Qualys, rÃ©sultats de lâ€™Ã©tude Â« Laws of Vulnerabilities 2.0 Â»
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 29/4/2009 15:00:00

Une nouvelle Ã©tude de la plus importante compilation de donnÃ©es de vulnÃ©rabilitÃ©s collectÃ©es en conditions rÃ©elles rÃ©vÃ¨le les tendances par marchÃ© vertical concernant la durÃ©e de vie moyenne, la prÃ©valence, la persistance et lâ€™exploitation des vulnÃ©rabilitÃ©s
Wolfgang Kandek, directeur technique de Qualys, Inc., le principal fournisseur de solutions Ã la demande pour la gestion des risques de sÃ©curitÃ© informatique et de la conformitÃ©, dÃ©voile son Ã©tude Â« Laws of Vulnerabilities 2.0 Â» et sâ€™appuie sur la plus importante compilation de donnÃ©es de vulnÃ©rabilitÃ©s disponible.

Lâ€™Ã©tude Laws 2.0 indique les tendances en matiÃ¨re de durÃ©e de vie moyenne, de prÃ©valence, de persistance et dâ€™exploitation des vulnÃ©rabilitÃ©s pour les 5 marchÃ©s critiques que sont les secteurs de la finance, de la santÃ©, de la vente au dÃ©tail, de la production et des services.

TirÃ©es de lâ€™analyse statistique de plus de 680 millions de vulnÃ©rabilitÃ©s, parmi lesquelles 72 millions sont critiques, ces tendances sâ€™appuient sur 80 millions de scans rÃ©seaux rÃ©alisÃ©s en 2008.

Â

MÃ©thodologie de lâ€™Ã©tude Â« Laws of Vulnerabilities 2.0 Â»

Les conclusions tirÃ©es de cette Ã©tude sont :

1. **DurÃ©e de vie moyenne** â€“ La durÃ©e de vie moyenne des vulnÃ©rabilitÃ©s critiques est restÃ©e de 30 jours pour tous les marchÃ©s concernÃ©s. Si lâ€™on prend chaque marchÃ© pris sÃ©parÃ©ment, lâ€™industrie des services connaÃ®t la durÃ©e de vie moyenne la plus courte, avec 21 jours.

Le secteur financier se classe en seconde place, avec 23 jours, le marchÃ© de la vente au dÃ©tail en troisiÃ¨me position, avec 24 jours et le secteur de la production est en derniÃ¨re place avec un cycle de vie moyen de 51 jours pour une vulnÃ©rabilitÃ©.

2. **PrÃ©valence** â€“ 60% des vulnÃ©rabilitÃ©s les plus rÃ©pandues et les plus critiques sont remplacÃ©es par de nouvelles vulnÃ©rabilitÃ©s chaque annÃ©e. Ce nombre a augmentÃ© par rapport Ã lâ€™Ã©tude Laws de 2004 oÃ¹ il Ã©tait de 50%. Dâ€™aprÃ¨s lâ€™Ã©tude Laws 2.0, les principales solutions pointÃ©es du doigt sont Microsoft Office, Windows 2003 SP2, Adobe Acrobat et le Plug-in Java de Sun.

3. **Persistance** â□□ Lâ□□Ã©tude Laws 2.0 signale que la durÃ©e de vie de la plupart, sinon de toutes les vulnÃ©rabilitÃ©s, est illimitÃ©e, un pourcentage important de vulnÃ©rabilitÃ©s nâ□□Ã©tant jamais totalement rÃ©solues. Cette tendance a Ã©tÃ© illustrÃ©e par des Ã©chantillons de donnÃ©es de MS08-001, MS08-007, MS08-015 et MS08-021.

4. **Exploitation** â□□ 80% des attaques de vulnÃ©rabilitÃ©s se produisent dÃ©sormais dans les 10 jours qui suivent la publication de la vulnÃ©rabilitÃ©. En 2008, lâ□□entitÃ© Qualys Labs avait consignÃ© 56 vulnÃ©rabilitÃ©s avec des attaques Ã zÃ©ro jour (Zero Day), dont la vulnÃ©rabilitÃ© RPC qui a engendrÃ© Conficker. En 2009, la premiÃ¨re vulnÃ©rabilitÃ© signalÃ©e par Microsoft, MS09-001, a Ã©tÃ© victime dâ□□une attaque dans les 7 jours qui ont suivi.

Â

Â

Le Patch Tuesday dâ□□avril de Microsoft mentionnait des attaques connues pour plus de 47% des vulnÃ©rabilitÃ©s publiÃ©es. Câ□□est cette tendance qui a le plus Ã©voluÃ© depuis lâ□□Ã©tude Laws 1.0 de 2004, qui signalait alors un laps de temps indicatif confortable de 60 jours.

Â« *Il est de plus en plus difficile dâ□□assurer la sÃ©curitÃ© en raison de lâ□□extrÃªme sophistication des attaques et de la fenÃªtre dâ□□exposition dÃ©sormais ramenÃ©e Ã quelques jours seulement pour les vulnÃ©rabilitÃ©s les plus critiques Â»*, dÃ©clare **Wolfgang Kandek**, directeur technique de Qualys et auteur de lâ□□Ã©tude Â« Laws of Vulnerabilities 2.0 Â».

Â« *Lâ□□objectif de cette Ã©tude est dâ□□aider les entreprises des diffÃ©rents secteurs dâ□□activitÃ©s Ã comprendre les tendances plus vastes, les dommages potentiels ainsi que les prioritÃ©s en matiÃ¨re de vulnÃ©rabilitÃ©s. Elles pourront ainsi prendre des dÃ©cisions plus efficaces et immÃ©diates pour protÃ©ger leurs rÃ©seaux. GrÃ¢ce aux rÃ©sultats gÃ©nÃ©rÃ©s par une Ã©tude comme Â« Laws of Vulnerabilities 2.0 Â», nous pouvons fournir, en temps rÃ©el, aux marchÃ©s, une approche statistique des tendances de ces menaces.* Â»

MÃ©thodologie de recherche pour lâ□□Ã©tude Â« Laws of Vulnerabilities 2.0 Â»

Cette Ã©tude sâ□□appuie sur une compilation anonyme qui ne permet pas dâ□□identifier un quelconque client, adresse IP ou rÃ©seau. Les donnÃ©es sont collectÃ©es via lâ□□infrastructure dâ□□analyse QualysGuard qui effectue plus de 200 millions dâ□□audits dâ□□adresses IP chaque annÃ©e.

De simples compteurs sont activÃ©s pendant lâ□□analyse des rÃ©seaux des clients et les donnÃ©es collectÃ©es sont ensuite synthÃ©tisÃ©es puis consignÃ©es quotidiennement Ã des fins dâ□□analyse et dâ□□Ã©tude.

Les rÃ©sultats complets de cette Ã©tude