International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 04, April-2018

Knock on the Door
(An Analysis of Cyber Events & Forensic Investigation)

Devesh Mishra
Technologist
Columbia University, New York, USA

***Abstract* - The Present Paper Presents An Analysis Of The Key Elements Of Forensic Investigation In The Case Of Cyber Events. It Investigates The Key Elements Of Investigations And Further Insures An Appropriate Course Of Action Is Defined And Executed.**

Keywords: Cyber security, Forensic Investigation

INTRODUCTION : WHAT IS A FORENSIC INVESTIGATION?

According to Digital Guardian, most of the biggest data breach occurred between 2005 or beyond. One of the reason could be an explosion of data in the form of volume, velocity, and variety. Product companies or Customers were not able to articulate the values, and we continue to lack security which is now becoming the nightmare for Enterprise. While performing forensics, the cyber specialist must remember the basics of any type of investigative forensics work. Planning, Documentation, chain of custody and the rules of evidence still apply and followed.

HOW MIGHT HACKERS MAY GAIN ACCESS TO SENSITIVE INFORMATION? WHAT ARE THE VIABLE SCENARIOS?

Hackers could have gained advanced access in multiple ways.

- Data Breach: - Data breach is growing at an unprecedented rate than ever before. Quarterly results are sensitive information for the institutions because it could potentially influence the shareholders to the organization. In this particular case, Possibility of "Personal E-mail Account" can't be ruled out. We need to identify how the key players (Finance, Sales, Marketing, IT executive teams) are accessing the Mission Critical application or system? What (or How) level of authentication has been granted to them? For example-One of the recent breach when Colin Powell's emails were compromised and posted on public domain (DClinks.com) for everyone to read. One of them had a Salesforce's acquisitions strategy. Colin Powell, a member of Salesforce Board, has access, through his personal email account, to sensitive information.

- Spear Phishing: - Spear Phishing is the common way to steal basic information. Usage of mobile devices continues to grow among industry, and it is easy to target mobile devices.

- Vendor or Partner account compromised: - Financials system are one of the key regimes of the In this case, the possibility of vendor account compromised cannot be ruled out. For example- Integration layers between suppliers and Institutions and the possibility of compromised during the stage, vendors are deeply engaged while processing their PO or Invoice through the financial system and they have connectivity between systems.

- Changing Behavior or Users Training- One of the greatest obstacle all organization face when it comes to thwarting spear phishing is changing user behaviors. For example- What level of information is shared on social networks, public domain and further click on malicious links?

- Internal breach- Possibility of an internal tip off can't be ruled out either by recording data with the smartphone during the sensitive For example- Recently, Government of India has completely banned the use of a cell phone during the high-level meeting. This step was taken after the breach of financial information.

- APT- Bad players might be targeting the specific group of players to gain financials advantage, Embarrass Institutions and damage its reputation.

In addition to this, hardware compromised, APT, lack of security governance and compliance process cannot be ruled out.

Possibilities of Cyber Events and why?

Combination of social, email account compromised and data breach (obtained from the Public or private domain) could have been the reason for this events.

Why?

Reputation cost: Bringing down the reputation in front of customers, shareholders are the biggest lost for any enterprise. Hackers target the financial system to defraud institutions and their clients and to further illegal activities.

Financial gains: - Financials gain from the "Market Share" perspective- Buying or selling the share based on the "Quarterly"

HOW WILL YOU RESPOND TO THE SUBPOENA?

Transparency is the key to communication. While responding, Institution should provide complete and accurate information, including relevant facts, a chain of events and information about the cyber events. For example

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 04, April-2018

- Description and magnitude of the event
- Details as requested (People, Process and Technology Incidents)
- Reporting cyber incidents or events through Suspicious Activity Reports(SARs)
- Known or suspected time, location, and characteristics or signatures of the event
- Indicators of compromise
- Relevant IP addresses and their timestamps, virtual wallets, logs, etc.
- Device identifiers
- Security Methodologies or Governance used
- Other information the Institutions believes is relevant

In addition to this, from the legal perspective, we need to bring Legal and compliance team on board before we respond.

WHAT BUSINESS INJURY CAN ARISE FROM SUCH INCIDENTS?

