



NOTA DE PRENSA

WatchGuard alerta sobre las amenazas más importantes en los entornos educativos

Madrid, 11 de noviembre de 2009.- WatchGuard® Technologies, proveedor global de soluciones de seguridad de red, ha elaborado un listado con las principales amenazas que afectan a la seguridad informática de escuelas y universidades.

Así, compañía destaca que las amenazas relacionadas con la educación se espera que incrementen. De acuerdo con el Departamento de Seguridad Nacional de Estados Unidos, el 25% de todas las infracciones de ciberseguridad se dan en las escuelas, y aunque la mayoría del profesorado considera que las redes de sus campus son más seguras ahora que hace un año, WatchGuard prevé que las brechas de seguridad, las vulnerabilidades y las amenazas continuarán infectando escuelas y universidades.

Según WatchGuard, se estima que los peligros que se citan a continuación liderarán las amenazas a redes, aplicaciones y datos en los entornos educativos:

- **Malware y Spyware** – En la medida en que los estudiantes y las facultades utilizan la web con propósitos educativos así como para entretenimiento, muchos se exponen sin darse cuenta a descargas por error, o a páginas web corruptas que inyectan diferentes tipos de software malicioso en sus ordenadores. Una vez infectados, se arriesgan a ser víctimas de robos de identidad o pérdidas de información personal a través de spyware y keyloggers.
- **Virus** – Actualmente, el email sigue siendo una de las principales vías para el suministro de virus. Lamentablemente, un reciente estudio pone de manifiesto que el 27% de los usuarios no mantiene sus antivirus actualizados. Con virus que adquieren propiedades polimórficas, las firmas de antivirus por si solas no son suficientes para detener la próxima oleada de nuevos virus.
- **Botnets** – Se estima que entre el 15 y 20% de los sistemas informáticos de todas las universidades y escuelas que están conectados a Internet forma parte de una botnet o red zombie. Como parte de una botnet, los sistemas de los centros educativos pueden utilizarse en una amplia variedad de exploits desconocidos, incluyendo la distribución de spam, ataques de negación de servicio, clics fraudulentos, robo de identidad y otros muchos.
- **Phishing** – Las estafas de phishing continúan ganando sofisticación y son más selectivas, estando algunas de ellas específicamente dirigidas a los estudiantes. Según un informe, los ataques de phishing a través de redes sociales alcanzan un ratio de éxito del 70%, porcentaje que indica que la mayoría de los estudiantes son vulnerables a este tipo de estafas o timos.
- **Hacking** – Tal y como revela un estudio realizado entre profesionales de TI del sector educativo, el 23% situó a los estudiantes “hackers” como una de las mayores amenazas a la seguridad de su red. Si los ataques son diseñados para alterar notas o calificaciones o con propósitos más siniestros, estos estudiantes que son piratas informáticos, continúan llevando al límite las redes y la protección de datos.

- **Control de Acceso** – El uso de dispositivos móviles y el acceso inalámbrico continúa siendo una molestia para los administradores de red. La preocupación por impedir el acceso a usuarios no autorizados a los recursos de TI de los centros educativos es el objetivo de muchos administradores. En la medida en que la utilización de dispositivos móviles se está incrementando, las escuelas deberán enfrentarse a mayores retos a la hora de gestionar el acceso autorizado a la red.
- **Redes Sociales** – El número uno de las amenazas a las redes de las escuelas y universidades son las redes sociales como Facebook o MySpace. Lamentablemente, éstas actúan como la plataforma perfecta para lanzar miles de ataques contra estudiantes y facultades, incluyendo spam, virus, malware o phishing, entre otros. A esto se suma que los ataques de ingeniería social son, a menudo, extremadamente exitosos debido al entorno de “confianza” que las redes sociales crean.
- Dada la naturaleza sensible tanto de estudiantes como de la información de las facultades, que poseen datos sobre números de la seguridad social, de tarjetas de crédito y otra información de identificación personal sensible, WatchGuard recomienda que las escuelas y universidades revisen sus controles de seguridad y políticas de TI con regularidad para cerciorarse de que cuentan con las soluciones de seguridad más efectivas y actualizadas.

Palabras clave:

Malware, Spyware, Viruses, Botnets, Phishing, Hacking, Control de Acceso, Redes Sociales, WatchGuard.

Cita:

- *“Con tanto en riesgo y tanto que ganar por parte de los cibercriminales, los campus en la actualidad son uno de los entornos TI más peligrosos”, asegura **Eric Aarrestad, Vicepresidente de WatchGuard Technologies**. “A diferencia de las empresas, que pueden dedicar importantes recursos a la protección de la red y de los datos, las escuelas y las universidades tienen recursos más limitados, sin embargo se enfrentan a algunos de los retos de seguridad sirviéndose de la interacción entre estudiantes y los recursos de TI de sus escuelas”.*

Acerca de WatchGuard Technologies, Inc.

Desde 1996, WatchGuard®Technologies, Inc. ha sido líder de tecnología avanzada de soluciones de seguridad de red, suministrando seguridad imprescindible a cientos de miles de negocios de todo el mundo. La familia WatchGuard Firebox® X de dispositivos de gestión unificada de amenazas de cable y wireless y las soluciones de acceso remoto WatchGuard SSL VPN suministran seguridad de red extensible, visibilidad de red sin comparación, gestión y control. Los productos WatchGuard están respaldados por el servicio WatchGuard Live Security®, un programa de formación, mantenimiento y soporte innovador. WatchGuard dispone de sede oficial en Seattle y tiene oficinas en Norte América, Europa, Asia Pacífico y Latino América. Para información más detallada, visite www.watchguard.es.

Para más información

WATCHGUARD
Carlos Vieira

spain@watchguard.com

Tel.:+34 619 548 912 / 902 636 626

