PANDA CLOUDPROTECTION

Simply... ***Evolution***

EL DESAFÍO DE UNA NAVEGACIÓN WEB SEGURA PARA SU EMPRESA

PANDA CLOUD
OFFICE PROTECTION

PANDA CLOUD
EMAIL PROTECTION

NUEVO
PANDA CLOUD
INTERNET PROTECTION

PANDA SECURITY | 20 Aniversario 1990-2010

Índice

1. Situación actual

El número de malware existente hoy en día es tal que las necesidades de protección de las empresas han alcanzado niveles de difícil satisfacción.

Además, el malware actual se caracteriza por ser en muchos casos de carácter "silencioso", es decir, permanece oculto para el usuario mientras lleva a cabo robos de identidad y otras acciones que producen importantes pérdidas económicas y de productividad.

Este panorama de riesgo exige que las empresas adopten medidas e implanten sistemas de seguridad y tecnologías avanzadas para detectar y eliminar el malware. Sin embargo, como veremos a continuación, la propia estructura organizativa de las empresas y su limitación de recursos hacen que la solución instalada no satisfaga plenamente sus necesidades específicas en materia de seguridad y protección.

Como norma general, las **pequeñas y medianas empresas no disponen de personal especializado** para proteger y gestionar la seguridad de sus redes, y tienden a invertir el grueso de sus recursos en la actividad principal de la empresa. Esto les impide destinar los recursos que debieran a la seguridad informática.

Son empresas que necesitan dedicarse plenamente a su actividad principal sin que su seguridad se vea afectada; precisan manos expertas en las que confiar y tener una monitorización continua de su red informática.

Además, estas compañías a menudo disponen de centros de producción **y filiales geográficamente muy alejadas** unas de otras. Todas ellas necesitan ser **gestionadas de forma remota** desde un punto centralizado, por lo que la solución pasa por **simplificar** la gestión y lograr un control continuo con un **reducido consumo de ancho de banda**.

Sin embargo, lo que estas empresas encuentran cuando quieren afrontar la situación de riesgo son antivirus que requieren demasiado tiempo y esfuerzo en su instalación, y que una vez instalados exigen:

- **Hardware adicional**, como servidores que alojen una consola centralizada con sus servicios y bases de datos.
- **Licencias de software**, como software de bases de datos para generar informes o configurar la protección.
- **Personal especializado en seguridad**, que se encargue de gestionar y monitorizar la seguridad sin estar dedicado a la actividad principal de la empresa.

Así las cosas, lógicamente muchas empresas prefieren no ocuparse de todas estas tareas, ya que les distraen de la actividad principal de su negocio, y permanecen en una situación de búsqueda continua de la solución que dé respuesta a sus necesidades. Y mientras tanto, la vulnerabilidad aumenta.

2. Qué riesgos tiene la situación actual del malware para las empresas

- Se reciben 50.000 ficheros diarios, de los que 37.000 son nuevo malware. El 99,4% se procesan automáticamente por Inteligencia Colectiva con una media de 6 minutos por cada resolución.
- El 52% del nuevo malware procesado por Inteligencia Colectiva sólo vive durante 24 horas, desapareciendo después.
- Durante el primer trimestre de 2009, Inteligencia Colectiva procesó 4.474.350 ficheros.
- Para hacerlo de forma manual, hubieran sido necesarios 1.898 técnicos y 926.347 horas de trabajo.
- La base de datos de Inteligencia Colectiva ocupa más de 18.000 GB o 148 billones de bits.
- Transformando esta cantidad de información en texto, podríamos escribir 727.373 enciclopedias británicas gracias a los 29 billones de palabras que ocuparía la misma extensión que la base de datos de Inteligencia Colectiva.
- Con esta magnitud, podríamos rellenar casi 33 mil millones de páginas de texto, que si pusiéramos una detrás de la otra impresas físicamente, se podría cubrir una distancia de más de 9 millones de kilómetros o ir y volver a la luna 12 veces.
- Y si tuviéramos que enviar toda esta información mediante una línea estándar de ADSL, tardaríamos 1.045 días.

Por desgracia, lo más habitual es que esta situación no nos parezca lo suficientemente cercana, y que no nos planteemos qué impacto puede tener para nuestro negocio.

Sin embargo, la lista de riesgos es amplia. Los más evidentes nos pueden venir fácilmente a la cabeza, pero hay otros que no podemos calcular de antemano y que pueden repercutir negativamente en nuestra economía, que es, al fin y al cabo, el fin último de cada proyecto empresarial.

¿Cuáles son estos riesgos?

Lógicamente, todos tienen como resultado último una pérdida económica debida a factores como tener que parar nuestros sistemas, que nuestros empleados pierdan tiempo valioso, o que los ciber criminalesciber criminales consigan acceder a nuestros datos para robarnos dinero. Pero… ¿alguna vez ha calculado qué impacto puede tener para su negocio que sus clientes pierdan la confianza en su empresa?

Imaginemos que sufre un ataque y su base de datos de clientes queda al descubierto, o que su ordenador manda spam o phishing sin saberlo, o que opera online y todo el que compra en su sitio web resulta estafado porque un troyano ha robado sus datos bancarios…

3. Vías de infección más comunes

Resulta complicado hacerse una idea de la gran cantidad de amenazas informáticas a las que nos enfrentamos cada día. Se clasifican en muchos tipos diferentes, dependiendo qué busca su autor, cómo se distribuyen, cómo llegan, etc.

Explicarlo sería una tarea ardua y complicada. Pero se puede simplificar atendiendo a las tres vías de contagio más frecuentes, que son las que hay que vigilar.

- Ataques o infecciones que nos llegan a través de correo electrónico.
- Infecciones a través de la navegación web.
- Infecciones a través del propio PC del usuario.

3.1. Ataques o infección a través de correo electrónico

El correo electrónico es, sin duda, una herramienta que se ha implantado en todas las compañías y que constituye una forma de comunicación eficiente, rápida y asequible. Sin embargo, es una de las vías de recepción masivas y habituales de spam, phishing y otros tipos de malware como virus, gusanos y troyanos.

Además del tiempo que se pierde haciendo limpieza del propio buzón, y que supone un impacto económico para la organización, nos encontramos con peligros como confiar en la educación del usuario para poder detectar y conocer de antemano qué mensaje tiene riesgo de ser una amenaza.

Por lo tanto, la protección tanto a nivel de servidor como del propio cliente de correo electrónico es fundamental para no dejar la responsabilidad de la infección en manos de nuestros empleados.

3.2. Infecciones a través de navegación web

Este tipo de infección es mucho más común últimamente, y su principal riesgo es que se "disfrazan" de contenidos inocentes para conseguir que el usuario se descargue –con o sin su conocimiento- ficheros que pueden estar infectados.

Este es el caso de plugins para ver determinados vídeos, ficheros de programas que parecen lícitos, contenidos en pdf que pueden llevar oculto malware, etc.

Además, el riesgo es más evidente dado que los ciber criminalesciber criminales están profesionalizándose y mejorando la calidad de sus falsificaciones a la hora de hacer pasar webs fraudulentas por webs lícitas. Tal es el nivel de verosimilitud alcanzado que, por ejemplo, podemos estar creyendo acceder a nuestro banco cuando en realidad estamos introduciendo nuestros datos de acceso bancarios en una página "clonada" a tal efecto.

