GUÍA COMPLETA

PARA PROTEGERTE DE NUEVOS ATAQUES DE RANSOMWARE

Datta
SOLUTIONS

Datta
SOLUTIONS

TRANSFORMANDO DESAFÍOS EN OPORTUNIDADES DIGITALES.

El ransomware es un tipo de software malicioso que secuestra los datos de las organizaciones y pide un rescate para liberarlos. Si los ataques tradicionales a nivel de sistemas de archivos de red o sistemas operativos Windows ya eran preocupantes, las nuevas amenazas a nivel de infraestructura virtual, como el reciente SEXi, son una verdadera pesadilla.

A continuación, te presentamos algunas medidas esenciales que debes tomar de inmediato para minimizar el riesgo de ser víctima de estas variantes de ransomware y para garantizar una recuperación rápida, segura y confiable:

Actualiza tu ambiente de vSphere:

- Mantén tus ESXi actualizados. Existen versiones con vulnerabilidades reconocidas que deben ser parcheadas a la brevedad.
- Implementa una estrategia para la aplicación regular de parches de seguridad.

Gestión de cuentas de usuario:

- Evita usar cuentas de administrador para tareas cotidianas. Utiliza autorización basada en roles con los privilegios mínimos necesarios para cada tarea.
- Protege rigurosamente tus credenciales administrativas. Si un atacante accede a ellas, no necesita una vulnerabilidad de ESXi para llevar a cabo su ataque.

Deshabilita servicios no necesarios:

- Servicios como SSH y Shell deberían estar activados solo cuando sea absolutamente necesario, ya que los atacantes pueden utilizarlos para realizar acciones maliciosas.

Ejecución de software firmado:

- Deshabilita la ejecución de software no firmado en tus hosts ESXi.

Autenticación multifactor (MFA):

- Configura MFA para tu ambiente virtual, añadiendo una capa extra de seguridad.

Monitoreo constante:

- Monitorea las actividades en tu ambiente virtual. Muchos ataques pueden detectarse a tiempo si se tiene visibilidad de las actividades sospechosas.

Capacitación y formación:

- Mantén campañas de entrenamiento continuas para usuarios y administradores sobre las mejores prácticas de seguridad.

Aseguramiento de respaldos:

- Asegura la recuperabilidad, aislamiento e inmutabilidad de tus respaldos. Un ataque que cifra tanto los datos productivos como los respaldos puede ser devastador.

Datta SOLUTIONS

Estas son solo algunas de las medidas básicas que debes considerar para proteger tu ambiente virtual de un ataque de ransomware.

En Datta, podemos ayudarte con estas y muchas otras medidas para minimizar el riesgo de ser víctima de un ataque. Ofrecemos soluciones personalizadas que pueden incluir:

- Análisis de tu ambiente virtual en busca de ESXi en versiones vulnerables.
- Creación y ejecución de un plan de actualización de vSphere a versiones seguras.
- Análisis de mejores prácticas para la gestión de roles, usuarios y permisos.
- Verificación e implementación de medidas de protección de datos, asegurando diseño, aislamiento e inmutabilidad para resistir ataques.
- Implementación de autenticación multifactor para el ambiente virtual.
- Aplicación de medidas de hardening recomendadas por VMware.

Contáctanos para crear una solución a la medida de tus necesidades y proteger tu infraestructura virtual contra las amenazas de ransomware.