2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

Well, It's Too Late Now: Being Properly Prepared for a Data Breach

I. Properly Preparing for a Breach Event

Preparing for a data breach can be a daunting task. Many organizations today do not have an accurate picture of all of their computer systems, the types of data that may be stored on them, or how they are all networked together. Organizations today must be willing to invest the time and resources required to be properly prepared when a data breach event takes place, because in today's world, it really is "when" and not "if". This panel discussion will examine how an organization can properly prepare for a breach event so it can be dealt with efficiently.

Data breaches are very often disaster-level events. While many businesses adequately plan for fires or natural disasters, data breach planning is often overlooked. We will present two case studies to illustrate how preparation, or the lack of it, can affect outcomes. These case studies will first examine an organization that was not properly prepared for a breach event and what happened as a result when they suffered an actual breach, and then, the very different results had by another organization that did have an effective recovery plan in place.

Inventory

Organizations of any size can benefit from creating and maintaining accurate inventories of digital assets. This would include an accounting of all servers, desktop workstation, laptops, printers, routers, and any other devices that are connected to the network. These inventories can be incorporated into a disaster recovery plan and can be utilized when responding to a breach event in order to determine where an organization's most important assets are.

As you will see in the case studies that we will be examining, an accurate accounting of digital assets can help an organization that suffers a breach related event to not only provide an efficient response, but also allows for a proper forensic investigation to determine exactly what happened. At the end of the day, this will help the organization return to a pre-loss condition more efficiently.

Accounting of Digital Assets - Location

Organizations with multiple locations should have an accurate accounting of inventory at each location. These inventories should be revised on a regular basis to ensure that they are accurate. In addition to listing physical locations, inventories should also include identifiers such as the make & model, form factor (e.g. desktop, laptop, tablet, etc.), operating system & version number, machine name, and network (IP) addresses. These details are almost always needed by responders and forensic investigators. Having this information immediately available, rather than having to collect it after a breach occurs, can speed up both remediation and forensic preservation and analyses.

Accounting of Digital Assets - Function

The inventory should also include the function of each system that has been identified. This is especially critical for systems that contain key data types that will be discussed shortly. Having this information on hand allows for more rapid triage and the identification of the systems most critical in both the initial response and subsequent forensic investigations. Specifically in the case of forensic investigations, clearly identifying these roles and functions beforehand can make the difference between needing to preserve and examine just a few key systems or requiring that a much larger number, possibly all of them, would need to be collected and analyzed.

Accounting of Digital Assets – Virtualization

Virtualization is a technology that allows for the running of an operating system (virtual machines) in a virtual environment. This technology allows a single host to run multiple instances of an operating system on a computer system simultaneously.

VM's have the added flexibility of creating periodic snapshots of an operating system's current state. Many organizations will typically generate these snapshots on a regular basis. If a breach event takes place, the current status of the virtual machine can easily be exported to a file for preservation and a previously captured clean snapshot can be reverted to, allowing for an organization to quickly return to a pre-loss condition without losing important evidence needed for forensic analysis.

As in previous examples, accurate inventories should be maintained for all VMs in an organization's environment to aid in the process of incident response.

Accounting of Digital Assets - Remote Access Considerations

Many organizations implement remote access solutions for employees without considering the risks of doing so. Remote Desktop Protocol (RDP) is a Microsoft solution that allows for remote connections to systems where it is enabled. The inherent issue with RDP is that it only requires a username and a password to connect. Bad actors will frequently launch automated, brute-force attacks against exposed RDP servers or will use lists of known breached accounts to connect remotely to them.

Multifactor authentication requires an extra credential to be utilized in order to login to an RDP server remotely. This unique, single-use credential is typically generated at regular intervals by a key fob device or by a smart phone application and is normally accessible to only

the authorized user. With this methodology, even if an attacker knows the credentials for a user, they still cannot connect to the RDP server without the extra authentication.

As you will see in the case studies we will be examining, multifactor authentication can prevent many common breaches that we see on a regular basis.

Accounting of Stored Data – Types of Data

It is crucial for inventories to detail what type of data is stored on each system that an organization utilizes. This data can be utilized in conjunction with disaster recovery plans to properly target and scope systems for forensic analysis after a breach event. Types of data that should be highlighted include business critical data, personally identifiable information (PII), protected health information (PHI), and financial data.

