Les fondamentaux de la cybersécurité

- et ses enjeux pour votre activité

Les fondamentaux de la cybersécurité

En 2015, tous les grands journaux de la planète ont consacré au moins un article à la cybercriminalité. *The Wall Street Journal, Die Zeit, Le Monde, El Pais, China Daily*, et bien d'autres, portent la plus grande attention à ce sujet. Et ils font bien : au cours des deux premiers mois de 2016, 36 cyberattaques majeures ont été lancées contre des administrations, des entreprises publiques et des sociétés privées du monde entier. Plus d'une attaque tous les deux jours.

Facebook® et Instagram, qui comptent parmi les réseaux sociaux les plus avancés techniquement, ont subi des interruptions de service de grande ampleur en 2015, bloquant l'accès des utilisateurs à leurs comptes. Comme le signale Infosecurity Magazine : « l'année 2015 marque un record en matière de déni de service distribué (DDoS), avec une pointe historique à 500 Gbit/s. En effet, les cybercriminels usent désormais de techniques multivectorielles pour extorquer de l'argent à leurs victimes. »

Toutes les grandes sociétés de sécurité prévoient une hausse des attaques, qui devraient également évoluer dans leurs formes. D'après une analyse prédictive globale menée par le site govtech.com, elles seront plus difficiles à détecter en 2016.

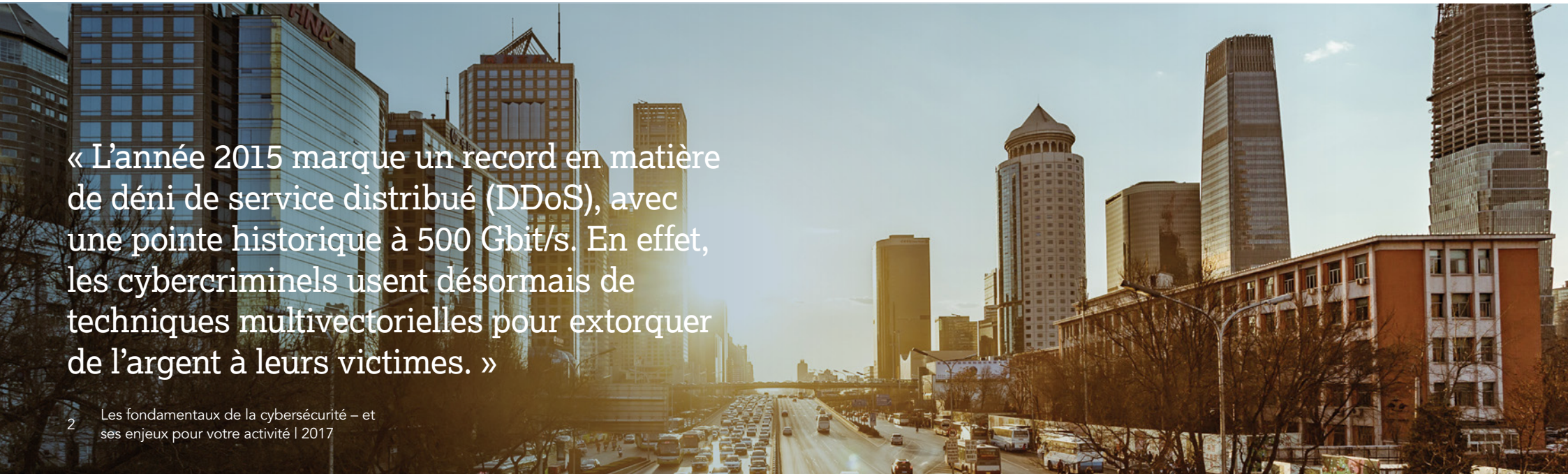
La Banque HSBC, l'une des plus grandes institutions de services bancaires et financiers au monde, a fait l'objet d'une nouvelle attaque DDoS à la fin du mois de janvier 2016. Rien qu'au Royaume-Uni, 17 millions de clients, particuliers et entreprises, se sont ainsi retrouvés sans accès aux services bancaires en ligne pendant plusieurs heures.

