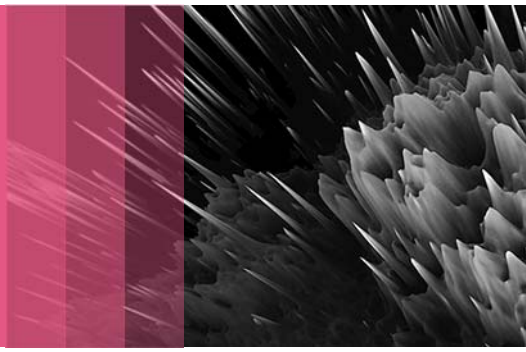
EXPOSER L'INCONNU

COMMENT LA TECHNOLOGIE DE BAC À SABLE COMBAT LES MENACES MODERNES



SOMMAIRE

Les cybercriminels sont de plus en plus habiles à dérober des données et perturber les réseaux, et font des ravages à grande échelle. Leurs attaques se produisent plus fréquemment et ce n'est qu'une question de temps avant que votre entreprise devienne une cible. Certaines entreprises en ont conscience et prennent des mesures correctives, mais la plupart ne s'apercevront même pas que des attaques se sont produites. La cybercriminalié est un « secteur » trois à cinq fois plus conséquent que celui de la sécurité.[1] L'économie pirate mondiale est réelle. Mais qu'est-ce que cela signifie ? Cela signifie que les menaces sont imminentes et qu'elles revêtent de multiples facettes. Leur évolution est au-delà de l'imagination. Cela signifie que votre entreprise est vulnérable.

La cybercriminalité est extrêmement avancée. Au fil des décennies, elle a causé des dégâts considérables aussi bien aux grandes qu'aux petites entreprises à travers le monde. Les agresseurs cachent des logiciels malveillants à l'intérieur de documents, de sites web, de serveurs et de réseaux. L'écosystème des pirates a évolué, avec des outils sophistiqués pour partager les vulnérabilités connues et dissimuler les programmes malveillants connus pour échapper à toute détection, transformant d'anciennes vulnérabilités en menaces inconnues. Ils se concentrent typiquement sur le vol de données, le sabotage des activités et l'atteinte à la réputation des entreprises.

Une faille se produit lorsque des individus non autorisés accèdent à des données confidentielles (ou les dérobent). Les failles permettent l'exfiltration des données confidentielles de l'entreprise, de données financières personnelles, de dossiers médicaux, de propriété intellectuelle et autres informations personnellement identifiables. Parmi les différents types de menaces, les fuites de données sont les failles de sécurité les plus fréquentes et les plus coûteuses. Sans un effort concerté, les données qui se déplacent aujourd'hui librement entre les réseaux internes et externes, les appareils mobiles, Internet et le Cloud, continueront d'être à la merci des pirates.

Apprenez à mieux protéger les actifs de votre entreprise et approfondir votre compréhension du paysage des menaces grâce à ce livre blanc. En décrivant les défis auxquels les entreprises doivent faire face, il souligne le besoin croissant de solutions complètes de protection contre les menaces persistantes avancées et zero-day.

« NOUS SOMMES APPELÉS À ÊTRE LES ARCHITECTES DE L'AVENIR, NON SES VICTIMES. »

R. BUCKMINSTER FULLER

[1] Conférence RSA de San Francisco | Keynote de Martin Roesch, Vice-président de Cisco

Juin 2015

LE PAYSAGE DES MENACES MODERNES

L'environnement des menaces de 2015 est marqué par des changements implacables. Tout est en train de changer sous nos yeux : la manière dont nous travaillons, nos perceptions, les types de menaces auxquels nous sommes confrontés, et les méthodes que les cybercriminels utilisent pour infiltrer les réseaux et confisquer des données. Ces nouvelles menaces en constante évolution sont devenues très complexes, apportant un nouveau lot de risques et d'incertitudes.

Les cybercriminels utilisent habilement des logiciels malveillants personnalisés, des techniques d'ingénierie sociale et de phishing pour contourner les technologies de sécurité traditionnelles. Les outils de piratage sophistiqués gardent une longueur d'avance en changeant constamment de vecteur de menace, laissant de nombreuses entreprises démunies face à ce rythme soutenu. Les nouvelles menaces nécessitent de nouvelles protections, ce qui met les logiciels malveillants inconnus à la pointe des attaques avancées... Typiquement, les protections reposant sur des signatures, telles que les antivirus et les systèmes de prévention d'intrusions, détectent et empêchent les logiciels malveillants *connus* d'infecter les entreprises. Cependant, sachant que la plupart des entreprises ont déployé ces technologies, les pirates se sont tournés vers la création de logiciels malveillants *inconnus,* qui ne sont souvent que des variantes d'un code précédent, afin de contourner plus facilement ces systèmes. Les solutions de prévention des menaces doivent protéger contre les menaces connues et inconnues pour être efficaces.

