12 PREDICCIONES DE SEGURIDAD PARA 2012

TREND MICRO™

Cada año por estas fechas, me reúno con mis equipos de investigación y comentamos lo que creemos que nos deparará el año entrante en cuanto a las amenazas con las que se enfrentarán nuestros clientes. Es un debate importante que nos ayuda no solo a compartir con usted información sobre las amenazas para las que creemos que debe estar preparado, sino también a guiarnos en el proceso de creación de productos y servicios que le ofrezcan protección frente a dichas amenazas.

Este año, al mirar hacia delante, hemos realizado 12 predicciones para 2012 que se incluyen en cuatro categorías principales:

- Grandes tendencias de TI
- Panorama de los dispositivos móviles
- Panorama de las amenazas
- Filtraciones de datos e infracciones

Al observar estas predicciones, comprobamos que las tendencias comunes reflejan la aparición de atacantes más sofisticados y el desinterés por los equipos de sobremesa. Se desvaneció la esperanza de que los nuevos sistemas operativos harían del mundo un lugar más seguro. Esto significa que en 2012 nuestros clientes deberán seguir avanzando hacia un modelo que se base más en los datos para obtener una seguridad y una privacidad eficaces a medida que se unan a la consumerización, la virtualización

y la nube. Por nuestra parte, en Trend Micro debemos seguir trabajando en estos ámbitos clave para ayudar a nuestros clientes a conocer estas tendencias de amenazas y a protegerse de ellas en 2012.

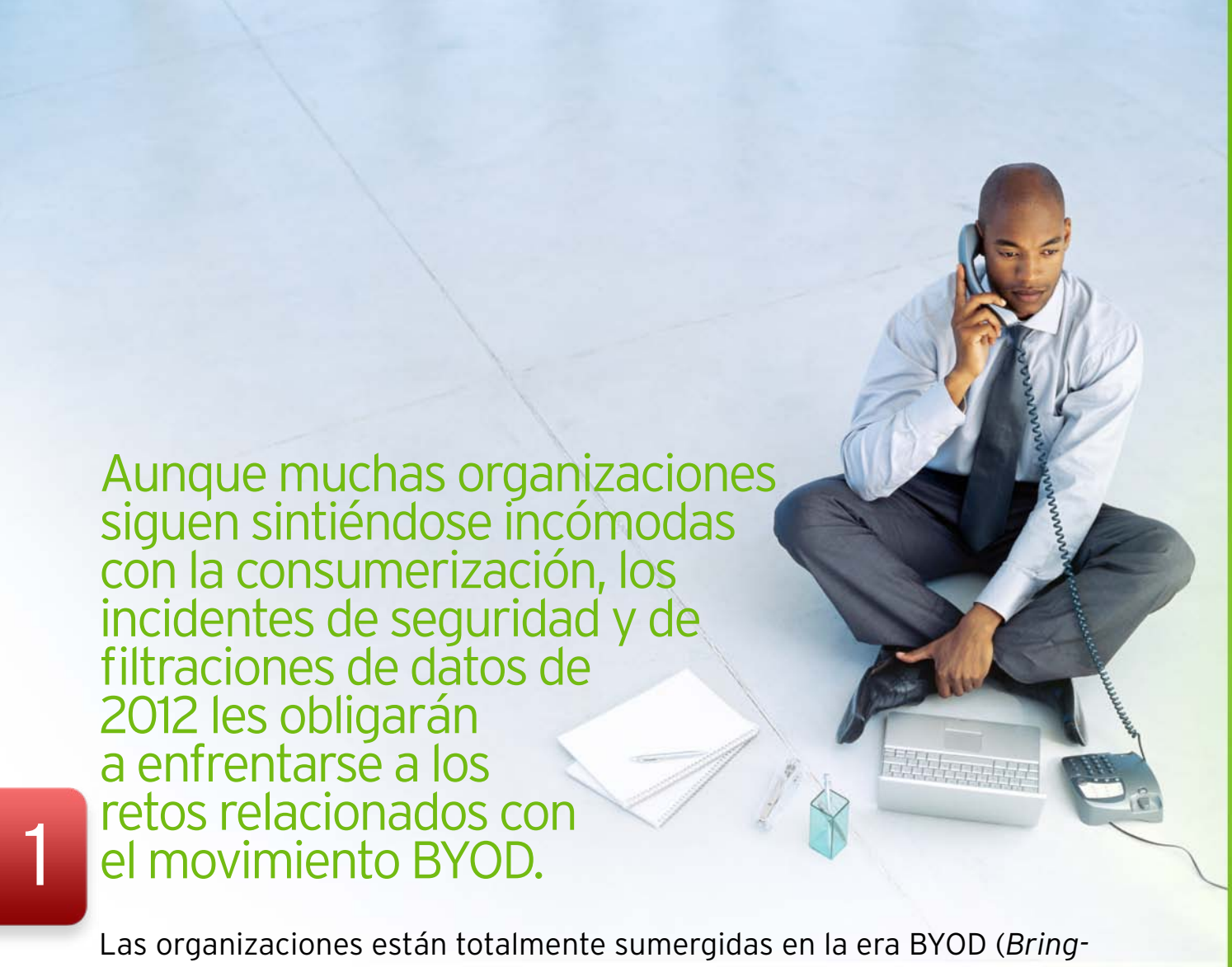
En Trend Micro, trabajamos continuamente para comprender no solo las amenazas actuales, sino también las tendencias que están por llegar, tal como indica el nombre de nuestra empresa ("trend" significa "tendencia" en inglés). Esto nos permite ayudarle a proteger mejor sus datos y activos.