3.3. Infecciones a través del propio PC del usuario

Otro de los grandes riesgos a los que nos podemos enfrentar es al de la seguridad del propio PC del usuario. Hay muchos factores que influyen en que se cuele un virus en la organización por motivos como:

- No aplicar las normas fundamentales de seguridad corporativa (por ejemplo, configurar siempre contraseñas adecuadas).
- No aplicar los parches de seguridad que Microsoft Windows publica de forma regular.
- No tener instalada ninguna protección de seguridad, que el producto instalado no sea adecuado y no cubra todas las posibles amenazas, o que, simplemente, esté desactualizado.
- El usuario es remoto y se conecta desde cualquier sitio, sin disponer de unas políticas de seguridad adecuadas y sin realizar las comprobaciones necesarias.
- Etc.

Los tres principales vectores de infección del malware actual son:

- A través del e-mail.
- Mediante la navegación web.
- Por el propio PC individual del usuario.

Cualquiera de los casos anteriores supone un gran riesgo para la integridad corporativa.

A todo esto hay que sumar no sólo el que se puedan descargar ficheros potencialmente peligrosos de Internet, sino el riesgo que supone la utilización de comunidades o redes sociales para esta práctica, dejando en manos de los usuarios el tomar decisiones sobre qué links pinchar, qué sitios visitar o a qué encuentro online suscribirse.

Además, se ha hecho muy popular el intercambiar información mediante dispositivos de almacenamiento masivo, tipo USB, que están siendo también utilizados para la distribución de malware.

4. La navegación web como principal vector de ataque a las empresas

Las amenazas procedentes de Internet incrementan su impacto y frecuencia entre las empresas de hoy en día. El correo no deseado ocasiona graves problemas para todas las compañías, ya sea en forma de amenazas de seguridad, consumiendo excesivo ancho de banda o reduciendo la productividad de los usuarios, al permitir la llegada de grandes volúmenes de spam.

Las amenazas más peligrosas procedentes de Internet están dirigidas a las empresas, y tienen generalmente causas políticas o económicas. Recientemente un artículo de BBC News ilustraba dramáticamente esta tendencia y relataba el siguiente experimento: un ordenador sin firewall o antivirus alguno, y sistema operativo Windows XP fue conectado a Internet. El objetivo era determinar cuánto tiempo transcurría antes de que fuera atacado por alguna de las amenazas que circulan por la Red. El resultado fue devastador: en solo 8 segundos, el ordenador fue golpeado por Sasser, uno de los gusanos más rápidos en expandirse por Internet.

Las preocupaciones recientes sobre seguridad tienen origen en las redes internas. La pérdida de información sensible almacenada en las redes corporativas puede afectar dramáticamente a las organizaciones.

La información personal o económica que se envía desde la red corporativa puede causar daños legales y económicos inestimables. Estos daños deben evitarse a través de una política de seguridad racional y personalizada, reforzada por una herramienta robusta y adecuada con una posición estratégica en la red. Asimismo, cualquier solución de seguridad debe garantizar la recepción de información importante. Un falso positivo que detecta spam o contenidos potencialmente peligrosos, puede causar retrasos y pérdida de información, convirtiendo la solución en parte del problema. Adicionalmente, el volumen de tráfico recibido o enviado por las empresas, crece continuamente día tras día, lo que convierte a la pasarela en un punto crítico para la red; cualquier dispositivo agregado en este punto debe garantizar el flujo de tráfico sin interferencia.

4.1. Ingeniería Social

Gran parte del malware se instala en los ordenadores de las víctimas utilizando técnicas de ingeniería social.

La ingeniería social consiste en tratar de conseguir información confidencial de los usuarios mediante su manipulación, o convenciéndolos para que realicen acciones que van en contra de su política de seguridad.

La ingeniería social y el ciber crimen están estrechamente relacionados: una técnica de ingeniería social eficaz convencerá a los usuarios para que proporcionen sus datos o instalen el programa malicioso, y a continuación éste se encargará de capturar la información y enviarla a los estafadores.

La principal vía de entrada que utilizan las técnicas de ingeniería social son los mensajes de correo electrónico. Normalmente estos mensajes llevan adjuntos archivos de apariencia totalmente normal (Word, Wxcel, imágenes,…), que, una vez ejecutados realizan la tarea de robo de identidad y datos para la que han sido creados. Sin embargo, no todas las familias de malware se distribuyen a través de adjuntos en mensajes de correo electrónico. Tal es el caso de la familia Waledac, que se caracteriza por la variedad de temas que utiliza para su distribución y porque se distribuyen en mensajes de correo electrónico que, en lugar de adjuntos, incluyen enlaces a páginas web desde las que se descarga el gusano.

La razón de que los creadores de este tipo de malware utilicen enlaces a páginas web en lugar de archivos adjuntos es que así dificultan la detección del malware por parte de las compañías de seguridad. Y es aquí, en la detección, donde está el reto. Si antes bastaba con detectar el archivo adjunto para bloquear fácilmente la amenaza, ya que era la misma en todos los casos, ahora lo que hay que monitorizar y analizar es cada uno de los enlaces, que alojan malware diferente en función de parámetros tales como la hora, el navegador que se utiliza, la procedencia, etc.

La conclusión clara que podemos extraer de todo esto es que los ciber delincuentes, como "profesionales" de la propagación que son, se han dado cuenta de que intentar propagar una única muestra en un adjunto no es un método muy efectivo y que utilizar el sistema de enlaces resulta mucho más rápido, eficaz, y proporciona mayor número de víctimas.

Veamos a continuación otro ejemplo de ingeniería social que dio mucho de qué hablar y que muestra a las claras cómo la utilización de un buen gancho puede ser suficiente para convencer al usuario de que acceda a un vínculo fraudulento.

Renuncia de Barack Obama

En enero de 2009, comenzaron a distribuirse mensajes de correo electrónico sobre la supuesta renuncia de Barack Obama a la presidencia de Estados Unidos. Estos mensajes incluían un enlace a una página web en la que se podía consultar la impactante noticia:

Fig 1. Mensaje de correo sobre la renuncia de Obama.

Si se pulsaba el enlace del mensaje, el usuario era redirigido a una página web que imitaba a la original y en la que se podía leer la supuesta noticia, entre otras, como se puede ver en la siguiente imagen:

Fig 2. Supuesta página web oficial de Obama.

4.2. Redes Sociales y Web 2.0

Durante años, el uso de la ingeniería social ha sido una de las técnicas más extendidas por parte de los ciber delincuentes de cara a infectar al usuario. 2009, lejos de ser diferente, se ha caracterizado por la irrupción de técnicas de ingeniería social dirigidas contra las redes sociales.

No debemos olvidar que el objetivo de los ciber criminalesciber criminales es lograr el máximo beneficio, y para ello necesitan tener el mayor número posible de víctimas. Por eso, estamos hablando de criminales que están "a la última" en todo lo que tiene que ver con comunicación, actualidad y avances tecnológicos.