Accounting of Stored Data – Encryption Considerations

Where possible, it is preferable to properly encrypt data at rest on all systems utilized by an organization. This would include business critical data, PII, PHI, and financial data. If a breach takes place where this type of data is properly encrypted at rest, the risk of bad actors decrypting and utilizing this data is greatly reduced. It is worth mentioning that common encryption schemes such as those employed by Microsoft Office products can be easily broken and should not be considered as a method of properly securing data.

Backup Plans – Online vs. Offline Backups

Most small to mid-size organizations will typically use an online backup solution. This solution utilizes a hard drive or series of hard drives mapped as a drive letter that is used to backup data. The problem with this type of solution is that it is always accessible which might actually seem like a good thing. However, in cases like this, when an organization suffers a ransomware event, because the backup device is always available as a mapped drive, this backed-up data will also typically be encrypted.

An offline backup solution can help to alleviate this issue. An offline backup solution also utilizes a hard drive or series of drives to perform backups; however, as its name implies, once the backup process has completed, the backed up data is taken offline and does not remain readily accessible. As such, if a network is infected with ransomware while the backup solution is offline, the data stored there cannot be encrypted, and the organization can return to a pre-loss condition in a much more efficient manner.

Ancillary Steps – Monitoring

In addition to the previously discussed activities, organizations should also implement logging and monitoring of all traffic entering and leaving the network. This can typically be achieved with a mid to high end router at the edge of the network. This logging can be crucial in an investigation to determine what may have taken place during a breach event and exactly when.

A good example of this would be for an investigation involving Emotet malware. Emotet is a highly advanced piece of malware whose original purpose was to capture banking credentials on infected systems. Emotet has evolved over the years with a modular framework that can

download and launch a variety of modules include password stealers, data stealers, and network sniffers. Emotet is also polymorphic, which means it is constantly updating and changing its code in order to evade detection. To make things even more challenging, Emotet leaves no artifacts on a system that can be examined to determine what the malware may have done.

Edge monitoring and logging could be extremely valuable in a situation like this to determine if a large amount of data may have been exfiltrated. This logging could also be utilized to determine that while Emotet was indeed installed on a system, it was not communicating outbound to the Internet.

Ancillary Steps – Incident Response Plans

Incident response plans are also crucial for organizations of any size. These plans tie all the data from the inventories together and also dictate how incidents should be responded to. One highlight of an incident response plan is to ensure preservation of data on any breached systems in order to facilitate a proper forensic investigation. Having such a plan in place at the time of an incident, rather than just improvising, helps everyone to know their roles and ensures that critically important actions are not forgotten or overlooked. Ultimately, having a well thought out plan can also help reduce the time and costs associated with the initial response, the full remediation process, and forensic investigations.

II. Case Study – An Unprepared Organization: Jon Doe CPA

Background

Jon Doe CPA is a small firm with three full-time employees located in Orange County, CA. Jon handles tax preparation for approximately 165 clients and also provides book-keeping services for 34 clients. As this is a small firm, Jon does not have in-house Information Technology (IT) support and instead pays a local IT support specialist, Joe Smith, on an as-needed basis. As Jon Doe CPA is a small firm, Joe sees no need for a detailed inventory of assets, stored data, or a disaster recovery plan.

Jon and his staff often work long hours during tax season and in order to have the ability to work from home, he asked Joe to enable RDP on the server. Joe knows that RDP can have security issues so decides to run it on a non-standard port.

As tax season opens and Jon starts to submit client tax documents, he starts receiving rejection notices indicating that the taxes have already been filed for a large number of clients. Suspecting that his computers may have been breached, Jon calls Joe who comes on site to take a look at the server. Jon also informs his insurance carrier of the issue.

Responding to the Breach

Jon is contacted by a breach coach assigned by the insurance carrier. The breach coach schedules a call with Jon, Joe, and a forensics firm, Acme Investigations, to discuss the incident.

Meanwhile Joe starts taking a look at the server and determines that there were several unauthorized RDP logins over the course of several weeks prior to the tax filing rejections. These logins utilized an account for a temporary employee Jon had hired the previous summer. When the temporary employee's duties were completed, her account was never deactivated. Joe

deletes the user profile for the temporary worker and runs multiple antivirus scans against the server. He tells Jon that RDP should be disabled until a multi-factor authentication solution can be implemented.

The Breach Investigation

The breach coach and Jon get on the phone with Acme Investigations to discuss the incident. Jon provides an overview of the rejected tax returns and Joe mentions that he did see unauthorized RDP access to the server and that he disabled RDP. He does not mention that he deleted the user profile for the temporary worker that had been breached. Joe states that all critical data is stored on the server only. As such, the server is scoped for a forensic analysis.

