CLEARNETWORK
YOUR CYBERSECURITY EXPERTS

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Healthcare

For matters of confidentiality, the identities in this case study have been obfuscated.

Staff
200

Patients
100/day

Locations
1 main - 3 satellite

Company Background:

A mid-sized healthcare organization within the United States that treats an average of 100 patients per day. The organization consists of approximately 200 staff members, including physicians, nurses, and support personnel. The organization is part of a large healthcare network in the Southwestern United States. The organization has 1 main facility and 3 satellite locations in rural areas.

Technology Background:

The company's digital infrastructure has recently undergone a cloud transition and now supports a Hybrid-Infrastructure. Approximately 75% of the organization's servers reside in a cloud environment. The remaining onsite assets are comprised of workstations, laptops, networking devices, and minimal legacy servers.

Domain: Microsoft Active Directory (Hybrid Cloud/On-Premise)
- **Email:** Microsoft Office 365
- **Remote:** Site-to-Site VPN & Remote Cloud Console Access
- **Firewall:** Fortinet
- **Virtualization:** Hyper-V
- **Servers:** Microsoft Windows Server 2016, 2012R2, 2008R2, 2003
- **Workstations:** Microsoft Windows 7 & 10 & Apple MacOS
- **Security:** Webroot Antivirus
- **SIEM:** None

The organization's information technology architecture was primarily based within a cloud environment. 25+ virtualized servers controlled most technical requirements, such as Active Directory, file sharing, DNS, DHCP, and more. Additionally, the new Electronic Medical Record (EMR) server was recently stood up within the cloud environment. The IT staff retained credentials to the cloud environment for server and database management. However, employees at the local site(s) level leveraged end-devices to conduct day-to-day operations. Workstations and laptops could be used on-premise and connected to the cloud environment for synchronization.

Four months prior to this cloud shift, the organization had leveraged a 100% on-premise environment. During the transition, 75% of the assets were moved to the new cloud environment. However, some critical systems remained within the confines of the physical locations. The systems that were kept on-premise included the archived EMR system and 2 critical file servers. However, during the migration, an IT administrator created a remote desktop server for easy file transfers from the on-premise environment to the cloud servers.

The Breach:

On the evening of May 21st, 2018, a phone call was placed to the healthcare organization's after-hours help desk support team. The call had been placed from a physician's assistant at one of the satellite locations. The employee had stated that one of the exam room PC's hosted a bright orange screen color with a message that read "Your files have been encrypted with ransomware. If you wish to unlock your files, contact the email address below". In this case, no price had been named in the ransomware attack.

- **10:10 p.m.:** 2nd call to IT Help Desk Support. This call came from a nursing manager at the main location and it became apparent that multiple workstations and laptops were experiencing the same symptoms as the satellite location.
- **10:30 p.m.:** The IT support team has assembled via a conference bridge and has begun to examine the incident. A call was placed to a 3rd party incident response organization to support the efforts.
- **11:00 p.m.:** After a brief review of the incident, the decision was made to begin investigating the data backup servers, cloud environment, and any remaining on-premise servers and workstations.
- **1:00 a.m.:** The 3rd party incident response team has engaged with the IT support managers and administrators. Upon reviewing the ransomware strain, it was decided that no decryption key currently existed for the variant. Therefore, options have been limited to restoring from backups or paying the ransom.
- **1:15 a.m.:** Upon reviewing the data backups, it was discovered that all recent data backups had been maliciously purged. Additionally, the file servers have all been encrypted as well. The cloud environment did not show symptoms of compromise.
- **1:35 a.m.:** The incident response team had also discovered that a remote desktop server was exposed to the internet over port 3389. The IT Director had no knowledge of this open route and queried the IT staff for knowledge of this gap. A junior systems administrator had recalled opening the system for transferring data to the new cloud environment and did not close the route after the migration.

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Manufacturing Industry

- **2:35 a.m.:** At the discretion of the healthcare organization, the decision was made to contact the attacker(s). An email was sent to the email address provided in the ransom screen by the IT Director.
- **6:45 a.m.:** The attacker(s) response was as follows: "We have your data hostage. All your systems are encrypted. You will not decrypt this problem unless you pay. We have also taken the healthcare data from your Electronic Medical Record System, files from your shares, and more. We have included samples of this sensitive data in these attachments. If you pay, we give you decryption key AND YOUR DATA BACK. We promise to destroy the data when this happens. You must pay us the equivalent of $500,000 US Dollars in Bitcoin. You have 12 hours until the price doubles".

Breach Anatomy:

Phase I: During the cloud migration, one of the systems administrators had been tasked with moving file shares, documents, and performing other actions regarding data transfers. The method that the administrator had chosen was to simply open a remote desktop session from the cloud servers to the on-premise server. With this method, they could simply copy and paste files with little complexity. However, the route was opened and never closed.

Phase II: Attackers had breached the open remote desktop server with ease and had remained on the network for more than 3 months performing reconnaissance, conducting attacks on other organizations, stealing sensitive data, exploiting internal systems, and mounting a strategy that would yield the most profits. The attackers had performed a brute force attack on the server and had resulted in the successful compromise of an administrator account with weak credentials. From the security logs, it showed that they had performed over 72 hours of brute force attacks before the account was finally compromised.

Phase III: Once inside of the network, the attackers moved laterally. They created multiple administrator accounts, installed malicious software and backdoors, and began to conduct vulnerability scanning on other internal systems. From this phase, they moved to leveraging hacking tools to exploit other systems that hosted vulnerabilities. Leveraging a common SMB vulnerability, the attackers were able to exploit virtually every workstation and laptop within the environment.

Phase IV: The attackers had also located the Electronic Medical Record (EMR) system. This system was leveraged internally for archival of medical records and held a wealth of Electronic Personal Health Information (ePHI) and other sensitive data. The attackers were able to compromise an administrator account on this system within a matter of minutes, due to the weak credentials leveraged. Additionally, the attackers also had gained access to the file shares. These file shares held billing information, employee data, human resources files, and other internal documentation. The attackers had downloaded the data from the EMR system and the file shares to local zip folders and had uploaded them to an external cloud storage site for later use.

Phase V: Once the attackers had sifted through the internal systems, stolen data, installed malicious software and backdoors, exploited workstations and laptops, they moved into the last phase of the nefarious project; Ransomware. Destruction would soon ensue as the attackers had mounted a series of plans to heavily exploit the organization. The attackers even left notes on the file servers that they had read through the internal emails of the employees and had evidence of corporate corruption and malpractice. They had even included screenshots of emails involving internal employees accepting bribes from pharmaceutical companies.

The gravity of this breach had brought the organization to a grinding halt on multiple fronts.

The Aftermath:

The healthcare organization went from a steady-state of operations to a complete stop within a matter of hours. However, it was apparent that the breach was ongoing for months and the attackers likely retained access to the environment. The decision was finally made to pay the ransom. However, due to the gravity of this breach, the authorities were involved. The organization ultimately ended up paying $500,000 to the attackers for the release of the decryption key and destruction of the sensitive data that had been stolen. However, little to no assurance was gained of the data destruction. The cost of the incident response team was over $100,000 and the associated HIPAA violation fees were upwards of $850,000. The total monetary cost of the breach was approximately $1.5 million dollars. However, these costs did not include the loss of reputation, clients, and other associated factors. The result of the alleged internal unethical practices was unknown as this was closely guarded by corporate attorneys and law enforcement.

A Preventable Breach:

The attacker(s) had free-reign on this organization for multiple months during this attack. They had performed overt reconnaissance and exploitation with no alarms, alerts, or signals to the staff that could have prevented such a devastating situation. If the organization had been proactively monitoring the network's security with a managed Security Information and Event Management platform (SIEM) and other services offered by ClearNetwork, the devious activities would have likely been discovered and halted. In fact, the entire breach could have been prevented and halted with the following ClearNetwork solutions and SIEM capabilities:

- **Change Management:** When the junior systems administrator had opened the floodgates for the attackers, by implementing a remote desktop protocol (RDP) over port 3389, an alert could have been sent by the SIEM. Changes in systems, ports, and protocols are closely monitored through the SIEM solution. If this had been implemented prior, the IT staff could have been notified of the open port and responded to accordingly.

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Manufacturing Industry

- **Brute Force Alerts:** When the attacker(s) had been performing the brute force attacks on the exposed RDP server and the internal EMR system, alerts could have been sent to inform the internal staff that the system was under attack.
- **Vulnerabilities:** The attackers were able to conduct vulnerability scanning throughout the network. The SIEM solution could have notified the staff that unauthorized scanning and reconnaissance was being conducted. Additionally, the built-in vulnerability scanning capabilities of the SIEM could have identified workstation and laptop vulnerabilities prior to the internal lateral attacks. If the vulnerability scanning had been configured through the SIEM or ClearNetwork regular vulnerability scanning, then the IT staff could have patched vulnerable systems and prevented such ease of this lateral movement.
- **Malware & Backdoors:** Many of the workstations and laptops were found with attacker-installed software. This software was used for creating remote access points throughout the network. The SIEM platform could have been leveraged to send alerts when and if unauthorized software was installed. IT staff should be apprised when software is installed on systems within the network. Additionally, the antivirus alerts were found on the local systems. However, these alerts and logs were not sent to a central authority such as a SIEM. The alerts remained on the local systems and never made it to the eyes of the IT staff. Users simply ignored the alerts or believed that the IT team was apprised of such activities.
- **Account Creation Monitoring:** Many accounts were created by the attackers. These accounts included full administrators and local users. Since the organization had recently shifted most assets to the cloud, Active Directory actions were held within the cloud environment and no alarms or alerts were generated since the attackers were not interfering with the cloud-based Active Directory infrastructure. These suspicious account creations could have been observed through the SIEM platform.
- **Suspicious Account Activity:** Since many accounts were leveraged to move laterally, log into remote systems, and perform other malicious actions; such activities may have been alerted on from the SIEM solution. However, account activities were not funneled to a central location for monitoring and therefore, the attacker(s) actions remained relatively covert without the capabilities for visibility.
- **Anti-Exploitation Alerts:** When the workstations and laptops were being exploited, alerts could have been sent to key staff members and given them opportunities to respond accordingly.
- **Data Exfiltration:** One of the most critical aspects of this case involved the unauthorized transfer of sensitive information to cloud storage sites. When the attacker(s) commenced the exfiltration tactics of the electronic medical records and sensitive employee data, alerts could have been tailored within the SIEM to report on such actions. Administrators could have responded to these alerts in a streamlined fashion.
- **Ransomware:** The final phase of the breach involved the release of ransomware on the network. However, the spreading and encryption mechanisms of ransomware can move relatively slowly; infecting single systems or groups of systems at one time. Critical SIEM alerts could have tipped the IT staff to begin containing the threat before the spread ratio encompassed most systems.

Enhancing the Security Posture

The healthcare organization fell victim to a series of attacks that could have easily been prevented. By engaging ClearNetwork for managed SIEM, vulnerability scanning, intrusion detection, behavioral analysis, and other services, the organization could have boasted a proactive and robust security posture. Due to the lack of security capabilities, the healthcare organization was subject to advanced exploitation and full network compromise. Avoiding data breaches and organizational compromises begins with a proactive defense and monitoring stance. The catalysts that enabled the attacker(s) to exploit this organization, exfiltrate sensitive medical records, and release ransomware were found to have been easily avoidable using ClearNetwork's security offerings.

Looking to protect yourself from this type of attack?

Clearnetwork USM would have caught this attack during its early stages. Our service utilizes SIEM and Log Management, Monthly or Bi-weekly Vulnerability Assessments, Intrusion Detection, Behavioral Analysis, Asset Discovery, Endpoint Detection and Response, File Integrity Monitoring and more. Everything is managed and watched by our expert security analysts each with years of experience in locating evasive threats. We also fully utilize your existing security investments like anti-virus and firewalls and over 200 other devices/services by constantly watching the logs for any sign of a threat and using that data with all our other collected data to paint a full picture of what's happening on the network. All of this offered by us in one solution, with no long term contract, and we offer a free 14 day proof of concept (POC) so we can demonstrate our value.

Please reach out to schedule a demo or talk in more detail.

sales@clearnetwork.com

800-463-7920 x3