CLEARNETWORK
YOUR CYBERSECURITY EXPERTS

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Higher Education

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

Organization Background:

A major university, based on the East Coast of the United States, with over 10,000 students and 500 faculty members. The university has been running for over 50 years and offers many undergraduate and masters programs. The university is a highly coveted institution that is on the leading-edge of many different academic areas. Many international students also attend the university and come from all over the world to study the specific programs that they offer. Another major factor for the attention to the university are the sports programs that are offered. The university offers division 1 sports in many different areas.

Technology Background:

A major university, based on the East Coast of the United States, with over 10,000 students and 500 faculty members. The university has been running for over 50 years and offers many undergraduate and masters programs. The university is a highly coveted institution that is on the leading-edge of many different academic areas. Many international students also attend the university and come from all over the world to study the specific programs that they offer. Another major factor for the attention to the university are the sports programs that are offered. The university offers division 1 sports in many different areas.

- **Domain:** Microsoft Active Directory (hybrid onsite and Microsoft Azure)
- **Email:** Microsoft Office 365
- **Firewall & VPN:** Palo Alto
- **Virtualization:** Microsoft Hyper-V
- **Servers:** 80% Windows Server 2012R2, 15% RedHat Linux, & 5% Windows Server 2003 (Legacy).
- **Workstations/Laptops:** Chromebooks, Dell Latitude, and various laptop types.
- **Security:** McAfee Antivirus, Palo Alto Intrusion Prevention, Cisco Umbrella Content Filter.
- **SIEM:** None

During the implementation of the newly-formed virtual infrastructure, the university had also begun a security and compliance assessment, being performed by an external security firm. The assessment included a full review of compliance and administrative items, physical security, and a deep review of systems security. The engagement also included a vulnerability assessment and penetration test. The 3rd party firm's duties were to uncover all vulnerabilities within the university's systems, physical security, and administrative areas.

The timeline for the assessment was proposed to be 60 days until the final deliverables were granted. Because of this assessment, certain security aspects of the infrastructure virtualization project were put on hold or were failed to be observed. This would soon prove to be a grave oversight that led to a series of security incidents. During the migration of servers and data to the cloud, the university was leveraging a series of remote desktop servers, hosted on the edge of the on-premise environment. These were supposed to be temporary servers for only data migration purposes.

Uncovering Evil:

During the final phases of the assessment, the 3rd party firm was conducting penetration testing on the external environment. The lead penetration tester noticed 3 externally-facing remote desktop servers on the edge of the environment. The remote desktop servers were directly exposed to the outside world and were found to be unprotected by the Palo Alto firewalls. Once the penetration testers discovered the servers, they began a series of reconnaissance techniques that exposed vulnerabilities on the servers that could potentially be exploited.

The 3rd party firm began exploitation of the systems and within less than one hour, they had exploited one of the remote desktop servers. This was very concerning because if the penetration testers could exploit it this easily, this meant that attackers could possibly do the same. Once the penetration testers had access to the server, they began some internal identification of lateral systems. However, during the lateral reconnaissance, the remote desktop server that they had exploited was suddenly demonstrating suspicious systems. The system became very slow and was showing multiple connections to non-U.S. IP addresses.

At this point, the information technology team of the university was notified by the penetration testers that the testing had been halted due to suspicious findings. It is common-practice for penetration testing companies to stop testing if a suspected system compromise is uncovered. The findings met the criteria for stopping a penetration test and the university's information technology team began to investigate.

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Higher Education

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

Compromise Dissection

- Once the internal IT team performed the initial investigation, it was found that one of the externally-facing remote desktop servers was exploited. The attackers placed malware on the remote host that captured credentials and granted them remote access. From there, the attackers moved laterally into the environment.
- Once the internal investigation began, it was discovered that the attackers had also compromised an internal accounting system, used by the registrar and bursar's office. This system held student financial information, among many other sensitive financial documentation for government grants, loans, and more.
- Due to a lack of network segmentation, the attackers also had adequate time to move into the PCI-DSS environment. The university had a main credit card processing server that was connected through site-to-site VPN's to the bookstore, sports arena, cafes, and other satellite locations that processed payment card transactions.
- Through manual sifting of Windows event logs, the team was able to determine that the attackers had also compromised several domain administrator accounts. Once they had untethered access to the Active Directory domain, several other administrator accounts were created and used in lateral movements across the environment.