Souvent utilisés librement dans les médias, il est important de bien comprendre les termes « attaques zero-day » et « menaces persistantes avancées », comment ces menaces se comportent et les techniques appropriées pour les contrer efficacement.

« LES CYBERCRIMINELS NE FONT PAS DE DISCRIMINATION. LES MENACES PERSISTANTES AVANCÉES CIBLENT À LA FOIS LES PETITES ET LES GRANDES ENTREPRISES. »

ATTAQUES ZERO-DAY

Les vulnérabilités zero-day sont des failles non détectées qui ne sont pas encore corrigées. Les attaques visent généralement à compromettre un système d'exploitation, un système de gestion de base de données, d'autres technologies de plate-forme ou une application spécifique. Les vulnérabilités peuvent exister pendant plusieurs heures voire plusieurs années, en fonction du temps nécessaire pour que leurs éditeurs les remarquent et publient un correctif. Certaines attaques zero-day s'étalent avec soin sur une longue période pour échapper à toute détection, tout en dérobant des données précieuses. Par exemple chez Sony, les pirates ont utilisé des techniques de phishing dans des pièces jointes pour installer du code malveillant. Le réseau de l'entreprise a été affaibli, et les données confidentielles, les contrats, les stratégies commerciales, et même les adresses email des dirigeants de Sony ont été exposés..[2]

La découverte d'une nouvelle vulnérabilité ou la création d'une nouvelle menace zero-day est très difficile, mais potentiellement très précieuse pour un pirate. Les attaques zero-day ne disposent pas d'une signature *connue*, et peuvent donc contourner les antivirus, les systèmes de prévention d'intrusions et d'autres technologies d'analyse, fournissant une fenêtre pour l'activité malveillante avant qu'elle ne soit détectée. En modifiant, chiffrant ou déguisant des exploitations de vulnérabilités, les pirates peuvent facilement transformer des logiciels malveillants connus en versions inconnues pour bénéficier des mêmes avantages, avec beaucoup moins de compétences et d'efforts nécessaires.

MENACES PERSISTANTES AVANCÉES

Typiquement lancées par des entreprises ou des États avec un financement important, les menaces persistantes avancées emploient de multiples techniques d'attaque en plusieurs étapes. Elles sont extrêmement difficiles à détecter car elles se produisent pendant des jours, des semaines, des mois voire des années. Elles se composent de multiples petits événements qui peuvent sembler inoffensifs individuellement. Lorsqu'elles sont finalement détectées, il est souvent trop tard. Les menaces persistantes avancées sont très dangereuses pour les entreprises. Conçues pour infiltrer les systèmes tout en échappant à la détection, elles permettent aux pirates de cibler une entreprise et d'accéder à ses actifs, pendant une certaine durée.

[2] Hesseldahl, Arik. Voici ce qui a permis aux pirates d'entrer dans Sony : une vulnérabilité zero-day. Recode. N.p., 20 janvier 2015. Web. 4 juin 2015. http://recode.net/2015/01/20/heres-what-helped-sonys-hackers-break-in-zero-day-

Les cybercriminels ne font pas de discrimination. Les menaces persistantes avancées ciblent à la fois les petites et les grandes entreprises. Vous n'avez pas besoin d'être un organisme gouvernemental, une grande institution financière, ou une entreprise de service public pour devenir une victime. Ce sont les données qui priment. Pratiquement toutes les entreprises disposent de données qui ne devraient pas tomber dans les mauvaises mains, et doivent atténuer ces menaces.

LES CONSÉQUENCES

Les conséquences de ne pas protéger les données et les réseaux de votre entreprise sont dramatiques et endommagent gravement toutes les parties impliquées. Il n'est pas nécessaire de chercher bien loin pour trouver des traces d'événements catastrophiques récents : Anthem, Target, Home Depot et Sony, pour n'en citer que quelques-uns.

