PAESSLER

WHITE PAPER

Monitorización de red como elemento esencial en el concepto de seguridad de TI

White Paper

PRTG NETWORK MONITOR

Autor: Daniel Zobel, Head of Software Development, Paessler AG
Publicación: julio 2013

Contenido

Introducción

De acuerdo con una encuesta de Paessler AG, las empresas se quieren proteger mejor de ahora en adelante contra amenazas cibernéticas y otros peligros. Se ha preguntado a unos 1 200 usuarios del software de Paessler PRTG Network Monitor. El resultado de la investigación revela que casi el 75 % de estos considera la herramienta como un componente de seguridad importante para su red. Este informe técnico resalta el papel que juega la monitorización de red como elemento de seguridad adicional en la red empresarial, dónde se encuentran los desafíos en este sentido y cómo se les puede hacer frente.

Situación actual

SEGURIDAD DE TI EN TODO EL MUNDO

Estudios sobre seguridad de TI en Alemania revelan que las empresas tienen un déficit en cuanto a sus medidas de seguridad. Además, los cibercriminales continúan desarrollando ataques digitales cada vez más inteligentes que dirigen de diferentes maneras. Un estudio de 2013 de 41st Parameter revela que dos terceras partes de los usuarios online ya han experimentado “ataques cibernéticos” con más de 1.5 milliones de víctimas nuevas todos los días.

El uso de dispositivos móviles significa una amenaza para la seguridad TI corporativa. Según The Trusted Mobility Index, una encuesta de 4.000 participantes de EE.UU., Reino Unido, Alemania, China y Japón, un 41% de los encuestados utilizando un dispositvo personal para el trabajo lo hacen sin tener permiso del empleador y una tercera parte de los profesionales de TI dijo que su empresa ya sufrió una amenaza de seguridad por dispositivos móviles.

Según cifras de Ponemon Institute las infracciones de TI cuestan a empresas por término medio $7.2 milliones por incidente, una cifra que ha incrementado continuamente en los años pasados.

Hay evaluaciones que expresan que las pérdidas causadas por “ataques cibernéticos” en todo el mundo valen más o menos $1 trillón. Por este motivo, las empresas de hoy en día deben dar más importancia a la seguridad de su infraestructura de TI.

PROTEGER LOS SISTEMAS DE TI

Muchas organizaciones dan por hecho que un firewall en activo y un escáner de virus actualizado es suficiente para proteger su infraestructura de TI. Sin embargo, los delincuentes cibernéticos desarrollan métodos cada vez más avanzados para acceder a los equipos o servidores de las empresas. A veces los programas de seguridad detectan troyanos, gusanos, etc. cuando ya es demasiado tarde. Una vez que un ataque malicioso consigue entrar en un equipo de la red de la empresa, es por lo general una cuestión de tiempo que llegue a todo el sistema. Las consecuencias son, entre otras, la manipulación de datos, la pérdida de información o la ocupación de capacidad de almacenamiento con fines delictivos. Si los sistemas internos de la empresa se ven afectados por un ataque de malware, no se puede llevar a cabo el intercambio de comunicación relevante entre diferentes oficinas de la empresa, el procesamiento de pedidos ni tampoco la comunicación con los clientes. El administrador debe invertir mucho tiempo para dar con las causas concretas del problema que se está produciendo en el sistema de la empresa. ¿Qué partes del sistema de seguridad han fallado? ¿Qué ámbitos o componentes han sido atacados mediante malware? ¿Es posible que haya otros motivos para la inactividad de sistemas aislados?

Para evitar situaciones de este tipo, o para hacerlas lo más improbables posible, es importante proteger toda la infraestructura de TI. Con este objetivo, las empresas necesitan un concepto de seguridad de TI completo. Además de contar con escáner de virus y firewall, normalmente este concepto se ve reforzado por software de codificación, filtro de contenidos, escáner de puertos y otras herramientas. Y lógicamente, para garantizar una protección de la red completa, no puede faltar la monitorización de red como elemento de seguridad complementario durante la planificación y ejecución del concepto de seguridad. Utilizar una solución de estas características enfocada a un objetivo concreto puede aumentar considerablemente el grado de seguridad del entorno de TI.

