

# Détecter et éliminer les actifs toxiques de son infrastructure IT

Publié le Vendredi 30 Octobre 2009



Par Jeremy D'Hoinne, Directeur Produit de Netasq. En 2008, l'industrie financière a tremblé lorsqu'elle a découvert des milliards de dollars d'actifs devenus toxiques et donc sans valeur. Cet épisode a ruiné des millions de personnes, surprises et choquées de constater que ce qui devait leur amener la fortune les a conduit à la banqueroute.

Même si le lien entre actifs financiers et actifs réseaux semble ténu, l'infrastructure IT est exposée à un mal qui comporte de nombreuses similitudes avec son homologue de la finance. Commençons par tenter une définition de la notion d'actif toxique IT. Un actif toxique IT est tout élément, censé participer à la bonne marche d'un SI, qui recèle un risque insoupçonné pour l'entreprise. Différents exemples vont nous aider à mieux comprendre les enjeux de ces risques cachés qui minent le système d'information. Des applicatifs malveillants à la virtualisation, voyons ce que les DSI et le RSSI doivent évaluer au quotidien.

Les applications et les ordinateurs infectés par des programmes malveillants, tels que les virus ou les chevaux de Troie, sont une illustration assez évidente du concept d'actif toxique. Lorsque l'ordinateur d'un collaborateur est infecté, il peut contaminer toute l'infrastructure et ouvrir les portes du réseau de l'entreprise à des inconnus. De nos jours, cette menace est bien assimilée par les DSI et les RSSI et de nombreuses solutions existent. Toutefois, l'explosion de la mobilité et de la convergence rendent cette menace plus concrète. En 2008, les pertes liées directement à la cybercriminalité sont estimées à plus de 250 millions de dollars.

La menace applicative ne se limite toutefois pas aux seuls codes malicieux. 500 nouvelles vulnérabilités applicatives apparaissent chaque mois. La maîtrise du parc applicatif est donc critique pour trouver les actifs potentiellement toxiques. Le dynamisme des systèmes d'information d'aujourd'hui oblige les responsables sécurité à connaître à chaque instant les applications utilisées et les risques associés à leur utilisation. Les solutions de sécurité doivent intégrer cet audit applicatif et la détection de vulnérabilité en temps réel. Si c'est le cas, l'administrateur peut distinguer les actifs sains (les applications souhaitées), des actifs toxiques (les applications non maîtrisées, inconnues ou obsolètes) !

## Les certifications

Il est naturel de penser que les certifications PCI-DSS, ISO 27001 ou encore les certifications critères communs constituent un actif fort de la politique de sécurité. C'est évidemment le cas, mais leur mise en place peut s'avérer être un remède pire que le mal. La certification PCI-DSS impose par exemple de nombreuses contraintes sur les mots de passe utilisateurs (section 8.5.9, 8.5.10 et 8.5.10). L'application à la lettre de ces contraintes crée parfois une réaction de l'utilisateur opposée au souhait d'améliorer la sécurité de l'accès au réseau. En effet, ces mots de passes sont complexes et les

utilisateurs doivent en changer régulièrement. Il est donc fréquent de les trouver notés sur un « Post-It », collé sur l'écran de l'ordinateur (ou sous le clavier), voire dans le portefeuille du collaborateur. La sécurité s'en trouve-t-elle améliorée ? Evidemment pas. Pourtant la mise en place de cette politique crée un sentiment de sécurité accru.

La certification d'un produit de sécurité par les critères communs est également un gage de confiance, que le RSSI recherche. Malheureusement, les critères nécessaires pour déterminer la qualité de cette certification sont souvent mal connus. En effet, la certification Critères Communs s'applique sur une cible de sécurité. Un produit peut donc être certifié EAL2+, EAL3+ ou EAL4+, mais sur des cibles complètement différentes. Il n'est pas rare de voir un produit dont la cible de certification implique des conditions d'utilisation inapplicables : stockage de l'équipement de sécurité dans un local gardé par des vigiles ; administration uniquement possible par connexion directe ; ou encore fonctions VPN et gestion des traces absents de la certification. Ainsi, derrière le même logo, se cachent des réalités bien différentes dont le responsable de la sécurité a rarement connaissance.

On le voit, la certification contribue pleinement à la sécurité du SI, à condition de l'accompagner d'un haut niveau d'information et d'une conduite patiente du changement.

## **La politique de sécurité**

Principal actif de la sécurité de l'entreprise, la politique de sécurité est potentiellement l'actif le plus toxique de l'infrastructure. De nombreux facteurs concordent à ce que le DSI ou le RSSI d'une entreprise pense, à tort, que son entreprise est bien protégée. La communication des éditeurs de solution de sécurité est souvent la racine même du mal. Pour simplifier, la métrique d'évaluation d'une solution de sécurité se fait sur 2 indicateurs principaux : les performances brutes, annoncées par le constructeur, et le nombre de menaces ou de signatures de protections, également fournies par le prestataire. Cependant, ces 2 mesures sont souvent antinomiques. En effet, dans de nombreux produits, les analyses applicatives (pare-feu applicatif et prévention d'intrusion) sont désactivées par l'éditeur de sécurité. Ainsi, les performances annoncées sont des performances brutes, sans inspection. Le second maillon de cette chaîne, l'installateur de la solution, a pour mission de préserver la continuité de service et les performances du réseau de son client. En conséquence, de nombreux produits de sécurité sont installés dans les entreprises, toutes protections désactivées !

