CSC

Le retour sur investissement du DNS : un guide pour réduire les risques et investir intelligemment

Arguments économiques en faveur de la sécurité DNS : coûts, réduction des risques et retour sur investissement

Pour les grandes entreprises, la protection de l'infrastructure du système des noms de domaine (DNS) est un impératif commercial. Les défaillances du DNS peuvent entraîner des temps d'arrêt importants, des risques juridiques et une atteinte à la réputation. Pourtant, la sécurité des domaines est souvent négligée dans les stratégies globales de cybersécurité.

Cet article d'analyse aide les décideurs à élaborer des arguments économiques convaincants en faveur de la sécurité DNS en mettant en évidence les coûts liés aux défaillances et en proposant des moyens concrets de communiquer sur les risques et le retour sur investissement (ROI).

Le coût réel d'une sécurité DNS défaillante

Une défaillance de la sécurité DNS peut entraîner une suite de répercussions qui dépassent largement le temps d'arrêt initial. La perte de revenus pendant une panne est souvent le coût le plus visible, mais les impacts indirects tels que les problèmes de conformité, les frais juridiques et l'atteinte à la réputation peuvent être plus difficiles à quantifier et s'avérer plus coûteux sur le long terme.

Les responsables de la cybersécurité considèrent de plus en plus les menaces liées aux noms de domaine, non plus comme des problèmes techniques isolés, mais comme des risques commerciaux majeurs. Dans le rapport CISO Outlook 2025, 70 % des personnes interrogées s'attendent à une augmentation des menaces de sécurité, et 98 % d'entre elles prévoient une augmentation au cours des trois prochaines années.[1] Face aux menaces croissantes, les organisations doivent donner la priorité aux contrôles fondamentaux qui favorisent la disponibilité, la confiance des clients et la continuité des activités.

> *« J'ai vu des équipes travailler 24 heures sur 24 pour remédier à une panne de DNS, pour se voir ensuite demander pourquoi l'entreprise n'avait pas mis en place des protections plus solides. C'est pourquoi il est important de traiter la sécurité DNS comme un investissement planifié, et non comme une solution apportée a posteriori.*
>
> **Mark Flegg**
> *Directeur principal, Sécurité des produits et des services, CSC*

Coûts directs et indirects : des répercussions croissantes

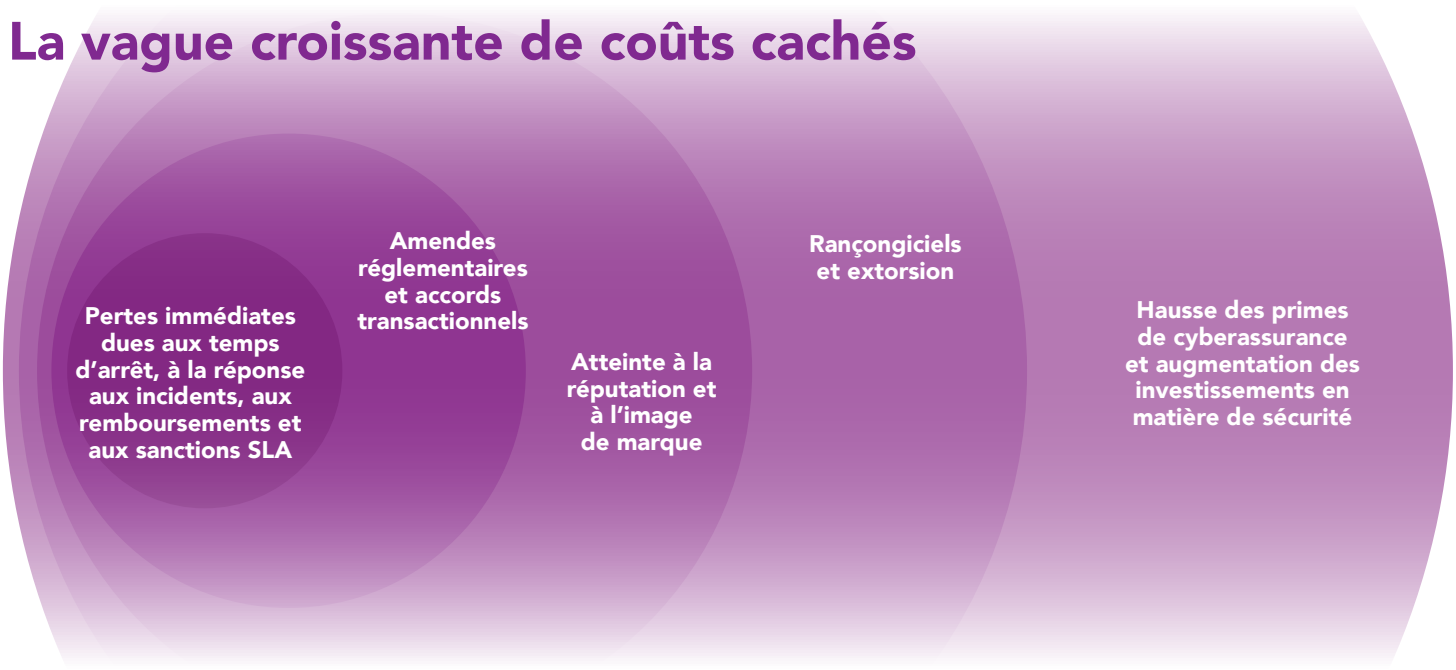
Les coûts directs correspondent aux dépenses immédiates et mesurables suivant une interruption de services essentiels, tels que :