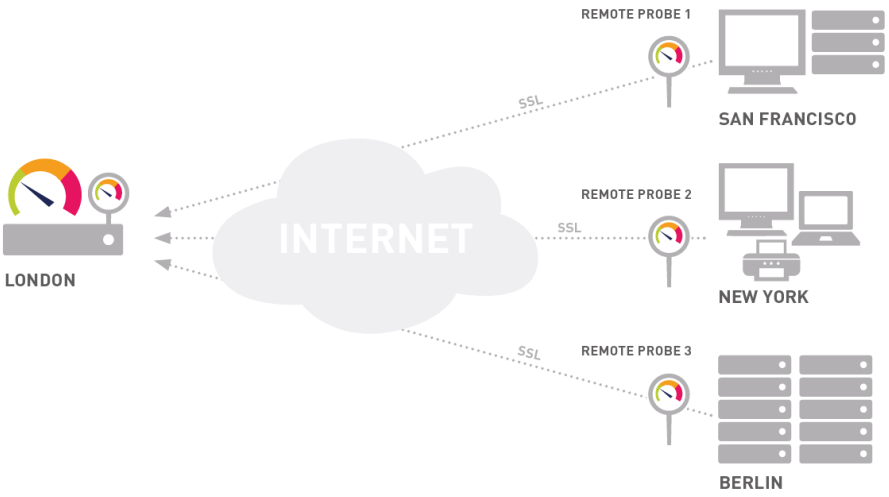
Sistema de alarma preventiva en la red

Una solución de monitorización de red sirve principalmente para tener controlada toda la infraestructura de TI y todos los dispositivos y sistemas. Fundamentalmente, los administradores pueden monitorizar todo lo que dispone de una interfaz definida que suministra información sobre su estado a través de un protocolo estándar. El software de monitorización solo debe contactar con el dispositivo o el servicio mediante una dirección IP, pudiendo consultar seguidamente el estado actual del dispositivo. De esta manera, el responsable de TI podrá tener controlado cualquier ámbito de su infraestructura de TI las 24 horas del día. El objetivo es alcanzar la máxima disponibilidad y el rendimiento óptimo en la red. Para ello, el sistema de monitorización de red debe cubrir los tres aspectos de seguridad más relevantes:

- La monitorización de los sistemas de seguridad originales
- La identificación de sucesos anormales
- Y la comprobación de los parámetros ambientales

Las empresas con diferentes oficinas pueden tener controlada de manera efectiva su red distribuida mediante el uso de „sondas remotas“ en las tres categorías desde una ubicación central. Una „sonda“ es un programa de software pequeño que monitoriza una red remota desde dentro y envía datos de monitorización al servidor de datos central. Así, un software de monitorización de red adecuado monitoriza cualquier componente de red tanto en la central como en las diferentes filiales de una empresa. Para ello, se configuran los denominados „sensores“ para la monitorización de los diferentes parámetros de todos los dispositivos y conexiones de la red. De este modo, el administrador tiene vigilada toda la red desde una ubicación central.