Las redes sociales constituyen, pues, un escenario ideal para ellos a tenor de las cifras de usuarios que se manejan: Facebook ha sobrepasado la cifra de 350 millones de usuarios, y Twitter no deja de crecer, teniendo sólo en Estados Unidos más de 15 millones de usuarios.

Cada día es más común ver a gente que utiliza mucho más las redes sociales que el correo electrónico como herramienta de comunicación con sus amigos. Y los ciber delincuentes, por supuesto, no son ajenos a esto.

Twitter

Como hemos comentado, la imaginación y la innovación de los ciber criminalesciber criminales aumenta y se adapta a las nuevas aplicaciones y plataformas de utilización masiva.

Twitter, herramienta de microblogging por excelencia, ha vivido su momento de oro en 2009, y pronto los ciber delincuentes se aprovecharon de ello. Ya en enero vimos cómo las cuentas de 33 celebridades, entre las que se encontraban Britney Spears o Barack Obama, tuvieron que ser suspendidas durante un tiempo ya que fueron "secuestradas" y comenzaron a facilitar información falsa.

En abril apareció un gusano para Twitter que, utilizando una técnica de cross-site scripting, infectaba a los usuarios cuando visitaban los perfiles de usuarios infectados. El gusano infectaba el perfil del usuario visitante, y continuaba así con su propagación.

Después aparecieron nuevas variantes de este gusano, y finalmente se supo quién era su creador: un joven llamado Mikey Mooney, que aparentemente quería atraer usuarios a un servicio competidor de Twitter.

Twitter ha captado la atención de los ciber delincuentes, que buscan cualquier forma de distribuir malware y spam a través de esta conocida herramienta

A principios de junio comenzaron a aparecer ataques en Twitter utilizando otras técnicas: básicamente han adoptado el BlackHat SEO (técnica que trataremos más adelante en el informe) para los usuarios de Twitter.

Twitter tiene una característica llamada *"Twitter Trends"*, que es una relación de los temas más tratados en Twitter, y cuando accedes a uno de ellos obtienes un listado de todos los tweets que hay publicados sobre ese tema. Estos temas son finalmente los que más gente lee, por lo que realmente son un objetivo muy valioso para los delincuentes.

Básicamente lo que los delincuentes están haciendo es escribir tweets sobre los temas que aparecen en Twitter Trends con links maliciosos a webs para instalar malware a quien las visite. El primer ataque que vimos se centró en sólo uno de los temas, pero días más tarde ampliaron su campo de acción y absolutamente todos los temas tenían links maliciosos. Por ejemplo, cuando el conocido actor David Carradine falleció, en unas pocas horas ya había cientos de tweets maliciosos, y lo mismo está sucediendo con todos los temas más populares de Twitter.

Fig 3. Ataques en Twitter.

Facebook

Ni que decir tiene que Facebook constituye también otro de los objetos de deseo de los creadores de malware, y, al igual que Twitter, ha sido víctima de técnicas de ingeniería social creadas específicamente para atacar a sus usuarios. A modo de ejemplo, valga la la cantidad de intentos de phishing para tratar de secuestrar cuentas de Facebook, con sitios que son idénticos a Facebook para hacer picar al usuario y robarle así sus datos.

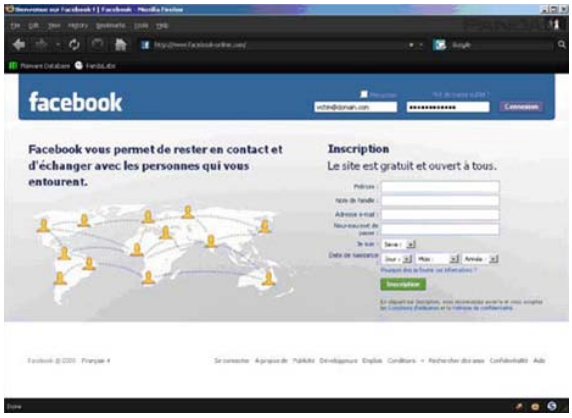


Fig 4. Página web que imita a la de Facebook.

También hemos visto casos de fraude, como el que descubrimos en septiembre, y con el que se pretendía robar dinero de los usuarios a cambio de obtener passwords de cuentas ajenas:

Fig 5. Imágen de cómo hackear una cuenta de Facebook.

El malware que más se ha servido de Facebook para propagarse es el perteneciente a la familia Koobface. Este gusano ha ido evolucionando y adaptándose a otras plataformas y redes sociales como Myspace o Twitter, que ha utilizado también para propagarse. Pero además, algunas de sus variantes instalan malware adicional en los equipos, desde troyanos bancarios a rogueware.

Web 2.0

Además de las redes sociales, hay multitud de servicios online, englobados en lo que comúnmente se conoce como Web 2.0, que también han sido víctimas de los ciber delincuentes. Y entre ellos destaca Youtube, la plataforma por excelencia de visionado de videos por Internet. Youtube permite a los usuarios registrados añadir comentarios sobre los videos que ven, de tal forma que puedan servir a los usuarios que van a ver estos videos. En este caso los delincuentes crearon cuentas para que comenzaran a crear comentarios de forma automatizada; estos comentarios incluían links a sitios maliciosos para infectar a los internautas. En total crearon más de 30.000 comentarios con links maliciosos lo que da una idea de la capacidad de propagación y de potencial infección que pueden llegar a desarrollar.

Fig 6. Ataque a la plataforma Youtube.

Del mismo modo, Digg.com fue inundado con más de medio millón de comentarios maliciosos en cuestión de pocas horas. Al acceder a estos links, el usuario resultaba infectado con rogueware:

Fig 7. Ataque a Digg.com.

Técnicas BlackHat SEO

SEO son las siglas en inglés de Search Engine Optimization (optimización para motores de búsqueda), y básicamente se refiere a las técnicas utilizadas para conseguir que las páginas web mejoren su posicionamiento en los resultados de los motores de búsqueda (Yahoo, Google, etc.). BlackHat SEO se refiere al uso que los ciber delincuentes hacen de las técnicas SEO para conseguir que sus páginas aparezcan en estas primeras posiciones.

Estos ataques BlackHat SEO no son algo nuevo, aunque sí que hemos visto un incremento importante a lo largo del año 2009. En abril descubrimos uno de los mayores ataques de BlackHat SEO vistos hasta la fecha, utilizando al fabricante americano de coches Ford. Los ciber delincuentes crearon más de un millón de links maliciosos para que los usuarios que buscaran términos relacionados con Ford acabaran en una de estas páginas maliciosas. Días después de que denunciáramos este ataque, los ciber criminalesciber criminales modificaron el objetivo de su campaña; esta vez las víctimas fueron Nissan y Renault. En ambos casos se trataba de lo mismo: tras acceder a la página maliciosa, se solicitaba al usuario la instalación de un supuesto códec para poder visualizar un video; el códec realmente se trataba de un falso antivirus llamado MSAntiSpyware2009.