Pertes liées aux temps d'arrêt : interruption des opérations, échec des transactions et perte de clientèle

Assistance informatique d'urgence et gestion des incidents : équipes informatiques internes ou spécialistes externes chargés de diagnostiquer les problèmes et de rétablir les services

Remboursements et sanctions liées à la violation des accords de niveau de service (SLA): compensation due aux clients ou partenaires en raison de violations du SLA

La vague croissante de coûts cachés



Cependant, les coûts directs ne constituent que l'onde de choc initiale de l'impact financier, comme le révèle un rapport de Splunk.[2] Alors que les répercussions se propagent, les coûts indirects, invisibles à première vue, commencent à s'accumuler et peuvent finir par dépasser les dépenses immédiates.

Amendes réglementaires et accords transactionnels : les entreprises qui exercent leurs activités dans des secteurs réglementés peuvent être confrontées à des infractions aux règles de conformité et à des poursuites judiciaires en raison d'interruptions de service ou de violations de données.

Atteinte à la réputation et à l'image de marque : la perte de confiance des clients peut avoir des conséquences à long terme en matière de positionnement sur le marché, de fidélisation de la clientèle et de croissance du chiffre d'affaires. Les organisations peuvent également avoir besoin de rassurer les parties prenantes, de répondre aux préoccupations des investisseurs et de donner de la transparence concernant les mesures prises pour répondre aux incidents.

Rançongiciels ou demandes d'extorsion } : si les attaquants manipulent les paramètres DNS pour rediriger le trafic ou bloquer l'accès, les entreprises peuvent être confrontées à des tentatives d'extorsion financière.

Augmentation des primes de cyberassurance et augmentation des investissements en matière de sécurité : une défaillance du DNS, en particulier celle impliquant une faille de sécurité, peut entraîner une augmentation des coûts d'assurance, les assureurs évaluant une exposition accrue aux risques.

Viser une disponibilité de « cinq neuf » (99,999 %), mais poser des questions plus pertinentes

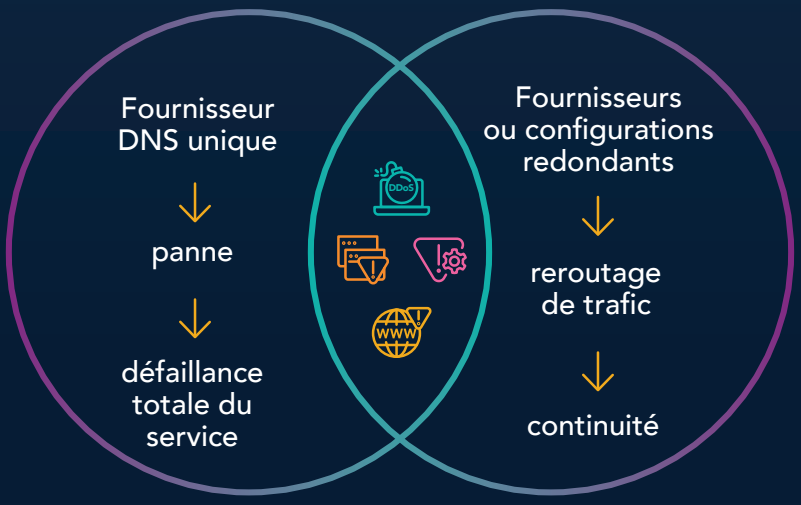
Pour les entreprises, les attentes en matière de disponibilité sont élevées. Le principe des « cinq neuf », soit 99,999 % de disponibilité, se traduit par moins de cinq minutes de temps d'arrêt par an. De nombreuses organisations considèrent cet objectif comme une référence en matière de fiabilité, mais les engagements relatifs au service DNS varient selon le fournisseur et le niveau de service. Dans la pratique, les antécédents réels d'un fournisseur, en particulier en cas de tension ou d'attaque, sont souvent un meilleur indicateur que les objectifs théoriques de disponibilité.

