White Paper

Wanna Cry and its Meaning for Health Informatics

Quick summary

The EternalBlue exploit was specific to Microsoft servers so products based on other technologies have missed this attack, but this fact is not any reason to relax.[1] A fix was available in March for this vulnerability [2] The current exploit enters the network through a corrupt PDF file attached to an email. [3]

Analysis

Ransomware attacks like EternalBlue are becoming more frequent. PALM gave a talk at Stanford HTF (Health Technology Forum) and one of the significant and frequent requests from the audience was what to do about Ransomware. Several issues of note in the current attack:

i. A ransomware attack always starts with a breach, so if the system is secure the risk of the initial breach is lowered.
ii. Hackers can sell ePHI (electronic Personal Health Information) for 10x the price of credit card data. So products in the healthcare marked become high value targets [4].
iii. In this attack there were no US medical institutes breached. The HIPAA requirements were a factor in saving the providers from attack. The only US Company mentioned was FedEx trucking.
iv. This hacker attack was an exploit released by the NSA called EternalBlue (the common name is WannaCry). EternalBlue was used by NSA to take remote control of Microsoft servers and exploited vulnerability in the Windows servers. Note that this vulnerability has a patch that MS issued and if a company keeps their patch level current they are not subject to this attack. Keeping patches up to date is a HIPAA requirement and included in any good security discipline.

Impact on Health Informatics products and lessons learned

1. Due to product development pressures, some healthcare software is painfully 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. Part of PALMs support for these efforts includes a Software Security Audit and System Hardening service to help the development team catch up to current threats.
2. Any product that does not use Microsoft technology in the servers so the system is not subject to this particular exploit.
3. However, 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.
4. Furthermore, many products use many common products such as WordPress, Linux, SQL Java, PHP, CentOS, etc. WordPress is the most frequently attacked framework in the web services market. The common products are also the subject of common attacks, so the risk is high. There are a number of exploits in these products that hackers can take advantage of and many are posted on hacker sites like the Dark Web.
5. Any breach will be expensive in reputation if not in Euros. So prudence and discipline are the best course with any system carrying personal and ePHI.

Recommendations

a) New developments should consider security issues during the design phase – see PALM's discussion "Practical Guide for Protecting Health Data". Even starting late is better than never. See PALM's service for HIPAA training, organization, risk management and process definition. Repairing and hardening servers and applications is covered in PALM's Software Security Audit and Site Hardening service.
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.

As previously pointed out, the best that can be done is to reduce / minimize the risk but never eliminate the threat. A recommended approach is to decide on a security budget and get as much done under this budget as possible including putting into place good practice so the company is ready when the breach occurs.

To avoid the danger of ransomware attacks, another good practice is to back up all critical data in a physically remote site which is part of the most enterprise best practice and required by HIPPA.

References

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

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

[3] Akamai, email warning, WannaCry Attack: Critical Insights and Actions for Akamai Customers

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