LIVRE BLANC

Limitez les risques de violation grâce à la surveillance de l'intégrité des fichiers, afin d'assurer la sécurité des données et la conformité à la norme PCI DSS

La fonctionnalité la plus importante de tout programme de sécurité informatique est sa capacité à détecter rapidement les violations de données et à y remédier sans délai. Pourtant, chaque jour, des données sensibles sont consultées sans même que les entreprises auxquelles elles appartiennent s'en rendent compte. Que la violation résulte d'une attaque ciblée perpétrée par des cybercriminels ou d'une erreur commise par un utilisateur privilégié, l'impact est absolument désastreux. Lorsque la violation passe inaperçue pendant une période prolongée, l'impact peut très vite prendre des proportions incalculables.

Le présent document traite de l'importance du processus de surveillance de l'intégrité des fichiers, qui a pour but de permettre la détection des attaques de cybercriminels, ainsi que des menaces internes. En effet, les conséquences de telles violations de données peuvent être très coûteuses. Le document aborde aussi la surveillance de l'intégrité des fichiers en tant que facteur clé pour assurer la conformité à la norme de sécurité informatique des données de l'industrie des cartes de paiement (PCI-DSS). En outre, la gamme de produits NetIQ de gestion des identités et de la sécurité sera présentée, ainsi que son importance dans l'optimisation de la sécurité et de la conformité.

NetIQ

NetIQ | LIVRE BLANC

Table des matières

Introduction 1

La surveillance de l'intégrité des fichiers : une pièce maîtresse dans le puzzle de la sécurité 1

- Perspective sur la menace interne 2
- Cyberattaques motivées par l'appât du gain 2
- Prendre les cybercriminels sur le fait 2
- Combattre les menaces internes et externes 3

Cas de conformité d'entreprise : PCI DSS 3

Gérer la surveillance de l'intégrité des fichiers à des fins de sécurité et de conformité :

- NetIQ Change Guardian 4
- Collaborer : Solutions NetIQ de gestion des identités et de la sécurité 4

Conclusion 5

À propos de NetIQ 5

Introduction

Nous vivons une époque où l'adage « on n'est jamais trop prudent » s'applique parfaitement. Malgré la sensibilisation croissante et la mise en oeuvre de mesures de sécurité et de protection, des affaires de violations de données continuent à faire la une de la presse spécialisée. Les chiffres sont alarmants : 143 millions d'enregistrements ont été compromis en 2009, après une série de six années pendant lesquelles le nombre d'attaques de ce genre a dépassé les 900 millions.[1] Encore plus inquiétant : ces violations ont eu lieu au nez et à la barbe des équipes chargées de la sécurité des informations, comme en témoigne l'affaire Heartland Payment Systems (une violation portant sur environ 100 millions de comptes de cartes de crédit est passée inaperçue pendant 18 mois).[2]

La surveillance de l'intégrité des fichiers : une pièce maîtresse dans le puzzle de la sécurité

La surveillance de l'intégrité des fichiers est devenue une pièce maîtresse du puzzle de la sécurité. En effet, les menaces envers les données sensibles des entreprises se caractérisent par une redoutable capacité à évoluer rapidement. Une nouvelle classe d'attaques s'est récemment développée, fomentées par des groupes organisés de criminels qui parviennent systématiquement et méthodiquement à obtenir l'accès aux systèmes en restant indétectables pendant une durée prolongée, ce qui leur permet d'atteindre leurs objectifs, qui vont généralement au-delà du gain financier immédiat. Ce scénario constitue une « menace persistante avancée » (Advanced Persistent Threat - APT) et se manifeste souvent par des violations exploitant des relations de confiance, en passant par exemple par des comptes légitimes, pour accéder et compromettre les systèmes ciblés. Des couches supplémentaires de protection, y compris des solutions de surveillance de l'intégrité des fichiers, doivent être mises en place pour protéger les données sensibles contre ce type de menace.

Selon le rapport publié en 2010 sur les violations de données par Verizon Business, en collaboration avec les services secrets américains[3], 48 % des infractions impliquaient du personnel interne, ce qui représente une augmentation considérable de 26 % par rapport à 2008. Dans la plupart des cas, l'élément précurseur des infractions les plus importantes a été identifié : il s'agissait de privilèges importants accordés à des membres du personnel. La portée du concept de menace interne augmente exponentiellement puisque, quand l'attaquant a pénétré le système (par exemple en utilisant un logiciel malveillant), il est presque impossible de le distinguer d'un membre du personnel.