De nombreuses entreprises s'appuient désormais sur une infrastructure basée sur le cloud et des plateformes tierces pour prendre en charge les services destinés aux clients, les applications internes et les processus métier essentiels. Si ces fournisseurs peuvent améliorer l'évolutivité et les performances, ils peuvent également introduire des risques pour les opérations, en particulier lorsque la disponibilité dépend d'un seul fournisseur, d'une seule région ou d'une seule configuration. La planification de la résilience du DNS doit inclure des stratégies de redondance conçues pour maintenir la disponibilité en cas de pannes, d'erreurs de configuration ou de dégradation en amont.

> *« Dans tout autre aspect, les entreprises prennent des dispositions pour faire face aux pannes : déploiement dans plusieurs régions, sauvegardes, systèmes de basculement. Mais trop souvent, le DNS est encore considéré comme « suffisant » avec un seul fournisseur ou une seule configuration. C'est là une présomption risquée pour un élément dont dépendent tous les services numériques.*
>
> **Mark Flegg**
> *Directeur principal, Sécurité des produits et des services, CSC*

Risque DNS lié à un point de défaillance unique ou architecture DNS résiliente

Ensemble, ces risques montrent pourquoi la sécurité DNS doit être considérée comme un élément central de la réduction des risques de l'entreprise, et non comme une considération secondaire en matière d'informatique. En outre, le rapport CISO Outlook 2025 indique que les responsables de la sécurité des systèmes d'information (RSSI) classent le détournement de domaine et de DNS parmi les principales menaces attendues au cours des trois prochaines années.[3]



Le DNS joue un rôle fondamental dans la disponibilité des sites Web, des e-mails et des applications internes, mais il est souvent insuffisamment protégé. Les risques sont loin d'être mineurs :

Attaques par déni de service distribué (DDoS) : des acteurs malveillants visent l'infrastructure DNS avec des attaques à gros volume, saturant les serveurs et provoquant des pannes.

Pannes de fournisseur : les entreprises qui s'appuient sur un seul fournisseur DNS risquent une défaillance complète si ce fournisseur subit des temps d'arrêt.

Erreurs de configuration : de simples erreurs de configuration, telles que des modifications inappropriées des enregistrements DNS, peuvent interrompre la totalité des services.

Détournement de domaines : des modifications non autorisées au niveau du registrar peuvent rediriger le trafic, ce qui entraîne des risques pour la réputation et la sécurité.

Quantifier le coût d'une défaillance DNS

Pour les entreprises qui cherchent à évaluer et à communiquer l'impact financier des risques liés à la sécurité DNS, la formule de perte annuelle attendue (Annualized Loss Expectancy ou ALE) offre une approche structurée pour quantifier les pertes potentielles. Cette méthodologie aide les responsables de la cybersécurité à traduire les risques techniques en termes financiers liés à l'activité, ce qui facilite la justification d'investissements proactifs dans la sécurité DNS.

Définition de la formule ALE :

SLE × ARO = ALE

Perte unique attendue (Single loss expectancy ou SLE) : l'impact financier d'une défaillance DNS unique, y compris les coûts directs (et, si possible, indirects).

Taux annuel d'occurrence (Annual rate of occurrence (ARO) : le nombre estimé de fois qu'un tel incident devrait se produire au cours d'une année.

Perte annuelle attendue (Annualized loss expectancy ou ALE) : la perte financière annuelle prévue en raison de défaillances de sécurité DNS.

