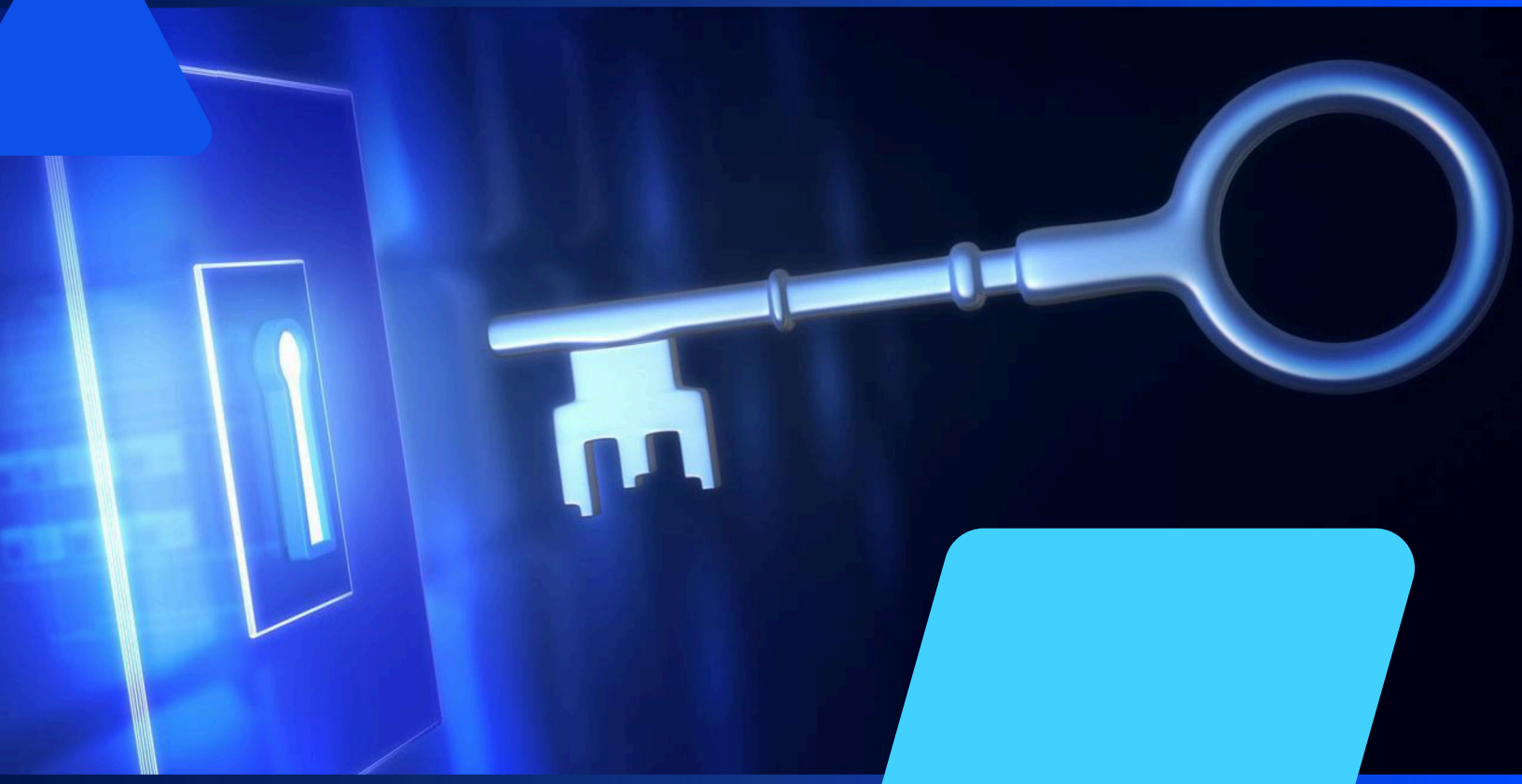
Verrouillage de registre :

Trop négligé, trop peu utilisé, mais essentiel pour la sécurité de votre nom de domaine



Markmonitor™

Rencontre :
Bonnie Wittenburg, responsable de la stratégie commerciale

Avec près de 30 ans d'expérience dans le secteur, Bonnie a conseillé certaines des plus grandes marques au monde pour élaborer des stratégies solides de gestion des noms de domaine. Elle est spécialisée dans la gestion des complexités propres aux organisations internationales, dans la rationalisation des portefeuilles, en vue de réaliser des économies et dans la simplification des processus.

