A news item came to light this week, but seemed to be noticed mainly by those in cybersecurity. The IT system of the Hollywood Presbyterian Medical Center in California was being held for ransom, and the hospital paid the $17,000 ransom this week.

The FBI is investigating and I am sure we will hear more about this in the near future. This incident brings up a lot of questions with few answers, but I can shed some light on a few of the questions now:

1. How was an outside entity able to “kidnap” an IT system?
Simple. They used “ransomware”. This is a program that takes control of a computer system. It’s like someone taking control of the steering wheel of your car and not giving it back to you until you give them money. They probably were able to hack into the computer system through an open port, an USB drive or a virus that was downloaded. And that leads me to my second question.

2. Why this particular hospital?
They were considered to be an easier target. This wasn’t a large hospital system like Mass General or UCLA Medical Center, but a small entity. If any manager thinks their organization is too small to be affected by cybercrime, then this incident shows they are wrong.

3. Why just $17,000?
That was just the ransom paid. Apart from the $17,000, you must also factor in the cost of spending 10 days without an IT system, the costs to reputation, and the possibility of lawsuits. The ransom is the smallest part of the damage here.

This, once again, proves that no company is too small to be hacked into. Companies must be on the defensive and never rest on their laurels. Just because you’ve never been hacked into is no guarantee that you will not be hacked into in the future.

Criminals see what happened at this hospital and are thinking that is a great way to make some money. Be safe and assume hacktivists are already looking at your IT and maybe even your SCADA systems. Ask yourself, will they be able to hack into your systems? While this hospital could afford the ransom, the true cost of the attack is much, much higher.

Cybersecurity

Tags

Cyber

Cybersecurity