En calculant le SLE et l'ARO à partir du profil de risque d'une organisation, les entreprises peuvent établir leur ALE, un indicateur concret permettant de mesurer l'exposition financière potentielle et de justifier les investissements préventifs dans la sécurité DNS.

« De nombreuses organisations ont du mal à quantifier le coût des menaces liées au DNS, ce qui rend les investissements en matière de sécurité plus difficiles à justifier. La formule ALE offre un modèle pratique pour évaluer le risque financier, aidant ainsi les décideurs à prendre conscience de l'impact commercial d'une sécurité DNS proactive.

Mark Eggleston
RSSI, CSC

Communiquer la valeur commerciale de la sécurité DNS

Malgré une prise de conscience croissante des menaces liées aux domaines, de nombreuses organisations estiment ne pas être encore suffisamment préparées. Dans le rapport CISO Outlook 2025, seules 22 % des personnes interrogées affirment disposer des outils adéquats pour faire face aux menaces liées aux domaines.[4] C'est précisément sur cet écart entre le risque et l'état de préparation que les initiatives DNS axées sur le retour sur investissement peuvent se montrer les plus convaincantes.

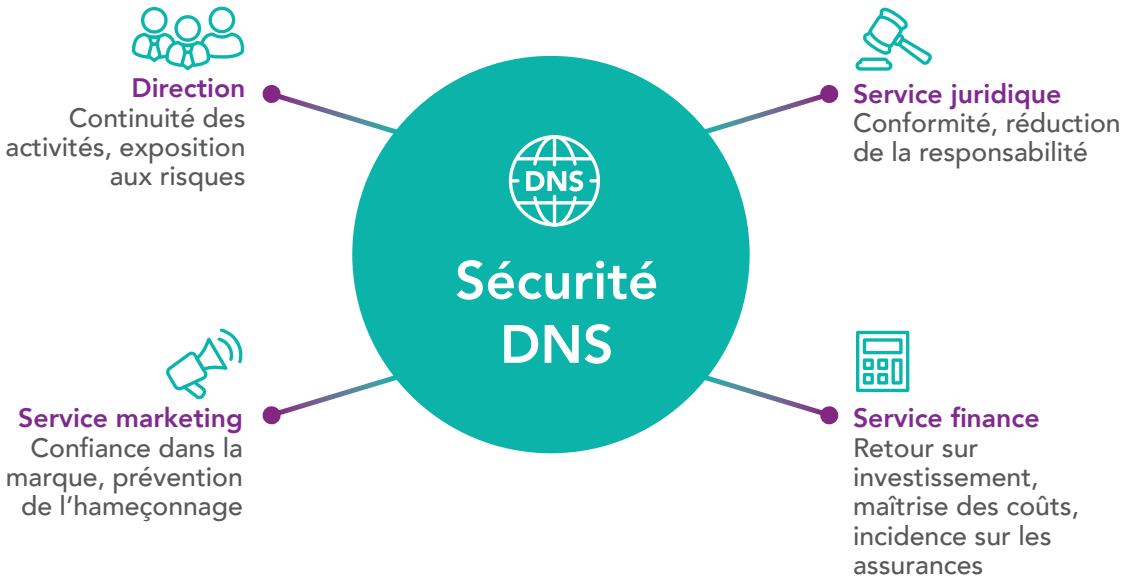
Pour obtenir le financement nécessaire, les responsables de la cybersécurité doivent traduire les risques liés au DNS en impact commercial en établissant un lien entre la sécurité des domaines et la disponibilité, la confiance des clients, l'exposition aux risques de non-conformité et la résilience opérationnelle.

> *« Le DNS n'a pas été conçu pour faire face aux menaces actuelles, mais il demeure le système indispensable pour assurer une navigation sécurisée des clients, des collaborateurs et des partenaires vers les sites appropriés. C'est pourquoi la sécurité DNS mérite le même niveau d'attention que les autres contrôles essentiels.*

Mark Flegg
Directeur principal, Sécurité des produits et des services, CSC

Comprendre votre public : adapter le message

Pour obtenir l'engagement d'investir dans la sécurité DNS, les responsables de la cybersécurité doivent aligner leurs messages sur les priorités des différentes parties prenantes. Si les équipes de sécurité se préoccupent principalement des risques techniques, d'autres services auront pour priorité des objectifs commerciaux, des préoccupations financières et des défis opérationnels. Présenter la sécurité DNS sous l'angle de l'intérêt propre de chaque équipe permettra d'augmenter les chances d'obtenir leur soutien.



