COMMVAULT®

4 formas de protegerse y recuperarse ante el ransomware

MANTENGA EL ACCESO A SUS DATOS PARA ASEGURAR UN SERVICIO DE CALIDAD

El número de incidentes de ransomware contra cualquier sector va en aumento. Se ha convertido en una fuente de ingresos fácil para los cibercriminales y por ello el número de ataques continúa creciendo cada año. Cuando un ataque tiene lugar con éxito, las organizaciones pierden acceso a archivos electrónicos críticos, quedando comprometido el servicio a sus Clientes. Para restablecer el acceso a estos datos, las organizaciones deben decidir si pagar el rescate –con la esperanza de que los archivos sean realmente liberados– o intentar una recuperación *ad hoc*, sin garantía de que los datos actuales vayan a ser recuperados con fiabilidad. A fin de mantener el necesario acceso a los datos de su compañía y asegurar la calidad de su servicio, considere estas buenas prácticas para protegerse y recuperarse con eficacia ante ataques de ransomware.

4 BUENAS PRÁCTICAS PARA PROTEGERSE CONTRA LOS ATAQUES DE RANSOMWARE

Implementar una estrategia de seguridad multi-capa (que incluya sistemas de protección como anti-malware, firewall personal, cifrado de discos y archivos, DLP, etc.) es fundamental para protegerse contra las crecientes amenazas de ciberseguridad. Sin embargo, incluso con todas estas soluciones de protección *endpoint*, todavía existe la posibilidad de sufrir brechas. Según se declara en el Cuadrante Mágico de Gartner sobre plataformas de protección Endpoint [6], "si tenemos en cuenta que el 44% de los clientes de plataformas EPP (*Endpoint Protection Platforms*) han sido atacados con éxito, parece claro que la industria está fallando en su objetivo principal: bloquear las infecciones maliciosas".

Para proteger los entornos IT del ransomware, son recomendables las siguientes buenas prácticas:

UNO: DESPLIEGUE UN PROGRAMA EFECTIVO DE SEGURIDAD DE LA INFORMACIÓN

Si su organización se está iniciando en la seguridad de la información, o si por el momento cuenta sólo con alguna capacidad parcial, debería plantearse adoptar los siguientes pasos, descritos en la Tabla 2, para poner en marcha un programa de seguridad eficaz.

PASOS	ACCIONES
SEPA DÓNDE ESTÁN ALMACENADOS LOS DATOS CRÍTICOS	Mantenga conocimiento sobre la localización de los datos • En el data center • En instalaciones remotas • En la nube • En los servidores del proveedor
HAGA INVENTARIO	• Conozca qué sistemas manejan los datos sensibles (almacenamiento, proceso, transferencia) • Conozca los flujos de datos • Determine qué sistemas presentan el mayor riesgo para sus operaciones
EVALÚE LOS RIESGOS	• Incluya registros electrónicos, medios físicos y la disponibilidad de sistemas, servicios o dispositivos críticos
APLIQUE CONTROLES DE SEGURIDAD	• Seleccione, aplique y gestione controles de seguridad en función de los riesgos
MONITORICE LA EFECTIVIDAD	Prepárese para un entorno de amenazas en continua evolución • Evalúe proactivamente la eficacia de su estrategia de seguridad de la información basada en riesgos, los controles de seguridad aplicados, y la implementación adecuada de las tecnologías de seguridad • Aplique acciones correctivas, remediación, y las lecciones aprendidas
EDUQUE A LOS USUARIOS	•Asegúrese de que se forma a los empleados sobre lo que han de hacer cuando reciban emails de remitentes desconocidos con adjuntos o enlaces sospechosos (para saber qué pasos seguir, vea el Apéndice).

Tabla 2) Componentes de un programa de seguridad efectivo

6. Gartner. Cuadrante Mágico para plataformas de protección *endpoint*. 1 de febrero, 2016.

DOS: PROTEJA SUS DATOS CON LAS MEJORES PRÁCTICAS TECNOLÓGICAS

Ante un cada vez mayor número de amenazas, y una creciente sofisticación de los ataques, las organizaciones sanitarias necesitan entender claramente la relación entre el coste de invertir en seguridad y educación de los empleados y el coste que supone la pérdida de acceso a datos críticos y el consiguiente impacto en la asistencia a los pacientes.

La seguridad de red es una buena "primera línea" de defensa contra los ataques de ransomware. Añadiendo la implementación de una serie de buenas prácticas tecnológicas, las organizaciones sanitarias protegerán mejor sus datos críticos y sus infraestructuras de TI. La Imagen 3 describe estas estrategias clave, que ayudarán a eliminar el potencial de infección por ataques de ransomware.

PASOS	ACCIONES
DETECCIÓN Y PREVENCIÓN	Emplee una solución de seguridad multifacética • Protéjase contra amenazas basadas en archivos (antivirus tradicionales), protección de descargas, protección para navegadores, tecnologías heurísticas, firewalls y un sistema de scoring de reputación de archivos a través de información proveniente de comunidades online. • Mantenga los sistemas y el software actualizados. Aplique todos los parches críticos.
USO DE EQUIPOS DE RESPUESTA RÁPIDA (CERT) EXTERNOS	• A menudo identificarán el problema antes que las empresas de antivirus • Pueden recomendarle pasos inmediatos para el filtrado manual (a las empresas de software puede llevarles días liberar un parche)
IDENTIFIQUE Y DETENGA LA INFECCIÓN	Defina una política integral de prevención • Incluyendo políticas para endpoints y redes, así como productos de protección como antivirus, antispyware o sistemas firewall • Limite la ejecución de programas no aprobados en los puestos de trabajo • Limite la capacidad de escritura de los usuarios finales de modo que, incluso si descargan y ejecutan una aplicación de ransomware, ésta no podrá cifrar archivos más allá de los permisos específicos del usuario • Incluya registros electrónicos, medios físicos y la disponibilidad de sistemas, servicios o dispositivos críticos.
MANTENGA UNA IMAGEN "GOLD" DE SISTEMAS Y CONFIGURACIONES	• Un aspecto esencial de las políticas de gestión de datos • Sencilla clonación de sistemas infectados con el master
MANTENGA UNA ESTRATEGIA DE BACKUP COMPLETA	• La forma más rápida de recuperar el acceso a los archivos críticos • Snapshots de volúmenes con mayor frecuencia (por ejemplo, cada 15 minutos) y almacenados por períodos de tiempo más largos. • Retirada de la red del sistema impactado. Eliminación de la amenaza. • Restauración de cualquier archivo afectado desde una copia de seguridad conocida
COMPRUEBE LA EFICACIA	Prepárese para un panorama de amenazas en evolución • Evalúe proactivamente la eficacia de su estrategia de seguridad de la información, los controles de seguridad aplicados y la correcta implementación de las diferentes tecnologías de seguridad. • Aplique acciones correctivas, mitigación y lecciones aprendidas
EDUQUE A LOS USUARIOS	• Asegúrese de que los empleados estén informados sobre qué hacer cuando reciben emails de remitentes desconocidos con adjuntos o enlaces sospechosos (consulte el Apéndice para conocer los pasos recomendados).

Tabla 3) Mejores prácticas tecnológicas

TRES: EMPLEAR ESTRATEGIAS DE BACKUP EFECTIVAS

Un ataque de ransomware es un *hacking* progresivo, que sigue funcionando tras el ataque inicial y puede ejecutarse en segundo plano durante una semana o más, aprendiendo el comportamiento de las rutinas de *backup*. Por todo ello, es importante mantener un backup permanente de los datos en otras ubicaciones como parte de los procedimientos de recuperación ante desastres.

Aquéllos usuarios que sólo utilizan *snapshots* como sistema de *backup* corren un riesgo aún mayor, ya que cuando se replica la instantánea u otra instancia, la fuente queda dañada también, ya que sigue a la replicación. La clave está en conservar una versión anterior de los datos en un lugar protegido.

PASOS	ACCIONES
APLIQUE PROCEDIMIENTOS DE BACKUP Y DISASTER RECOVERY	• Realice directamente una copia general de backup, en lugar de varias versiones almacenadas en el mismo sistema. • Cuente con copias externas de los datos más allá de los snapshots que se mantienen en el sistema de origen.

Tabla 4) Mejores prácticas de protección de datos.

CUATRO: EDUCAR A LOS EMPLEADOS PARA SECURIZAR SUS *ENDPOINTS*

Por último, será esencial educar al personal sanitario en las mejores prácticas de seguridad para mantener seguros los sistemas y la información médica protegida (PHI, por sus siglas en inglés). Recuérdeles, sobre todo, que han de actuar con sentido común. Estas prácticas, que se describen en el *Internet Security Threat Report* [7], están detalladas en la Tabla 5.

PASOS	ACCIONES
FORME A LOS USUARIOS EN LAS MEJORES PRÁCTICAS DE SEGURIDAD	• No abra los archivos adjuntos a menos que sean esperados o que provengan de una fuente conocida y fiable. • No ejecute software que se descargue de Internet (si es que esta acción es posible) a menos que provenga de una fuente fiable o que la descarga haya sido escaneada en busca de malware. • Tenga cuidado al hacer clic en enlaces contenidos en emails o programas de redes sociales, incluso cuando provenga de fuentes de confianza o personas conocidas. • Emplear una conducta segura en las redes sociales. Los temas más candentes son un cebo idóneo para las estafas. No todos los enlaces conducen a páginas de inicio de sesión reales. • Invitar a los empleados a dar la voz de alarma si ven algo sospechoso. • Si los usuarios de Windows ven una advertencia que indica que están "infectados" después de hacer clic en una URL o utilizar un buscador (indicativo de falsas infecciones de antivirus), eduque a los usuarios para salir del navegador usando Alt-F4, CTRL-W o con el administrador de tareas y, a continuación, avisar al servicio de asistencia.

El 75 por ciento de los hospitales de EEUU consultados en una reciente encuesta declaró haber sido atacado con ransomware en el último año.

HEALTHCARE IT NEWS
7 de Abril de 2016

7 Symantec. Internet Security Threat Report, Volumen 21. Abril de 2016.

EMPLEAR LAS MEJORES PRÁCTICAS DE PROTECCIÓN ENDPOINT	• Implementación de soluciones *plugin* de reputación de URLs que muestren la reputación de los sitios web de las búsquedas. • Restringir el software a las aplicaciones aprobadas por la empresa y evitar la descarga de software desde sitios de intercambio de archivos. Descargue paquetes sólo desde sitios web de proveedores de confianza. • Implementar autenticación de dos pasos en cualquier sitio web o aplicación que lo ofrezca. • Asegurarse de que los médicos tengan diferentes contraseñas para cada cuenta de email, aplicaciones e inicios de sesión, especialmente para sitios y servicios relacionados con su trabajo.

Tabla 5) Prácticas recomendadas para empleados y endpoints.

CONCLUSIÓN

Asegurar la información médica protegida y otros datos críticos es una necesidad para las organizaciones sanitarias, para aportar la mejor asistencia posible a los pacientes y mantener el cumplimiento de la normativa vigente. Proteger toda esta información ante los ataques de ransomware debería ser una prioridad para estas organizaciones, a fin de evitar la pérdida de la disponibilidad de la información y sistemas críticos. Proteger los datos clínicos prestando atención a las mejores prácticas en materia de seguridad, tecnología, sistemas de backup y formación de empleados. Como resultado, los datos críticos permanecerán seguros y mejorará la continuidad del negocio, a la vez que se mitigarán los riesgos de ransomware.

RECURSOS

1 **commvau.lt/2agPXQ7**

Si quiere saber más sobre cómo Commvault® puede ayudarle a gestionar de manera inteligente sus datos, visite commvault.es

COMMVAULT®

PROTECT. ACCESS. COMPLY. SHARE.

COMMVAULT.ES | 91 626 60 42 | INFO-IBERIA@COMMVAULT.COM