Selon le rapport de Verizon, dans de nombreux cas, un pirate informatique pénètre dans le réseau de la victime (par exemple par le biais de références d'identification volées ou faibles) et installe des logiciels malveillants sur les systèmes afin de subtiliser des données. Bien que l'utilisation de logiciels malveillants personnalisés au cours de ces attaques n'ait pas progressée, ces logiciels sont devenus de plus en plus difficiles à détecter, ce qui leur permet de contourner avec succès les contrôles standard. En l'occurrence, un logiciel malveillant personnalisé a effectivement été utilisé dans le cas de Heartland, ainsi que dans d'autres affaires importantes de violation de cartes de crédit.

D'après, Forrester Research[4], la meilleure façon de réduire le risque de ce type d'attaques consiste à déployer des outils de surveillance de l'intégrité des fichiers qui fournissent des alertes immédiates si un logiciel non autorisé est en cours d'installation ou si des fichiers stratégiques sont modifiés ou qu'un utilisateur privilégié y accède.

Le déploiement de logiciels de surveillance de l'intégrité des fichiers est non seulement une excellente stratégie pour se protéger contre les violations de sécurité, mais il est également exigé par la norme de sécurité informatique des données de l'industrie des cartes de paiement (PCI-DSS). Plus précisément, la norme PCI DSS impose le déploiement de logiciels de surveillance de l'intégrité des fichiers afin d'alerter le personnel d'une modification non autorisée de fichiers système stratégiques, de fichiers de configuration ou de données. Selon Verizon Business, plus de 79 % des sociétés victimes de violations de données interrogées dans le cadre de son rapport publié en 2010 n'étaient pas conformes à la norme PCI DSS.

En détectant les accès non autorisés et les changements non gérés apportés aux fichiers système, la surveillance de l'intégrité des fichiers réduit les risques dans les domaines suivants :

- **Violations de données** par des membres internes ou des utilisateurs privilégiés, et attaques utilisant des logiciels malveillants.
- **Instabilité du système** causée par des modifications imprévues ou non autorisées de la configuration du système.
- **Mauvaises performances** souvent provoquées par des changements apportés en dehors des processus gérés de contrôle des changements.
- **Échec de conformité** résultant d'une incapacité à faire preuve de rigueur et à contrôler l'accès aux données sensibles.

La surveillance de l'intégrité des fichiers est un élément important de tout programme de sécurité informatique performant.

---

[1] L'équipe Verizon Business spécialisée dans les risques, en collaboration les services secrets Américains, « 2010 Data Breach Investigations Report », Verizon Business, juillet 2010, http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf?&src=/worldwide/resources/index.xml&id=.

[2] John Kindervag, « PCI X-Ray: File Integrity Monitoring », Forrester Research, Inc., 26 octobre 2009, http://www.forrester.com/rb/research.

[3] L'équipe Verizon Business spécialisée dans les risques, en collaboration avec les services secrets américains, « 2010 Data Breach Investigations Report ».

[4] John Kindervag, « PCI X-Ray: File Integrity Monitoring. »

Perspective sur la menace interne

Au niveau le plus élémentaire, il existe deux sortes de menaces internes : malveillantes et non-malveillantes.

Les menaces non-malveillantes comprennent l'exposition des systèmes ou des données stratégiques par erreur, ou en raison d'un manque de discernement ou d'un acte involontaire. Elles peuvent résulter de l'utilisation du courrier électronique ou d'autres applications, ou encore de la perte ou du vol d'ordinateurs portables et de smartphones. Étant donné que les périphériques mobiles appartenant aux employés ou à l'entreprise font de plus en plus partie du paysage de la sécurité informatique, les contrôles de sécurité et les stratégies de défense existants ne sont sans doute pas suffisants pour limiter l'exposition via ces vecteurs. En conséquence, les menaces internes non-malveillantes deviennent une préoccupation croissante.