Direction : l'impact de la sécurité DNS sur l'activité de l'entreprise

La direction se concentre sur les performances financières, la gestion des risques et le positionnement sur le marché par rapport à la concurrence. Le DNS étant essentiel à la disponibilité des systèmes, il est également au cœur de la continuité des activités et de la reprise après sinistre : deux priorités absolues pour les dirigeants. Le DNS étant essentiel à la disponibilité des systèmes, il est également au cœur de la continuité des activités et de la reprise après sinistre : deux priorités absolues pour les dirigeants.

> *« Les membres du conseil d'administration ne s'intéressent pas au DNS : ils se soucient de la protection de la marque et des risques de cybersécurité. Évitez les détails techniques et présentez le sujet en termes économiques. Pour vous faire une idée, consultez la manière dont la cybersécurité est abordée dans des publications telles que The Wall Street Journal.*
>
> **Mark Eggleston**
> *RSSI, CSC*

Service juridique : conformité réglementaire et réduction de la responsabilité

Les équipes juridiques de l'entreprise accordent la priorité au respect des réglementations du secteur et à la réduction de l'exposition à la responsabilité. De nombreux cadres réglementaires en matière de confidentialité et de sécurité des données, notamment le Règlement général sur la protection des données (RGPD), la Loi californienne sur la protection de la vie privée des consommateurs (CCPA) et la Directive sur la sécurité des réseaux et de l'information (NIS2), exigent des contrôles de sécurité rigoureux pour protéger les informations sensibles. Sans une sécurité DNS adéquate, les entreprises s'exposent à des violations de données, des incidents d'hameçonnage et des transferts de domaine non autorisés, qui peuvent tous entraîner des poursuites judiciaires ou des sanctions.

Service marketing : protection de la réputation et prévention du hameçonnage

Les équipes marketing sont responsables de la réputation de la marque, de la confiance des clients et de l'engagement numérique, autant d'éléments qui peuvent être compromis par des menaces liées au DNS. En présentant la sécurité DNS comme une stratégie de protection de la marque plutôt qu'un simple enjeu informatique, vous la rendez plus pertinente pour ce public.

> *« La sécurité des domaines va au-delà des préoccupations traditionnelles en matière de cybersécurité ; il s'agit de protéger l'ensemble de l'écosystème numérique contre les sites frauduleux. Les RSSI peuvent considérer cet aspect comme un risque secondaire, mais c'est une priorité absolue pour le marketing et l'image de marque.*
>
> **Mark Eggleston**
> *RSSI, CSC*

Service finance et achats : rentabilité, retour sur investissement et avantages en matière d'assurance

Les responsables financiers et les équipes d'achat évaluent les investissements en fonction du coût, de l'efficacité et d'un retour sur investissement mesurable. Puiser des exemples concrets dans l'actualité est un moyen efficace de démontrer l'impact financier des risques liés à la sécurité des domaines. Il suffit parfois d'une simple action, comme le partage d'un lien vers le récit d'un incident récent, pour aider les équipes financières à prendre conscience des conséquences tangibles d'un sous-investissement. Une bonne protection DNS peut également réduire le taux d'interruption des activités, contribuant ainsi à la stabilité financière.

Au lieu de formuler le problème comme une mesure de protection technique, présentez la sécurité DNS comme un élément qui contribue à la réussite de l'entreprise. Vous obtiendrez ainsi un soutien plus large au sein de l'organisation et l'assurance que la protection DNS sera considérée comme une priorité stratégique.

Prouver le retour sur investissement : développer des arguments économiques convaincants en faveur d'une sécurité DNS proactive

Pour obtenir des investissements dans la sécurité DNS, il ne suffit pas de mettre en avant les risques ; il faut également démontrer des avantages financiers et opérationnels mesurables. Les RSSI et les responsables de la cybersécurité doivent traduire les préoccupations en matière de sécurité en une valeur ajoutée claire pour l'entreprise, en montrant comment l'investissement dans la sécurité DNS permet de réduire les coûts, de rationaliser les opérations et de minimiser les risques financiers.

