

NETASQ propose ses conseils pour faire face au Top 5 des menaces en 2012

Paris, le 23 janvier 2012

NETASQ, acteur de référence et pionnier sur le marché de la sécurité informatique, propose ses conseils pour faire face aux challenges à venir de l'année 2012, notamment pour 5 menaces identifiées comme majeures.

Fabien Thomas, CTO - Directeur Architecture et Sécurité de NETASQ, précise « *Comme toute industrie, l'industrie de la cyber criminalité a atteint une certaine maturité et les innovations portent désormais sur une sophistication accrue des techniques éprouvées, plutôt que de nouveaux types d'attaques.* »

1. La gestion des vulnérabilités reste la priorité numéro 1

La majorité des infections par malwares continuent d'être des failles connues pour lesquelles des correctifs existent déjà (XSS, injection SQL, etc directory traversal), alors la gestion des vulnérabilités doit continuer à être l'une des premières priorités pour tous les professionnels de la sécurité. En plus de cette gestion des correctifs de base, un nombre embarrassant d'intrusions sur le réseau en 2011 étaient toujours le résultat d'erreurs telles que des pare-feux incorrectement configurés ou des mots de passe faibles.

2. L'ingénierie sociale

Bien que l'ingénierie sociale ne soit pas nouvelle, la montée exponentielle de l'adoption des réseaux sociaux - à la fois dans et hors du lieu de travail - a considérablement augmenté son efficacité et son utilisation. La réponse à cela doit être une combinaison de formation des utilisateurs et le contrôle des applications au niveau du périmètre réseau ou pare-feu. Cependant, comme un nombre croissant d'entreprises commencent à exploiter le potentiel des réseaux sociaux pour le marketing ou pour d'autres utilisations, le simple blocage d'applications telles que Facebook ne suffit plus et se doit d'être complété par une analyse plus fine du flux de données avec la détection des menaces et l'élimination se produisant à la volée.

3. Les attaques ciblées / les menaces persistantes avancées/ l'hacktivisme

En plus des motivations financières habituelles - vol direct de données ou d'interruption des concurrents - on constate une augmentation dans le piratage de l'activisme politique, parfois désigné sous le terme *hacktivisme*. Que ce soit parrainé par des personnes ayant de

fortes convictions politiques ou le travail des groupes indépendants comme Les Anonymous ou Lulzsec, de telles attaques ont au moins servi à rehausser le profil et la sensibilisation de la sécurité informatique.

L'autre conséquence de cette complexité croissante des menaces est une réduction continue de l'efficacité des signatures d'attaques spécifiques. En dépit d'une intensification des efforts des chercheurs en sécurité autour du globe, les stratégies de défense sont trop dépendantes de la détection par signatures et donc vouées à l'échec.

L'analyse du protocole, l'application, le contexte et le comportement du trafic deviendront donc des ajouts de plus en plus importants pour le mix de prévention des intrusions en 2012.

4. La technologie d'IPv6 n'est pas encore mature

Contrairement aux prévisions initiales l'adoption d'IPv6 est beaucoup plus lente que prévue et l'une des principales raisons de ce décalage est que la technologie n'est pas encore mure et introduit de nouvelles vulnérabilités.

NETASQ conseille donc de reporter cette migration au moins pour cette année, tout en utilisant le temps dégagé pour planifier une transition contrôlée une fois que la majorité des problèmes technologiques auront été identifiés et atténués.

5. Augmentation des attaques SCADA (Supervisory Control and Data Acquisition)

Les deux dernières attaques de ce type Stuxnet et Duqu ont fait des ravages dans toute l'industrie, mais ceci est également lié au fait que les systèmes de contrôle industriel appelés SCADA se sont révélés particulièrement vulnérables en raison de leur ancienneté relative et leur faible sécurisation.

Malheureusement, de par leur nature même puisque faisant partie intégrante du procédé industriel, comme la production d'énergie par exemple, ils constituent non seulement des cibles faciles mais également très attrayantes. Cette tendance semble donc susceptible d'augmenter et NETASQ recommande aux professionnels de la sécurité responsables de tels systèmes de garder leurs systèmes de prévention d'intrusion à jour régulièrement et de mettre à niveau leurs périmètres de sécurité si besoin.

A propos de NETASQ

Avec plus de 75.000 firewalls UTM déployés dans des entreprises de toute taille, des institutions gouvernementales et des organismes de défense, **NETASQ** développe des solutions sans équivalent sur le marché en termes de performances, de protection et de contrôle. Leur certification au plus haut niveau européen (**EU RESTRICTED, OTAN et EAL4+**) les rend tout à fait uniques.

Pour en savoir plus: <http://www.netasq.com>

Photos et logos : <http://www.netasq.com/marketing/marketing.php>

Contact Presse

<p>onechocolate communications</p>	<p>NETASQ</p>
<p>Xavier Delhôme / Edouard Fleuriau-Chateau</p>	<p>Marie-Pierre CZABAK / Manon HASARD</p>
<p>+33 1 41 31 75 09 / +33 1 41 31 75 16</p>	<p>+33 1 46 21 82 38 / +33 3 20 61 90 49</p>
<p>xavierd@onechocolatecomms.fr</p>	<p>marie-pierre.czabak@netasq.com</p>
<p>edouardfc@onechocolatecomms.fr</p>	<p>manon.hasard@netasq.com</p>