RISK ASSESSMENT 2 Notes

Security Issues that may pose a threat:

Brief summary after reading several sources (PARAGRAPH LONG = Links to sources)

A Malware (Worm), recently has been poking its head out after a long hiatus. SQL Slammer worm attacks servers that have not yet been patched for the known vulnerabilities that have plagued MS SQL Servers for the past 14 years. Nov 28 – Dec 4, 2016 (1 week) there was a big noticeable surge in SQL Slammer attacks. The attacking IP's all originated from China, Vietnam, Mexico and Ukraine. They attacked 172 countries, where 26% of the attacks were targeted directly towards The United States. The Slammer Malware attacks a specific host from several places. Changing the listening port to UDP 1434. This very small file sits on the hard drive and jams the network by sending ridiculous amounts of infectious files that are infecting any and all networks it comes into contact with that have not yet patched the known vulnerabilities. The SQL Slammer Worm patch has been available from Microsoft since 2002, but SQL Server 2000 expired 2013. It is important to notice, that there are still many unpatched SQL Servers Systems connected to the net. These servers are still targets waiting for The SQL Slammer Malware to infect them, it's just a matter of time. These malware packets are so small, they can travel even on the poorest networks, even when other packets won't be able to travel in the same conditions. Since this is the only surge of this malware. Security company, CheckPoint reacted stating that they don't know if it will continue, so they didn't react at the threat at the time of the report to them.

Determine what the impacts of the issues will have on security

The SQL Slammer Malware, scans and propagates subnets so very fast, that it doesn't take very long to infect many new target hosts. Many devices we don't think about also have SQL Servers. Vending and cash machines use MS SQL Servers in order to track inventory. On its first run in 2003 in just 10 minutes, it set a record of infecting 10,000 servers and overloading 75,000 networks by drastically slowing down hosts internet traffic.

What does the story mean to us right now? Point out assets, applications, business process, etc that are implicated Describe the risk, the business impact. Be realistic and measured not every vulnerability possess an existential threat to the organization (paragraph long)

ASSETS

Our assets are our data, reputation and business in general. We need to protect it from any attack that may stop it from performing at its best capabilities.

APPLICATIONS

This application can debilitate the whole network the organization is on and destroy a lot if not most of the daily business transaction. It can eventually will spread the infection to all unpatched networks attempting to connect, download or access the organizations infected networks. By drastically slowing down or crashing networks near and far.

BUSINESS PROCESS

In order to save time from any security incidents that may affect your business, data and/or reputation. All patches and vulnerabilities need to be addressed immediately. Reassess the network with the data sensitivity and for awareness of what is on the network as well. Set controls for future happenings of the same sort. So we know what data types are valuable to us and need to be backed up and what types of data we could survive if damaged and lost. Among other controls that need to be layered and methodical at the same time. With the idea in mind if data or an event like this ever happens, what are our fail safe methods that will allow us to keep working without losing a beat.

DESCRIBE THE RISK / DESCRIBE THE BUSINESS IMPACT

The worm was first spotted in Jan 2003. It exploits the buffer overflow vulnerability in Microsoft SQL Server 2000 or MSDE 2000. SQL Slammer Worm infects the server using the UDP Port 1434 which carries out distributed denial of service attaches on the target IP addresses. These attacks consist of sending massive amounts of packets out at once jamming up the network to where it is moving very slow or crashes it. The packet itself is very small in size. May be half a paragraph in size. So it is very light and can be transmitted very easily over weak / slow networks. The packet sits on the hard drive, executing the code of jamming up the hosts network. This can stop all business and costs the organization loss of potential income gained as well as loss of business, data loss with possibility of losing reputation as well.

Outline the steps we should take in the short term. (Paragraph) What controls can we realistically put in place to reduce our risk today? {Paragraph)

In order to save time from any security incidents that may affect your business, data and/or reputation. Any organization running out-of-date systems, needs to expect huge risks of things going wrong with the known vulnerabilities. First thing first, we need to find out what exactly is stored on the networks we own. Then, find and fix any vulnerabilities by patching them. The next step we need to set up the controls for our networks by investing in and gaining as much expertise as possible with the systems at hand, such as using Vulnerabilities Management, Change Controls, Configurations Management, Asset Management, Patch Management. Avoiding using the tools and systems at hand will only cause you to get sooner or later. Whereas it is just cheaper to fix it now. By just getting as familiar as possible with the practices for upgrading to the newest Microsoft SQL Server.

Outline the long-term fix for the issue. What we need to plan for in the future to make sure we have an effective, sustainable, scalable control in place for this? In some cases, you may not need to, or be able to, implement a BIG FIX. The short term mitigation might be your permanent fix. That's OK, as long as you can support that assessment.

Dig Deeper on Security patch management and Windows Patch Tuesday news

- **Microsoft delays Windows zero-day patch; researcher drops exploit code**
-
- **More than 200 vulnerabilities found in Trend Micro security products**
-
- **January Patch Tuesday sparse before Windows security updates change**
-
- **SSL certificate validation flaw discovered in Kaspersky AV software**