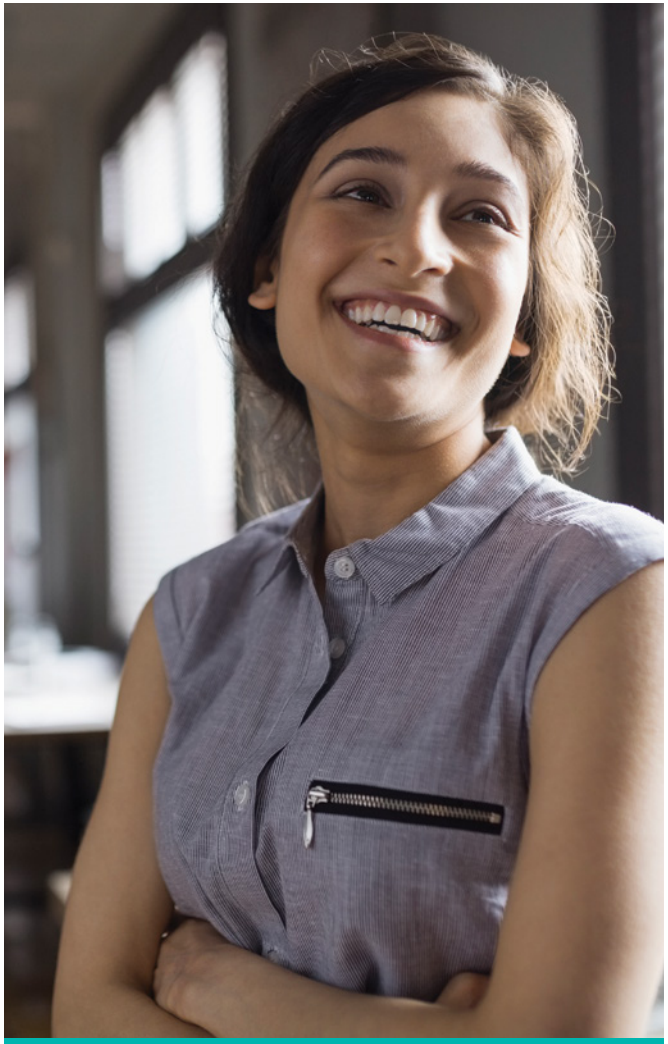
En février 2016, les données du système de paie de Snapchat ont été la cible d'une campagne de phishing lancée par des cybercriminels se faisant passer pour le PDG de l'entreprise. Lorsque les informations confidentielles des clients et des employés sont dérobées pour être revendues au marché noir, la panique s'installe, et c'est bien légitime.

La liste des cyberattaques est sans fin

Si vous travaillez pour l'une des sociétés qui ont été victimes d'une attaque DDoS ou d'une campagne de phishing, vous savez parfaitement ce qu'il en coûte à l'entreprise. Si vous n'avez pas encore vécu un tel incident, il est temps d'apprendre à vous en prémunir. Et de comprendre pourquoi, en tant que professionnels du marketing, du juridique et du service informatique, vous êtes concernés par ce qui représente, de nos jours, le plus grand des risques pour l'entreprise.

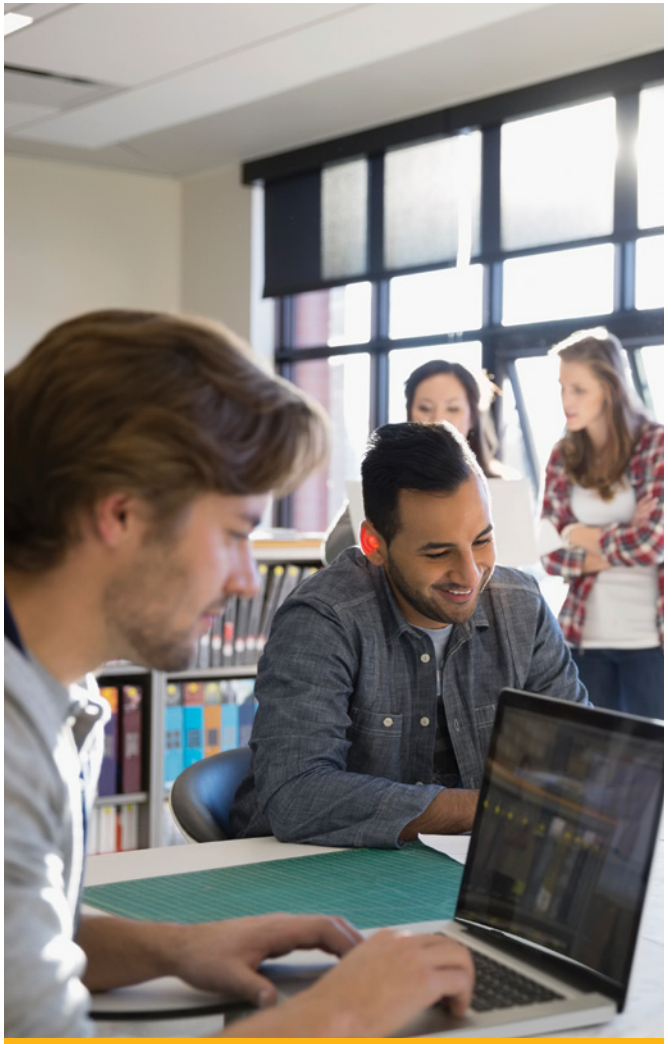
Ce bulletin d'information explique pourquoi la cybersécurité doit être prise au sérieux, et quelles mesures peuvent être prises pour protéger votre marque et votre entreprise.