FIGURA:
Monitorización de redes distribuidas mediante „sondas remotas“



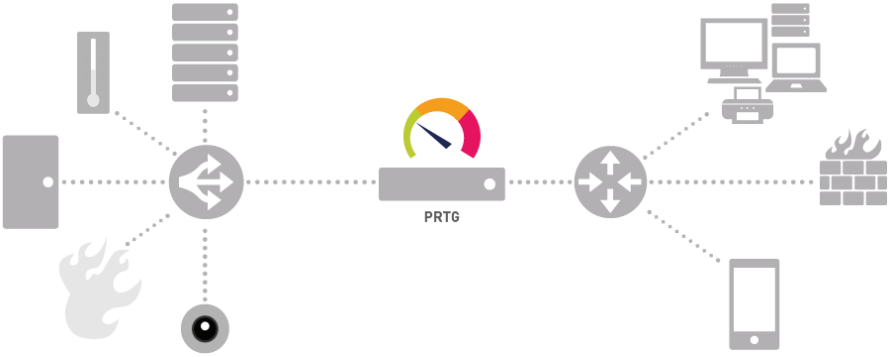
Si el software de monitorización detecta inactividad o proceso anormal, envía de inmediato una alarma por SMS o e-mail al administrador de sistemas responsable. De esta manera, los administradores de TI no dependen de un lugar físico y siempre estarán informados sobre todo lo que ocurre para poder reaccionar con rapidez.

El sistema de alarma preventiva de la solución de monitorización se basa en valores de límite definidos. Si se superan, se activa el software de alarma. El administrador tiene la posibilidad de permanecer siempre en contacto con la instalación de monitorización y de comprobar de inmediato la alarma a través de la interfaz web o de la aplicación para smartphones. Por medio de los datos a tiempo real procedentes de la monitorización, puede valorar directamente las dimensiones de la avería y poner las medidas oportunas.

Monitorizar los aspectos de seguridad

Los responsables de TI desean poder reaccionar con la misma velocidad en caso de ataques de malware. Si las soluciones antivirus y los firewalls detectan los ataques demasiado tarde, los problemas causados pueden paralizar por completo todo el sistema. En este caso los administradores solo pueden reaccionar ante el problema en lugar de prevenirlo y evitar que ocurra. Esto explica que disponer de un escáner antivirus y firewall no es suficiente para garantizar una seguridad completa de la red. Si las empresas integran una solución de monitorización de red en su concepto de seguridad, los peligros potenciales para la red de la empresa se podrán descubrir a tiempo.

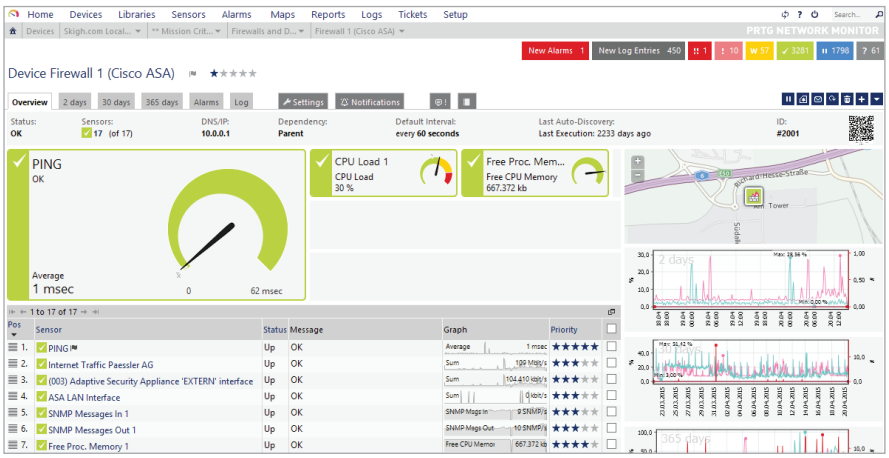
FIGURA:
Garantizar la seguridad completa de la red



COMPROBAR EL FIREWALL Y EL ESCÁNER DE VIRUS REGULARMENTE

Una tarea relevante de la solución de monitorización de red consiste en comprobar el buen funcionamiento de los sistemas de seguridad existentes, como p. ej. firewalls y escáneres de virus. Para ello, la solución de monitorización registra, p. ej., todos los datos sobre el rendimiento y el estado del firewall. Si no funciona adecuadamente, el riesgo de sufrir un ataque de malware en la red aumenta. Estos „ataques maliciosos“ podrían tener como consecuencia que de repente la CPU ejecute programas sin coordinación alguna o que los puertos se abran sin que sea necesario. Para que esto no ocurra, los administradores reciben a tiempo la información sobre cualquier aspecto llamativo del firewall.

