Incident Manager Diary 2024-09-13 #1

Engwald Clinic - Av. San Martin 7100 - Eldorado

Scenery

The Engwald clinic specializes in providing primary care services and experienced a security incident on Tuesday morning 12/09/24 at approximately 9:00 a.m. Several employees reported that they were unable to use their PCs to access files such as medical records.

The company ceased operations because employees could not access the files and software necessary to do their jobs.

Additionally, employees also reported that a ransom note appeared on their PCs. It stated that all company files had been encrypted by an organized group of unethical hackers calling themselves MITNICK and known for targeting organizations in the healthcare and transportation sectors. In exchange for restoring access to the encrypted files, the ransom note demanded a sum of money in exchange for the decryption key.

The attackers gained access to the company's network via targeted phishing emails, which were sent to several company employees. The emails contained a malicious attachment that installed malware on employees' PCs once downloaded.

Once the attackers gained access, they deployed their ransomware, which encrypted critical files. The company was unable to access critical patient data, leading to significant disruptions to its business operations. The company was forced to shut down its IT systems and contact several organizations to report the incident and receive technical support.

Incident Manager Diary

| Date | 12/09/2024 | | |
| --- | --- | --- | --- |
| Entry N` | #00001 | | |
| Description | The Engwald clinic experienced a security incident. Several employees reported that they were unable to use their PCs to access files such as medical records.  The company ceased operations because employees could not access the files and software necessary to do their jobs. | | |
| Tools Used | * Targeted phishing emails * Malicious attachment that installed malware * Encryption ransomware | | |
| The 5 W's  Capture the 5 W's  of the incident | 1. Who caused the incident?  Organized group of unethical hackers calling themselves MITNICK and known for attacking organizations in the healthcare and transportation sectors.  2. What happened?  The attackers gained access to the company's network via targeted phishing emails, which were sent to several employees. The emails contained a malicious attachment that installed malware on employees' PCs once downloaded. Once the attackers gained access, they deployed their ransomware, which encrypted critical files.  Employees also reported that a ransom note appeared on their PCs. It stated that all company files had been encrypted by MITNICK and that in exchange for the decryption key to restore access to the files, the note demanded a sum of money.  3. When did the incident happen?  Tuesday, November 12, 2024 at 9:00 AM  4. Where did the incident happen?  Employees' units at the Engwald Clinic, Eldorado, Misiones, Argentina.  5. Why did the incident happen?  Employees clicked to download attachments from the phishing email sent by MITNICK, which contained and installed malware on employees' PCs. This malware helped MITNICK access company accounts and deploy its encryption ransomware. | | |
| Additional Notes: | Globe Systems was contacted to unlock the ransomware using CryptoHash Unlocking Tools, and will also install an AVAST Online AntiSPAM filter. It is recommended not to open attachments from sources not listed in the Clinic's email address books. | | |