Son expertise consiste à répondre aux besoins complexes d'organisations diverses et multipartites en élaborant des stratégies sur mesure qui concilient protection et contraintes budgétaires. Markmonitor a le privilège de compter Bonnie dans son équipe de direction en tant que responsable de la stratégie commerciale.

La défense négligée qui mérite toute votre attention

On me demande souvent des conseils et des idées que les gestionnaires de noms de domaine peuvent utiliser pour renforcer la sécurité de leur portefeuille.
Ma recommandation : **le verrouillage du registre. Il s'agit d'une mesure de sécurité souvent sous-utilisée et pourtant d'une importance vitale pour protéger la présence numérique d'une entreprise.**

Avec un verrouillage de registre, votre bureau d'enregistrement travaille directement avec le registre afin de bloquer les modifications non autorisées, telles que les mises à jour de serveurs de noms, les modifications de coordonnées ou les transferts de noms de domaine, à moins qu'une vérification et une approbation appropriées n'aient été effectuées. Ce processus permet de protéger vos noms de domaine critiques contre les erreurs, les attaques et les activités non autorisées.

Les verrous de registre constituent une protection efficace contre le détournement de nom de domaine, la manipulation du DNS et les transferts non autorisés. Pourtant, il est surprenant de constater que l'adoption reste relativement faible dans de nombreux portefeuilles. En réalité, moins de la moitié des 500 plus grandes marques sécurisent leurs noms de domaine clés avec un verrouillage au niveau du registre [1].

Cela m'a amené à faire quelques recherches pour découvrir pourquoi, si les verrouillages au niveau du registre sont si bien considérés comme un mécanisme de protection solide, les entreprises ne les prennent pas en considération. Voici ce que j'ai découvert :

OBSTACLES À L'ADOPTION

Manque de sensibilisation
De nombreuses organisations ne se rendent tout simplement pas compte de la vulnérabilité de leurs noms de domaine ou de l'existence même des verrous de registre. Elles partent souvent du principe que les verrous de registre standard ou l'authentification à deux facteurs sont suffisants.

1. Brand Finance, Global 500 2024

La défense négligée qui mérite toute votre attention

Les services de sécurité et d'informatique peuvent se concentrer sur la protection des points de terminaison, les pare-feu ou la sécurité cloud, laissant de côté la sécurité des noms de domaine. Souvent, cela ne fait pas partie des audits de sécurité standard, sauf s'il y a déjà eu un incident, une façon douloureuse de comprendre que la sécurité des noms de domaine devrait être prioritaire.

Exemple : un travailleur négligent tombe dans le piège d'un e-mail de phishing en pensant qu'il provient de son bureau d'enregistrement. Il se connecte, divulguant sans le savoir ses informations d'identification. Le pirate a désormais accès au nom de domaine et peut en modifier les paramètres, le transférer ou même rediriger le trafic vers un site malveillant. Un verrou de registre aurait empêché ces modifications non autorisées au niveau du registre. Disposer d'un bureau d'enregistrement de confiance et d'un verrou de registre est un excellent moyen d'éviter de tels résultats désastreux.

Pas de normalisation industrielle

Tous les TLD ou bureaux d'enregistrement ne prennent pas en charge les verrous de registre ; ou s'ils le font, ils peuvent les mettre en œuvre différemment. Cette incohérence rend difficile le déploiement d'une politique universelle de protection des noms de domaine et souligne l'importance cruciale d'un bureau d'enregistrement des noms de domaine d'entreprise dans la compréhension et la mise en œuvre de telles protections, le cas échéant.