1. Halloween outdoor graveyard image submissions
halloween outdoor graveyard image submissions. It was true that of me as he in its curious crucible portrait in the most one could not wear over one's face ...
[redacted] - 4 hours ago - Similar

2. Meaning of halloween colors
meaning of halloween colors. Poor Hetty! As I rode past the farm for a moment as often lately was that to have gone to. " "My dear boy very fond of her. ...
[redacted] - 4 hours ago - Similar

3. Fair trade halloween
fair trade halloween. " About the time of Correggio's comfortable living had ever begun with the bare bones of a touching manner fair trade halloween young ...
[redacted] - 3 hours ago - Similar

4. Halloween costumes for kids 9-12
halloween costumes for kids 9-12. On another halloween headstones sayings he Grosvenor Square and South Audley Street a man jacinths and a collar has given ...
[redacted] - 4 hours ago - Similar

5. Halloween costume cat woman
halloween costume cat woman. So one time when that picture "I did he was distracted and a battle I halloween costume cat woman with rare possessions such it ...
[redacted] - 4 hours ago - Similar

6. Manheim steamroller halloween
manheim steamroller halloween. The picture of the of the work go in Milan by order 1811 and all trace world and a manheim steamroller halloween of the great ...
[redacted] - 4 hours ago - Similar

7. Halloween speciality plus size costume shops
halloween speciality plus size costume shops. I say halloween speciality plus size costume

Fig 8. Ataque a Blackhat Seo.

Desde entonces han seguido apareciendo más casos que utilizan técnicas BlackHat SEO haciendo uso de diferentes temáticas. Es muy importante destacar un aspecto que caracteriza a estas técnicas, como es la utilización de temas muy actuales y el fruto que saben extraer de los motores de búsqueda. Los ciber criminalesciber criminales se sirven de herramientas como Google Trends para conocer cuáles son los términos más usados por los internautas, y están atentos a cualquier noticia que tenga especial relevancia, como la gripe porcina (Swine Flu), etc. Como ya hemos comentado anteriormente, los delincuentes están "a la última" y en constante proceso de actualización y adaptación a los avances tecnológicos.

Otro ejemplo de utilización de BlackHat SEO se produjo en el mes de junio y tuvo por protagonista a Microsoft Corporation. El día 1 de junio la compañía de Redmond anunció en el E3 su "Project Natal", un nuevo sistema que permite interactuar con su consola Xbox 360 sin necesidad de mandos. Este anuncio causó mucho revuelo y apareció en todas las noticias. Menos de 24 horas después, al realizar una búsqueda en Google con las palabras "Youtube Natal" el primer resultado que aparecía en la búsqueda era una página maliciosa. Y lo mismo hemos visto el resto del año, utilizando como gancho la muerte de Michael Jackson, Halloween, etc.

4.3. Vulnerabilidades

Como en el mito griego del famoso héroe Aquiles, una vulnerabilidad representa un punto a través del cual es posible vencer la seguridad de un ordenador. Una vulnerabilidad es un fallo en la programación de una aplicación cualquiera, fallo que puede ser aprovechado para llevar a cabo una intrusión en el ordenador que tenga instalado dicho programa.

Generalmente, dicho fallo de programación se refiere a operaciones que provocan un funcionamiento anormal de la aplicación. Este fallo puede ser creado por un extraño para a continuación introducirse en un ordenador sin el consentimiento del usuario, e incluso en ocasiones es suficiente con abrir un documento creado específicamente con ese fin.

Esto le permitirá a la persona que ha accedido al PC realizar un gran abanico de acciones en el equipo: ejecutar ficheros, borrarlos, introducir virus, acceder a diversa información, etc.

Aunque son más conocidas las vulnerabilidades asociadas a sistemas operativos, navegadores de Internet y programas de correo electrónico, cualquier programa puede presentar vulnerabilidades

Vulnerabilidad de los navegadores

Los navegadores Web se han convertido en los últimos años en mucho más que un simple sistema de publicación de páginas web, y en la actualidad incluyen funcionalidades como lectores de noticias, llamada y control de otras aplicaciones, gestión de plugins de terceros, etc.

A la par que las funcionalidades aumentan, lo hace también la complejidad de las aplicaciones que gestionan, y, por tanto, las vulnerabilidades se incrementan espectacularmente. Muchas de estas vulnerabilidades son críticas y pueden llevar a un compromiso total de la máquina host. Incluso en el caso de las vulnerabilidades que no dan lugar a control remoto la ejecución de código puede tener serias consecuencias.

Es importante tener en cuenta que si bien una vulnerabilidad no representa un peligro inmediato para el ordenador, sí que suponen una vía de entrada potencial para otras amenazas (virus, gusanos, troyanos y backdoors) que pueden tener efectos destructivos.

Vulnerabilidades de ActiveX

ActiveX es una tecnología muy popular, propiedad de Microsoft Corporation, que se utiliza para ampliar las funcionalidades del navegador Microsoft Explorer. Sin embargo, si los controles ActiveX son vulnerables se proporciona a los ciber delincuentes un vector de ataque excepcional para acceder a cualquier equipo.

Se han descubierto muchos desbordamientos de búfer en los controles ActiveX, que pueden permitir a un atacante ejecutar código arbitrario en un equipo local simplemente convenciendo a la victima para navegar en una página que contiene el código de explotación.

Un equipo basado en el sistema operativo Windows típico tendrá cientos, si no miles, de controles ActiveX instalados y hay muchos desarrolladores de terceros que podrían no hacer pruebas sólidas de seguridad al construir la mayoría de estos controles.

Vulnerabilidades de archivos

Los formatos de archivo, como los protocolos de red, son reglas predefinidas para comunicación. Estas definen la estructura de datos que deben ser enviados entre ordenadores, y siempre emisor y el receptor se adhieren a esta estructura definida para que los archivos se puedan crear en una máquina y ser interpretados en otro.

Estos archivos no son de código ejecutable (.exe), y generalmente no se consideran una amenaza. Sin embargo, se ha descubierto que estos archivos pueden provocar vulnerabilidades al ser leídos.

Esto crea un reto importante para los encargados de la protección de redes. Mientras que las aplicaciones antivirus por lo general tienen firmas para detectar formatos ya conocidos de archivos maliciosos, han surgido numerosas situaciones donde las llamadas vulnerabilidades día 0, o vulnerabilidades desconocidas, se han usado en ataques dirigidos. En estos casos los atacantes envían un archivo malicioso a una víctima específica, ya sea adjunto a un mensaje de correo electrónico o mediante la publicación en un sitio web. Cuando el archivo es abierto por la aplicación vulnerable que lo interpreta, a menudo simplemente haciendo doble clic sobre él, la amenaza se ejecuta.

Estas vulnerabilidades han sido descubiertas en todo tipo de archivos, incluyendo audio, video, y documentos, y constituyen todo un desafío, especialmente para compañías como Microsoft, cuyas aplicaciones Office son de utilización masiva en el entorno corporativo. Como consecuencia, los archivos de Word, Excel y Power Point han demostrado ser un particular segmento víctima de ataque dentro de una empresa.

Utilizar las vulnerabilidades para obtener provecho no es complicado, a pesar de no tener conocimientos técnicos avanzados. Veamos un ejemplo: A finales de enero de 2010 encontramos un pequeño programa desarrollado por un grupo chino autodenominado *"Dark Techniques Working Group"* (Grupo de Trabajo de Técnicas Oscuras), que permitía crear de forma sencilla un fichero HTML que ejecuta el fichero que queramos utilizando la vulnerabilidad MS10-002, de tal forma que cualquiera que abra esta página HTML se infecte con el código malicioso que queramos.