Espero que las predicciones de este año le resulten útiles, además de interesantes, para que 2012 sea un año seguro.

Raimund

Raimund Genes
Director de tecnología de Trend Micro

GRANDES TENDENCIAS DE TI



Aunque muchas organizaciones siguen sintiéndose incómodas con la consumerización, los incidentes de seguridad y de filtraciones de datos de 2012 les obligarán a enfrentarse a los retos relacionados con el movimiento BYOD.

1

Las organizaciones están totalmente sumergidas en la era BYOD (*Bring-Your-Own-Device*, o uso de dispositivos propios de los empleados). Cuantos más datos corporativos se almacenan y se abren en dispositivos que los administradores de TI no controlan totalmente, aumenta la probabilidad de que se produzcan incidentes de pérdidas de datos que se pueden atribuir directamente al uso de dispositivos personales que no están correctamente protegidos. No cabe duda de que en 2012 ocurrirán incidentes de esta índole.

El desafío real para los propietarios de los centros de datos será gestionar la creciente complejidad a la hora de proteger los sistemas físicos, virtuales y basados en la nube.

2

Si bien aún es posible que se produzcan ataques dirigidos específicamente a equipos virtuales y servicios de computación en la nube, los atacantes no necesitarán recurrir a ellos inmediatamente, ya que los ataques dirigidos convencionales continuarán siendo eficaces en estos nuevos entornos. Las plataformas virtuales y en la nube son igual de fáciles de atacar, pero más difíciles de proteger. Por ello, la carga recae en los administradores de TI, responsables de proteger los datos confidenciales de las empresas cuando estas adoptan dichas tecnologías. Aplicar parches a una gran variedad de servidores virtualizados supone un reto, lo que permite a los hackers piratear servidores, desviar tráfico y/o robar datos de sistemas vulnerables.

PANORAMA DE LOS DISPOSITIVOS MÓVILES

Las plataformas de los dispositivos smartphone y las tablet, especialmente *Android*, sufrirán más ataques de ciberdelincuentes.

