RANSOMWARE IN HEALTH IT

Ransomware has become more prevalent in recent years. Hackers are able to breach security and access up-to-date patient information. Then, they deny the hospital access to the records until they are paid the money they are requesting..

Typically, ransomware infects victim machines in one of three ways::

- through phishing emails containing a malicious attachment
- via a user clicking on a malicious link
- by viewing an advertisement containing malware

Beware of the following cyberattack techniques:

Emails masquerading as government announcements

Fraudulent emails have included logos and other imagery associated with the Centers for Disease Control (CDC) and the World Health Organization (WHO). Emails include links to items of interest, such as "updated cases of the coronavirus near you." Landing pages for these false links may look legitimate, but the sites are often malicious and may be designed to steal email credentials.

Operational and industry disruption

The spread of COVID-19 is disrupting temporary supplies and revenue in some industries. Cybercriminals hope victims will mistake their malicious emails for legitimate ones. For example, emails with subject lines like “Coronavirus – Brief note for the shipping industry,” have been sent to employees of companies in industries being disrupted by the virus. Some campaigns have even been disguised to look like invoices, shipping receipts and job applications.

Hidden malware

There has been a rise in malicious emails directing recipients to educational and health-related websites riddled with malware.Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software.

Tips

- Be skeptical of emails from unknown senders or familiar people (like your company’s CEO or your doctor) who do not usually communicate directly with you.
- Don’t click on links or open attachments from those senders.
- Don’t forward suspicious emails to co-workers.
- Note grammatical errors in the text of the email; they’re usually a sure sign of fraud.
- Report suspicious emails to the IT or security department.