Les budgets consacrés à la sécurité n'augmentent pas toujours au même rythme que les cyberrisques. Dans le rapport CISO Outlook 2025, seules 7 % des personnes interrogées font état d'une augmentation significative de leur budget entre 2024 et 2025, tandis que 80 % signalent une augmentation modérée.[5]

Dans cet environnement, les investissements DNS doivent démontrer une réduction mesurable des risques et une résilience des opérations.

Réduire les coûts grâce à la réduction des risques et à l'efficacité

Une stratégie de sécurité DNS solide contribue à une réduction plus large des cyberrisques, ce qui peut aider les organisations à conserver une bonne réputation auprès des assureurs et à s'aligner sur les cadres de sécurité largement acceptés. Bien que les polices de cyberassurance n'offrent généralement pas de remises spécifiques au DNS, le renforcement des protections des domaines témoigne d'une bonne pratique informatique et réduit les menaces.

Les organisations privilégient également les méthodes reproductibles et évolutives, en particulier lorsque la rapidité de réponse est cruciale. Dans le rapport CISO Outlook 2025, 50 % des personnes interrogées affirment avoir développé et testé régulièrement des plans de réponse aux incidents, et 50 % déclarent utiliser une solution de surveillance et d'application basée sur l'IA.[6] La sécurité DNS s'inscrit dans cette évolution vers la maturité opérationnelle en améliorant la visibilité, en accélérant les mesures de réduction des risques et en renforçant la continuité en cas de dysfonctionnement.

Qu'il s'agisse de la gestion des configurations DNS, de la surveillance des menaces émergentes ou de la réponse aux incidents, l'automatisation joue un rôle essentiel dans la réduction de la charge de travail manuel liée aux opérations de sécurité des domaines. Elle revêt également une importance croissante pour la gestion des certificats numériques : avec le raccourcissement des cycles de vie des certificats résultant des changements du CA/Browser Forum jusqu'en 2029, les organisations pourraient devoir renouveler leurs certificats SSL (Secure Sockets Layer) et TLS (Transport Layer Security) beaucoup plus fréquemment, avec une moyenne de huit renouvellements par an à l'avenir. Cette évolution rendra l'automatisation des workflows de renouvellement indispensable pour éviter les expirations et les interruptions de service.

Utiliser des modèles financiers pour quantifier le risque DNS

Les dirigeants et les équipes financières réagissent mieux à une prise de décision fondée sur les données. Les modèles de quantification des risques cyber (CRQ), tels que l'équation de la perte annuelle attendue ou le cadre d'analyse factorielle des risques liés à l'information (FAIR™), aident les organisations à estimer les pertes financières potentielles résultant d'attaques liées au DNS, de temps d'arrêt ou d'incidents de détournement de DNS. En appliquant ces modèles, les responsables de la cybersécurité peuvent présenter des chiffres concrets qui démontrent comment un investissement proactif empêche des pertes financières beaucoup plus importantes.

La réalisation d'évaluations des risques fondées sur des scénarios est une autre façon d'illustrer les interruptions potentielles de l'activité et l'impact financier causé par les défaillances du DNS. En modélisant des scénarios d'attaque réels, les organisations peuvent visualiser les coûts cachés d'une stratégie de sécurité DNS insuffisante.

Renforcer le renseignement sur les menaces et la hiérarchisation des risques

Pour garder une longueur d'avance sur les menaces en constante évolution, il est nécessaire de disposer d'une visibilité continue sur les risques potentiels. Les organisations qui rejoignent des groupes de partage d'informations spécifiques au secteur, tels que le Conseil national des centres de partage et d'analyse de l'information (ISACs), reçoivent des alertes précoces et des informations sur les attaques émergentes liées au DNS.

De plus, la mise en place d'une gestion continue de l'exposition aux menaces permet aux équipes de sécurité de donner la priorité aux vulnérabilités DNS les plus urgentes, garantissant ainsi une allocation efficace des ressources afin d'atténuer les scénarios présentant le plus grand risque avant qu'ils ne s'aggravent.

Mesurer les économies réalisées grâce à notre calculateur de coûts DNS

Comprendre les avantages financiers de la sécurité DNS nécessite une modélisation claire des coûts. Le calculateur de coûts DNS interne ci-dessous propose une formule destinée à aider les entreprises à estimer le coût réel des temps d'arrêt DNS, en tenant compte de variables telles que les transactions perdues, les coûts de remédiation et les interruptions opérationnelles.