Reputation cost is the biggest cost for the Institutions in the case of such incidents. In addition to this, financial loss, loss of customer and shareholders confidence may not be easy to get around for the "Institutions" especially when you are trying to expand or seeking partnerships (M&A case), IP's, etc.

WHAT ACTIONS IN ADVANCE MIGHT PROTECT INSTITUITIONS FROM SUCH INJURIES, OR AT LEAST MINIMIZE EXPOSURE?

"Prevention is always better than cure". When an incident like this 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.

Threat Assessment- Conduct a comprehensive threat assessment and develop a risk management strategy to identify, report, and mitigate cyber-events and cyber enable crime.

A layer of Defense (Playbook) - Creating the layer of defense at every layer (Database, application, network, security,) across the enterprise to minimize the risks. Create a dynamic playbook and keep it relevant.

Unstructured data: - Enterprises are securing the sensitive data, most of them are in a structured format and creating layers around it but unstructured data is the new attack vector for hackers. As the level of unstructured data on the rise for the various use case and it is opening the new gateway for hackers. Use of unstructured information in the social media

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, Institutions should include the appropriate process in place while dealing with any forensic Investigation

- Documenting system data and time
- Key word search in log files.
- Evaluation file slack and unused or unallocated space
- Validate Anomalies
- Categorize the level of threats
- 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.

"IT Business Edge provides a slideshow illustrating 8 Ways to Prevent Data Breaches (Links to an external site.)Links to an external site, including tips such as instituting end user security awareness, performing regular vulnerability assessments, and other helpful tactics."

-WHAT KIND OF LEADERSHIP STYLE DO YOU NEED TO USE TO DEAL WITH THIS SITUATION, AND WHY? ALSO, THIS CASE IS THE LONGEST (TWICE AS LONG AS THE OTHERS) … HOW DOES THIS AFFECT THE LEADERSHIP STYLE YOU NEED TO EMPLOY IN THE WORKSHOP?

This case requires special attention because Institutions is engaged in multi front war (Security to Internal Stakeholders/consumers, Defending current state, responding to Law enforcements in the form of a subpoena and further Prepare for future)

Cyber Risks are dynamic in nature and dynamic mindset is essential while dealing with such situations. We certainly can't wait until something to happen but solid preparation (Known or Unknown enemy) will help us to improve our security layers and minimize the damage in case of any adventures.

In this situation" Leadership of something who understand the difference between "Glaciers" and "Rivers"- In other words, a person should know "How to defend" but finding the way to get things done will be quite essentials. In addition to this, Leaders should have "Maverick" style in certain situations.

- Response
- Intelligence
- Operations
- Visibility
- Implementation and execution skills

Responding in such situations will not only require a high level of understanding from social, political, economic and technology landscape but Mix of "Transformative and Transactional leadership" skill will be necessary. It is important for the leaders to secure today but setting up the cornerstone for tomorrow is essential.

Successful leaders should be able to articulate around "People", "Process" and "Technology" and lead from the front while dealing with crisis situations.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 7 Issue 04, April-2018

CITATIONS

[1] http://www.connellfoley.com/assets/htmldocuments/HOW%20TO%20RESPOND%20TO%20CYBERSMEAR_0.pdf (Links to an external site.)Links to an external site.

[2] https://digitalguardian.com/blog/history-data-breaches (Links to an external site.) Links to an external site.

[3] https://www.forbes.com/sites/forbestechcouncil/2017/06/05/the-big-unstructured-data-problem/#27460ab5493a (Links to an external site.)Links to an external site.

[4] https://www.secureworks.com/blog/advanced-persistent-threats-apt-a (Links to an external site.)Links to an external site.

[5] https://blog.datalossdb.org/ (Links to an external site.)Links to an external site.

[6] https://www.sans.org/reading-room/whitepapers/incident/developing-computer-forensics-team-628 (Links to an external site.)Links to an external site.

[7] Cyber Security Guidelines for Healthcare Providers Threats and Defense from Ransomware "http://dx.doi.org/10.17577/IJERTV6IS120005

[8] http://www.heritage.org/node/14814/print-display (Links to an external site.)Links to an external site.

[9] https://www.itbusinessedge.com/slideshows/show.aspx?c=79585