Les membres malveillants du personnel, souvent motivés par l'appât du gain ou par la colère contre leur employeur, peuvent causer d'importants dommages sur une longue période et contribuer à des violations externes. L'histoire a montré que les infractions les plus graves sont causées par des utilisateurs autorisés disposant de privilèges élevés qui n'étaient pas adéquatement surveillés, ou par des utilisateurs dont les privilèges d'accès n'étaient pas gérés de façon adaptée tout au long du cycle de vie de leur identité. Dans son denier rapport sur les risques, Verizon indique que 24 % des attaques internes ont été commises par des employés ayant récemment subi un changement au niveau professionnel.

Cyberattaques motivées par l'appât du gain

Plusieurs des violations de sécurité les plus financièrement dévastatrices de la dernière décennie ont été le résultat d'attaques ciblées, personnalisées et sophistiqués, perpétrées par des pirates informatiques. La violation subie par Heartland Payment Systems est l'un des exemples les plus connus, en raison de son ampleur (les experts en sécurité estiment que 100 millions de cartes de crédit émises par 650 sociétés de services financiers peuvent avoir été compromises). L'impact financier a été colossal pour Heartland (perte de 300 millions de dollars américains en capitalisation boursière et plus de 30 millions de dollars de pertes directes).[5]

Le ver Stuxnet est un autre exemple d'attaque multi-vecteurs sophistiquée. Selon Bruce Schneier[6], le ver Stuxnet « est un logiciel malveillant "révolutionnaire", si retors dans son exploitation des vulnérabilités non corrigées et si sophistiqué dans son approche pragmatique, que les chercheurs en sécurité chargés de le désosser sont persuadés qu'il a été conçu par des professionnels épaulés par une structure gouvernementale ». Le programme semble avoir effacé environ un cinquième des centrifugeuses nucléaires en Iran, ce qui a contribué à retarder, mais pas à détruire, la capacité du pays à fabriquer ses premières armes nucléaires.[7] Les experts avertissent que le ver, conçu pour infiltrer les systèmes de contrôle industriel, pourrait être utilisé comme modèle pour saboter les machines essentielles aux centrales, réseaux électriques et autres infrastructures.

Prendre les cybercriminels sur le fait

L'un des plus grands changements dans les techniques d'attaque les plus sophistiquées est leur degré élevé de discrétion. Ainsi, la violation passe inaperçue pendant une période prolongée au cours de laquelle les systèmes ciblés sont exploités. Par exemple, dans le cas de Heartland Payment Systems, la violation n'a pas été détectée avant 18 mois. Qui plus est, elle n'a même pas été découverte par l'équipe de sécurité interne de Heartland, mais par des tiers.

Ces attaques sophistiquées prennent diverses formes et utilisent plusieurs vecteurs d'attaque. Cependant, les attaques types de fraude en ligne ont en commun un certain nombre d'étapes et de caractéristiques. Dans son rapport sur les violations de données publié en 2010, Verizon Business a constaté que dans un peu moins de la moitié des cas en 2009, il y a eu une indication de reconnaissance avant l'attaque, le plus souvent sous la forme d'empreinte système, de scannage et d'énumération. Dès que le périmètre de l'organisation victime a été infiltré, près de 40 % des pirates ont réussi à compromettre le système en quelques minutes ou quelques heures.

---

[5] John Kindervag, « PCI X-Ray: File Integrity Monitoring. »

[6] Bruce Schneier, « Schneier on Security: The Stuxnet Worm », http://www.schneier.com/blog/archives/2010/09/the_stuxnet_wor.html (consulté le 10 février 2011).

[7] William J. Broad, John Markoff, & David E. Sanger, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, New York Times, 15 janvier 2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html (consulté le 10 février 2011).

Selon le rapport de Verizon, dans environ 68 % des cas, il a fallu des semaines voire des mois avant que certaines entreprises ne découvrent ces violations. Si la violation est détectée, c'est le plus souvent grâce à des contrôles d'arrière-plan effectués par les sociétés de cartes de crédit ayant mis en oeuvre une technique connue sous le nom de Point de vente commun (Common Point of Purchase - CPP) généralement utilisée pour identifier la fraude.

