Mesa 7

Nota :
https://www.welivesecurity.com/la-es/2021/07/05/ataque-masivo-ransomware-revil-comprometio-mas-1000-companias-mundo/

¿Qué tipo de amenaza es?
Ransomware para cifrar la información.

¿Cómo comienza y cómo se propaga esta amenaza?
Por medio de un instalador de una actualización automática de un software muy usado, seguido de una propagación a máquinas de clientes

¿Hay más de una amenaza aplicada ?
Se evidencia la existencia de un virus Gusano por la facilidad de poder moverse entre servidores e infectar los mismos.

¿Qué solución o medida recomendarían ?

A. Realizar backups de datos importantes y de manera regular, alojando la info en un medio externo para no tener que pagar por un rescate.
B. Una vez infectado el equipo aislarlo de la red o apagarlo para evitar extender la amenaza.
C. Mantener buenas políticas de seguridad a nivel empresarial.
D. Uso de Máquinas virtuales para aislar el sistema principal.Actualización constante del SO con los últimos parches de seguridad.
E. Un cortafuegos bien configurado e instalar una solución antimalware o obtener algún tipo de herramienta Anti Ransomware.