Les systèmes compromis peuvent entraîner des temps d'arrêt, la perte de propriété intellectuelle et des coûts de reprise, notamment liés à la restauration des systèmes à partir de sauvegardes. Le coût moyen d'une fuite de données est de 136 euros **par dossier** selon une étude de Ponemon, et pour les nombreux incidents impliquant des milliers, voire des millions de dossiers, le coût total moyen d'une seule fuite est passé à 3,35 millions d'euros, soit une augmentation de 23 pour cent en 2015.[3]

Réputation et confiance des clients

Les fuites de données peuvent causer des dommages durables à votre marque et votre réputation. La valeur moyenne d'une marque diminue de 21% en conséquence directe d'une faille de sécurité. Rétablir sa réputation prend du temps. En fin de compte, une fuite de données entraîne une baisse de la confiance des clients parce que votre entreprise n'a pas été en mesure de protéger leurs dossiers personnels.

Ressources drainées

L'incident Target de 2013 est peut-être un des meilleurs exemples de perte financière extrême pour les entreprises qui sont victimes d'une faille de sécurité. Les pertes totales déclarées à ce jour dépassent 219 millions d'euros. Ce chiffre inclut les coûts des assurances, les frais de réémission de cartes pour les clients, les engagements auprès des organismes de crédit, les frais juridiques, les frais d'enquête, et Certaines sources estiment que les coûts atteindront finalement plus de 1,94 milliard d'euros avec les pertes liées à la fraude.[4] Cela ne comprend pas les coûts potentiels pour les clients qui sont préoccupés par le vol d'identité et la réputation de leur cote de crédit.

Les institutions financières ont généralement à leur charge le coût de réémission des cartes, ainsi que la responsabilité initiale des activités frauduleuses effectuées avec les cartes de crédit compromises. Dans certains cas, les émetteurs peuvent tenter de récupérer ces sommes auprès des détaillants qui n'ont pas correctement protégé leur réseau et leurs données conformément aux normes telles que PCI/DSS. Les institutions financières peuvent réclamer de nombreux dédommagements, pour les coûts associés à l'information des clients, à la fermeture des comptes compromis et l'ouverture de nouveaux comptes, à la réémission des cartes de crédit, et au remboursement des pertes des clients.

Il est également important de noter que les grandes entreprises comme Target et Sony ne sont pas les seules à être piratées. Comme indiqué précédemment, ce sont les données qui priment. Les cybercriminels recherchent des opportunités dans les entreprises de toute taille. Ils sont attirés par la facilité, ce qui fait des petites entreprises une cible de choix. Selon une étude de Trustwave, 90% des fuites de données ciblent les petites entreprises.[5] Elles sont régulièrement frappées par des techniques d'ingénierie sociale et de phishing. Les pertes financières peuvent être énormes.

STATISTIQUES

- Toutes les 24 secondes, un hôte accède à un site web malveillant.
- Toutes les 34 secondes, un logiciel malveillant inconnu est téléchargé.
- Toutes les 3 minutes, un bot communique avec son centre de commande et de contrôle.
- Toutes les 5 minutes, une application à haut risque est utilisée.
- Toutes les 6 minutes, un logiciel malveillant connu est téléchargé.
- Toutes les 36 minutes, des données confidentielles sortent des entreprises.

---

[3] Korolov, Maria. Ponemon : Le coût moyen d'une fuite de données est maintenant de 136 € par dossier. Ponemon : Le coût moyen d'une fuite de données est maintenant de 136 € par dossier. OSC, 27 mars 2015. Web. 4 juin 2015

[4] Weiss, N. Eric et Rena S. Miller. La fuite de données Target et autres fuites : (2004) : n. pag. *La fuite de données Target et autres fuites :* Service d'études du Congrès, 4 février 2015. Web. 20 juin 2015 <https://fas.org/sgp/crs/misc/R43496.pdf>.

[5] Trustwave. 2015 Rapport Sécurité Trustwave. (2015) : *Rapport Sécurité Trustwave.* Trustwave, 2015. Web. 1er juin 2015 <https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf>.

L'ultime leçon

Les failles peuvent mettre votre entreprise à genoux. Elles entravent l'activité normale et peuvent provoquer jusqu'à l'arrêt complet de votre entreprise. Vous avez la responsabilité ultime de veiller à ce que les données de votre entreprise soient protégées. Alors, comment pouvez-vous protéger votre entreprise à l'ère numérique ? Vous avez besoin de technologies intelligentes et modernes ; des technologies capables de détecter et bloquer les menaces inconnues.

