Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 12, December - 2017

Cyber Security Guidelines for Healthcare Providers Threats and Defense from Ransomware

Devesh Mishra
Technologist
Graduate Student at Columbia University,
New York, United States

This paper will evaluate the threat vector, risks assessment and remediation plan during a specific situation for the Healthcare industry. The scope of this paper will address the Ransomware-"WannaCry" event from the National Health Service (NHS), UK perspective and reflects on our sense and ability to response in that situations

Keywords— NHS

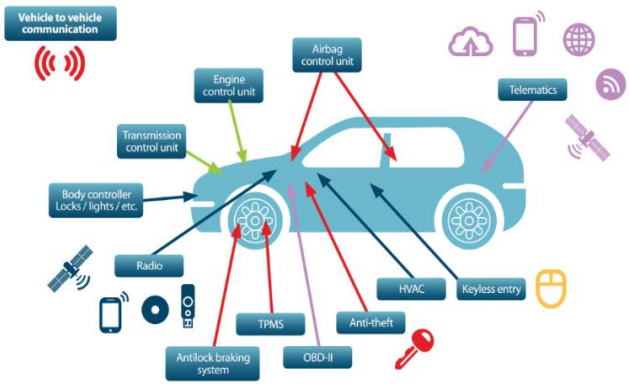
I. INTRODUCTION

Change is inevitable in every industry. But in healthcare, the pace of change is driven by regulatory flux, changing political landscape and the constant evolution of technology. Today's healthcare organizations face an unprecedented array of new challenges in the form of the Ransomware. Although ransomware attacks have recently become common, the first ransomware was developed by Dr. Joseph Popp, a biologist from Harvard, in 1989. Ransomware is a type of malware that prevents the organization from accessing certain of complete parts of the system. For example, a department (Emergency) with in the hospital could be locked during the critical stage of the critical system like Electronic health record (EHR). In the situations users won't get into the system unless they pay ransom. Attacking hospital IT and steal patient information is just the tip of the iceberg when it comes to cyber threats but hacks of implanted devices are an even more sobering threat. The scale of the problem in not limited to steal the computer data and sell on the black market but the healthcare hardware's- Like MRI machine, ventilators, endoscopes and other critical operating devices are nothing but the computers. These computers come with hardware and software that the vendors are responsible for supporting. These machines require significant investment for the providers and lot of cases these devices are still operating on extended support or Out of date support. That means the old devices can easily become the target of hackers.

The unprecedented attacks on "NHS", using software called WannaCry, exploits a vulnerability in windows. According to "Digital Guardian "WannaCry is a ransomware variant that propagates themselves without relying on traditional malware attack vectors like phishing emails or drive-by downloads. WannaCry self-propagates by exploiting a critical severity non-zero-day vulnerability in various Microsoft operating systems known as MS17-010 (CVE-2017-0144), which enables remote code execution against Microsoft Server Message Block 1.0 (SMBv1). Once it infects a machine, WannaCry behaves like a worm, scanning networks for vulnerable systems with port 445 open to further spread.

II. ATTACK SURFACE AND STEPS TO MINIMIZE THE ATTACK SURFACE

Perhaps the reason for "NHS" attack was using an obsolete version of Windows (XP, 2003) for which Microsoft had stopped providing security updates in April 2014. Data acquired by software firm Citrix under freedom of information laws suggested 90% of trusts were using Windows XP, then a 15-year-old system. Attack surface is one of the important aspects of "Defense in depth" for example, the diagram below outlines a connected vehicle surface. It is through these vectors that hackers would attempt to send malware to a connected vehicle. If they able to bypass the key security system it may potentially be able to effect vehicle critical safety functions. These attacks are in the form of an external facing web application, interfaces, SQL injection, EDI etc.



III. STEPS TO MINIMIZE THE ATTACK SURFACE

The most common attack vector by ransomware attackers is through malicious email attachments or phishing (URL). In this case, First, and foremost thing to do, raise awareness among your employees, clients, business partner about the significance of maintaining cyber hygiene.