Professionnels du marketing

Services juridiques et avocats spécialistes des marques



Professionnels du service informatique

Professionnels du marketing

Les enjeux de la sécurité informatique pour votre unité

Que votre entreprise utilise internet pour diffuser de l'information ou pour l'e-commerce, une attaque DDoS ou un piratage peut lui coûter des millions, mais aussi nuire à son image de marque. En cas d'incident, pendant que le service informatique fait son possible pour remettre le site web en service et le sécuriser, vous aurez certainement à gérer une crise de relations publiques et à rassurer votre clientèle en espérant qu'elle vous reste fidèle malgré l'attaque.

Comment oublier le piratage du site de rencontres Ashley Madison, qui a révélé au grand jour les données personnelles de 32 millions d'internautes souhaitant nouer discrètement des relations extraconjugales ? Un véritable cauchemar en termes de réputation.

La cybercriminalité ne cesse de croître et les techniques d'attaque évoluent. Si vous ne savez pas quelles mesures ont été prises dans votre entreprise, ou quel est le prestataire de sécurité désigné, vous devez organiser une réunion pour aborder tous les points évoqués ici. En parallèle, créez une équipe de gestion de crise qui réunit des acteurs clés des services informatique, juridique et marketing, ainsi que de la direction, afin d'élaborer un plan permettant à l'avenir de maîtriser tous les aspects de la sécurité et de la défense des droits de l'entreprise.

Marketing
Introduction

Étape 1
Audit et consolidation

Étape 2
Sécurisation et surveillance

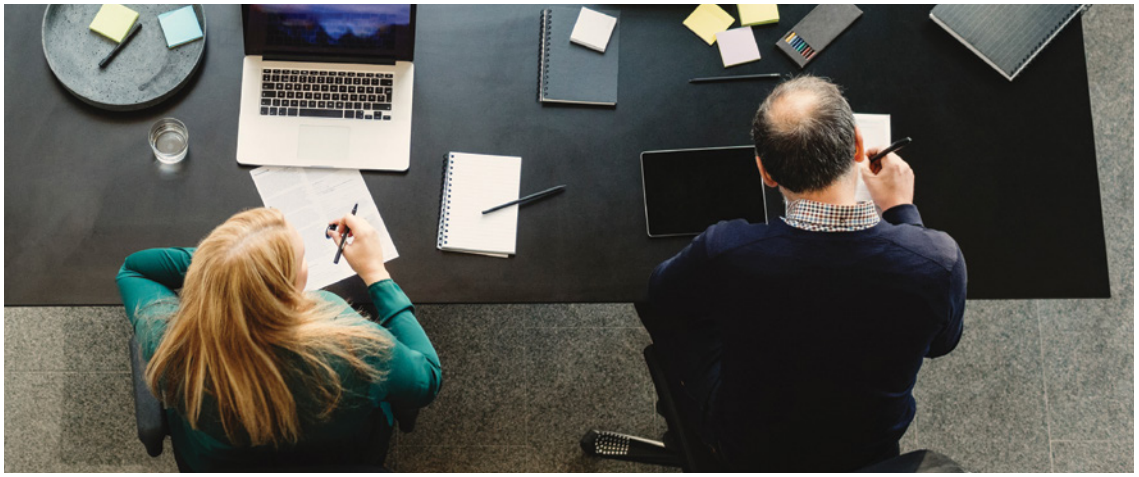
Étape 3
Communication et sensibilisation

Professionnels du marketing

Les enjeux de la sécurité informatique pour votre unité

Étape 1 : Tout d'abord, pour vous défendre contre les cyberattaques, vous devez identifier les actifs numériques de votre entreprise. Demandez à votre prestataire de protection des marques en ligne de procéder à un audit. Cherchez le nombre de noms de domaine détenus par votre entreprise, ceux qui sont actifs et ceux utilisés de manière défensive. Vous devez aussi savoir le nombre de noms d'utilisateur sur les réseaux sociaux et à quel endroit sont conservés les identifiants correspondants, au cas où la personne chargée d'animer ces réseaux quitte votre service. Comment les applications mobiles sont-elles gérées ? Et votre entreprise applique-t-elle des certificats de sécurité SSL adaptés à ses sites web, notamment pour le commerce en ligne ?

Lorsque vous avez toutes les réponses à ces questions et une vision claire de la situation, la consolidation de votre portefeuille est la meilleure option, car elle établit une vue d'ensemble unique de tous les actifs. En la matière, vous en remettre au service juridique ou IT ne suffit pas. Tous les acteurs du marketing, et en particulier ceux qui veillent à la présence et à la réputation en ligne de l'entreprise, doivent connaître la teneur du portefeuille numérique.



