Cómo proteger a su organización del

RANSOMWARE

Ransomware es una sofisticada clase de malware que retiene su información hasta que se pague un rescate.

Prevención

- Realice copias de seguridad de sus archivos
- Use filtros de correo para los empleados
- Eduque a los usuarios finales
- Vulnerabilidades de patch
- Provea la menor cantidad posible de privilegios
- Use aplicaciones de confianza

Detección

- Use una herramienta robusta de alertas para marcar las invasiones de malware
- Reconozca los síntomas de un ataque de malware, como archivos accesados, renombrados, eliminados o encriptados de forma masiva.

Secuestro

- Utilice una herramienta de detección automática de ransomware para detectar y neutralizar las amenazas instantáneamente.
- Apague los sistemas infectados y aíslelos de la red para proteger a sus otros servidores de archivos.

Restauración

- Antes de recuperar sus archivos de una copia de seguridad, asegúrese de que el malware ha sido totalmente eliminado de su red.
- Obtenga los detalles del ataque de ransomware –cómo quién hizo qué y desde dónde- para identificar la fuente de la amenaza y prevenir futuras afectaciones.

Pagar o no pagar

- Si su organización experimenta un ataque de ransomware, nunca pague el rescate; nada como el honor para responder a los ladrones.
- De acuerdo con el **Boletín de Seguridad de Kaspersky 2016,** una de cada cinco compañías que pagan el rescate, no obtiene su información de vuelta.
- Visite nomoreransom.org para reportar esta clase de crímenes cibernéticos y aproveche las herramientas de detección de ransomware disponibles.