Acme Investigations obtains a remote image of the server and begins their analysis. It is quickly determined that there was indeed unauthorized RDP access using the temporary employees account Acme also determines that not only is the profile deleted for the breached account, but the bad actor also traversed to another desktop located in Jon's office.

Acme gets on the phone with Jon, the breach coach, and Joe. At this time Joe mentions that he did indeed delete the breached user profile as he was worried it may contain malware and he wanted to get Jon back up and running as soon as possible. When queried about the desktop workstation that the bad actor traversed to, Jon states he forgot to mention that it is an old desktop that is used infrequently and that it contains personal and financial data for approximately 60 old clients.

This additional system is added to the scope of the investigation and a forensic image is obtained remotely which is then shipped to Acme for analysis. It is determined that the bad actor created an archive of all the old client data that was stored on the system and uploaded it to a server offsite.

As the breached user profile was deleted from the server, Acme was unable to determine what exactly happened with regards to the data stored there.

Returning the Insured to a Pre-Loss Condition

Due to the fact that Joe was over-aggressive with his response to Jon's incident, Acme was unable to conduct a proper forensic analysis of the server. As such, it was deemed necessary to notify Jon's entire client base of the breach. As no detailed system inventory was in place, Jon and Joe had forgotten to mention the desktop with old client data which delayed the investigation. Jon was also required to provide notification to all of his old clients about the breach.

Lesson Learned

- Had Joe not deleted the breached profile on the server, a full forensic investigation could have been conducted. This investigation may have been able to show that the data for only a small subset of Jon's client base had been viewed or exfiltrated from the server which would have required a smaller list of notifications.
- If Jon and Joe had an accurate accounting of digital assets, the desktop containing old client data would have been added to the original scope which would have resulted in a more efficient investigation.

III. Case Study - A Properly Prepared Organization: Jane Doe CPA

Background

Jane Doe CPA is a medium sized firm with five employees and approximately 620 clients. Jane has a full-time employee that handles IT for the firm, Steve Johnson. Steve maintains an accurate inventory of all systems, stored data, and remote access policies. Steve also has each workstation set up so that no client data may be stored locally and must be stored on the server. Steve has also taken the time to design an incident response plan.

As tax season opens and Jane starts to submit tax returns, she immediately receives rejections for nine clients. At this time, Jane informs Steve of what has taken place and contacts her insurance carrier.

Responding to the Breach

Using the incident response plan he designed, Steve immediately determined that RDP was breached on the office server one week prior to the first rejection. Steve disabled RDP to prevent any further unauthorized access and had all staff change their passwords.

Jane is contacted by a breach coach assigned by the insurance carrier. The breach coach schedules a call with Jane, Steve, and a forensics firm, Acme Investigations, to discuss the incident.

The Breach Investigation

Jane provides an overview of the rejected tax returns and Steve mentions that he did see unauthorized RDP access to the server and that he disabled RDP. He states that Jane's account was breached and that beyond running antivirus scans and disabling RDP, no other remediation has been performed. Steve also states that no client data is stored on local desktops and that RDP was only available on the server located at the office. As such, only the server was scoped for forensic analysis.

Acme Investigations obtains a remote image of the server and begins their analysis. It is quickly validated that there was indeed unauthorized RDP access using Jane's account. Because Steve did not delete any data that would be relevant for a forensic investigation, Acme was able to determine that bad actors had logged into the server remotely a total of five times in the week prior to the first rejected tax return. During these connections the bad actors spent four days using the system to make several purchases from Amazon utilizing stolen credit card data. This credit card data was not related to information stored on Jane Doe's systems, but is typical of the kind of additional illicit activities often found to have occurred on compromised computer systems. There was also a large amount of traffic to various online dating sites, which again, is not unusual to be found in these incidents.

On the final day that the bad actors connected to the server, they gathered data for a total of ten Jane Doe clients and stored it in a zip archive file. Steve's conservative approach to his response preserved a number of forensic artifacts which allowed Acme to determine that the zip file had been exfiltrated, or uploaded, from the server by the bad actor.

Returning the Insured to a Pre-Loss Condition

Due to the fact that Steve was properly prepared for a breach event, the investigation was able to ascertain that data for only ten clients was accessed, greatly reducing the notification requirement that otherwise would have been required.

Lessons Learned

- Steve took the time to create system and data inventories as well to implement an incident response plan. Steve utilized this information to provide an efficient response to the breach while preserving critical data that would be required for an accurate forensic investigation.
- Due to Steve's preparation, only ten of Jane's clients were required to be notified.