(Propagation of Ransomware)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 12, December - 2017

When an incident like Ransomware happens, we should switch to "Basic" and see where we lack and look for an opportunity for improvements. Here are a couple of things we could try and go from there. We need to create a compelling structure called "Defense in depth" to minimize the attack surface if following areas.

- Network Attack surface- Attack will often by Network
- Software Attack Surface- Attack will happen in the form of web applications
- Human attack surface- Insider, Partner, phishing email etc.

In addition to this, follow the followings.

- Threat Assessment- Conduct a comprehensive threat assessment and develop a risk management strategy to identify, report, and mitigate threat
- Deploy Intrusion detection and prevention for all mission critical system
- Crafting an encryption and account management policy
- A layer of Defense (Playbook) - Creating the layer of defense at every layer (Database, application, network, security,) across the enterprise to minimize the risks
- Patch all software, particularly any systems containing the MS17-010 vulnerability – Microsoft has released a patch for vulnerable legacy systems including Windows XP and Windows 2003
- Disable SMBv1
- Back up mission critical data to a secure location
- Audit (Internal/External) - Internal and external audit should be in place to detect any access related issues (VPN, Application, AD, Network, Server,). In addition to this, TechSpectrum should include the appropriate process in place while dealing with any forensic Investigation
- Establish Relationships with Regulators, Law Enforcement, and other relevant vendors: It is often forgotten that consumers, business, Law enforcement and regulators all have a common goal in prevention data breached and mitigated the risks.

A. Elements of Analysis

In the case of incident or event detail analysis of detection, prevention, and logging technology at multiple layers is required so that we don't miss the important link of the chain. This approach creates additional redundancy in security monitoring operations so that complete visibility is not lost. In order to investigate any security incident we need evidence, which can be identified and collected from different sources in the form of alerts, logs, information available in public domains.

Event and Log Management:

In the case of "Ransomware" event and to playbook effectively we need to have all security logs and events into a searchable nexus of data and metadata.

Logs from operating systems, services, database and applications (particularly audit-related data) are frequently of great value when an incident occurs, such as recording which accounts were accessed and what actions were performed. Logs can be used for analysis by correlating event information. Depending on the event information, an alert can be generated to indicate an incident.

Alerts generated from IDPS, Antivirus software, Third party monitoring service and file integrity software etc. provides sets of valuable information. In addition to this, Security Information and management system (SIEM) can be used for this purpose. SIEM can provide a relevant set of information and help prioritize area to focus depends on what we are trying to protect as long as the meaningful set of the data is regularly fed to the tool. A log management system can store the large set of data but variety and quality of data is important for the meaningful insights

Vulnerability Management:

Most of the recent ransomware attack happened because of a unpatched version of software's, so from the enterprise perspective it is essential to have patching plan in place (Software, desktop, printer etc.). For example- Wannacry virus is one of the examples of Operating system patching. In 2016, "Unpatched JBoss servers can become infected with Samas by exploiting the vulnerabilities addressed in CVE-2010-0738, CVE-2010-1428, and CVE-2012-0874 which was made public between 26th April, 2010, and 21st January, 2013"

Access Control:

Actively updating user accounts to ensure that employees never have more access to a sensitive computer system that is not necessary. For example- if the employees had access to certain systems and didn't access the system in last 90 days, access will be terminated by default. In addition to this, Audit the vendor account regularly to make sure they are in compliance.

Profiling Network and policy:

Profiling is a way to address the behaviors of the system. Based on the nature of the behaviors you can identify what is right and what is not right in the system. For example, running the integrity check to derive the checksums for critical files and monitoring network bandwidth usage to determine what the average and peak usage levels are on various days and times. Organizations should use profiling as one of several detection and analysis techniques.

Log Retention Policy:-

An average time to find out about incidents is greater than 235 days so technically incidents may not be discovered until days, weeks, or even months later know about the incidents so, it is important to have a log retention policy in place that specifies how long log data should be maintained because older log entries may show reconnaissance activity or previous instances of similar attacks.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 6 Issue 12, December - 2017

Culture and Behavior (Awareness Program):-
Organization culture and behavior is non-technical but powerful aspects of analysis. Human error, including failing for phishing attacks, is the leading cause of major cyber-attack today. Healthcare system should regularly remind people of the importance of information security best practices through required training and other activities.