3

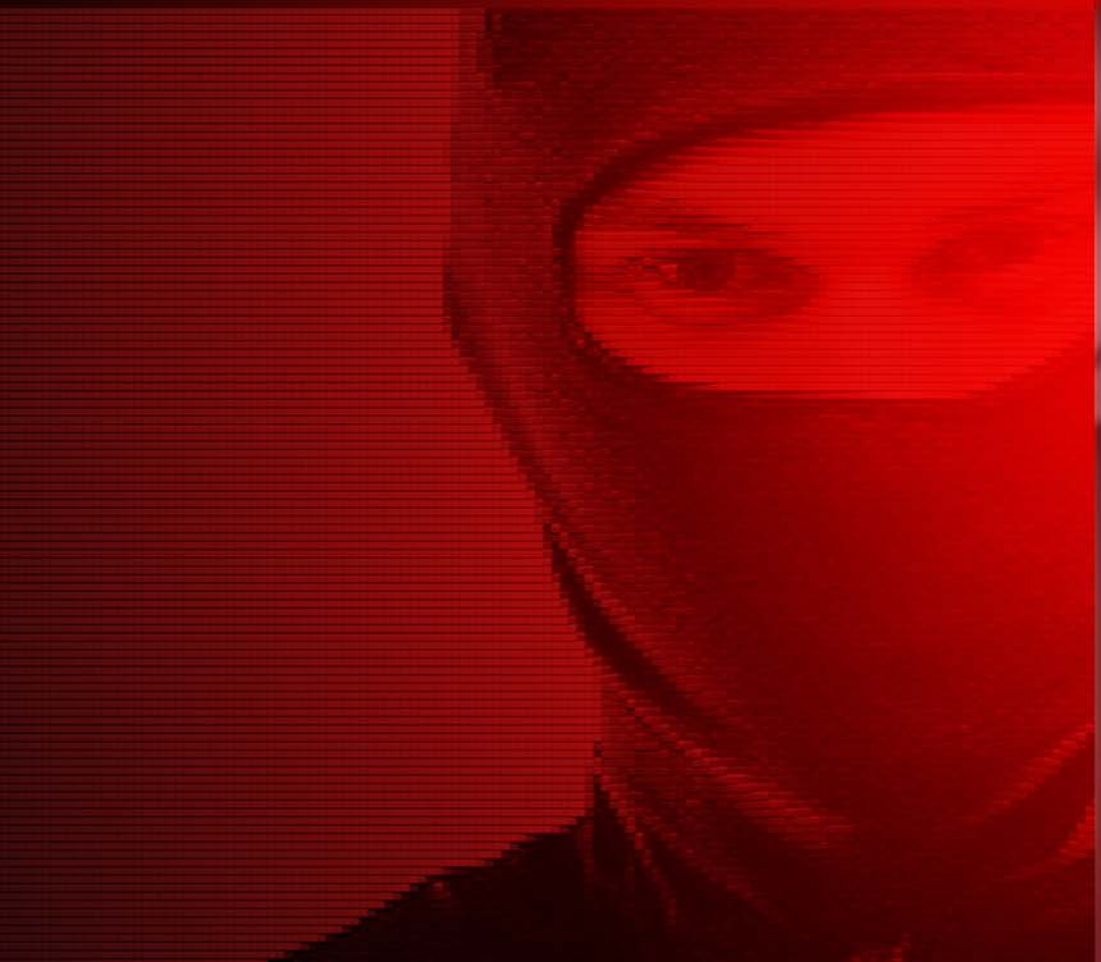
A medida que aumenta el uso de dispositivos smartphone en todo el mundo, las plataformas para móviles se vuelven objetivos más tentadores para los ciberdelincuentes. La plataforma *Android*, concretamente, es uno de los objetivos de ataque favoritos debido a su modelo de distribución de aplicaciones, que la convierte en una plataforma totalmente abierta para cualquier empresa. Creemos que esta tendencia continuará en 2012, aunque otras plataformas también estarán en el punto de mira.

Se detectarán vulnerabilidades de seguridad en aplicaciones para móviles legítimas, con lo que los ciberdelincuentes podrán extraer datos con mayor facilidad.

4

Actualmente, las amenazas de las plataformas para móviles aparecen en forma de aplicaciones maliciosas. En el futuro, es de esperar que los ciberdelincuentes también ataquen aplicaciones legítimas. Es probable que detecten vulnerabilidades o errores de código que faciliten el robo o la exposición de datos de usuarios. Para agravar más el problema, son pocos los desarrolladores de aplicaciones que cuentan con un proceso de gestión y resolución de vulnerabilidades sólido, lo que significa que el tiempo de exposición de estos fallos puede ser mayor.

