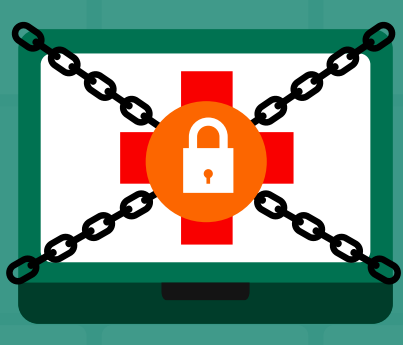
ManageEngine
DataSecurity Plus



DIRECTRICES DE LA HIPAA SOBRE LOS ATAQUES DE RANSOMWARE

Ransomware

Software malicioso dise ad para capturar, codificar y mantener los datos como rehenes hasta que las v ctim paguen un rescate.

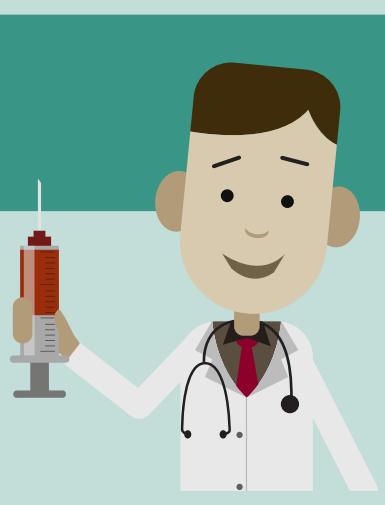
HIPAA

Normas que deben seguir las empresas de salud para protege mantener la confidencialidad de informaci n de identificaci n personal de salud.

¿Cómo puede el cumplimiento de la HIPAA ayudar a prevenir las infeccione de malware, incluidos los ataques de

La norma de seguridad de la HIPAA obliga a las empresas a adoptar medidas de seguridad que eviten el ransomware, como por ejemplo:

- Realización de análisis de riesgos para identificar las amenazas y vulnerabilida de la PHI.*
- Educar a los usuarios finales sobre la protección contra el software malicioso.
- Detección de software malicioso.
- Aplicar el principio del mínimo privilegio para limitar el acceso a la información PHI.



¿Cómo puede el cumplimiento de la HIPAA ayudar a las empresas a recuperarse de las infecciones de ransomware?

HIPAA mandates organizations follow a few key procedures to respond to and recover from a ransomware attack, including:

- Detección y análisis inicial del ataque ransomware.
- Realización de actividades posteriores incidente que incluyan un análisis forense en profundidad.
- Restaurar los datos perdidos durante ataque de ransomware.
- Contener el impacto y la propagación ransomware.
- Remediar las vulnerabilidades que permitieron la propagación del ransomware.

Elanálisis posterior a la violación debe incluir una evaluación de si hubo una violación de la PHI como resultado del incidente de seguridad del ransomware.

¿Es una violación de la HIPAA si el ransomware infecta el sistema de una entidad cubierta?

- Si la ePHI** se codifica como resultad de un ataque de ransomware, entonce ha producido una violación de la HIPA
- Si la organización puede demostrar qu existe una "...baja probabilidad de que PHI se haya visto comprometida", entonces el ataque de ransomware no dado lugar a una violación de la HIPA

¿Cómo pueden las empresas demostrar que un ataque de ransomware no ha puesto en pelig la PHI de sus clientes?

Si una organización se enfrenta a un ataque de ransomware, la HIPAA exige que s informe de la violación si se ha visto comprometida alguna PHI. Sin embargo, si un organización puede demostrar que la PHI no fue robada o comprometida durante ataque, puede evitar el proceso de notificación de la violación. Las organizaciones plantearse las siguientes preguntas cuando investigan si la PHI se ha visto compro

- ¿Qué tipo y cantidad de PHI estuvo involucrada en el ataque?
- ¿En qué medida se ha mitigado el riesg para la PHI?
- ¿Realmente se adquirió o se visualizó PHI?
- ¿Quién utilizó la PHI y a quién se le reveló?

¿Se trata de una violación notificable s PHI comprometida ya estaba cifrada p cumplir con la HIPAA?

- No, ya que la ePHI cifrada para cumplir con la HIPAA ya no se considera "PHI segura".

* PHI - Información de salud protegida

** ePHI - Información de salud protegida electrónicamente

Fuente: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf