CompuNet

PROTEGEMOS TU INFORMACIÓN

CompuNet
PROTEGEMOS TU INFORMACIÓN

RECOMENDACIONES CONTRA EL RANSOMWARE

El siguiente documento tiene como fin entregar 14 recomendaciones o medidas para contener y asegurar de mejor manera los sistemas ante la oleada de ransomware prevista para el siguiente año.

MEDIDA

01

RANSOMWARE

Se recomienda implementar una solución endpoint AntiRansomware de manera tal de poder controlar cualquier evento de día cero. Adicionalmente, se recomienda utilizar un AntiRansomware a nivel perimetral, los cuales, protegen de amenazas en el perímetro impidiendo su entrada a la red.

MEDIDA

02

RESPALDOS

Para abordar las amenazas de tipo RANSOMWARE y similares, es necesario extender el respaldo hacia las estaciones de trabajo mediante la implantación de soluciones que puedan mantener "versiones" de los datos permitiendo la recuperación de una versión determinada.

MEDIDA

03

ACTUALIZACIONES

La implementación de un sistema de gestión de actualizaciones es, más que deseable, critica. El vector de ataque ampliamente empleado por las amenazas es la explotación de vulnerabilidades documentadas aprovechando la inexistencia de políticas y/o procedimientos para actualizar los sistemas de información. Esto permite la movilidad horizontal y vertical: La primera, infectando nuevos hosts de la red y la segunda para obtener credenciales con mayores privilegios dentro de la organización o host comprometidos.

MEDIDA

04

ANTIMALWARE

Actualmente, los software o motores antimalware son la primera línea de defensa sirviendo como línea preventiva y reactiva. Es altamente relevante que esta primera línea de defensa esté correctamente actualizada, con sus filtros debidamente activos y en operación.

MEDIDA

05

GESTIÓN DE CREDENCIALES CON PRIVILEGIOS

Es deseable implantar políticas de gestión de credenciales con privilegios y controlar el uso y acceso de estas. El mercado señala a las soluciones PIM (Privileged Identity Management) y PAM (Privileged Access Management) como candidatas para abordar esta problemática mediante la implantación de buenas prácticas y compliance.

MEDIDA

06

ANTISPAM

Con una herramienta ANTISPAM debidamente actualizada y con filtros efectivos es una línea de seguridad, a nivel de perímetro, la cual permite detener una amplia cantidad de amenazas. Es ideal complementar esta herramienta con alguna solución de detección de ataques avanzados las cuales proveen otra perspectiva, mucho más moderna y adecuada, apoyadas fuertemente en Cloud Computing para hacer revisiones exhaustivas de los correos electrónicos y sus adjuntos. Finalmente, educación de usuario final y evaluación de riesgo para campañas de Phishing.

MEDIDA

07

ACCESOS REMOTOS

Es recomendado revisar los accesos remotos existentes y las correspondientes políticas aplicadas. Es deseable que:

- Se acote únicamente hacia el o los hosts necesarios de acceder de manera remota
- Se acote únicamente hacia el o los puertos de servicio necesarios para la operación
- Se mantenga un registro completo de auditoria de todos los accesos remotos
- Se extienda la aplicación de políticas hacia terceros
- Idealmente se complemente con una solución tipo NAC
- La autenticación remota debe implementar, idealmente, doble factor
- Se debe emplear siempre y únicamente accesos mediante VPN SSL o IPSEC
- L2TP y PPTP deben ser abandonados
- Eliminar cualquier tipo de acceso basado en NAT u otro tipo de PORT MAPPING
- Si no afecta al negocio y no se cumplen las recomendaciones anteriores; Eliminar el acceso remoto

MEDIDA

08

CICLO DE VIDA Y SOPORTE TECNOLÓGICO

Llevar un inventario actualizado de los activos de red, hacer un levantamiento de riesgos asociado a los activos inventariados e implantar un plan de tratamiento y gestión de riesgos, es hoy en día la base para los sistemas de gestión de seguridad de la información los cuales, como erróneamente se asume, no solo son un desafío tecnológico y/o técnico, más bien se trata de una necesidad corporativa que afecta e impacta a todas las operaciones de negocio.

MEDIDA

09

WEB FILTER & APP CONTROL

Una adecuada política de filtro de seguridad permitirá reducir la exposición de los usuarios con sitios web que sean conocidos como distribuidores de malware. Así también, en la actualidad es posible identificar el tráfico aislando aplicaciones determinadas, las cuales pueden ser un vector de riesgo de infección, tales como CHAT en línea (Facebook Messenger, WhatsApp Web, Telegram u otros. Esto, por la posibilidad de transmisión (recepción para este caso) de archivos adjuntos maliciosos.

MEDIDA

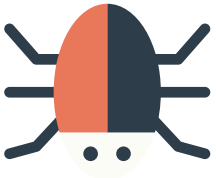
10

ARCHIVOS

Con vector de infección nos referimos al medio sobre el cual este archivo ingresa a la organización. Dado que existen múltiples medios tales, y no limitado a estos, como:

- Adjuntos de Correo Electrónico
- Descargados desde la web (email web, web storage, etc.)
- Medios Removibles
- Servidores de Archivos
- Otros

Se hace necesaria una política que controle los tipos de archivos permitidos o aptos para la organización.

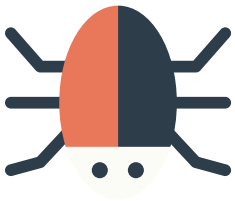


MEDIDA

11

VISIBILIDAD Y CONOCIMIENTO

Obtener visibilidad con respecto a los activos de información existentes en la red corporativa o institucional y, de estos activos, conocer en detalle su funcionamiento, versión, origen, etc. Es hacia lo que todo departamento de seguridad (y también TIC) debe propender.



MEDIDA

12

MONITORIZACIÓN Y CORRELACIÓN

Soluciones tipo SIEM de propósito general o específicos de seguridad permiten aplicar buenas prácticas de gestión y seguridad, estar norma bajo compliance y, principalmente, obtener visibilidad y conocimiento respecto al comportamiento, uso y abuso de los activos de información.

MEDIDA

13

RECURSOS COMPARTIDOS

Los servidores de archivos son ampliamente usados en las organizaciones, aunque es deseable emplear sistemas de gestión documental dado que son mucho más eficientes, permiten el versionamiento de archivos, el control y gestión de acceso además de ser más interoperables al emplear HTTPS (HTTP no debería siquiera ser considerado a estas alturas).

MEDIDA

14

CONTROL DE DISPOSITIVOS & DLP

Las herramientas de gestión y control de dispositivos permiten implantar políticas discriminando tipos y medios USB, Wireless, Bluetooth, CIF, entre otras.

En este punto es vital controlar el acceso WIFI de los usuarios corporativos, obligando a que estos no puedan emplear redes NO seguras o NO permitidas. Es también necesario bloquear la posibilidad de habilitar BRIDGE entre la red corporativa y otras redes WIFI o USB TETHERING (Smartphones).

CompuNet®

PROTEGEMOS TU INFORMACIÓN

(+56) 2 2236 6029
ventas@compunet.cl
www.compunet.cl
San Pio X 2460 , Of 1206
Providencia, Santiago Chile,
CP 7510041