PALM Associates, Inc.

Software product development for communications.

White Paper

White Paper 21

WannaCry - a Wakeup Call for Health Informatics

Quick summary

WannaCry is Ransomware which enters a server through a variety of attack vectors including email [1]. Once it has access to critical files, a ransom ware attack will encrypt the files making them unusable until the attacker provides the key. Usually this is after paying the 'ransom'. The WannaCry attack evolved from NSA's EternalBlue which is an exploit specific to Microsoft servers [2]. The WannaCry exploit infected a range of Microsoft Windows systems, most significantly healthcare servers in the EU. Because of its specificity to Microsoft, any product based on other technologies or in an organization meticulous about keeping current on the patch level and using sound security practices avoided this attack. But this is no reason to relax [3].

Analysis

Ransomware attacks like WannaCry are becoming more frequent. At Stanford's Health Technology Forum PALM's presentation was met with audience requests for more direction on what to do about Ransomware. Several issues of note in the current attack:

i. The WannaCry, using the common name, was an exploit based on leaked details of an NSA developed offensive weapon called EternalBlue. EternalBlue was said to be used by NSA to take remote control of Microsoft servers using a vulnerability in these Windows servers and secretly known by NSA [3]. Note that this vulnerability has a patch that MS issued months before the attack and if a company kept the patch level current they were not subject to this attack. Keeping patches up to date is a HIPAA security requirement and is a practice with any good security discipline.

ii. A ransomware attack always starts with a breach, so if the system is secure the risk of the initial breach is lowered.

iii. Hackers can sell electronic Personal Health Information (ePHI) for 10x the price of credit card data making products in the healthcare market become high value targets [4].

iv. In the WannaCry attack there were no US medical institutes breached. The only large US Company mentioned as being affected was FedEx trucking. The HIPAA security requirements were a factor in saving the providers from attack.

Impact on health informatics products and lessons learned

1. Due to product development pressures, some healthcare software is vulnerable to common attacks because of the shortcuts which had to be taken to rapidly get a product into the market. Security becomes a problem after market introduction.
2. While a product that does not use Microsoft technology is not subject to this particular exploit, all healthcare products do store ePHI making the product a high value target. In addition many developments have a long list of common software coding problems that give them high vulnerability and risk.
3. Furthermore, many products use a variety of common tools such as WordPress, Linux, SQL Java, PHP, CentOS, etc. WordPress is the most frequently attacked framework in the web services market. Common products are also the subject of common attacks and the risk is high.

There are a number of exploits in these products that hackers can take advantage of and many are posted on Internet hacker sites.

4. Any breach will be expensive in reputation if not in currency. Prudence in engineering security measures and discipline in keeping security processes up-to-date are the best course with any system carrying personal and ePHI.

Recommendations

a) New developments need to consider security issues during the design phase. See PALM's discussion "Practical Guide for Protecting Health Data." Starting late is better than never. Repairing and hardening servers and applications is covered in PALM's Software Security Audit and Site Hardening service which offers HIPAA training, organization, risk management and process definition.
b) After acceptance testing, export the changes to all servers. PALM can help define and implement automation to accomplish this task.
c) Begin some of the planned security processes outlined in the master plan provided by PALM's HIPAA/NIST training regimen.

The goal is to reduce or minimize the risk but that risk cannot be entirely eliminated. Security can become a financial black hole, so a recommended approach is to decide on a security budget and achieve as much under this budget as possible. This includes putting into place good practices so the company is ready when a breach occurs. At a minimum, an incident response team is briefed and ready, patch levels are maintained and current, HIPAA/NIST guidelines followed and periodic security reviews held.

To avoid the danger of ransomware and other attacks, good practice is to back up all critical data in encrypted storage at a physically remote site which is part of best practice for most enterprises and required by HIPPA.

References

[1] Akamai, email warning, WannaCry Attack: Critical Insights and Actions for Akamai Customers, https://blogs.akamai.com/2017/05/wannacry-what-we-know.html

[2] "Microsoft SMBv1 Vulnerability", (2017, March 16). US-CERT.

[3] Https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#6b6dd4f9e599

[4] Http: //www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924