Diario Gestor de Incidentes 2024-09-13 #1

Clinica Engwald - Av. San Martin 7100 - Eldorado

Escenario

La clínica Engwald está especializada en la prestación de servicios de atención primaria y experimentó un incidente de seguridad un martes 12/09/24 por la mañana, aproximadamente a las 9:00 a.m. Varios empleados informaron de que no podían utilizar sus pcs para acceder a archivos como registros médicos.

La empresa dejó de funcionar porque los empleados no podían acceder a los archivos y programas informáticos necesarios para realizar su trabajo.

Además, los empleados también informaron de que en sus pcs aparecía una nota de rescate. En ella se decía que todos los archivos de la empresa habían sido cifrados por un grupo organizado de hackers no éticos autodenominados MITNICK y conocidos por atacar organizaciones de los sectores de la sanidad y el transporte. A cambio de restaurar el acceso a los archivos cifrados, la nota de rescate exigía una suma de dinero a cambio de la clave de descifrado.

Los atacantes consiguieron acceder a la red de la empresa mediante correos electrónicos de phishing dirigidos, que se enviaron a varios empleados de la empresa. Los mensajes contenían un archivo adjunto malicioso que instalo malware en los pcs de los empleados una vez descargado.

Una vez que los atacantes obtuvieron acceso, desplegaron su ransomware, que cifró archivos críticos. La empresa no pudo acceder a los datos críticos de los pacientes, lo que provocó importantes interrupciones en sus operaciones comerciales. La empresa se vio obligada a apagar sus sistemas informáticos y a ponerse en contacto con varias organizaciones para informar del incidente y recibir asistencia técnica.

Diario Gestor de Incidentes

| Fecha | 12/09/2024 | | |
| --- | --- | --- | --- |
| Entrada N` | #00001 | | |
| Descripción | La clínica Engwald experimentó un incidente de seguridad. Varios empleados informaron de que no podían utilizar sus pcs para acceder a archivos como registros médicos.  La empresa dejó de funcionar porque los empleados no podían acceder a los archivos y programas informáticos necesarios para realizar su trabajo. | | |
| Herramientas Usadas | * Correos electrónicos de phishing dirigidos * Archivo adjunto malicioso que instalo malware * Ransomware de cifrado | | |
| Las 5 W's  Capture las 5 W's  del incidente | 1. Quién (Who) causó el incidente ?  Grupo organizado de hackers no éticos autodenominados MITNICK y conocidos por atacar organizaciones de los sectores de la sanidad y el transporte.  2. Que (What) sucedió ?  Los atacantes consiguieron acceder a la red de la empresa mediante correos electrónicos de phishing dirigidos, que se enviaron a varios empleados. Los mensajes contenían un archivo adjunto malicioso que instalo malware en los pcs de los empleados una vez descargado, una vez que los atacantes obtuvieron acceso, desplegaron su ransomware, que cifró archivos críticos.  Los empleados también informaron de que en sus pcs aparecía una nota de rescate. En ella se decía que todos los archivos de la empresa habían sido cifrados por MITNICK y a cambio de la clave de descifrado para restaurar el acceso a los archivos, la nota exigía una suma de dinero.  3. Cuando (When) sucedió el incidente ?  Martes, 12 de Noviembre de 2024 a las 9:00 AM  4. Donde (Where) sucedió el incidente ?  Pcs de empleados en la Clínica Engwald, Eldorado, Misiones, Argentina.  5. Porque (Why) sucedió el incidente ?  Los empleados clickearon en descargar los archivos adjuntos del email de phishing que se envió MITNICK, que contenía e instalo malware en los pcs de los empleados, ese malware ayudó a MITNICK a acceder a las cuentas de la empresa y poder desplegar su ransomware de cifrado. | | |
| Notas Adicionales: | Se contactó a Globe Sistemas para desbloquear el ransomware mediante Herramientas de Desbloqueo de CriptoHash, también instalará un filtro AntiSPAM Online de AVAST. Se recomienda no abrir archivos adjuntos de fuentes no agendadas en las libretas de contactos de mails de la Clínica , | | |