Post Incident Activity

Once the extent of the compromise had been determined, several regulatory issues came into play. Private student information was protected under the Family Educational Rights and Privacy Act (FERPA) and payment card information was also protected as per Payment Card Industry Data Security Standards (PCI-DSS). Therefore, multiple parties had to be notified of the compromise and this led to a series of supplemental investigations. Additionally, it was unknown what level of information was exfiltrated from the environment as event logs were not centralized or correlated.

Potential Prevention with Clearnetwork

The university was attacked with some fairly rudimentary techniques that ultimately led to the compromise of student data and sensitive financial information. If the organization had been leveraging a managed Security Information and Event Management platform (SIEM) and other services offered by Clearnetwork as part of the Managed Detection and Response (MDR) service, then the devious activities could have been discovered and stopped. The attackers implemented an external attack on the university's external remote servers. Once they had access to the server, they were able to move freely throughout the environment. If the University had been proactively monitoring, then the lateral activities could have been detected.

- **Remote Desktop Server:** If the University was performing asset discovery and having regular vulnerability scans performed with Clearnetwork's MDR service then the vulnerabilities, ports, protocols, and services related to the exposed remote desktop server could have been detected. This would have given the University staff time to respond and to shut down the services before they were exploited.
- **Placement of Malware:** If the University had monitoring in place from Clearnetwork's MDR service then the malware events could have been detected from a centralized location. Alerts could have been sent to administrators and prompted them to investigate quickly.
- **Credential Cracking:** The attackers seamlessly compromised Active Directory passwords with ease. The techniques that they leveraged required the use of tools that could have been detected with Clearnetwork's MDR service. Not only did the attackers compromised local system credentials on the remote desktop server, they also performed password spraying techniques across the organization. This methodology led them to compromise the 1st administrative accounts. Once access was gained into a domain administrator account, the compromise grew exponentially. The use of such tools and techniques could have been detected and alerted on with Clearnetwork's MDR service.
- **Malicious Creation of New Accounts:** Clearnetwork's MDR service would have also been collecting event logs from Active Directory and alerting on new administrator account creations. However, no such tool was leveraged by the University and this gave the attackers the space that they needed to create additional accounts and perform many variations of lateral movements. This granted them the freedom to create strong footholds within the organization systems.
- **Improper Network Segmentation:** If the organization had been leveraging Clearnetwork's MDR service, then there is a good chance that they may have been advised on the potential problem and realized that the network was segmented improperly. With asset discovery inside of the Clearnetwork's MDR service solution, they could have detected systems that were supposed to be isolated but were not. By not detecting the PCI-DSS scoped systems the attackers were able to move quickly to servers that held private and confidential payment card information. This opened the door for the attackers to compromise such data and ultimately left the University in a position in which they had to disclose such information to regulatory officials for supplemental investigations.

sales@clearnetwork.com
800-463-7920 x3

Cyber Breach Case Study: Higher Education

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

- **Lack of Antivirus Coverage:** While the University was under the impression that all systems were equipped with anti-virus, this was found to be not the case. Many systems were not equipped with anti-virus or the antivirus was not functioning properly. This gave the attackers the ability to infect systems that were not equipped with anti-virus without being detected from the central antivirus console. If Clearnetwork's MDR service was used, an audit across all systems could have been performed that could have detected a lack of antivirus on systems an organizational staff could have addressed this sooner.

Moving Forward

A seemingly simple migration to a virtualized infrastructure resulted in the temporary lapse of attention that led to a full network compromise for the University. If the University had been leveraging Clearnetwork's MDR service, then it is very likely that all aspects of this attack could have been detected in time to respond. However, no alerts were triggered, no logs were sent, and no response was initiated. It was only upon the penetration testers discovery of the external remote desktop service and exploitation that the issues were brought to the surface. While the University had invested in upgrading the technological infrastructure, security was a relative afterthought.

A proactive stance in today's threat landscape is required by all organizations, both large and small. With such sensitive data that universities hold, it behooves them to implement adequate security controls and monitoring services such as Clearnetwork's MDR service. Through the use of Clearnetwork's MDR service, this compromise could have likely been stopped in its tracks. However, this led to gaining the attention of each and every IT team member, executive, director, and manager in a very reactive an alarming way. Being proactive about your security is no longer an option. The stakes in 2020 are too high to adopt a merely reactive posture. Preparing today with Clearnetwork's MDR service can position your University to proactively respond to the security threats of today in this ever-advancing technological age.

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