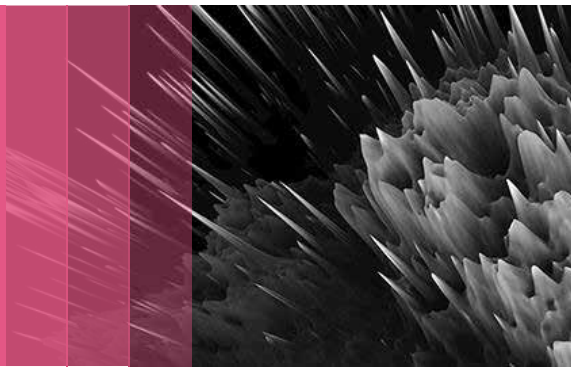
Check Point
SOFTWARE TECHNOLOGIES LTD.

SECURITY CHECKUP

THREAT ANALYSIS REPORT



Su red corporativa ofrece acceso a información valiosa y confidencial. Esa información nunca debe caer en las manos equivocadas. ¿Puede garantizar que no existen "sorpresas" ocultas que amenazan la información crítica de su compañía? ¿O que no tiene malware oculto, puertas traseras, fugas de datos u otras vulnerabilidades? La detección temprana de las amenazas ocultas le permitirá abordar de inmediato todos estos riesgos y mejorar la seguridad. Con Check Point, puede descubrir los riesgos que amenazan la seguridad de su compañía.

El Security Checkup de Check Point es una evaluación de seguridad que identifica estos riesgos en su red corporativa. Al final de la evaluación, le proporcionamos un extenso informe con el análisis de amenazas detectadas. Un experto en seguridad revisará con usted este informe, que incluye todos los incidentes de seguridad detectados durante la evaluación y las recomendaciones para protegerse frente a esas amenazas. Nuestros expertos serán sus asesores, para ayudarle a abordar cualquier problema de seguridad y hacer mucho más segura su compañía.

RIESGOS PARA LA SEGURIDAD

El informe identifica todos los posibles riesgos para la seguridad:

- Aplicaciones y páginas web de alto riesgo que utilizan los empleados habitualmente como: Aplicaciones de intercambio de archivos P2P, anonimizadores proxy, aplicaciones de almacenamiento de archivos, páginas web peligrosas, y mucho más.
- Análisis de amenazas malware que incluye los equipos infectados con bots, virus, y malware desconocido (ataques de día cero y malware que no pueden detectarse por los sistemas de antivirus tradicional).
- Vulnerabilidades utilizadas en servidores y equipos de la organización, indicadoras de posibles ataques.
- Información confidencial enviada fuera de la organización a través de emails o web.
- Análisis del ancho de banda que identifica las aplicaciones que hacen un mayor consumo de este y los sitios web a los que acceden, para comprender quién y por qué está saturando su ancho de banda en la red.
- *Para los clientes de Check Point*: Cumplimiento y buenas prácticas, comparando la configuración de las reglas actuales básicas con las recomendaciones de buenas prácticas de Check Point y también con otros estándares como PCI, HIPAA, ISO.

El informe Security Checkup incluye recomendaciones para ayudarle a comprender los riesgos, y cómo protegerse frente a ellos.

DESCUBRA LOS RIESGOS EN SU RED CORPORATIVA

EL INFORME INCLUYE:

- Equipos infectados con malware
- Acceso a aplicaciones web y sitios web de alto riesgo
- Vulnerabilidades utilizadas y ataques a su red
- Incidentes de fuga de datos
- Recomendaciones para proteger su red de estos riesgos

27 de mayo de 2015

RIESGO CERO PARA LA RED

La evaluación Security Checkup despliega un gateway de seguridad dentro de la red que inspecciona todo el tráfico. El gateway no está conectado inline, evitando el cambio de configuración de la red y la consecuente interrupción o tiempo de inactividad. En su lugar, inspecciona una copia del tráfico (mirrored) usando el Monitor Port conectado a un dispositivo Test Access Point (TAP) o un Mirror Port (también denominado Span Port) en un conmutador de la red. De esta forma se eliminan todos los desafíos que implica la conexión inline, asegurando la inspección solo de una copia del tráfico de red. Dado que el Monitor Port no transmite ningún tráfico a la red, no es necesario realizar ningún cambio en la configuración de la misma y no existe el riesgo de una interrupción o parada.

EVALUACIÓN INSITU

Cualquier organización puede participar en un Security Checkup, con independencia de si utilizan o no soluciones de Check Point. Los expertos en seguridad dirigen las evaluaciones in-situ que incluyen cuatro pasos:

1. **Instalación del Security Gateway de Check Point** - Un experto en seguridad instala el Security Gateway de Check Point sobre el cuál se realizará la evaluación. Luego activa y configura todos los Software Blades involucrados: Application Control, URL Filtering, IPS, Anti-Bot, Antivirus, Threat Emulation, DLP, Identity Awareness si es necesario, SmartEvent u otros.
2. **Inspección del tráfico de red** - Una vez que el dispositivo esté instalado y conectado a la red corporativa empieza a inspeccionar el tráfico de la red. Para asegurar una inspección en profundidad, recomendamos monitorizar el tráfico durante al menos una semana, y cuanto más tiempo mejor.
3. **Análisis de resultados** - Tras retirar el dispositivo de la red, el experto de seguridad analizar los resultados y genera el informe Security Checkup.
4. **Informe con los resultados** - Un experto en seguridad presentará los resultados obtenidos identificando los puntos débiles de la red. Entonces estudiarán qué tecnologías de seguridad y soluciones pueden ser las mejores para proteger su red frente a esas amenazas.

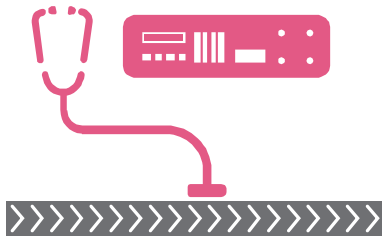
¿CUÁLES SON SUS BENEFICIOS?

- Una mejor comprensión de la exposición a riesgos para la seguridad de su red corporativa.
- Identificación y priorización de las brechas de seguridad que requieren mejora.
- Presentación de la última tecnología de seguridad que cubre todos los aspectos de la seguridad de red

PROGRAME UN SECURITY CHECKUP

Para realizar un Security Checkup, contacte con su Account Manager o envíe un email a **info_iberia@checkpoint.com.**

INSPECCIONAR UNA COPIA DEL TRÁFICO IMPLICA RIESGO CERO PARA LA RED



Más información: checkpoint.com/securitycheckup

27 de mayo de 2015