LA SOLUTION DU BAC À SABLE

Le terme « bac à sable » renvoie à l'image d'un enfant jouant dans un jardin ou une cour d'école. Dans le monde numérique, c'est en fait assez similaire. Tout comme un bac à sable est un environnement sûr pour les jeux d'enfants (sans risquer de détruire d'autres parties du jardin), un bac à sable est un environnement sûr pour évaluer les fichiers suspects, afin qu'ils ne fassent pas de ravages sur vos réseaux et vos données. La technologie de bac à sable est devenue une arme puissante pour la cybersécurité, et à juste titre. Elle repère de manière extrêmement efficace les fichiers malveillants et les attaques ciblées qui échappent aux défenses traditionnelles reposant sur des signatures, telles que la technologie antivirus.

Voici comment cela fonctionne :

Le bac à sable capture un fichier exécutable ou un document, et active ce fichier dans une machine virtuelle ou « émulateur », qui permet une analyse approfondie que l'antivirus ou le pare-feu n'est tout simplement pas en mesure d'effectuer. Dans cet environnement contrôlé, les menaces potentielles sont identifiées et étudiées pour découvrir leur comportement, sans qu'elles puissent accéder aux systèmes de production ou au réseau. Les fichiers et/ou les logiciels qui se révèlent être malveillants sont traités en conséquence. Cette technique de sécurité importante empêche les fichiers et les logiciels malveillants d'endommager votre réseau et de dérober vos données.

Le bac à sable est très efficace et absolument nécessaire pour détecter les menaces inconnues. Avec l'évolution du paysage des menaces modernes, le bac à sable deviendra une partie intégrante de l'arsenal de défense de chaque entreprise.

BAC À SABLE TRADITIONNEL

Plusieurs entreprises de cybersécurité proposent des technologies de bac à sable pour analyser les logiciels malveillants potentiels. Cependant, tous les bacs à sable ne sont pas égaux. Certains détectent les logiciels malveillants inconnus mais ne les *bloquent* pas réellement. Les bacs à sable plus avancés partagent des renseignements sur les logiciels malveillants nouvellement identifiés avec des réseaux de renseignement dans le Cloud. Cela accélère la circulation des nouveaux renseignements sur les attaques pour permettre aux entreprises connectées de se protéger rapidement. Il est important de comprendre la différence entre bac à sable traditionnel et avancé pour faire face à la pléthore de nouvelles méthodes d'attaque.

L'approche traditionnelle du blocage des logiciels malveillants inconnus et zero-day consiste à capturer et exécuter les fichiers suspects dans un bac à sable à l'extérieur du réseau, « imitant » ainsi un système d'exploitation standard pour l'observation. À l'aide des outils du bac à sable, les fichiers sont ensuite activés de diverses manières pour simuler l'ouverture des fichiers par un utilisateur réel. L'analyse détermine enfin si quelque chose d'anormal se produit au-delà du comportement escompté.

Les cybercriminels sont intelligents. Ils savent que ces protections existent dans certains réseaux et mettent en œuvre des techniques de contournement. Ils réussissent même à développer des logiciels malveillants qui parviennent à savoir quand ils sont à l'intérieur d'un bac à sable pour instruire le logiciel malveillant de ne pas s'installer tant qu'il n'est pas à l'extérieur du bac à sable, sur un poste réel. Une autre approche commune utilisée par les pirates consiste à intégrer des périodes de veille dans les logiciels malveillants, pour s'activer au bout de plusieurs minutes voire plusieurs jours après l'infection, soit longtemps après que le fichier est considéré comme étant sain. D'autres techniques courantes consistent à détecter les mouvements de la souris ou à chiffrer les menaces dans les pièces jointes. Ces techniques de contournement évoluées nous montrent que la technologie actuellement en place est insuffisante. Les solutions de sécurité doivent rapidement évoluer afin de conserver de l'avance sur les pirates.

« LA TECHNOLOGIE DE BAC À SABLE EST DEVENUE UNE ARME PUISSANTE POUR LA CYBERSÉCURITÉ. »

LE BAC À SABLE AVANCÉ

Les solutions traditionnelles de bac à sable (au niveau du système d'exploitation) sont un élément essentiel pour stopper les attaques zero-day et détecter les logiciels malveillants en cours d'exécution. Cependant, grâce à certaines des techniques décrites ci-dessus, les logiciels malveillants réussissent à échapper à toute détection. Pour cette raison, une protection avancée est nécessaire : Les bacs à sable traditionnels détectent les attaques dans les fichiers exécutables et les fichiers de données. Les bacs à sable avancés y ajoutent la possibilité de détecter les logiciels malveillants dans les fichiers de données avant qu'ils ne soient entièrement déployés, en analysant l'activité au niveau des instructions du processeur durant la phase d'exploitation de vulnérabilité, lorsque l'attaque tente d'obtenir des privilèges d'exécution illicites auprès du système d'exploitation. Le bac à sable traditionnel, combiné à la puissance du bac à sable avancé, fournit une protection sophistiquée, puissante et résistante aux tentatives d'évasion pour détecter et bloquer les logiciels malveillants inconnus.