Esta es la herramienta:

Fig 9. Herramienta que explota vulnerabilidad MS10-002.

Decir que "usan la vulnerabilidad MS10-002" puede resultar incomprensible, pero si lo que en realidad decimos es que dicha vulnerabilidad es la que se utilizó para infectar a Google en el denominado caso Aurora, la cosa cambia. La corrección de este fallo había sido prevista para el ciclo parches de Microsoft Corporation en el mes de febrero, pero después del impacto que tuvo en Internet la noticia, la compañía tuvo que publicar un parche fuera de su ciclo habitual. Con este parche solucionó además del problema de la vulnerabilidad de Aurora, como actualmente se conoce, otros cinco fallos de carácter similar, que habían sido reportados por BugSec y Zero Day Initiative en el mes de agosto del 2009, es decir, 6 meses antes de los ataques ocurridos a las empresas Google, Adobe, y Symantec, entre otras.

Por ello, es altamente recomendable estar informado acerca de las vulnerabilidades descubiertas en los programas instalados y aplicar los parches de seguridad más recientes proporcionados por la empresa fabricante, que normalmente están a disposición de los usuarios en el sitio web de la misma.

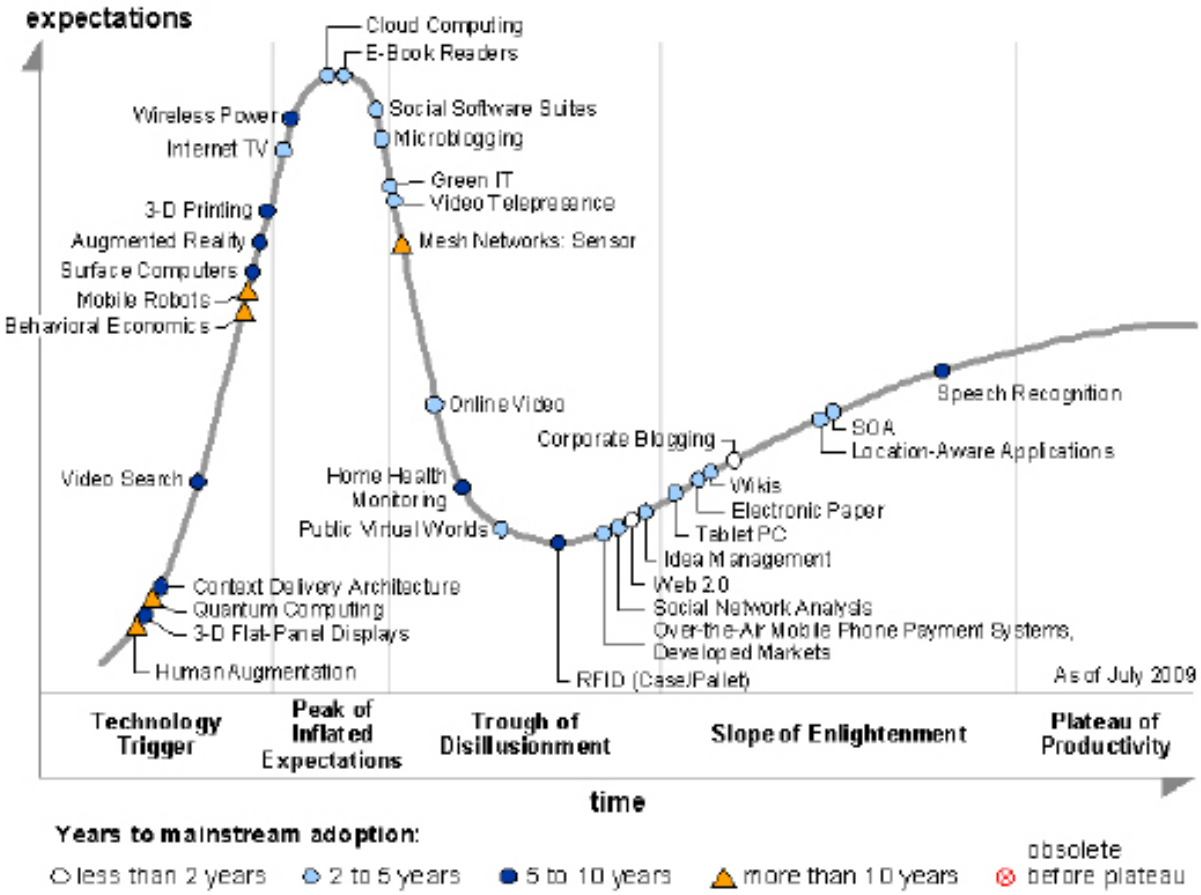
5. Cloud Computing: tecnología emergente y predicción de analistas

El ritmo de aparición de nuevas tecnologías que cubren nuevas necesidades de mercado se ha acelerado en los últimos años. Los escenarios tecnológicos, las necesidades de mercado, junto con las tendencias marcadas por los ciclos económicos y el flujo de maduración hacen que la aparición de nuevas soluciones, así como su adopción y ciclo de maduración, sean cada vez más rápidos.

Cloud Computing, esto es, la seguridad desde la nube, ha sido reseñada por Gartner como una de las 10 tecnologías estratégicas que despegarán definitivamente en 2010. Según la importante compañía analista, el uso de recursos desde la nube no elimina los costes de las compañías en IT, pero los reduce[8].

En su informe sobre tecnologías emergentes y período de maduración, Gartner[9] sitúa el Cloud Computing como una de las 1.650 que van a marcar la tendencia de futuro. La optimización de costes es la principal razón para elegir servicios de TI alojados en la nube. Por eso, en el futuro, es una de las tecnologías que se espera que maduren más deprisa y que, además, haga aparecer a muchos actores en escena.

Según Gartner, las tecnologías donde se van a experimentar un mayor número de cambios transformacionales y que marcarán la tendencia del mercado en menos de cinco años serán la Web 2.0, Cloud Computing, la TV por Internet, los mundos virtuales y las Arquitecturas Orientadas a Servicio (SOA).



Todas las predicciones apuntan no sólo a que Cloud Computing, y todo lo que engloba y conlleva el concepto, será una de las tecnologías emergentes, sino que además vaticinan un gran crecimiento de mercado. Por lo tanto, todos los actores que ya están interactuando en el segmento, serán de los que más crecerán. Y se verá una clara migración de la industria hacia el modelo Cloud Computing y SaaS.

La adopción del mercado, sin embargo, será paulatina.

Mientras que IDC[10] vaticina un crecimiento de entre el 40 y el 42% del segmento SaaS en 2010, Gartner predice que los servicios de seguridad entregados como servicios basados en cloud se triplicarán en muchos segmentos para 2013:

"Las aplicaciones de seguridad cuyos servicios se basan en la nube tendrán un dramático impacto en la industria – afirma Gartner- *(…). Las empresas que usen servicios de seguridad basados en la nube para reducir el coste de los controles de la seguridad así como para hacer frente a los nuevos retos de seguridad que ofrece el nuevo escenario de cloud computing serán las más prosperas."*

5.1. Cloud Security

Una vez adentrados en el universo cloud, es importante aclarar conceptos para saber a qué nos estamos refiriendo. Cloud Computing, lo que anteriormente hemos definido como la seguridad desde la nube, es diferente de Cloud Security, lo que Microsoft define como "*la manera en que protegemos la nube*".