Professionnels du marketing

Les enjeux de la sécurité informatique pour votre unité

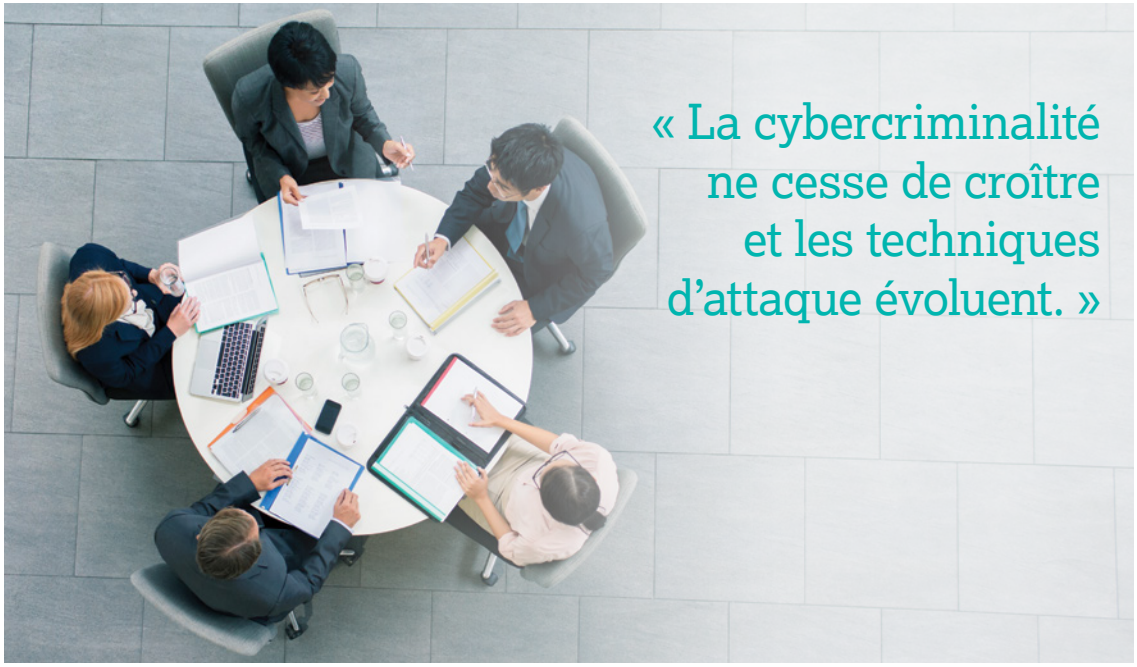
Étape 2 : Une fois le portefeuille consolidé, le moment est venu de prendre des mesures simples et rentables pour sécuriser vos noms de domaine clés, c'est-à-dire, en général, vos principaux sites web ou portails destinés à la clientèle. Travaillez de pair avec le service informatique ou juridique, si c'est à lui que revient la gestion quotidienne de ces actifs auprès de votre prestataire de protection des marques numériques. Vous seul pouvez leur indiquer les noms de domaine qui vous semblent les plus importants pour l'entreprise. Des mécanismes de protection tels que la double authentification et le blocage au niveau du registre et du registraire avec une autorisation manuelle tripartite empêchent le piratage de vos noms de domaine critiques et les protègent contre toute modification ou suppression non autorisée. La mise en œuvre de ces mécanismes est relativement peu coûteuse, et met vos sites clés à l'abri.

« Comment oublier le piratage du site de rencontres Ashley Madison, qui a révélé au grand jour les données personnelles de 32 millions d'internautes souhaitant nouer discrètement des relations extraconjugales ? Un véritable cauchemar en termes de réputation »

Professionnels du marketing

Les enjeux de la sécurité informatique pour votre unité

Étape 3 : Maintenant que vos sites stratégiques sont en sûreté, assurez-vous de bien comprendre les différents types d'attaques et les conséquences qu'elles peuvent avoir pour vos clients et votre entreprise. Dès que votre entreprise traite des informations confidentielles, comme les coordonnées bancaires, adresses et données personnelles des clients, il est absolument essentiel de sensibiliser vos clients à la prévention du phishing. Vous pouvez notamment informer vos clients que votre entreprise ne leur demandera jamais de communiquer des informations personnelles par e-mail. Votre prestataire devrait être en mesure de vous proposer une solution contre le phishing adaptée aux spécificités de votre entreprise et de votre marque, et de vous aider à élaborer une formation pour les employés. Consultez votre service informatique pour déterminer les mesures de protection adoptées en interne, car ces services varient d'un prestataire à l'autre.



