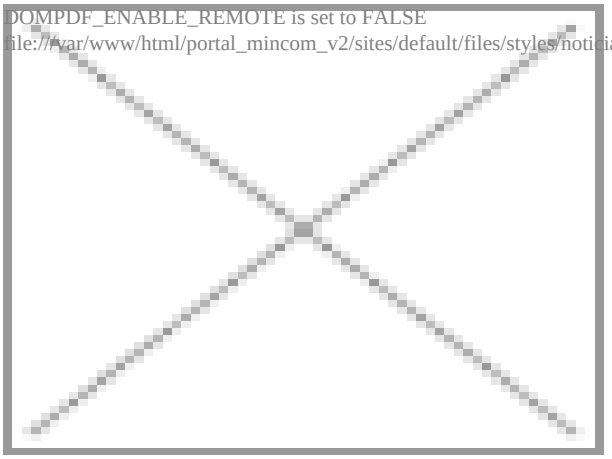

Fuente:
Siliconweek

Desde HP advierten sobre las desconfiguraciones que sufren los servidores y los errores de programación que se pueden encontrar en el software.

Que haya grupos de ciberdelincuentes dispuestos a jugar malas pasadas a usuarios y empresas no significa que sea imposible protegerse y, mucho menos, que haya que ponérselo fácil.

Ésa es la teoría. Pero parece que esa meta de seguridad ideal de momento no se está consiguiendo, al menos si nos fijamos en un par de datos que aporta el último **informe sobre ciberriesgo de HP Security Research**.

En este estudio de HP se revela que **más de dos quintas partes de las brechas**, un 44% de ellas en concreto, se producen **por vulnerabilidades antiguas**. Y por antiguas nos referimos a aquellas que tienen como mínimo un par de años y que incluso pueden llegar a alcanzar los cuatro años de vigencia.

Tanto es así que HP señala que el top 10 de los problemas que se vivieron el año pasado tenía como origen **código que era viejo**. Éste habría sido escrito realmente hace mucho.

“Muchos de los principales riesgos de seguridad son problemas conocidos por nosotros **desde hace décadas**, que dejan a las organizaciones expuestas a riesgos de forma innecesaria”, resume el vicepresidente sénior y director general de Enterprise Security Products, Art Gilliland.

Se sabe que **lo más común** en cuestión de vulnerabilidades **es la desconfiguración del servidor** y que las acciones contra software se basan sobre todo en errores de programación.

Disponible en:

http://www.siliconweek.es/security/virus/un-44-de-las-brechas-de-segurid... [1]

Links
[1] http://www.siliconweek.es/security/virus/un-44-de-las-brechas-de-seguridad-aprovecha-fallos-de-hasta-4-anos-de-antiguedad-76504#bJCwIXAlYXo30O3D.99