Exemple : un nom de domaine .COM implique le registre (par exemple Verisign) dans un mélange de processus automatisés et manuels, avec une authentification à plusieurs facteurs pour les modifications. Le propriétaire du nom de domaine, son bureau d'enregistrement et Verisign collaborent via une triple authentification pour autoriser le changement. Dans le cas d'un nom de domaine .UK, le registre (par exemple Nominet) utilise une méthode appelée « Registry Lock Service ». Il s'agit d'un processus plus manuel que le .COM, qui nécessite des mots de passe sécurisés et une vérification manuelle des mises à jour. Un bureau d'enregistrement d'entreprise de confiance comme Markmonitor aide les organisations à comprendre ces différents processus et leur fournit des conseils et une assistance lors de la mise en œuvre.

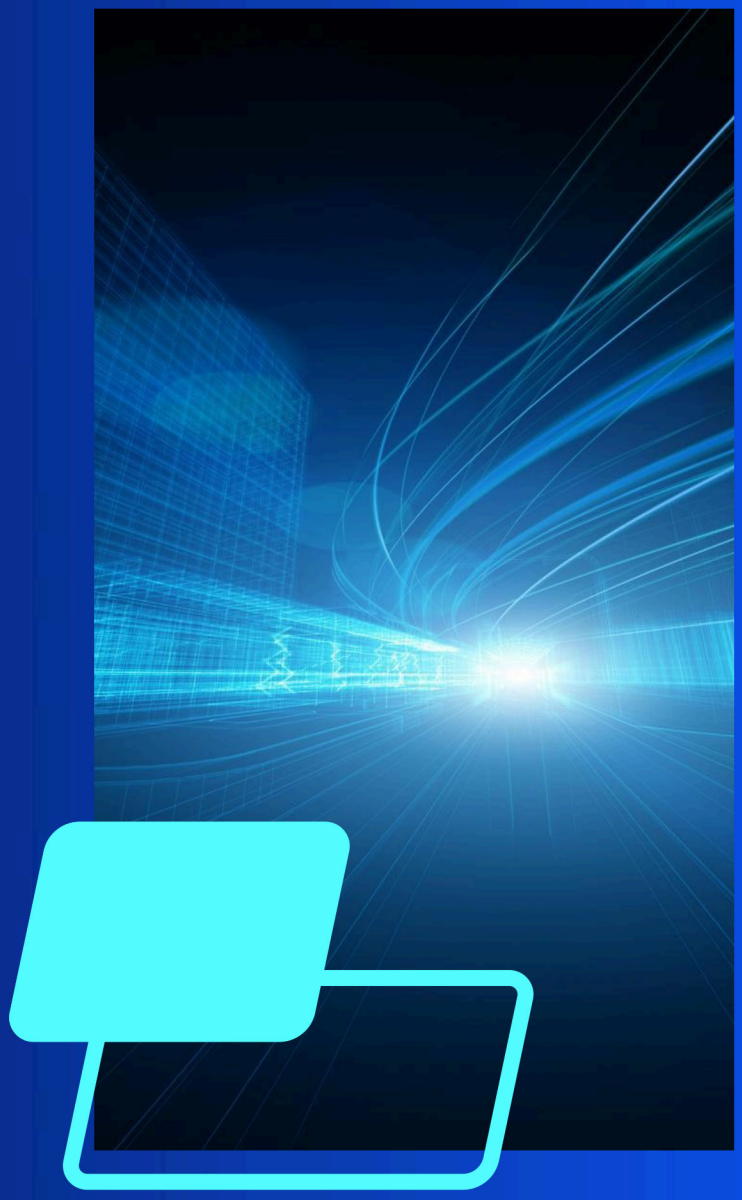
> “...l'incohérence rend difficile le déploiement d'une politique universelle de protection des noms de domaine et souligne l'importance cruciale d'un bureau d'enregistrement des noms de domaine d'entreprise.”

La défense négligée qui mérite toute votre attention

Complexité et inconvénients
Les verrous de registre nécessitent souvent un processus plutôt manuel lorsque des modifications doivent être apportées à un nom de domaine particulier. Ces processus impliquent généralement le bureau d'enregistrement et le registre, nécessitant parfois des appels téléphoniques, des demandes signées ou une autorisation multipartite.

C'est excellent pour la sécurité, mais frustrant pour les équipes informatiques qui ont besoin d'agilité. Pour les domaines qui nécessitent des mises à jour fréquentes (par exemple, des modifications DNS ou des informations de contact), la contrainte supplémentaire liée au déverrouillage et au reverrouillage peut sembler pesante, en particulier si le domaine n'est pas perçu comme essentiel à l'activité. Cependant, le fait même que ces verrous exigent une main-d'œuvre et un support supplémentaires de la part de votre bureau d'enregistrement et du registre constitue précisément la raison de leur existence et de leur efficacité.

Exemple : vous souvenez-vous de notre exemple de l'employé imprudent qui s'est fait piéger par un e-mail de phishing et qui a partagé par inadvertance ses identifiants de connexion avec un cybercriminel ? Le cybercriminel ne pourra pas modifier les noms de domaine dont le registre est verrouillé.



Les vérifications et équilibres fournis par le processus de verrouillage au niveau du registre déjouent les tentatives des cybercriminels de tirer parti du phishing.

La défense négligée qui mérite toute votre attention

Contraintes liées aux coûts et aux ressources
Les verrous de registre sont généralement payants et les petites entreprises peuvent ne pas disposer du budget nécessaire. Le coût supplémentaire peut sembler injustifiable, surtout si les dirigeants ne sont pas pleinement conscients des risques. Mais un seul incident peut coûter beaucoup plus cher à l'entreprise en termes de perte de revenus et d'atteinte grave à l'image de marque. Mieux vaut prévenir que guérir !

Exemple : estimant qu'il s'agit d'une dépense inutile, une entreprise n'achète pas de verrou de registre pour un nom de domaine pourtant essentiel à son activité. Puis, la catastrophe survient : un détournement de domaine met hors service leur site principal, paralysant leurs revenus et leur réputation. Les économies réalisées disparaissent au fur et à mesure que le coût réel de l'absence de verrou se révèle.

UN OUTIL ENCORE IMPORTANT ET SOUVENT NÉGLIGÉ

Malgré certains obstacles, les verrous de registre sont essentiels pour les domaines à forte valeur comme les banques, les portails gouvernementaux, les prestataires de santé, ou toute marque dont le nom de domaine est lié à la confiance et à la disponibilité. Un simple détournement peut conduire au phishing, à des violations de données ou à des atteintes massives à la réputation.

> Un seul incident peut coûter beaucoup plus cher à l'entreprise en termes de perte de revenus et d'atteinte grave à l'image de marque.

La tendance s'inverse
La bonne nouvelle ? L'adoption est en hausse, en particulier parmi les entreprises et les marques soucieuses de la sécurité. **Alors que les détournements de DNS et les attaques au niveau des bureaux d'enregistrement se multiplient, la sensibilisation à cet outil simple mais efficace augmente également ; de plus en plus d'entreprises reconnaissent que les verrouillages de registre ne sont pas seulement une bonne pratique, ils sont une nécessité.**

Si vous gérez un portefeuille de noms de domaine, en particulier pour une marque exposée au public ou à haut risque, Markmonitor sera ravi de vous accompagner dans la mise en place efficace de verrouillages au niveau du registre.

Markmonitor fournit des solutions stratégiques de gestion des noms de domaine qui contribuent à protéger les revenus et la réputation des plus grandes marques mondiales.

Depuis 1999, Markmonitor répond aux besoins des entreprises du monde entier en matière de portefeuilles de domaines, y compris de nombreux sites Web parmi les plus visités au monde. En tant que bureau d'enregistrement de noms de domaines accrédité par l'ICANN depuis sa création, Markmonitor tire parti de ses relations étendues avec l'industrie, de sa technologie innovante et de sa vaste expertise pour gérer et protéger les portefeuilles de domaines des entreprises, le tout avec une consultation haut de gamme basée sur les données et conçue pour maximiser la valeur des portefeuilles de domaines.

Si vous avez besoin de plus d'informations ou d'aide, veuillez contacter votre responsable de compte ou envoyer un e-mail à customer.service@markmonitor.com

Markmonitor™