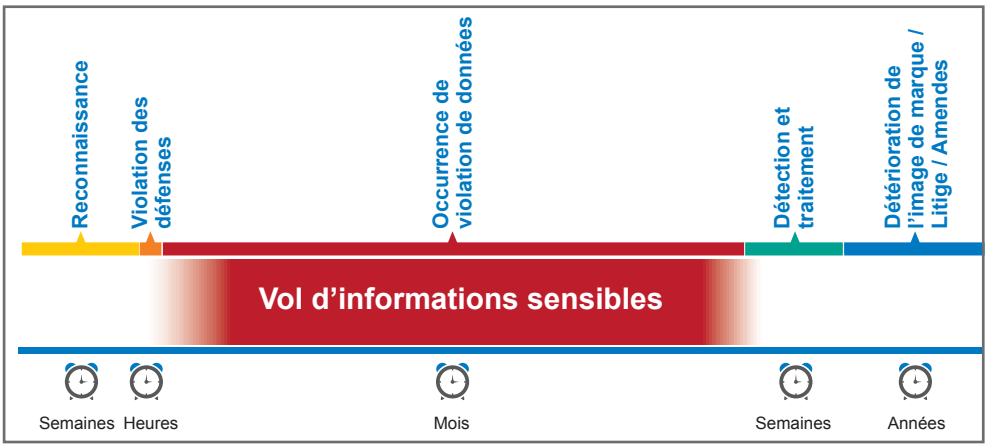

Figure 1. *Historique d'une violation type de données*

Combattre les menaces internes et externes

La forte augmentation du nombre de violations impliquant des membres du personnel par rapport à l'an dernier (+26 %) peut conduire à se demander si ce type d'attaques correspond à une épidémie. Quelle que soit la source de cette augmentation, il existe des stratégies simples qui peuvent être mises en oeuvre pour veiller à ce que les données sensibles des entreprises soient protégées. Le rapport de Verizon nous apprend d'une part que les employés bénéficient souvent de plus de privilèges qu'ils n'en ont besoin pour effectuer leurs travail et, d'autre part, que l'activité des utilisateurs privilégiés n'est souvent pas surveillée comme il le faudrait. Il suffirait de surveiller les utilisateurs privilégiés en temps réel pour identifier toute activité non autorisée ou inhabituelle. Les utilisateurs privilégiés ayant souvent accès à des fichiers et données sensibles ou stratégiques, le recours à la surveillance de l'intégrité des fichiers peut permettre de réaliser un suivi des accès et des modifications apportées aux fichiers système, fichiers journaux de sécurité, fichiers de données sensibles ou partages stratégiques. Dans le cas de fichiers système sur des systèmes stratégiques ou des fichiers de données sensibles, des alertes en temps réel sur les changements peuvent être configurées pour vous permettre d'identifier immédiatement l'apparition d'un problème.

N'oubliez pas que lorsqu'un pirate obtient l'accès à un compte utilisateur interne, il est impossible de distinguer son comportement d'une activité légitime. L'utilisation de la surveillance de l'intégrité des fichiers permet de détecter la modification de fichiers associés à une menace persistante avancée. Cette activité pourrait alors faire immédiatement l'objet d'une enquête, avant qu'une violation plus coûteuse ne puisse se produire. La détection précoce d'une telle menace peut permettre à une équipe de sécurité de réduire de manière significative le temps de réponse et de limiter les dégâts.

Cas de conformité d'entreprise : PCI DSS

Si la conformité à la norme PCI-DSS réduit les risques de violation de données, elle constitue également une raison de plus de déployer des solutions de surveillance de l'intégrité des fichiers. La norme de sécurité informatique des données de l'industrie des cartes de paiement est une obligation contractuelle pour les entreprises qui manipulent des renseignements sur les détenteurs de cartes Visa, MasterCard, Discover, American Express, Diner et Club.[8] Dans ses conditions 10 et 11, la norme PCI-DSS précise en effet que la surveillance de l'intégrité des fichiers est obligatoire.

Condition 10.5. Assurance de la sécurité du suivi d'audit (fichiers journaux)

> *« Analyser les journaux à l'aide d'un logiciel de surveillance de l'intégrité des fichiers ou de détection des modifications pour s'assurer que les données de consignation ne peuvent pas être modifiées sans entraîner le déclenchement d'une alerte (bien que l'ajout de nouvelles données ne doive pas entraîner d'alerte). »*

En rendant obligatoire l'utilisation d'un logiciel de surveillance de l'intégrité des fichiers ou de détection des changements sur les journaux et en indiquant que toute modification doit générer une alerte, la condition 10.5 de la norme PCI-DSS garantit la sécurité du suivi d'audit.