L'objectif est clair : découvrir les menaces de manière proactive et bloquer les techniques de contournement. Bien qu'il existe d'innombrables vulnérabilités, il n'existe qu'une poignée de méthodes d'exploitation pouvant être utilisées pour télécharger un logiciel malveillant et l'exécuter. Le bac à sable avancé détecte l'utilisation de techniques d'exploitation, en examinant attentivement l'activité du CPU de l'hôte du bac à sable et son flux d'instructions au niveau du code d'assemblage, avant que le code malveillant n'ait une chance de s'exécuter. En conséquence, il retire toute possibilité aux pirates d'échapper à la détection. La vitesse et l'efficacité de la détection, et le fait que l'attaque est détectée avant que le logiciel malveillant n'atteigne le poste, font du bac à sable avancé la meilleure technologie de détection des menaces inconnues. Lorsque vous combinez les analyses approfondies du bac à sable au niveau du système d'exploitation et au niveau du processeur, vous obtenez une puissante technologie d'élimination des menaces de nouvelle génération.

Grâce à cette technologie de pointe, vous pouvez désormais combler les lacunes des défenses en détectant les menaces au stade de la *pré*-infection. Une fois capturés, les nouveaux logiciels malveillants (précédemment *inconnus*) sont ensuite transformés en logiciels malveillants *connus* et documentés par la création d'une signature. Les futures tentatives d'utilisation de la même attaque seront bloquées au niveau de l'antivirus ou du système de prévention d'intrusions, et n'auront pas besoin d'être analysées de nouveau dans le bac à sable.

Le bac à sable avancé contient toutes les fonctionnalités du bac à sable traditionnel plus une protection au niveau du processeur, pour se concentrer sur la phase d'exploitation de l'attaque. Il est en mesure de détecter et de bloquer les menaces persistantes avancées et zero-day, ainsi que les logiciels malveillants avancés qui tentent d'échapper à toute détection.

Facteurs clés à considérer dans le choix d'une bonne solution de bac à sable :

- ***Détection** et **blocage** des attaques*
- *Résistance aux techniques d'évasion*
- *Détection rapide et efficace*
- *Prise en charge des types de fichiers courants*
- *Prise en charge des objets web tels que Flash*

IMPORTANCE

Pendant que les techniques de contournement évoluent et deviennent plus intelligentes, la technologie doit continuer de s'adapter pour protéger votre entreprise. Les bacs à sable répondent aux problèmes croissants des logiciels malveillants inconnus, des menaces persistantes avancées et des attaques zero-day. Ces défis dépassent les technologies antivirus. Les logiciels malveillants inconnus contournent les solutions de sécurité traditionnelles avec une facilité apparente. Les bacs à sable peuvent détecter et bloquer ces types d'attaques avant qu'elles n'aient une chance d'infiltrer votre entreprise.

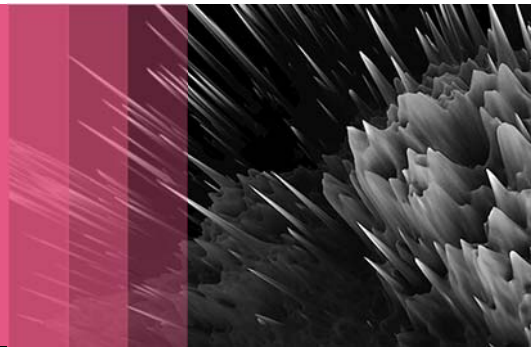
Essentiellement, la solution de bac à sable vous permet d'adopter une approche *proactive* de la sécurité, plutôt que *réactive*. Lorsque vous devez constamment réagir aux problèmes *après* qu'ils se produisent, plutôt que de les empêcher, vous perdez du temps, de l'énergie et de l'argent que votre entreprise n'a peut-être pas les moyens de dépenser.