> *« Vous n'avez pas besoin d'un modèle complexe pour estimer la valeur de la sécurité DNS. Une fois que vous avez établi le lien entre les temps d'arrêt DNS et leur impact réel sur l'activité (perte de productivité, transactions perdues et temps de reprise), le retour sur investissement devient beaucoup plus facile à justifier.*

Mark Flegg
Directeur principal, Sécurité des produits et des services, CSC

Calculateur de coûts DNS	Données
Effectif nécessaire pour gérer le DNS	2
Salaire annuel par membre du personnel	75 000 $
Coût des avantages sociaux ~ 30 % des frais de personnel	45 000 $
Coûts annuels en matériel, logiciels et bande passante	40 000 $
Coût total d'exploitation du DNS interne	**160 000 $**
Coût proposé du service DNS externe	50 000 $
Économies totales réalisées grâce à l'usage d'un service DNS externe	**110 000 $**

Remarque : les chiffres indiqués sont donnés à titre d'exemple.

En présentant, preuves à l'appui, des économies quantifiables, des gains d'efficacité opérationnelle et une réduction de l'exposition financière, les responsables de la cybersécurité peuvent élaborer une analyse de rentabilité convaincante en faveur d'un investissement dans la sécurité DNS, qui répond directement aux priorités des dirigeants, des équipes financières et des gestionnaires des risques.

Considérer la sécurité DNS comme une priorité stratégique

La sécurité DNS est un élément essentiel, mais souvent négligé, de la stratégie de cybersécurité d'une organisation. Comme l'a montré ce rapport, le coût des défaillances de sécurité DNS ne se limite pas aux temps d'arrêt, mais inclut également les pertes financières, les sanctions réglementaires et l'atteinte à la réputation.

Au-delà de la mise en œuvre de contrôles techniques, les RSSI et les responsables de la sécurité doivent communiquer sur la sécurité DNS en termes économiques. En adaptant leur message aux priorités de la direction, en quantifiant les risques et en démontrant le retour sur investissement, les organisations peuvent obtenir les investissements nécessaires pour protéger leurs actifs numériques.

Prendre dès maintenant des mesures proactives pour renforcer la sécurité DNS peut prévenir des incidents coûteux à l'avenir. **Contactez CSC aujourd'hui pour discuter d'une solution sur mesure afin de protéger votre organisation.**

cscdbs.com

« Voici comment obtenir en trois points l'adhésion des dirigeants en matière de cybersécurité :

1. Tisser des liens : identifiez les priorités des dirigeants et adoptez une approche cohérente et stratégique.
2. Parlez leur langage : présentez la cybersécurité comme un enjeu de gouvernance. Utilisez des guidelines comme celles de la National Association of Corporate Directors (NACD).
3. Montrer les progrès réalisés : utilisez des tableaux de bord ou d'autres supports visuels clairs pour illustrer l'impact des investissements en sécurité.

Mark Eggleston
RSSI, CSC

Discutons

1 800 927 9800 | cscdbs.com

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 domaines 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 DomainSec℠ peut les aider à identifier leurs failles en matière de cybersécurité et leur permettre de protéger leurs actifs numériques et leurs marques 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. CSC propose également une protection de la marque en ligne (une combinaison de la surveillance de la marque en ligne et des activités de remédiation) et une vue multidimensionnelle des différentes menaces à l'extérieur du pare-feu ciblant des noms de domaine spécifiques. Des services de protection contre la fraude, qui luttent contre l'hameçonnage dès les premiers stades de l'attaque, viennent compléter 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. Visitez cscdbs.com.

[1]CSC, The CISO Outlook 2025, 2025, https://www.cscdbs.com/en/resources/2025-ciso-cybersecurity-outlook-report/.
[2]Splunk, The Hidden Costs of Downtime, 2024, https://www.splunk.com/en_us/form/the-hidden-costs-of-downtime.html.
[3]CSC, The CISO Outlook 2025.
[4]CSC, The CISO Outlook 2025.
[5]CSC, The CISO Outlook 2025.
[6]CSC, The CISO Outlook 2025.

DBS03112026