L'illusion de sécurité provoquée par l'acquisition de ce type de produits est totale. Les éditeurs qui tentent de faire croire que la qualité de la sécurité est directement proportionnelle au nombre de signatures de leur moteur sème la graine d'une sécurité illusoire. En effet, un discours axé sur cette métrique masque souvent une technologie obsolète, basée uniquement sur la création de protections postérieure à l'apparition de l'attaque. Aujourd'hui, 80% du trafic est lié à l'utilisation du web, qui est très sensible aux fausses alertes et porteur de flux de plus en plus complexes. D'autre part, les attaques sont désormais capables de s'étendre à l'échelle mondiale en quelques minutes. Les analyses proactives et la compréhension des protocoles applicatifs est donc impérative.

La création d'autorisation et de règles d'accès est l'un des piliers d'une bonne politique de sécurité. Chaque règle constitue un actif de cette politique, destiné à renforcer la sécurité de l'ensemble. Une autorisation peut se décomposer en 4 éléments qui doivent répondre chacun à une question. Qui ? Où ? Pourquoi ? Quand ? L'explication de ce concept nécessiterait un niveau de détail trop important, mais la base se situe dans les 4 questions citées. Le danger pour la politique de sécurité et l'oubli d'un de ces éléments.

### **Le pare-feu orienté utilisateur**

Prenons le cas de la notion de Firewall orienté utilisateur (« User-based Firewall »). Ce discours agressif vise à rendre archaïque la notion d'adresse IP et occulte la réponse à la question « Où ? ». Il s'oppose à la contrainte historique de certains produits de sécurité qui force l'administrateur à définir des règles en fonction des interfaces réseaux d'entrée et de sortie du trafic. On ne peut nier l'intérêt pour un administrateur de créer des règles qui obligent à connaître l'utilisateur qui se connecte. Restreindre l'utilisateur ou le groupe d'utilisateurs répond à la question « Qui ? ». C'est cependant loin d'être suffisant. La règle qui consiste à dire « J'autorise l'utilisateur Bob à se connecter au serveur d'application » ne répond pas à la question « Où ? ». Cette règle est un actif toxique de la politique, car son manque de précision représente un risque. Souhaite-t-on vraiment que l'utilisateur puisse accéder à ce serveur depuis n'importe quel ordinateur ou téléphone, quelque soit son état ? Pour illustrer à l'extrême ce concept, il suffit de penser aux conséquences d'une règle « Autoriser Bob à utiliser le protocole web » : pas de restriction sur l'ordinateur de l'utilisateur (Où ?), pas de restriction sur la période (Quand ?), ni sur la destination (Pourquoi ?). Cette règle autorise donc Bob à se connecter depuis son téléphone portable au milieu de la nuit, le week-end, vers n'importe quel serveur web interne de l'entreprise. Cela met beaucoup de pression sur la fiabilité de l'authentification dont on a vu plus haut quelle peut parfois être mise à rude épreuve.

On le voit, même si on se restreint aux règles et à l'analyse des flux, la réalité de la politique de sécurité peut être bien différente de l'objectif du DSI ou du RSSI. La communication trop agressive des éditeurs de sécurité, détourne parfois l'attention des fondamentaux, qui méritent une attention toute particulière. Heureusement, des outils de vérifications et d'alertes existent pour avertir l'administrateur durant l'édition de sa politique. Une revue régulière, supervisée par un regard indépendant est également une bonne pratique à respecter.

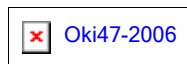
Le système d'information est une entité vivante de l'entreprise. Les évolutions structurelles, organisationnelles, l'adoption de nouvelles technologies comme la voix sur IP ou les lourdes migrations à venir lors de l'arrivée d'IPv6 sont autant de facteurs de risques. Un système est rarement aussi vulnérable que dans les périodes qui précèdent ou qui suivent les migrations.

### **La virtualisation et le « cloud computing »**

La virtualisation et le « cloud computing » sont en train d'arriver dans nos entreprises. Ils promettent de nombreux bénéfices, notamment pour la continuité de service et seront peut-être les actifs

prépondérants des infrastructures de demain. Toutefois, par sa nature même, la virtualisation induit de nouveaux risques, dont l'ampleur est parfois difficile à évaluer. La couche applicative supplémentaire de l'hyperviseur ajoute un foyer de vulnérabilités. Le regroupement de nombreuses images logicielles sur le même serveur physique tend à atténuer, voire à supprimer, la notion de zone démilitarisée. Il est recommandé d'éviter de placer plusieurs serveurs de sensibilité différente au sein d'un même serveur physique, mais l'objectif de la virtualisation n'est-il pas de se libérer de ces contraintes ? Le « cloud computing », s'il est accepté, va également profondément changer la donne en matière de sécurité. La nature même des flux qui entrent et qui sortent de l'entreprise sera complètement modifiée. La sécurité déportée chez un prestataire diminue la visibilité pour l'administrateur, soucieux de la sécurité de ses données.

« La sécurité n'est pas un produit, c'est un process ». Cette citation de Bruce Schneier date de 1999 et rappelle que les femmes et les hommes de l'entreprise font ou défont sa sécurité. La sécurité est avant tout une question de vigilance et d'attention. Si on l'oublie, on court le risque de laisser nos actifs devenir toxiques.



Copyright © 2009 ITChannel - All right reserved