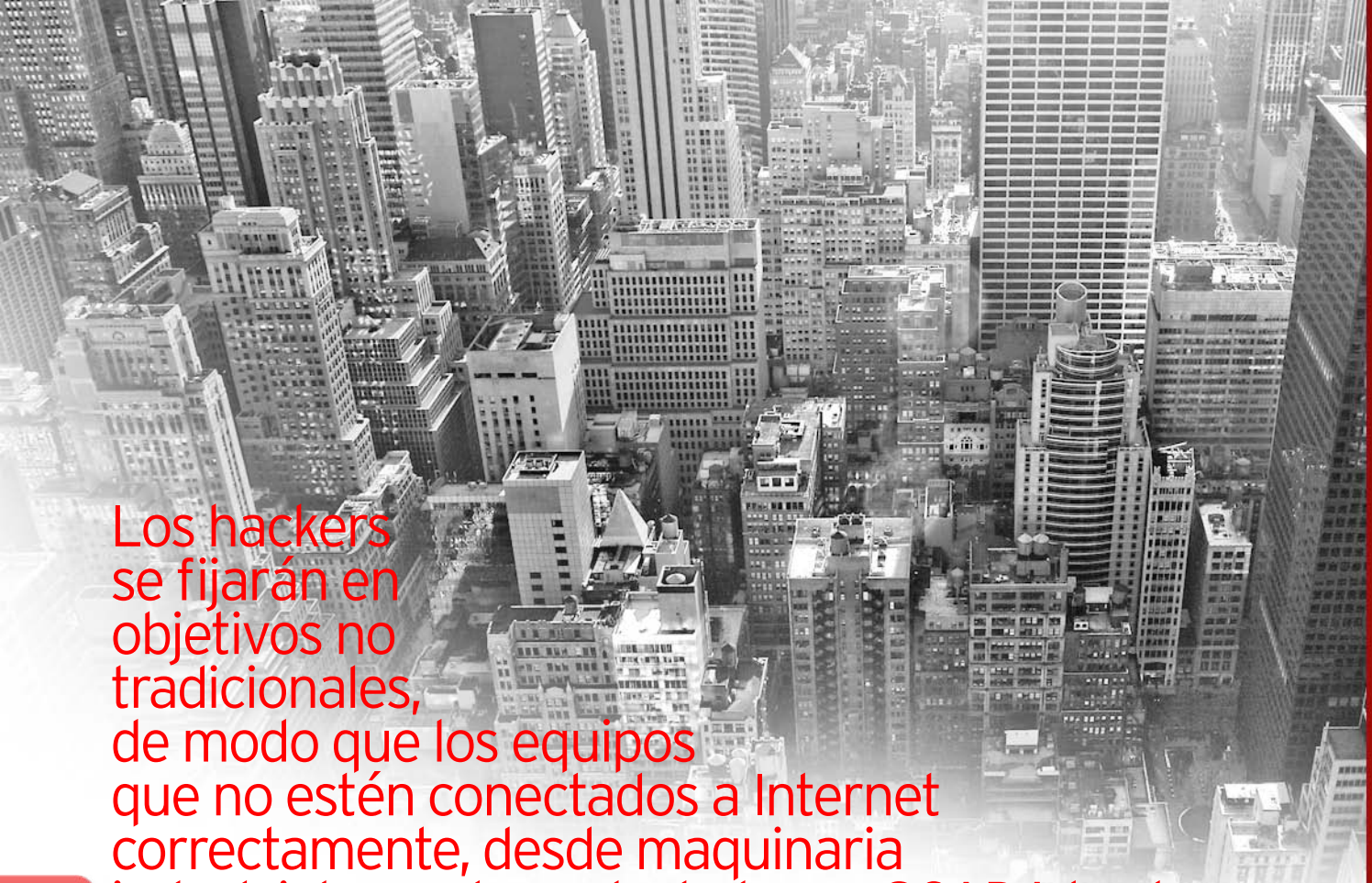
PANORAMA DE LAS AMENAZAS



Aunque las redes robot serán más pequeñas, crecerán en número, con lo que será más difícil realizar intervenciones para el cumplimiento eficaz de la ley.

5

Las redes robot, la herramienta de ciberdelincuencia tradicional, evolucionarán como respuesta a las acciones llevadas a cabo por el sector de la seguridad. Es posible que haya llegado el fin de las redes robot masivas. Puede que las sustituyan un mayor número de redes robot más pequeñas pero más manejables. Las redes robot más pequeñas reducirán los riesgos frente a los ciberdelincuentes, ya que si se pierde solo una, no supondrá un problema tan grave como antes.



Los hackers se fijarán en objetivos no tradicionales, de modo que los equipos que no estén conectados a Internet correctamente, desde maquinaria industrial pesada controlada por SCADA hasta dispositivos médicos, sufrirán ataques.