FIGURA:
El software monitoriza el estado del firewall



Además del firewall, el software de monitorización también puede comprobar el escáner de virus en el servidor central de correo electrónico. Así las empresas se aseguran de que siempre está activo. Mediante sensores especiales, la solución de monitorización comprueba también el Windows Security Center y determina si, p. ej., el escáner de virus o el programa antimalware están actualizados y funcionan correctamente en todos los equipos de la empresa. Por lo tanto, los equipos cliente de la empresa siempre estarán protegidos ante malware.

BLOQUEOS DE ANCHO DE BANDA COMO INDICADOR DE PROBLEMAS

Una solución de monitorización de red ayuda también a los administradores a medir los anchos de banda de circuitos alquilados, conexiones o dispositivos de red (routers, switches), etc. Con la monitorización detallada de la utilización del ancho de banda, se pueden detectar también indirectamente ataques de malware. Indicios de esto son, por ejemplo, los tiempos de respuesta prolongados en aplicaciones y páginas web. Una de las causas podría ser un programa de malware que absorbe una parte importante del ancho de banda. Para detectar dichas irregularidades, el software de monitorización monitoriza diferentes direcciones de IP, números de puertos, protocolos, etc. mediante esnifing de paquetes o sensores de flujo. Estos sensores xFlow reúnen toda la información enviada y la mandan para que la evalúe el software de monitorización. Así, el administrador puede analizar los datos casi a tiempo real, reconocer problemas a tiempo y realizar otros procesos para la eliminación del problema. Este tipo de monitorización del ancho de banda es idóneo para redes con un tráfico de datos muy elevado. Si el aprovechamiento del ancho de banda supera los valores límite establecidos o difiere considerablemente del promedio o de la fluctuación habitual, esto indica que se están produciendo influencias o actividades anormales, como por ejemplo ataques de malware. En este caso, y gracias al software de monitorización, el administrador puede comprobar qué dirección de IP, conexión o protocolo consume la mayor parte del ancho de banda y reaccionar al respecto.