---

[8] PCI Security Standards Council, LLC, « About the PCI Data Security Standard (PCI DSS), » https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml (consulté le 29 mars 2010).

Condition 11.5. Accès et changements apportés aux fichiers système et au contenu stratégique

> *« Déployer des logiciels de surveillance de l'intégrité des fichiers pour alerter le personnel de toute modification non autorisée des fichiers de configuration, des fichiers de contenu ou des fichiers système stratégiques, et configurer ces logiciels pour comparer les fichiers stratégiques au moins une fois par semaine. »*

La condition 11.5 de la norme PCI-DSS vise à offrir aux entreprises des moyens de défense performants contre l'exploitation des ressources stratégiques, en particulier les serveurs. Pour que les entreprises puissent assurer la protection de leurs systèmes stratégiques, elles doivent connaître les changements apportés aux fichiers et systèmes de fichiers et pouvoir en rendre compte. Les éléments importants sont les suivants :

- Utilisateur à l'origine du changement
- Objet du changement (fichiers, registre ou paramètres de configuration)
- Date et heure du changement
- Valeur antérieure au changement
- Valeur postérieure au changement
- Changement autorisé dans le cadre du processus de gestion des changements ou non

Gérer la surveillance de l'intégrité des fichiers à des fins de sécurité et de conformité : NetIQ Change Guardian

Les menaces auxquelles font face les professionnels de la sécurité évoluent dans un écosystème des plus complexes. Quelle que soit la menace (grave attaque de logiciel malveillant ou accès non autorisé à des données sensibles par un membre interne du personnel), le risque pour les données critiques et l'infrastructure peut être considérablement réduit grâce à la technique de détection en temps réel des accès et des modifications apportées aux fichiers et systèmes sensibles qu'offre une solution de surveillance de l'intégrité des fichiers.

Les entreprises qui mettent en oeuvre une technologie de surveillance de l'intégrité des fichiers prennent une mesure essentielle pour protéger leurs données sensibles, mais s'assurent également de répondre aux exigences de conformité (qui exigent le déploiement de solutions de surveillance de l'intégrité des fichiers) et évitent ainsi de coûteuses pénalités et autres conséquences fâcheuses de la non-conformité.

La famille de produits NetIQ® Change Guardian™ adopte une approche de surveillance de l'intégrité des fichiers en temps réel qui assure :

- la détection en temps réel des changements apportés aux systèmes et fichiers stratégiques ;
- la génération d'alertes même si le contenu a simplement été visualisé sans avoir été modifié ;
- l'intégration du système d'alerte aux principales solutions de gestion des événements et des informations de sécurité (SIEM), telles que NetIQ® Security Manager™.
- la garantie que le processus d'alerte fournit des informations essentielles, telles que la personne ayant initié le changement, les éléments modifiés, le moment du changement et l'état antérieur au changement ;
- la satisfaction aux exigences de conformité en prouvant la capacité de l'entreprise à surveiller l'accès aux données sensibles ;
- la détection des changements sur vos plates-formes les plus importantes : Microsoft Windows, Active Directory (notamment les stratégies de groupe), UNIX et Linux.

La gamme NetIQ Change Guardian fournit des produits de détection en temps réel des changements non gérés apportés à des fichiers stratégiques, les configurations du système, et Active Directory (y compris les objets de stratégie de groupe), pour s'assurer que vos équipes de sécurité peuvent protéger de façon proactive des informations sensibles des entreprises et les données des clients à la fois contre les attaques malveillantes et les dommages accidentels. Ces solutions fournissent les informations nécessaires pour rapidement prendre des décisions avisées, limiter le risque de perte de données d'entreprise et maximiser le retour sur vos investissements de sécurité existants.

Collaborer : Solutions NetIQ de gestion des identités et de la sécurité

Le changement non géré de la configuration des systèmes et infrastructures stratégiques représente un risque important et croissant pour la sécurité des données d'entreprise et des informations sur la clientèle et pour la stabilité du système. NetIQ Change Guardian renforce votre capacité à détecter tous les changements non gérés et à réagir efficacement, de manière à réduire considérablement les risques d'activités malveillantes et à assurer la protection complète des données.