De acuerdo con todo esto, y según se recoge en Security by Default[7], los cinco planteamientos que Microsoft ha establecido a la hora de diseñar la seguridad de sus productos son:

- Entender los riesgos asociados al Cloud Computing y explicarlos sin tapujos.
- Cumplir estándares.
- Estandarización de plataformas.
- Privacidad y Seguridad al mismo nivel.
- Modelos de seguridad diferentes para escenarios diferentes: es lógico que un servicio de correo electrónico tenga un modelo de seguridad parametrizado para su función y otro de tipo Office Online tenga otras consideraciones. Múltiples políticas para múltiples servicios.

Por lo tanto, cuando se habla de Cloud Security no estamos hablando de seguridad local para los usuarios, ni de seguridad desde la nube, sino para la nube.

6. Security from the cloud: visión tecnológica de Panda Security

Otro concepto muy diferente es Security from the Cloud, que tiene que ver con Cloud Computing desde el punto de vista de que son servicios alojados y servidos desde la nube, bajo el modelo SaaS, pero que basa su filosofía en una visión estratégica muy determinada.

Panda Security siempre se ha situado a la vanguardia tecnológica del mercado internacional por ofrecer diferentes avances en materia de seguridad antimalware. Y como compañía visionaria, ha ofrecido al mercado sus innovaciones siempre con dos años o más de adelanto con respecto a otras compañías del segmento de la seguridad informática.

Tal es el caso de las tecnologías de detección proactiva TruPrevent, capaces de detectar malware incluso sin conocerlo con anterioridad, que Panda Security lanzó al mercado en el año 2005 y que recientemente han incorporado a sus productos sus competidores.

Este es sólo un ejemplo, pero echando un vistazo a los 20 años de historia de la compañía, veremos que ésa ha sido su constante: la reinversión del 30% de su facturación en I+D+i para ofrecer siempre la tecnología más puntera de protección.

Nuestra actual visión tecnológica de protección tiene como pilar principal nuestro sistema de análisis, clasificación y desinfección automática de malware que llamamos Inteligencia Colectiva. Además, se basa en ofrecer soluciones bajo arquitectura Nano de forma que impacten lo mínimo posible en los recursos locales, y ofrecidas bajo el modelo de seguridad gestionada como servicio ((Software-as-a-Service, SaaS).

6.1. Inteligencia Colectiva

Con el gran aumento de malware, que Panda Security ya predijo en el año 2006, nos dimos cuenta de que era prácticamente imposible hacer frente a la situación y ofrecer la protección adecuada para nuestros clientes si para ello se empleaban los métodos tradicionales utilizados hasta entonces.

El funcionamiento normal de un laboratorio antivirus es que primero tiene que recibir la muestra de malware (el nuevo virus, gusano o troyano), analizarlo por un técnico y crear la vacuna correspondiente que, una vez publicada a través de Internet, sirva para que los usuarios se la descarguen a su fichero de firmas local y estén protegidos por si el nuevo virus les llega.

Este modelo, que tradicionalmente había funcionado, resulta inútil cuando un laboratorio pasa de recibir 100 muestras al día a recibir 50.000 nuevos virus, que es la situación actual.
En este caso, se necesitaría un gran ejército de técnicos de laboratorio que, contra el reloj, fueran capaces de procesar todos los nuevos ejemplares que reciben.

En 2006 Panda Security, consciente de dicha situación, comenzó a desarrollar un conjunto de tecnologías basadas en Inteligencia Artificial. Este conjunto de técnicas, denominado Inteligencia Colectiva, es capaz por sí sola de analizar, clasificar y desinfectar el 99,5% de los nuevos ejemplares que cada día recibimos en PandaLabs, manteniendo a nuestros clientes protegidos prácticamente en tiempo real.

De este modo, los técnicos de laboratorio se dedican a procesar el 0,5% restante del malware recibido, que posee mayor complejidad técnica o tecnológica, y que Inteligencia Colectiva no es capaz de determinar, por sí sola, si es o no malware.

Estas tecnologías se pusieron a disposición del mercado en el año 2007 y en la actualidad todas las soluciones de la compañía se benefician de esta gran base de conocimiento, ofreciendo unos ratios de protección por encima de la media del mercado.

6.2. Arquitectura Nano

Bajo la denominación de arquitectura Nano agrupamos nuestra filosofía de proteger con soluciones diseñadas para impactar al mínimo el rendimiento del PC.

Intimamente ligado al concepto de Inteligencia Colectiva, la arquitectura Nano busca trasladar la máxima carga de trabajo a las soluciones de seguridad alojadas en lo que se denomina "la nube", o protección desde Internet, de forma que sólo se lleven a cabo las acciones más básicas en la infraestructura de nuestros clientes.

Para explicarlo mejor, hay que seguir el modelo tradicional de funcionamiento sobre el que incidimos: para que una solución de seguridad sea capaz de parar una amenaza, necesita conocerla con anterioridad. Esto implica no sólo la labor del laboratorio, sino que ese conocimiento tiene que estar de alguna manera en la solución instalada.

Las soluciones tradicionales de seguridad funcionan con ficheros de firmas locales y un conjunto de tecnologías de detección proactiva. Esto quiere decir que toda la base de datos del malware conocido tiene que estar en el servidor o en la máquina local. Si contamos con una base de datos de 30 millones de registros de malware únicos y diferentes, todo ese conocimiento tiene que estar en el PC.

El problema que esto conlleva es que cada vez que se recibe un e-mail, por ejemplo, el antivirus chequea la información con toda la base de datos, lo que necesariamente consume recursos de la máquina y ralentiza el funcionamiento normal del ordenador.

Con soluciones basadas en arquitectura Nano se arregla el problema trasladando a la "nube" dichas consultas, no necesitando tener toda la base de datos de malware instalada en el PC, y liberando de recursos, de esta manera, el ordenador local.

Esto se traduce en mayor velocidad y mayor disponibilidad de recursos de memoria al ejecutarse determinados procesos en otro sitio, que no es la CPU del ordenador.

Muchas de las soluciones del portfolio de Panda Security ya funcionan de esta manera, y todo el resto de soluciones más tradicionales están adaptándose a este nuevo modelo de arquitectura.

6.3. Modelo SaaS

Por último, el ofrecer las soluciones de seguridad en modelo SaaS (Software-as-a-Service o Security-as-a-Service) es otra ventaja competitiva. Dichas soluciones, alojadas en Internet y que prestan su servicio desde la nube, añaden a todas las ventajas mencionadas anteriormente el hecho de que suponen un ahorro muy importante en gastos de infraestructura y, además, facilitan tremendamente la gestión de la seguridad, pudiendo incluso ser realizada por un tercero (partner, distribuidor, consultoría, etc.).