« La cybercriminalité ne cesse de croître et les techniques d'attaque évoluent. »

Services juridiques et avocats spécialistes des marques

Les enjeux de la sécurité informatique pour votre unité

Selon les marchés sur lesquels vous opérez, la cybercriminalité peut être considérée comme un délit. Aux États-Unis, par exemple, une attaque DDoS est un délit fédéral, c'est-à-dire que toute personne commettant un tel acte peut être poursuivie au civil et au pénal à l'échelon fédéral (plutôt qu'au niveau de l'État). Mais, en attendant que le coupable soit mis hors d'état de nuire, vous devrez mobiliser toute votre expertise pour empêcher ces attaques.

Les cabinets juridiques sont vulnérables en raison des informations confidentielles qu'ils conservent pour leurs clients. C'est aussi une profession où les évolutions se font lentement. Prenons par exemple l'affaire Mossack Fonseca. Dans un éditorial, John McAfee a estimé qu'il s'agissait de « la cyberattaque la plus vaste et la plus nuisible à ce jour [...] les données publiées contenaient 11,5 millions de documents retraçant la constitution et les actions de 214 000 sociétés offshore, ainsi que les noms et les manœuvres financières de plus de 14 000 clients[1]. » Mossack Fonseca est le quatrième cabinet juridique au monde spécialisé dans la protection des avoirs. À qui les cybercriminels s'en prendront-ils la prochaine fois ?

Le service juridique est également chargé d'enregistrer et de gérer des noms de domaine et des noms d'utilisateur de réseaux sociaux à des fins promotionnelles et défensives, selon la politique observée par l'entreprise en matière de propriété intellectuelle en ligne. Mais votre service s'occupe-t-il également des aspects sécuritaires ?

Juridique
Introduction

Étape 1
Sécurisation et surveillance

Étape 2
Communication et sensibilisation

Services juridiques et avocats spécialistes des marques

Les enjeux de la sécurité informatique pour votre unité

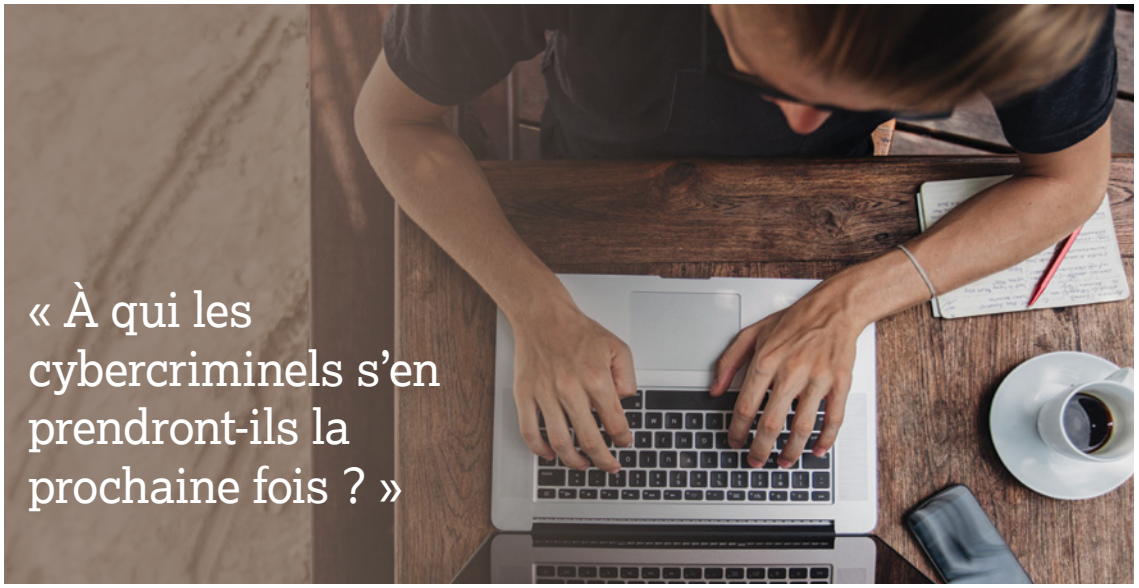
Étape 1 : Votre prestataire de protection des marques doit vous proposer des mécanismes tels que la double authentification et le blocage au niveau du registre et du registraire avec autorisation manuelle tripartite. Ces mécanismes sont en effet les plus efficaces et les plus rentables pour sécuriser les noms de domaine stratégiques, tels que les sites web et portails destinés à la clientèle. Ils évitent le piratage des noms de domaine et empêchent toute modification ou suppression non autorisée. Pour dresser une liste complète des noms de domaine essentiels à l'entreprise, faites intervenir le service marketing, qui connaît et utilise plusieurs des noms de domaine les plus importants.