NetIQ propose une solution intégrée qui permet aux équipes de sécurité de mettre en oeuvre une infrastructure plus exhaustive de sécurité et de conformité, à la fois évolutive et capable de limiter la charge de travail. NetIQ Change Guardian fonctionne conjointement avec les meilleurs outils d'automatisation de workflow et avec NetIQ® Directory and Resource Administrator™ pour un contrôle granulaire des accès administratifs, dans le but de former une solution automatisée performante et intégrée de gestion des identités et de la sécurité. NetIQ Change Guardian s'intègre également étroitement avec des solutions SIEM telles que le produit primé NetIQ Security Manager, de manière à présenter des informations corrélées, complètes et pertinentes en temps réel aux équipes de sécurité et de conformité. Ces produits aident conjointement les entreprises non seulement à protéger leurs données, mais aussi à se conformer à d'importantes réglementations, notamment la norme PCI-DSS.

Conclusion

Comme la surveillance de l'intégrité des fichiers est capable de détecter rapidement les accès non autorisés ou les changements au niveau des systèmes stratégiques, cette solution est essentielle pour assurer la prévention des violations de données dues aux attaques ciblées de logiciels malveillants et aux activités intentionnelles ou non du personnel. La surveillance de l'intégrité des fichiers est également un élément important de la conformité à la norme PCI-DSS, expressément mentionné dans les conditions 10.5 et 11.5 pour aider à assurer que les accès et les modifications aux systèmes stratégiques sont connus et rigoureusement documentés. Afin d'assurer la sécurité et la conformité, il convient d'intégrer un logiciel de surveillance de l'intégrité des fichiers aux solutions SIEM, afin d'établir une corrélation avec d'autres événements de sécurité et de veiller à ce que les données et systèmes stratégiques soient sécurisés.

La famille de produits NetIQ Change Guardian vous procure en temps réel des services de détection et d'alerte en cas de modification des fichiers et de la configuration du système pour les hôtes essentiels. Outre le fait de réduire le risque de violation de données et d'attaques internes, ces produits répondent aux questions « qui, quoi, quand et comment » en cas de modification d'autres composants essentiels au sein de votre infrastructure, notamment Active Directory et les stratégies de groupe.

Exploités conjointement avec des solutions SIEM traditionnelles, ces produits offrent un moyen performant et efficace pour accélérer le recueil d'informations et la prise de décision et réduire le risque de violations.

Pour en savoir plus sur la façon de vous conformer aux exigences en matière de surveillance de l'intégrité des fichiers, visitez le site www.netiq.com ou appelez votre représentant ou partenaire local NetIQ.

À propos de NetIQ

NetIQ est un fournisseur international de logiciels informatiques d'entreprise dont les efforts sont constamment axés sur la réussite de ses clients. NetIQ comble, à moindres frais, les besoins de ses clients et partenaires en matière de protection des informations. De plus, notre société gère les aspects complexes des environnements d'applications dynamiques hautement distribués.

Notre portefeuille comprend des solutions automatisées et évolutives, spécialisées dans la gestion des identités, de la sécurité et de la gouvernance, ainsi que des opérations informatiques. Les entreprises sont ainsi en mesure de fournir, mesurer et gérer en toute sécurité des services informatiques à l'échelle de leurs environnements physiques, virtuels et en nuage. Associées à notre approche pratique et orientée client de la résolution des problèmes informatiques récurrents, ces solutions aident les entreprises à réduire les coûts, la complexité et les risques.

Pour en savoir plus sur nos solutions logicielles reconnues par les professionnels de l'industrie, visitez le site **www.netiq.com**.

562-FR1007-001 DS 07/12

France

Tour Franklin
100/101, Quartier Boieldieu
92042 Paris la Défense Cedex
France
Tel: +01 55 62 50 00
Fax: +01 55 62 51 99

Email : contact-fr@netiq.com
info@netiq.com
www.netiq.com
http://community.netiq.com

Pour obtenir la liste complète de nos bureaux d'Amérique du Nord, d'Europe, du Moyen-Orient, d'Afrique, d'Asie-Pacifique et d'Amérique latine, visitez la page : **www.netiq.com/contacts.**

Suivez-nous :