POINTS À CONSIDÉRER SUR UNE SOLUTION DE BAC À SABLE

- ✓*Protection contre les toutes dernières cybermenaces :* Choisissez une solution avec plusieurs couches de protection pour faire face aux toutes dernières cybermenaces connues et inconnues. Une solution résistant aux tentatives d'évasion stoppera plus de logiciels malveillants.
- ✓*Blocage des logiciels malveillants au périmètre du réseau :* De nombreuses solutions ne font que détecter les logiciels malveillants et ne peuvent les empêcher d'infecter le réseau. Cela augmente les risques et compromet la posture de sécurité de l'entreprise.
- ✓*Analyse d'un large éventail de types de fichiers, y compris tous les types d'archives :* Les logiciels malveillants compressés dans les fichiers d'archivage (zip, rar, etc.) ne sont pas détectés par certaines solutions, ce qui en font un véhicule d'attaque très courant pour les pirates.

Juin 2015

CONCLUSION



Vous échangez chaque jour des centaines de fichiers avec des entreprises et des individus en qui vous avez confiance. Toutefois, certains des documents que vous recevez comportent des menaces pour votre sécurité. Vous prenez un risque chaque fois que vous ouvrez une pièce jointe.

De nombreuses entreprises ont protégé leurs systèmes et leurs données grâce à un logiciel antivirus, un pare-feu, ou en segmentant leur réseau. Les récentes failles de sécurité prouvent que la protection de base ne suffit plus. Ces méthodes, bien qu'elles soient essentielles et très utiles pour certains types de menaces, sont sans défense contre les menaces persistantes avancées et zero-day. Vous devez évaluer et analyser les menaces potentielles avant qu'elles ne pénètrent dans votre réseau. Un bac à sable vous permet de stopper les fichiers malveillants avant qu'ils n'infectent le réseau de votre entreprise en le verrouillant rapidement. Les fichiers sains quittent le bac à sable pour l'environnement public. Protégez votre entreprise à tous les points.

CE N'EST PLUS UNE OPTION

Même les antivirus, les antibots et les systèmes de prévention d'intrusions les plus efficaces ne peuvent protéger contre les logiciels malveillants inconnus. Dès qu'une nouvelle vulnérabilité est identifiée, il existe un délai plus ou moins long pendant lequel les logiciels malveillants l'exploitant réussissent à rester inaperçus dans les réseaux, car il n'existe pas encore de correctif pour remédier à la vulnérabilité, ou le correctif n'a pas encore été installé dans l'infrastructure informatique. Ce délai fournit suffisamment de temps aux agresseurs pour installer une tête de pont dans votre entreprise. La technologie de bac à sable avancée qui combine à la fois des analyses au niveau du système d'exploitation et du CPU comble cette lacune, en protégeant de manière proactive vos biens précieux contre les menaces persistantes avancées et zero-day.

Ces menaces sont réelles. Combien d'autres failles doivent se produire avant que les entreprises ne prennent les bonnes mesures préventives ? Combien de temps avant de réaliser que la technologie de sécurité d'hier ne suit pas le rythme des menaces modernes et des pirates sophistiqués ? Combien de temps avant que nous prenions au sérieux la sécurité des réseaux et des données ? L'une des plus grandes leçons que nous pouvons tirer est que la plupart des failles de sécurité dévastatrices qui se sont produits en 2014 et 2015 pouvaient être évitées, si les bonnes technologies et les bonnes solutions avaient été implémentées.

Pour en savoir plus sur la prévention des menaces et comment le bac à sable de future génération peut protéger votre entreprise, demandez une analyse Check Point Security Checkup sur www.checkpoint.com/resources/securitycheckup.

« LORSQUE VOUS ÊTES CONSTAMMENT SUR LA DÉFENSIVE, ET QUE VOUS DEVEZ CONSTAMMENT RÉAGIR AUX PROBLÈMES APRÈS QU'ILS SE PRODUISENT, PLUTÔT QUE DE LES EMPÊCHER, VOUS PERDEZ DU TEMPS, DE L'ÉNERGIE ET DE L'ARGENT QUE VOTRE ENTREPRISE N'A PEUT-ÊTRE PAS LES MOYENS DE DÉPENSER. »

CONTACTEZ-NOUS

Siège mondial | 5 Ha'Solelim Street, Tel Aviv 67897, Israël | Tél. : +972 3 753 4555 | Fax : +972 3 624 1100
Email : info@checkpoint.com

Siège français | 120 avenue Charles de Gaulle, 92200 Neuilly sur Seine | Tél. : +33 (0)1 55 49 12 00
Email : info_fr@checkpoint.com | www.checkpoint.com

Juin 2015