« Les cabinets juridiques sont vulnérables en raison des informations confidentielles qu'ils conservent pour leurs clients. »

Services juridiques et avocats spécialistes des marques

Les enjeux de la sécurité informatique pour votre unité

Étape 2 : Maintenant que vos sites stratégiques sont en sûreté, assurez-vous de bien comprendre les différents types d'attaques de phishing et les conséquences qu'elles peuvent avoir pour vos clients et votre entreprise. Dès que votre entreprise traite des informations confidentielles, comme les coordonnées bancaires, adresses et données personnelles des clients, il est absolument essentiel de sensibiliser vos clients à la prévention du phishing. Vous pouvez notamment informer vos clients que votre entreprise ne leur demandera jamais de communiquer des informations personnelles par e-mail. Votre prestataire devrait être en mesure de vous proposer une solution contre le phishing adaptée aux particularités de votre entreprise et de votre marque, et de vous aider à élaborer une formation pour vos employés. Consultez votre service informatique pour déterminer les mesures de protection adoptées en interne, car ces services varient d'un prestataire à l'autre.



Professionnels du service informatique

La sécurité informatique est votre priorité, nous le savons

Il est inutile d'expliquer la gravité des cybermenaces à des experts de la sécurité informatique. Pour Steve Durbin, directeur général de l'Information Security Forum, « les attaques seront toujours plus innovantes et plus sophistiquées ». Si vous avez la responsabilité, totale ou partielle, de la sécurité informatique de votre entreprise, une seule question prévaut : pourrez-vous dormir sur vos deux oreilles ?

Par exemple, la base de données de Verizon Enterprise Solutions a été piratée au mois de mars 2016. Cette attaque a eu des répercussions sur l'entreprise de cybersécurité, mais elle expose également ses clients à des risques en aval, car les données dérobées pourront servir à des attaques de phishing futures.

Quelle que soit l'entreprise, la responsabilité de la sécurité informatique est incommensurable. Une attaque de déni de service ou de phishing, un vol de mots de passe, le téléchargement de données confidentielles ou encore la mise en danger du réseau vous coûtera certainement votre poste.

Mais la sécurité informatique est-elle au sommet des priorités de votre entreprise ? Faites-vous appel aux bons prestataires pour garantir la disponibilité permanente des systèmes critiques ? Si vous n'en êtes pas certain, il est temps d'agir.

Professionnels du service informatique

La sécurité informatique est votre priorité, nous le savons

Étape 1 : Demandez-vous jusqu'à quel point votre entreprise peut résister à une attaque et quel budget elle peut raisonnablement consacrer pour remédier à un tel incident.

Dans une étude récente, Arbor Networks constatait que la plus vaste attaque de déni de service avait atteint une charge record de 500 Gbit/s[1]. Si ce débit est hors norme – pour l'instant – il n'en est pas moins le signe d'une tendance inquiétante, car les attaques DDoS deviennent de plus en plus ambitieuses chaque année. Vous devez également déterminer quelle durée d'interruption de service votre entreprise peut se permettre, sachant que le coût horaire moyen des attaques DDoS s'élève à 100 000 USD, selon une enquête menée par le magazine *CIO Insight*.

Si votre entreprise externalise ses services DNS, vous devez exiger de votre prestataire qu'il vous tienne informé de ses performances. Il doit être en mesure de vous garantir une disponibilité permanente pour la résolution DNS. Vous devez également lui demander d'effectuer un audit de vos actifs numériques afin de savoir ce que votre entreprise possède et combien de fournisseurs DNS elle utilise. La multiplication des fournisseurs entraîne confusion et manque d'efficacité et peut aboutir au non-renouvellement de certificats de sécurité, à une mauvaise gestion des actifs, à un nombre excessif d'identifiants à protéger, etc.

Si vous gérez votre propre DNS en interne, il est également judicieux de revoir cette stratégie. La gestion en interne du DNS mobilise du personnel pour la maintenance et de l'argent pour l'équipement, les logiciels et la bande passante. Et le système peut rapidement devenir vulnérable. En interne, il est au mieux difficile de gérer convenablement un DNS compte tenu de la capacité matérielle et de la bande passante nécessaire pour y parvenir. Contactez un fournisseur pour avoir une estimation des économies que vous pourriez réaliser en externalisant le DNS et pour évaluer les gains en termes de sécurité pour votre entreprise.

Professionnels du service informatique

La sécurité informatique est votre priorité, nous le savons

Étape 2 : Formez vos employés et vos clients pour qu'ils sachent détecter les attaques de phishing et créez une adresse e-mail spécifique pour qu'ils vous signalent les cas douteux.

