-conformité aux réglementations de type RGPD. Outre les actifs numériques, les solutions CSC permettent de sécuriser les marques en ligne face aux sites Web contrefaits, à la fraude et aux violations des droits de propriété intellectuelle. Les solutions CSC surveillent et contrent ce type d'attaques, et offrent des services de conseil et d'action en contrefaçon. Plus d'infos sur ***cscdigitalbrand.services/fr***.

Références

1.krebsonsecurity.com/2019/09/secret-service-investigates-breach-at-u-s-govt-it-contractor/
2.cscglobal.com/cscglobal/pdfs/DBS/Digital-Asset-Security-Checklist-EN.pdf
3.us-cert.gov/ncas/alerts/AA19-024A
4.krebsonsecurity.com/2019/02/a-deep-dive-on-the-recent-widespread-DNS-hijacking-attacks/
5.ncsc.gov.uk/news/ongoing-DNS-hijacking-and-mitigation-advice
6.cscglobal.com/cscglobal/pdfs/DBS/Cyber-Security-Report-June-2019-EN.pdf
7.beckershospitalreview.com/cybersecurity/hackers-steal-california-hospital-s-website-domain-email-addresses.html
8.eweek.com/security/dmarc-email-security-adoption-soars-as-us-government-deadline-hits