NORMAN protege solución Alfresco

Reference case: Bauer AG and Norman

NORMAN®

Norman Network Protection

Norman Network Protection es una potente puerta de enlace de seguridad de contenidos que protege la infraestructura de comunicación de las organizaciones frente a malware de tipo virus, spyware, gusanos y troyanos. Ello permite que las operaciones de red de las organizaciones sigan funcionando con un alto rendimiento, completa transparencia y sin preocuparse de posibles infecciones por software dañino. Norman Network Protection se suministra como una solución “todo en uno” con un terminal de alto rendimiento o como una versión de software.

Sólo con conectar el equipo con Norman Network Protection a la red, puede proteger toda la infraestructura de los riesgos de Internet o proteger áreas de la red esenciales para la empresa con el fin de evitar que sean infectadas por código malicioso.

Cuando NNP detecta un archivo malicioso que se está transfiriendo a la red, finaliza activamente la transferencia y bloquea la ruta de red concreta para evitar que otros usuarios o sistemas accedan al mismo archivo.

La latencia ya no es un problema: Las soluciones proxy tradicionales tienen varios inconvenientes. La consecuencia más importante es la latencia en el tráfico de datos generada por el propio proxy. El proxy retiene toda la secuencia de archivos, mientras que NNP evita este problema al retener únicamente los datos necesarios para realizar un análisis en busca de malware.

Bauer AG emplea la solución Norman

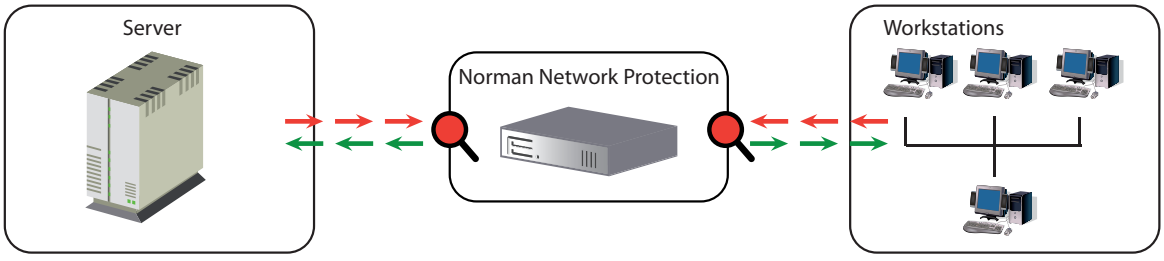
Las aplicaciones basadas en una base de datos presentan necesidades especiales a la hora de elegir una protección antivirus adecuada. La protección antivirus local está tan mal considerada como la limitación a un mero analizador basado en firmas. Por eso, para proteger su nueva solución de Gestión de Contenidos Empresariales (ECM), Bauer AG ha apostado por el analizador antimalware Norman Network Protection.

El grupo constructor y fabricante de maquinaria Bauer AG desarrolla y construye maquinaria para ingeniería civil, y lleva a cabo en todo el mundo enormes proyectos de obras públicas y cimentación, construcción de puentes y depuradoras, y rehabili-tación de edificios históricos. Unos 8.000 empleados en todo el mundo deben manejar todos los datos e informaciones necesarios en su trabajo. Para ello, Bauer AG utiliza un sistema de Gestión de Contenidos empresariales (ECM). El grupo se decidió por la solución Open Source Alfresco, en la que en un principio confiaron para la creación de una base de datos central y por la posibilidad de acceso desde cualquier lugar. Para la implementación de Alfresco en la central de Schrobenhausen, cerca de Múnich, Bauer AG colaboró con dmc digital media center GmbH, empresa especializada en soluciones de software individuales para grandes empresas y uno de los pocos proveedores informáticos en Alemania con experiencia en Alfresco. Bauer instaló Alfresco en tres servidores de ECM. Dos de los servidores se utilizan en la red productiva y, por motivos de redundancia, cada uno de ellos cuenta con dos tarjetas de red. El tercer servidor Alfresco forma parte de una red de pruebas en la que se evalúan distintos escenarios.
Alfresco presenta un sistema de archivos virtual para el almacenamiento de documentos.

Los usuarios de Microsoft Office pueden guardar sus documentos de la forma habitual, en carpetas, mientras que para su almacenamiento, los archivos se convierten automáticamente en XML o PDF, por ejemplo. Antes del almacenamiento, una solución antivirus comprueba la existencia de malware en los archivos. Puede suceder que “se cuele” un código malintencionado desconocido para el que aún no haya registrada una firma, con lo que se guardaría en el sistema de EMC un archivo infectado. Los escáneres de virus basados en el servidor, como los que se utilizan en los servidores de archivos, no pueden emplearse en la mayoría de los sistemas de ECM y por tanto tampoco en Alfresco. La razón es que los archivos no se guardan en el servidor en el formato que esperan los escáneres de virus clásicos. Pero si no obstante se utilizara un escáner de virus de esta forma, se borrarían o se desplazarían los archivos del servidor a un sistema incoherente, porque el sistema de EMC no se da cuenta de estas manipulaciones. Si bien es verdad que siempre se evita guardar el dañino en cuanto se detecta, en el peor de los casos puede destruirse todo el sistema y ser necesario volver a crearlo de forma laboriosa.