D'après le rapport Phishing Activity Trends[2], le nombre total de sites de phishing uniques détectés du 1er au 3e trimestre 2015 était de 630 494 et rien ne laisse entrevoir un ralentissement. Dans une récente enquête, *Infosecurity Magazine* estime que « 2016 sera l'année de la menace véhiculée par l'homme ». Cette prévision se confirme dans l'enquête Attendee Survey réalisé en 2015 par Black Hat auprès des professionnels de la sécurité, où l'erreur humaine arrive en tête des vulnérabilités de l'entreprise face à la cybercriminalité[3].

Limiter l'erreur humaine est sans doute le remède le plus efficace. Les employés doivent apprendre à connaître les différents types de phishing et être conscients qu'ils concernent autant les ordinateurs de bureau et PC portables que les téléphones mobiles et les tablettes. Vous pouvez ainsi renforcer la sécurité de l'intérieur. Veillez également à ce que vos clients sachent comment vous communiquez avec eux et quelles informations ne doivent jamais être mentionnées dans un e-mail ou à une personne qui les contacte par téléphone (mots de passe, informations de cartes bancaires, etc.). Le meilleur des conseils que vous pouvez leur donner serait, en cas de doute, d'appeler au numéro habituel fourni avec votre abonnement ou votre carte bancaire et de faire vérifier les derniers messages ou appels reçus.

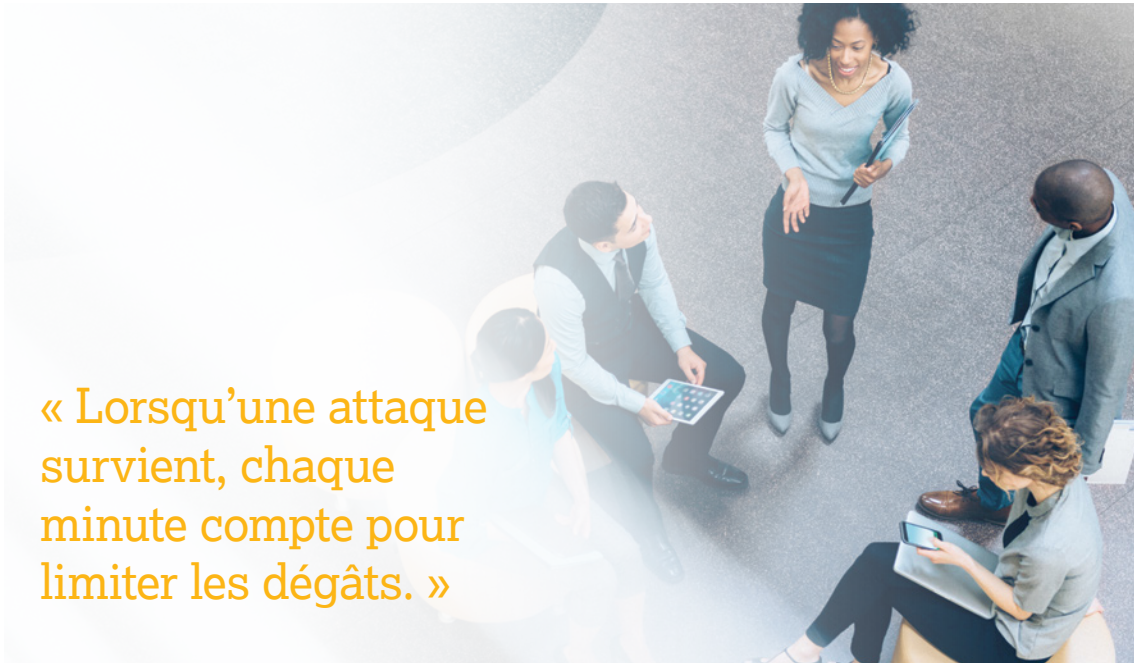
Ensuite, vérifiez que votre solution de lutte contre le phishing convient à votre entreprise et respecte vos contraintes de signalement. En matière de détection, elle doit fournir des leurres du type « honeypots » ou « spam traps », des flux d'informations sur la fraude émis par des tiers de confiance ainsi que des dispositifs de surveillance de marque avec détection d'image. En outre, vous devez demander à votre prestataire de vous fournir des rapports interactifs et flexibles de manière à pouvoir mesurer l'efficacité du programme.

Lorsqu'une attaque survient, chaque minute compte pour limiter les dégâts. Lorsque vous analysez votre solution de lutte contre le phishing, consultez les services marketing et juridique de l'entreprise pour vous assurer qu'elle contient des mesures appropriées pour la défense des droits : neutralisation des sites abusifs, expertise post-incident, dispositifs contre le détournement de marque, retrait de contenus, etc. Cet aspect de la solution peut vous sembler secondaire maintenant, mais il sera d'une importance cruciale pour vos collègues du marketing et du juridique, en particulier en cas d'attaque.