Filter the data:
It is impossible for the enterprise to review each and every category of events and logs. But filter the unwanted category of data (for example-email filter) which is not relevant to the enterprise. That way security professional can focus on the categories which are of greater potentials. Business email compromise with the help of "spear phishing" can be avoided up to a certain extent with the help of this approach.

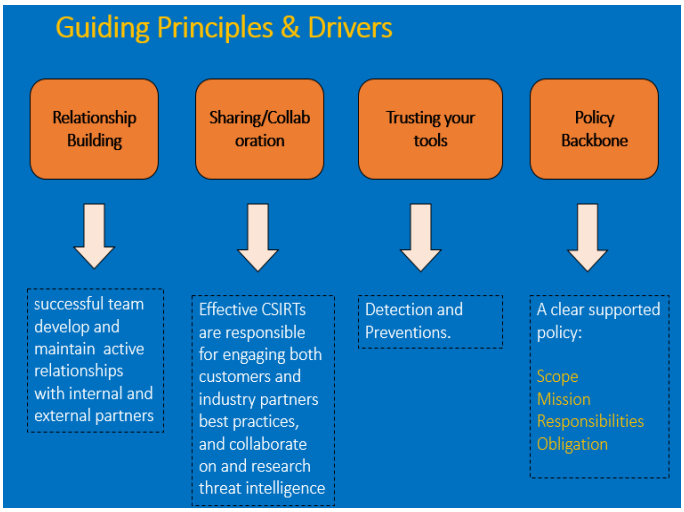
B. Units

According to Digital Guardian Incident response is a term used to describe the process by which an organization handles a cyberattack, including the way the organization attempts to manage the consequences of the attack or breach (the "incident"). Ultimately, the goal is to effectively manage the incident so that the damage is limited and both recovery time and costs, as well as collateral damage such as brand reputation, are kept at a minimum.

The CIRT normally operates in conjunction with other enterprise groups, such as site security, public-relations and disaster recovery teams. According to Bollinger-An Incident response team cannot exist in a vacuum. Just like a firefighter doesn't rebuild a burned-out house or calculate the possible insurance payout. CIRT demands effective collaboration and support across other groups

SANS institute provide six key steps for effective incident response

- Preparation – Preparation is the key, we can't wait for incident to happen
- Identification- Identification is a process through which incidents are detected
- Containment- The purpose of the containment is to prevent the further damage
- Eradication – Response to the incident
- Recovery- Testing, monitory and validating systems while putting them back to production.



Involvements of following team players are required as part of effective CIRT team

CISO: - Chief Information Security Officer (CISO) is responsible for the overall safety of the organization. This role requires mix skills of transformational and transaction leadership. Successful leaders should be able to articulate around "People", "Process" and "Technology" and lead from the front while dealing with crisis situations.

IT, networking services, Application and database teams

Information Technology is the most significant factor of a CIRT success. In order to respond during the case of event or non-event, you need to understand the different layer of IT (Network, Architecture, Database, Application etc.). IT is usually responsible for day-to-day operations for example-Network team is responsible for securing the DNS management, Directory administrators, Load balancer etc. Earning the trust of IT team enable a better response to incidents and mitigations.

Identify and Acquire Necessary Resources -The Success of CIRTs depends on allocation and availability of right resources in functional and technical areas. CIRT process must be validated, to ensure all participants understand the roles and responsibilities. This validation may be performed as a tabletop exercise, regular business continues testing, regular cyber exercise etc.

REFERENCES

[1] https://argus-sec.com/attack-surface/
[2] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
[3] https://hbr.org/2017/06/11-things-the-health-care-sector-must-do-to-improve-cybersecurity
[4] https://www.gartner.com/document/1893114?ref=solrAll&refval=186486734&qid=0626320862c86613c5002fdd1e173c67
[5] http://www.nbcnews.com/news/world/why-wannacry-malware-caused-chaos-national-health-service-u-k-n760126
[6] https://digitalguardian.com/wannacry-ransomware-protection