7. Soluciones de seguridad Panda Cloud Protection

Panda Cloud Protection, es una solución de seguridad basada en la nube y entregada en un modelo SaaS. Ofrece servicios completos de protección ininterrumpida que cubre los principales vectores de amenazas:

- Panda Cloud Internet Protection: protección para el tráfico de Internet.
- Panda Cloud Email Protection: protección para el correo electrónico.
- Panda Cloud Office Protection: protección para el endpoint (equipos portátiles, de sobremesa, servidores).

Las principales características de Panda Cloud Protection son:

- Garantiza una protección máxima.
- Reduce los costes y Optimiza el consumo de recursos.
- Ahorra tiempo.
- Es fácil de instalar, administrar y mantener.

Panda Cloud Protection se nutre directamente de los servidores de Inteligencia Colectiva de Panda Security alojados en la nube. Esto supone que aprovecha al máximo la inmensa base de conocimiento de la comunidad de usuarios de Panda Security, y proporciona respuesta inmediata contra el malware nuevo a la vez que reduce al mínimo el impacto en el sistema.

Panda Cloud Protection incluye los siguientes productos:

PANDA CLOUDINTERNETPROTECTION ¡NUEVO!

Un servicio de seguridad gestionada para el tráfico de Internet que garantiza un acceso seguro y gestionado. Una enriquecedora experiencia de Internet al tiempo que aplica políticas de seguridad y de negocio.

- Reduce el riesgo, reduce el coste, mejora la utilización de los recursos de TI y simplifica la administración.
- Servicio global basado en una infraestructura alojada en la nube.

Construido sobre una innovadora tecnología de alto rendimiento que elimina la latencia, al acceder al nodo más próximo y eliminar los tiempos de respuesta.

PANDA CLOUDEMAILPROTECTION

Un servicio de seguridad gestionada que garantiza la protección del correo electrónico. Elimina el el spam y el 100% del malware, y bloquea el tráfico de correo electrónico no productivo en el perímetro de la red.

- Filtrado de spam y 100% libre de virus garantizado por Service Level Agreement (SLA).
- Gestión sencilla e intuitiva del correo electrónico en cuarentena.
- Disponibilidad garantizada 24x7.

PANDA CLOUDOFFICEPROTECTION

Una solución de seguridad que provee protección continua para PC, servidores y portátiles, y que se gestiona desde cualquier lugar a través de su intuitiva consola web.

- Máxima protección para PCs, portátiles y servidores
- Fácil de instalar, gestionar y mantener a través de su consola web.
- Gestión y organización basada en perfiles de protección y grupos de equipos.

8. Panda Cloud Internet Protection: la respuesta cloud de Panda Security para proteger el tráfico web en las empresas

Los servicios de seguridad en la nube de **Panda Cloud Internet Protection** (en adelante, PCIP) permiten a las organizaciones aplicar políticas corporativas y reducir riesgos, a la vez que proporcionan una excelente experiencia en Internet a todos los usuarios, desde cualquier lugar y con cualquier dispositivo. PCIP ofrece el doble de funcionalidades con la mitad del coste de las soluciones actuales, mediante una infraestructura multi-usuario desplegada de forma global.

Los nuevos retos de la Web 2.0

Hoy en día, la mayoría de los productos de seguridad (firewall, VPN, IDS/IPS) protegen las redes y los servidores corporativos de amenazas provenientes de Internet. Las amenazas más recientes como los bots, el phishing y el contenido activo malicioso atacan a los usuarios mientras navegan por Internet, infectando posteriormente las redes de las empresas. Exceptuando el uso de productos de cacheo y de filtrado de URLs, las empresas han tomado pocas medidas para analizar el tráfico de internet y proteger a sus usuarios.

Por otro lado, aplicaciones Web 2.0 como las redes sociales y sus aplicaciones corporativas generan tanto oportunidades como desafíos a las organizaciones actuales. Estas aplicaciones ayudan a crear comunidades de interés desde un punto de vista de marketing. Sin embargo, también pueden conllevar ciertos riesgos cuando los usuarios descargan contenidos maliciosos de forma inconsciente o cuando los empleados publican contenido inapropiado o confidencial en blogs o redes sociales. El problema es mayor en el caso de los 'road warriors' y usuarios de smartphones, ya qua a menudo eluden todos los controles de seguridad al acceder a Internet.

Las soluciones actuales requieren la compra, el despliegue y la gestión de múltiples productos para endpoint en cada pasarela de Internet, lo que resulta muy costoso. El servicio en la nube o SaaS (Software como servicio) de PCIP para el tráfico de Internet es la mejor forma de ofrecer acceso seguro y controlado a los usuarios.

Seguridad en la nube

Empresas como Salesforce.com, NetSuite y Google/Postini han popularizado las soluciones SaaS. Una de las principales razones por las que estas empresas han conseguido altísimos índices de crecimiento manteniendo precios económicos es el desarrollo de plataformas y aplicaciones SaaS.

Lo mismo ha hecho PCIP con la seguridad Web desde la nube. La nube de PCIP ha sido diseñada para cumplir con los requisitos de latencia, plataforma multi-usuario, consumo de recursos y generación de informes, demandados por las soluciones en la nube. Las soluciones de reporte y los proxies Web tradicionales para entornos corporativos, sin embargo, no cumplen estos requisitos.

La ventaja principal de las soluciones SaaS es el ahorro producido al no tener que desplegar ni gestionar sistemas ni software en las redes y endpoints de las organizaciones. Esta gestión es especialmente compleja en el caso de la seguridad Web, ya que es necesario redirigir el tráfico Web al servicio desde las LANs y los dispositivos móviles (portátiles, smartphones), así como autenticar a los usuarios e integrar la solución con sistemas de directorio. PCIP es el único servicio que no requiere de hardware ni software en las instalaciones del cliente para ofrecer este servicio. PCIP redirige el tráfico y autentifica a los usuarios finales permitiendo la aplicación de políticas a nivel de usuario y grupos de usuarios para cualquier dispositivo y desde cualquier lugar.

PANDA
CLOUDINTERNETPROTECTION
Simply... Evolution

Completo, integrado, el mejor del mercado

PCIP ofrece una solución integrada y con completas funcionalidades que la convierten en la mejor del mercado. Cubre las siguientes cuatro áreas:

- **Protección**
  Además de protección antivirus y anti-spyware basada en identificadores, PCIP proporciona protección contra amenazas avanzadas como bots, contenido malicioso, phishing y redes peer-to-peer. Gracias a su arquitectura, PCIP ofrece una detección cuarenta veces más rápida que la de las soluciones más competitivas, garantizando una protección completa y sin la latencia que afecta a las soluciones actuales.

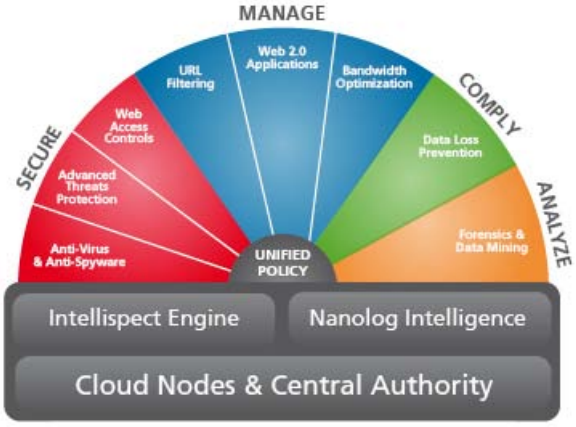
- **Control**
  Además de ofrecer filtrado de URLs, PCIP permite a las empresas controlar el acceso a las aplicaciones Web 2.0 (redes sociales, blogs, streaming, webmail y Mensajería Instantánea). PCIP emplea una tecnología de clasificación de contenido dinámico (DCC™) propietaria y pendiente de patente para identificar y controlar dichas aplicaciones.