6

En 2012, se intensificarán los ataques dirigidos a sistemas de control de supervisión y adquisición de datos (SCADA), así como a otros equipos accesibles a través de redes, puesto que determinados hackers de amenazas irán más allá del robo de dinero y datos valiosos. STUXNET y otras amenazas de 2011 evidenciaron que los sistemas SCADA se han convertido en un objetivo activo. Se espera que esto derive en ataques de pruebas de concepto contra sistemas conectados a redes, como la equipación médica.

7

Los ciberdelincuentes encontrarán formas más creativas de ocultarse de la ley.

Cada vez más, los ciberdelincuentes intentarán obtener beneficios mediante el uso indebido de fuentes de ingresos en línea legítimas como la publicidad en línea. Esto les permitirá eludir el cumplimiento de la ley y sortear a los reguladores antifraude contratados por entidades bancarias y otras agencias financieras.

FILTRACIONES DE DATOS E INFRACCIONES

Existirán más grupos de hackers que supondrán una mayor amenaza para las organizaciones que protegen datos muy confidenciales.

8

Grupos en línea como Anonymous y LulzSec, que dirigían sus ataques a empresas e individuos por distintos motivos políticos, alcanzaron gran renombre en 2011. Es probable que en 2012 estos grupos estén aún más motivados. Dispondrán de una mayor cualificación tanto para acceder a las organizaciones como para evitar la detección por parte de los profesionales de TI y las agencias para el cumplimiento de la ley. Las organizaciones se verán obligadas a tratar con esta nueva amenaza y a aumentar sus esfuerzos para proteger la información corporativa importante.

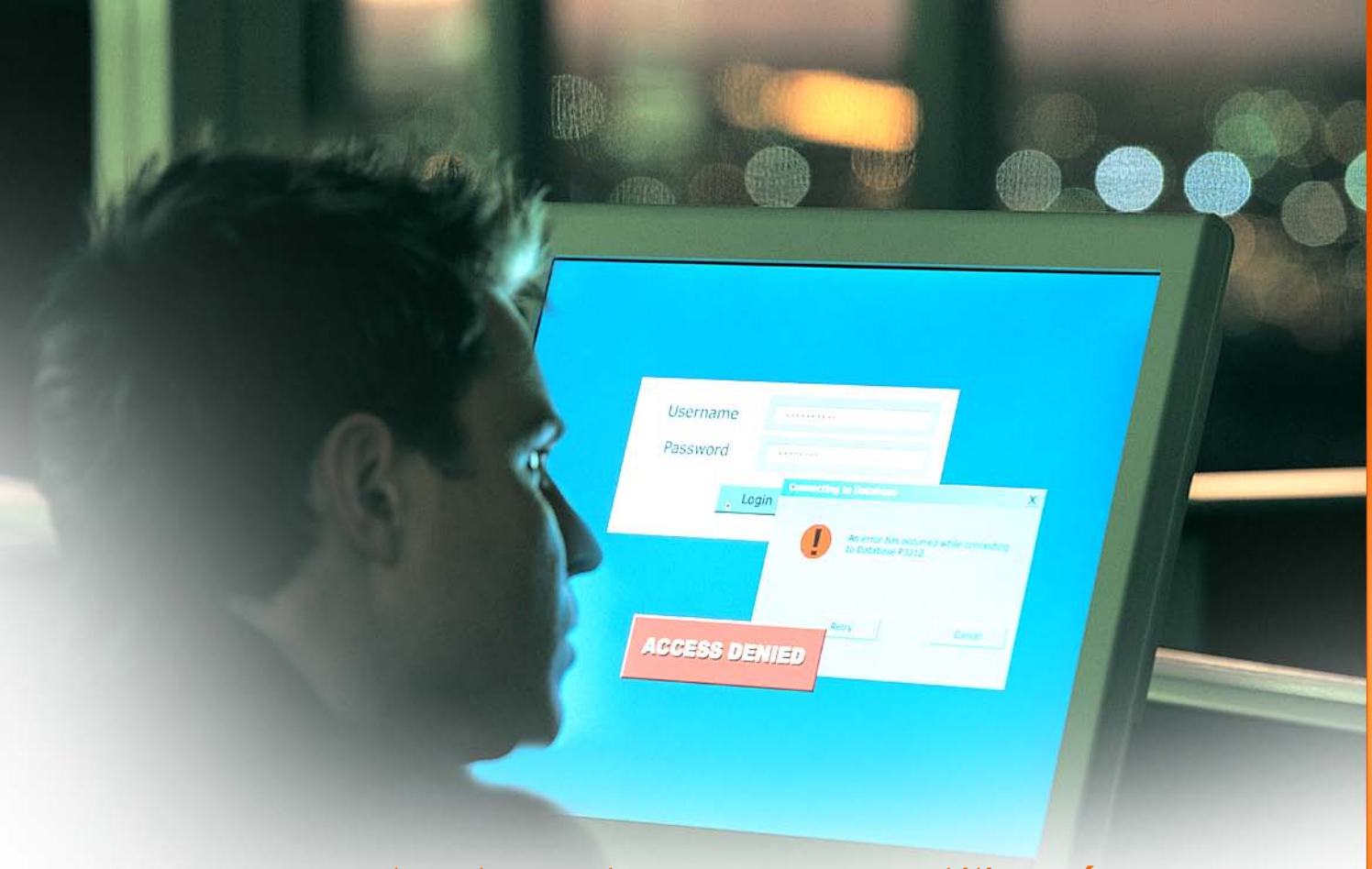
La nueva generación de redes sociales redefinirá el concepto de "privacidad".