Análisis previo a la carga

Bauer AG quería evitar a toda costa los virus del servidor. Por eso se utilizó una protección antimalware que se puede instalar a modo de dispositivo antes de los accesos de los servidores de ECM en la red empresarial. Los archivos se analizarían al cargarse y descargarse, pero no durante su almacenamiento en el sistema de archivos, por lo que un escáner de virus instalado en el servidor de forma local resulta obsoleto. Además, la probabilidad de infección por parte de malware desconocido debía mantenerse lo más baja posible. Por eso, además del analizador clásico basado en firmas, se utilizaron componentes de protección proactivos como parte integrante de la solución. ”Las soluciones antimalware basadas exclusivamente en firmas ya no sirven en una época en la que diariamente surgen más de 5.000 nuevos virus”, explica Roland Bauer, Director Técnico Informático de Bauer AG. “Nuestras sedes se extienden por todo el planeta, por lo que fácilmente podemos ser una de las primera empresas en que se introduzca un virus”. Además, Bauer tenía las ideas claras en cuanto a los protocolos de análisis. Además de HTTP, que se utiliza al almacenar los archivos en el sistema de archivos a través de la web y de WebDAV, también tenían que analizarse los archivos almacenados durante la habilitación de red normal. Para ello se utiliza CIFS. No obstante, este protocolo es tenido en cuenta por muy pocos antivirus, así que Bauer AG decidió probar la solución Norman Network Protection (NNP), del especialista noruego en productos antimalware Norman.



Norman Network Protection se instala en cualquier punto de la red empresarial y analiza todos los archivos antes de su almacenamiento en un servidor.

Inclusión de CIFS/SMB

NNP es un analizador de malware totalmente transparente que se suministra como paquete de software o instalado en un servidor estándar, y que se instala fácilmente en cualquier punto de la red empresarial, por ejemplo, en la entrada y la salida de una aplicación de base de datos. Los componentes proactivos reducen totalmente el riesgo de infección por malware desconocido. Se utiliza la solución Norman SandBox, basada en comportamientos. Simula un ordenador con un entorno en el que los archivos desconocidos pueden ejecutar sus instrucciones sin ninguna traba. Todas las actividades del archivo se observan y evalúan y, dado el caso, el archivo y la ruta se bloquean.

Desde hace poco tiempo, SandBox incluye la funcionalidad "DNA Matching" (Comparación de ADN). El proceso aprovecha que en muy pocas ocasiones el software malintencionado es totalmente desconocido y compara las subrutinas de los archivos desconocidos con las subrutinas de las familias de malware ya conocidas. NNP analiza los protocolos ideales para la transmisión de malware: HTTP y CIFS/SMB, pero también FTP, SMTP, POP3, RPC, TFTP e IRC en tiempo real. No sólo se analizan los documentos cargados, sino también la descarga. El análisis durante la descarga hace que el documento también se compruebe a través de las firmas disponibles durante ese tiempo, antes de que llegue al usuario.

Tiempos de latencia mínimos

A finales de 2008 comenzó la prueba de funcionamiento de NNP antes del acceso a un servidor Alfresco. "El trabajo de instalación fue el mínimo posible, ya que no hubo que adaptar los componentes existentes en la red ni modificar la configuración de la red, del proxy ni de la puerta de enlace", explica Bauer. Entre otras cosas, el proceso de análisis observado ofreció unas latencias similares a las conocidas en los proxys. También en este aspecto NNP ha demostrado su valía. Un astuto truco reduce los tiempos de transmisión molestos: mientras que durante el análisis de un archivo los proxys retienen todo el flujo de datos hasta que han recibido y analizado todos los datos para después reenviarlos al destino, NNP envía uno de los archivos que se van a analizar inmediatamente a los receptores con la excepción de algunos paquetes de datos. Si se identifica código malintencionado, los paquetes de datos retenidos se descartan y, con ello, el archivo entero.

La evaluación de la fase de prueba desembocó en una apuesta unánime por NNP. Bauer AG adquirió una licencia de tres años para un total de cinco ejemplares de la solución, para proteger los tres servidores de ECM. Cada uno de los ejemplares de Norman Network Protection instalados en los servidores de HP protege una de los dos accesos de cada servidor de ECM. La quinta versión de NNP se ejecuta antes del tercer servidor Alfresco. Bauer afirma que "Al elegir los protocolos analizados y la proactividad, Norman Network Protection ofrece el nivel necesario de funcionalidad para proteger de forma óptima nuestra solución de ECM".

Norman Data Defense Systems
Camino Cerro de los Gamos 1, Edif.1
28224 Pozuelo de Alarcón
MADRID

Fon: +34 (0)91 790 11 31
Fax: +34 (0)91 790 11 12
Email: norman@normandata.es