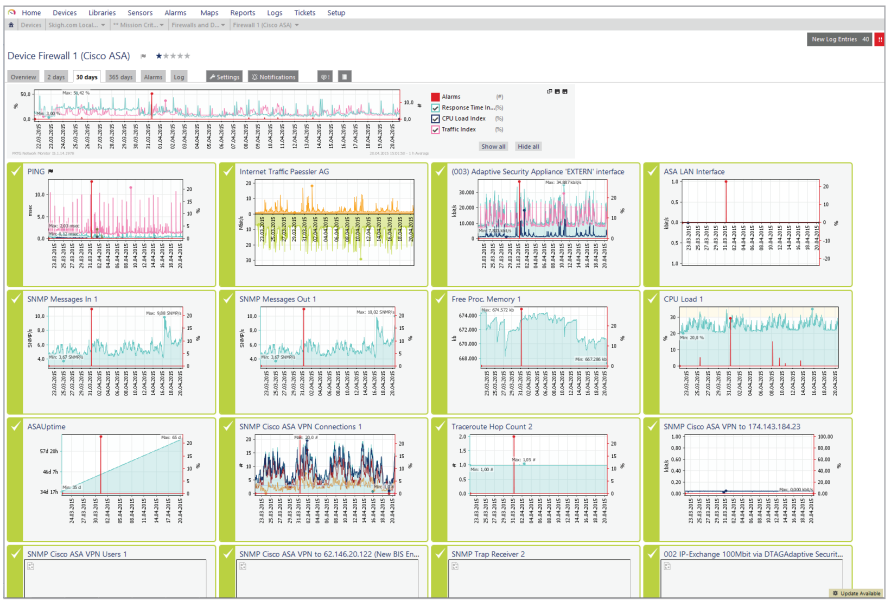
MONITORIZACIÓN DE PARÁMETROS FÍSICOS AMBIENTALES

No hay que olvidar que la monitorización supone una ventaja para la seguridad de todo el edificio, ya que permite la monitorización de influencias ambientales y medioambientales. Dispositivos especiales con sensores de humo y desprendimiento de gas avisan a tiempo de incendios o sucesos similares. Además, los sensores de cierre del edificio se pueden configurar de tal manera que envían una alarma si las puertas, ventanas o armarios de servidor están abiertos. Asimismo, los responsables de TI pueden medir la tensión de corriente con el hardware correspondiente y transmitir estos valores al software de monitorización de red que identifica las fluctuaciones en la corriente eléctrica e informa al administrador. Gracias a las numerosas posibilidades de monitorización, el equipo de TI sabe en todo momento si su red está funcionando en un entorno seguro o si se deben hacer modificaciones a corto, medio o largo plazo.

Evaluar los resultados

Las soluciones de monitorización de red de alta calidad evalúan todos los datos de monitorización en informes, y los presentan para una mayor claridad en gráficos o paneles. La información generada por el software reúne los valores identificados de cada uno de los componentes y sistemas en informes fáciles de leer. El administrador no solo recibe las actividades del firewall o del escáner de virus en forma de informe, sino que también recibe parámetros de rendimiento como la carga de RAM y CPU actual de todos los servidores y ordenadores. Además, los responsables de TI podrán visualizar la disponibilidad de todos los dispositivos de red. El informe también incluye las tendencias significativas en cuanto a la carga de ancho de banda y de red. En caso necesario, el administrador puede realizar comparativas entre los datos históricos y los actuales en diferentes situaciones. Si los datos actuales son peores que los históricos, es imprescindible realizar una optimización. Además, puede encontrar comportamientos similares de diferentes sensores mediante un análisis automático de datos de monitorización, identificando así conexiones desconocidas hasta el momento entre los diferentes componentes de red. Los análisis de datos históricos, así como la identificación de sensores con conductas similares, son de especial ayuda en los estudios comparativos en redes complejas, para investigar la carga exacta y el tipo de aprovechamiento de la red, y para cerrar huecos de seguridad potencialmente peligrosos.

FIGURA:
Evaluación de los resultados con gráficos



Resumen

Las empresas solo ofrecen una seguridad adecuada en el marco de la gestión de seguridad si todos los ámbitos cuentan con un concepto de seguridad completo. En este punto la monitorización de red funciona como un elemento esencial y estratégico añadido en el concepto de seguridad de TI. Dicho concepto debe ir más allá del aprovechamiento de firewalls y escáneres de virus. Para alcanzar la máxima seguridad posible, de manera que toda la red de la empresa cuente con una protección más eficiente ante ataques de malware o periodos de inactividad, todos los ámbitos de TI deben estar monitorizados. Por lo que el reconocimiento de tendencias y desarrollos es un factor de vital importancia para descubrir amenazas potenciales. Un software de monitorización de red asume, por tanto, las tareas del sistema de alarma preventiva. Esto convierte al software sea una ampliación necesaria del concepto de seguridad, y que contribuye a alcanzar la seguridad y el control deseados en la empresa.

SOBRE PAESSLER AG

Paessler AG es lider en la industria, proporcionando la solucion de monitorizacion y prueba más potente, costeable y fácil de usar. Los diferentes productos de software que ofrece Paessler proveen tranquilidad, confidencia y comodidad para negocios de todos los tamaños – desde pequeñas empresas hasta empresas multinacionales, incluyendo más del 70% de las compañías Fortune 100. Basada en Nuremberg, Alemania, el ámbito de Paessler cubre mas de 150,000 instalaciones activas de sus productos. Fundada en 1997, Paessler AG sigue siendo empresa privada y es reconocida como miembro activo tanto de Cisco Solution Partner Program como de VMware Technology Alliance Partner.

Es posible descargar freeware y versiones de prueba de todos los productos en www.es.paessler.com/prtg/download.

Paessler AG · www.paessler.es · info@paessler.com