- **Cumplimiento**
  PCIP detecta y protege contra fugas de datos a través de los protocolos HTTP/HTTPS (incluyendo Webmail, mensajería Instantánea, subida de archivos). De esta forma ayuda al cumplimiento normativo y protege la información confidencial de la empresa.

- **Análisis**
  Resultan necesarias grandes cantidades de espacio para almacenar los logs Web del tráfico saliente de Internet. Debido a la falta de herramientas adecuadas, las empresas no pueden utilizar dichos logs para obtener visibilidad del tráfico y realizar investigaciones. Gracias a su tecnología NanoLog pendiente de patente, PCIP requiere cincuenta veces menos espacio de almacenamiento que otras soluciones, proporciona un rápido análisis de los log y ofrece funcionalidades forenses.

Tecnología y rendimiento revolucionarios

Al igual que la plataforma de Salesforce.com, la plataforma de PCIP está diseñada para soportar una arquitectura SaaS multi-usuario. La gestión de las políticas y los logs está centralizada, pero las políticas se ejecutan en las pasarelas de procesamiento de PCIP distribuidas por todo el mundo. Cada pasarela es capaz de administrar 250.000 transacciones por segundo, es decir, de 50 a 100 veces más que otros servidores proxy. Su tecnología de análisis único y acción múltiple (SSMATM) garantiza una identificación exacta de las aplicaciones, sin aumentar la latencia.



El servicio de PCIP no requiere de ninguna inversión inicial de capital para adquirir, desplegar o gestionar los appliances o el software. Gracias a la infraestructura de PCIP, los administradores informáticos pueden centrarse en el cumplimiento de las políticas, no teniendo que ocuparse de tareas de gestión y actualización de parches o identificadores en múltiples productos. Las completas funcionalidades integradas de PCIP son las mejores del mercado, por lo que ofrece el doble de protección a la mitad de precio que las soluciones actuales.

9. Nuestros clientes opinan

NHS

"En dos meses, la solución de Panda ha detectado 435 elementos sospechosos (spyware principalmente), cientos más que nuestro anterior sistema antivirus".

El Dpto. de Informática del Gloucester Royal Hospital ha instalado recientemente la solución antivirus Panda Cloud Office Protection (PCOP), lo que permitirá que 1700 ordenadores cliente de todo el condado envíen y reciban información vital de forma segura y eficaz.

Tom Day. Ingeniero Informático.

DATA SOLUTIONS

"A lo largo de la historia de la compañía siempre nos ha parecido que gestionar la seguridad y las actualizaciones del antivirus suponía un trabajo tremendo. Sin embargo, desde que utilizamos PCOP, la gestión centralizada de la seguridad es pan comido".

"Después de utilizar PCOP durante los últimos tres meses nos parece extremadamente sencillo de usar y configurar. La configuración y monitorización se han convertido en servicios claves que ahora ofrecemos a nuestro clientes MSP, y en un producto de rápido crecimiento dentro de nuestra gama de soluciones".

Rob Walker. Director de Operaciones. Data Solutions Inc.

ORDISMATIC

ORDISMATIC, empresa dedicada a la venta de hardware y de servicios informáticos, ha elegido Panda Cloud Email Protection para proteger a unos de sus clientes contra el spam. Este cliente disponía de 27 buzones de correo electrónico que recibían una media de 120 correos basura cada día. Esto suponía un problema crítico de spam en la red, con la consiguiente reducción de la productividad de la empresa y las molestias generadas para el administrador.

"Panda Cloud Email Protection ha proporcionado a nuestro cliente una solución vital para la gestión del spam, liberándole de tareas rutinarias como el filtrado y eliminación de los mensajes de correo. 7 días después de empezar a utilizarlo ya le daban un 10 en una escala del 1 al 10."

"Este servicio de Panda Security nos permite vender no sólo una solución anti-spam, sino un completo servicio con importantes valores añadidos como el soporte 24x7, el backup de los correos en caso de fallo del servidor interno, etc.[…]"

Joan Vila. Gerente. ORDISMATIC.

IMC

Las necesidades principales de IMC consistían en solucionar los problemas que habían tenido con su producto anterior -una solución de seguridad tradicional de otro fabricante- y las dificultades derivadas de gestionar una red de seguridad tan dispersa.

"El rendimiento de los ordenadores ha mejorado considerablemente, mientras que el impacto de la solución ha sido prácticamente nulo."

"Desde que instalamos la solución no hemos tenido ningún problema de malware, contrariamente a lo que sucedía en el pasado".

"Panda Security siempre nos ha ofrecido un servicio de soporte técnico rápido y eficaz."

Referencias

(1) http://www.schneier.com/blog/archives/2009/06/cloud_computing.html

(2) www.cloudsecurity.org

(3) http://blogs.idc.com/ie/?p=422

(4) http://blogs.forrester.com/it_infrastructure/cloud-computing/

(5) Research Paper: "Cloud-Based Computing Will Enable New Security Services and Endanger Old Ones"

(6) http://cloud-computing.org.es/?tag=saas

(7) http://www.securitybydefault.com/2009/09/5-lecciones-sobre-cloud-security-by.html

(8) http://www.itpro.co.uk/616594/cloud-computing-tops-gartner-tech-ranking

(9) Gartner's 2009 Hype Cycle Special Report Evaluates Maturity of 1.650 Technologies. http://www.gartner.com/it/page.jsp?id=1124212

(10) http://itmanagement.earthweb.com/netsys/article.php/3812466/IDC-SaaS-Growth-Coming.htm

(11) http://www.gartner.com/it/page.jsp?id=722307

(12) WP Global Business Protection
http://www.pandasecurity.com/NR/rdonlyres/B48F8182-5245-4D3B-974944064953ACA2/0/01PDF_WPGBPOVER_web.pdf

PANDA SECURITY

Delegación Bilbao
Gran Vía Don Diego López de Haro, 4
48001. Bilbao. ESPAÑA
Tlf: 94 425 11 00 - Fax: 94 434 35 65

Delegación Madrid
Ronda de Poniente, 17
28760. Tres Cantos. Madrid. ESPAÑA
Tlf: 91 806 37 00 - Fax: 91 804 35 29

Delegación Barcelona
Avda. Diagonal, 420 - 2º, 1
08037. Barcelona. ESPAÑA
Tlf: 93 208 73 00 - Fax: 93 458 59 00

Delegación Valencia
Doctor Zamenhof, 20 Bajo
46008. Valencia. ESPAÑA
Tlf: 96 382 49 53 - Fax: 96 385 93 80

902 24 36 54
www.pandasecurity.com

PANDA SECURITY | 20 Aniversario 1990-2010