Los hackers ponen en evidencia la incompetencia de las empresas proveedoras de seguridad informática, lo que hace innegable la cuestión de que las actuales tecnologías de mitigación de amenazas están quebrantando la confianza en toda la industria que las suministra, indicó un estudio elaborado por SafeNet.

Cuando se les preguntó a los encuestados si tenían confianza en la capacidad de la industria de la seguridad informática para detectar o prevenir violaciones de seguridad, sólo 19 por ciento estaban seguros, 49 por ciento seguía sin estar convencido de que la industria puede parar las amenazas actuales, y 33 por ciento consideró que se han vuelto menos confiables en su capacidad para hacerlo.

El análisis señala que 66 por ciento de los profesionales de seguridad creen que van a sufrir fuga de datos dentro de los próximos tres años.

La investigación revela que uno de cada cinco de los profesionales de seguridad en las empresas no confiarían la seguridad de sus datos personales en sus propias redes y uno de cada tres, es decir, el 35 por ciento afirmaron que sus inversiones en seguridad están dirigidas a tecnologías erróneas, sin embargo, 95 por ciento continuará invirtiendo en las mismas estrategias de seguridad de datos.

En tanto, tres de cada cuatro, es decir 74 por ciento, indicó que sus defensas perimetrales son efectivas, y 29 por ciento dijo que si una violación al perímetro de la red se produce, sus datos de gran valor no estarían a salvo.

Así, más de 74 por ciento de los entrevistados indicaron que mientras ellos creen que sus defensas de perímetro de red son efectivas para mantener aislados a usuarios no autorizados, 31 por ciento de esos mismos encuestados reconocieron que sus defensas han sido violadas en el pasado. Lo que es más preocupante es que 20 por ciento dijo que desconocía si sus

redes habían sido violadas, lo que indica que los encuestados pueden no tener la tecnología adecuada para detectar si una violación a la seguridad interna o externa se ha producido.

Los resultados de la encuesta cuestionan "si las organizaciones cuentan con la tecnología de protección de datos suficiente para grabar pistas de auditoria precisas, hacer cumplir y mantener el control de sus datos, ya sea en las instalaciones, en la nube o en un entorno virtual".

El 95 por ciento de los encuestados afirmó que han mantenido o aumentado su inversión en seguridad perimetral; sin embargo, 55 por ciento considera que su empresa no está gastando lo suficiente en seguridad.

Las inversiones en tecnologías de redes perimetrales continúan creciendo, incluso de cara al creciente robo de datos, que no han podido abordar adecuadamente.

'Ciberamenazas': algo está cambiando

¿Estamos inmersos en una 'ciberguerra'? Durante los últimos diez años se viene anunciando que los próximos conflictos internacionales podrían ser, de hecho, guerras en el 'ciberespacio'. O al menos tendrán un enorme componente de lucha en red.

Estados, pero también empresas y ciudadanos, se ven cada vez más afectados por estos ataques, que pueden tener diferentes objetivos, desde el robo de la propiedad intelectual hasta la desestabilización de infraestructuras críticas.

¿Ha llegado la hora de afirmar que la 'ciberguerra' ya está aquí, o se trata de una exageración fruto de la 'fantasía' de los medios de comunicación y alimentada por las compañías de seguridad informática?

Varios acontecimientos en los últimos tiempos marcan la importancia de un fenómeno de dimensiones globales. Uno de los más recientes y graves fue protagonizado por el célebre virus Stuxnet contra Irán en 2010, que fue capaz de dañar y retrasar el programa nuclear iraní y cuya autoría fue enseguida atribuida a Israel y EEUU.

Un ataque similar cuyo origen está también en Israel y EEUU fue protagonizado por el virus Flame, cuya detección fue publicada en 2012 y categorizado como el 'software' de espionaje más complejo descubierto hasta la fecha.

Otro caso destacado fue la serie de 'ciberataques' contra Estonia procedentes de Rusia en 2007 -con bloqueos a sitios oficiales, bancos y medios- a raíz de un conflicto diplomático desembocó en la apertura de un importante centro de análisis de ciberamenazas de la OTAN en ese país.

También Corea del Sur ha sufrido algunos 'ciberataques' sonados en 2009 y 2011, de los cuales acusa invariablemente a su vecino y enemigo, Corea del Norte.

No todo son amenazas creadas por estados para atacar a otros estados. El surgimiento de grupos como Anonymous o Lulzsec han llegado a comprometer instituciones públicas y compañías de varios países con sus intrusiones en algunos sitios web -aprovechando fallos de seguridad- y la publicación de datos comprometedores. Parece que nadie está a salvo, ni siquiera el FMI o la mismísima CIA.

Años de experiencia

EEUU lleva años acumulando experiencias y desarrollando 'ciberarmas', pero ha sido en los últimos años y bajo el mandato de Barak Obama cuando parece haber pisado el acelerador, con la creación de un mando específico.

De hecho, Estados Unidos planea considerar los ataques cibernéticos como acciones de guerra, a las que podría responder con armas convencionales. Otros países, como Alemania, han anunciado a bombo y platillos la creación de centros especializados en la lucha contra el cibercrimen.

Desde hace años, este tipo de información ya no se oculta. Tal y como afirmó en 2010 **Ian Lobban**, director del Cuartel General para las Comunicaciones Gubernamentales del Reino Unido (GCHQ), varios países ya están utilizando técnicas de 'ciberguerra' para atacarse entre ellos y necesitan permanecer alerta todo el día para proteger sus sistemas informáticos.

Compañías

Mientras tanto, el propio diario The New York Times remarca que cada vez más compañías reconocen en público haber sufrido 'ciberataques', cosa impensable hasta hace relativamente poco por la mala imagen que se proyecta.

Las empresas quizá se ven amparadas por un efecto cadena que hace que reconocer estos ataques no les hace parecer 'descuidadas', sino 'víctimas'. No en vano, nombres tan destacados del sector de Internet y las nuevas tecnologías como Twitter, Facebook y Apple ya han admitido recientemente haber sido víctimas de ataques de mayor o menos gravedad, un camino marcado en su día por Google que en 2010 denunció intrusiones en GMail desde China. Incluso meduios como el Wall Street Journal y el Washington Post han admitido ser objeto de ataques.

Recuerda el diario neoyorquino el gran impacto que tuvo un informe de la compañía antivirus McAfee, que aseguraba que cerca de 80 organizaciones, entre las que se encontrarían Naciones Unidas y gobiernos y empresas en todo el mundo, se vieron afectadas por un masivo 'ciberataque'. Y el pasado año, la compañía de procesos de pago Global Payments reconoció a regañadientes una intrusión en sus sistemas que afectó a MasterCard, Visa, American Expressy Discover Financial Services, junto con bancos y otras franquicias contarjetas de pago vinculadas a dichio servicio.

Empresas tan sensibles como Lockheed Martin, el principal proveedor de tecnología del Pentágono, tuvo que reconocer en 2011 frecuentes 'ciberataques' tras publicarse uno de ellos, cuyas consecuencias trató de minimizar.

Mientras que en Washington el presidente Obama quiere fomentar un mayor intercambio de información sobre 'ciberamenazas' entre el Gobierno y las empresas privadas -aunque de forma voluntaria-, la Comisión Europea quiere ir un poco más allá y anunció en Bruselas su intención de obligar legalmente a determinadas empresas y administraciones públicas a informar sobre 'ciberataques' u otros incidentes de seguridad digitales.