9

La información confidencial de los usuarios suele acabar en línea, gracias principalmente a los propios usuarios. La nueva generación de jóvenes usuarios de redes sociales presenta una actitud diferente respecto a la protección y al uso compartido de la información. Son más proclives a revelar datos personales a otras empresas, como ocurre en los sitios de las redes sociales. Asimismo, tampoco suelen tomar medidas para restringir información a grupos específicos como sus amigos. En pocos años, las personas con conciencia de la privacidad serán una minoría, lo cual supone una perspectiva ideal para los atacantes.

A medida que la ingeniería social pasa a ser la tendencia predominante, las empresas se convierten en objetivos fáciles.

Hasta la fecha, las estratagemas de ingeniería social más sofisticadas se han dirigido contra grandes empresas. Sin embargo, hoy en día los ciberdelincuentes son tan expertos en redes sociales que cada vez les cuesta menos dirigir ataques a empresas de forma individual. Este hecho, junto con el gran volumen de información personal que está disponible en línea, permitirá a los ciberdelincuentes llevar a cabo ataques precisos y más personalizados contra empresas de todos los tamaños. Como sucedía con los ataques anteriores, los ciberdelincuentes seguirán centrándose en la obtención de acceso a las cuentas bancarias en línea de las empresas.



11 Los nuevos hackers de amenazas utilizarán sofisticadas herramientas de ciberdelincuencia para alcanzar sus propios fines.

En 2012, continuará aumentando el número de ataques dirigidos. No obstante, los ciberdelincuentes no serán los únicos que utilicen estos ataques. Cuando la eficacia de las amenazas persistentes avanzadas sea más evidente, otros colectivos como grupos activistas, corporaciones y gobiernos utilizarán herramientas y tácticas de ciberdelincuencia similares para lograr sus objetivos.

12 En 2012 se producirán más incidentes causados por infección de malware y ataques de hackers.

Las grandes empresas continuarán sufriendo ataques de perfil elevado en 2012. Los datos empresariales importantes y críticos se extraerán mediante infecciones de malware y ataques de hackers. Como resultado, se producirán incidentes de pérdida de datos significativos, que pueden afectar a miles de usuarios y a su información personal. Estos incidentes pueden derivar en pérdidas significativas directas e indirectas para los colectivos implicados.

Trend Micro Incorporated, líder global de seguridad en la nube, crea un mundo seguro para intercambiar información digital con sus soluciones de seguridad de contenidos de Internet y de gestión de amenazas para empresas y particulares. Trend Micro es una empresa pionera en seguridad de servidores con más de 20 años de experiencia que ofrece seguridad del más alto nivel adaptada a las necesidades de nuestros clientes, detiene las amenazas más rápidamente y protege la información en entornos físicos, virtualizados y basados en la nube. Con el respaldo de la infraestructura de Trend Micro™ Smart Protection Network™, nuestra tecnología, productos y servicios de seguridad basados en la nube líderes del sector consiguen detener las amenazas allá donde surgen, en Internet, y cuentan con la asistencia de un equipo de más 1.000 expertos en amenazas en todo el mundo. Si desea más obtener más información, visite **www.trendmicro.com**.

TREND MICRO™

Securing Your Journey to the Cloud