Professionnels du service informatique

La sécurité informatique est votre priorité, nous le savons

Étape 3 : Veillez à protéger vos noms de domaine stratégiques avec des mécanismes de double authentification et de blocage au niveau du registre et du registraire avec autorisation manuelle tripartite. Il s'agit là des méthodes les plus efficaces et les plus rentables pour empêcher le piratage des noms de domaine et toute modification ou suppression sans autorisation. C'est aujourd'hui l'une des fonctions de sécurité les plus ignorées, alors qu'un simple appel téléphonique suffit pour la mettre en place.



« Lorsqu'une attaque survient, chaque minute compte pour limiter les dégâts. »

Avantages de CSC® Digital Brand Services

La sécurité informatique est une préoccupation majeure pour les entreprises. Les cyberattaques ciblent leurs actifs numériques au moyen de techniques adaptatives et elles peuvent rapidement engendrer des problèmes coûteux, aussi bien pour les résultats financiers de l'entreprise que pour son image de marque.

Fort heureusement, les technologies de sécurité évoluent. CSC offre une gamme complète de services de cybersécurité conçus pour vous protéger de ces attaques.

Nous avons conclu un partenariat avec **Verisign®** pour proposer des services de protection contre les attaques DDoS. Les entreprises peuvent ainsi réduire le risque de catastrophe en détectant et en filtrant le trafic malveillant destiné à perturber ou paralyser les services en ligne. Le réseau de Verisign comporte des plates-formes d'analyse de trafic et de détection de premier ordre, avec des mécanismes de mitigation des attaques DDoS répartis dans le monde entier. Il peut ainsi monter en puissance afin de contrer les attaques les plus vastes et les plus complexes.

Nos options d'authentification sophistiquées empêchent tout accès sans autorisation à vos actifs numériques, tandis que nos services de lutte anti-phishing sécurisent la messagerie e-mail de votre entreprise. Nous proposons également des services de certificats numériques et de DNS d'entreprise à la pointe de la technologie pour protéger le point névralgique de votre marque numérique contre les attaques DDoS.

CSC NameProtect® est la première application qui permet de surveiller les noms de domaine, les contenus internet, les médias sociaux, les marques de commerce mondiales et les enregistrements de noms de société sur un seul et même portail. Le système intégré de gestion de dossiers vous aide à organiser vos données avec plus d'efficacité, puisqu'elles sont centralisées et accessibles à plusieurs utilisateurs. L'application permet également de suivre les changements de contenu, de WHOIS et de popularité des sites, ainsi que le changement de statut des dépôts de marque, avec alertes automatisées et fonction d'archivage pour la collecte de preuves. L'application de CSC NameProtect regroupe aussi tous les rapports dont vous et vos collègues pouvez avoir besoin ainsi que des données de veille pour que vous disposiez d'une parfaite vue d'ensemble de vos biens numériques.

CSC Digital Brand Services se fera un plaisir de mener un audit de sécurité de vos actifs afin de déterminer si votre entreprise est vulnérable aux cybermenaces. Pour de plus amples informations sur les prestations que CSC Digital Brand Services peut vous proposer, rendez-vous sur **cscdigitalbrand.services/fr.**

À propos de CSC

CSC Digital Brand Services aide les entreprises à prospérer sur internet. Comptant parmi les principaux registraires de noms de domaine pour les entreprises à l'échelle mondiale, CSC Digital Brand Services est aussi un prestataire de premier plan pour les services liés au programme des nouveaux gTLD de l'ICANN. Nous proposons une suite de services visant à préserver les actifs numériques de nos clients et à faire valoir leurs droits de propriété intellectuelle, notamment des outils de veille sur internet et de défense des droits, et des services dédiés aux marques et aux noms d'utilisateur de réseaux sociaux. Pour préserver et sécuriser les ressources web de nos clients, nous proposons des certificats SSL qui protègent les transactions en ligne, des services DNS d'entreprise, et des services anti-phishing qui neutralisent les attaques par e-mail. Grâce à des outils technologiques de pointe et à un service clientèle réputé pour sa qualité, CSC Digital Brand Services permet aux entreprises de capitaliser sur la valeur de leurs marques, de s'ouvrir à de nouveaux marchés et de contrer les menaces qui apparaissent sur internet.

[1]http://uk.businessinsider.com/john-mcafee-panama-papers-evidence-we-need-better-cybersecurity-2016-4?r=US&IR=T

[2]http://docs.apwg.org/reports/apwg_trends_report_q1-q3_2015.pdf

[3]http://www.infosecurity-magazine.com/industry-insight-trends-2016/

cscdigitalbrand.services/fr