GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Implementing and Auditing CIS Controls (Security 566)"
at http://www.giac.org/registration/gccc

Paying Attention to Critical Controls

GIAC (GCCC) Gold Certification

Author: Edward Zamora, ezamora@mastersprogram.sans.edu
Advisor: Stephen Northcutt

Accepted: August 20, 2015

© 2015 SANS Institute, Author retains full rights.

Abstract

International organizations such as the Australia DSD, the European Commission and the US NSA have developed their lists of top mitigations and actions they consider necessary for organizations and governments to implement. It has been further established by the international information security community that the twenty critical security controls are the top relevant guidelines for implementing and achieving greater security. Many of the controls require the deployment and installation of security software. But is installing software all there is to it? Will an organization be better defended by buying lots of security products? In one particular use case, attackers were able to break through the network defenses of an organization that implemented many of the security controls but did not do so properly. Under the sense of false security, the senior leadership woke up to some bad news when they learned that gigabytes of data were stolen from the organization's network after controls were in place. The implementation of security controls should be done with careful planning and attention to detail. This paper covers what the attackers did to circumvent the controls in place in the organization, how they could have implemented the critical controls properly to prevent this compromise, and what an organization needs to do to avoid this pitfall.

© 2015 The SANS Institute Author retains full rights.

1. Introduction

Research has shown the tendency of companies not paying close attention to the importance of security as in the case of the Target security breach in 2014 (Ponemon Institute LLC, 2015, p. 2). In spite of this common trend, many of the companies that were compromised and made headlines had security controls in place including JP Morgan, E-Bay and the Sony PlayStation Network (Ponemon Institute LLC, 2015, p. 1). The issues were not always an absence of capable personnel, tools, and products to detect and prevent attacks (The Home Depot, 2014). The issues in many cases were a lack of attention to detail and proper configuration of security controls (Vijayan, 2014). In one such case an organization that was familiar with the critical controls and implemented a portion of them, fell victim to their lack of attention to detail and false sense of security.

For the purposes of protecting the privacy of the organization in this case, the company is referred as the ABC Datacenter Corporation. The ABC Datacenter Corporation deals in storing information for several companies. Many companies contract with ABC Datacenter to use their mass storage facilities as file repositories and data warehouse. This practice of using data warehousing is very common for large and small businesses (Guerra & Andrews, 2013). According to publicly available information on the Internet about the ABC Datacenter Corporation, it was disclosed on their website that the company was in the process of a merger. Mergers can be quite complicated and require several careful considerations to ensure a smooth transition of information and assets (El Abed, 2009, p. 5). The ABC Datacenter Corporation bought out the Tonden File Company that was also a data warehouse with clients of their own. As is the case with most mergers and acquisitions, sharing of information was taking place across these companies' networks during the move of systems (El Abed, 2009, p. 1).

On an otherwise uneventful work day, a spear phishing email was received by a group of users in the marketing department of the ABC Datacenter Corporation. These particular set of marketing employees had their email addresses listed on the company website. When they received the email, many of them opened the attachment that seemed normal to them but really contained malicious code. The code opened up a connection to

© 2015 The SANS Institute Author retains full rights.

© 2015 SANS Institute, Author retains full rights.

malicious servers over the Internet. Once the workstations connected to the attacker's servers, the hackers uploaded tools such as privilege escalators and backdoors. This same pattern of attack using spear phishing or targeted attack emails to gain access and compromise systems were used in major data breaches including the RSA and Epsilon breaches (TrendLabs APT Research Team, 2012).

As it turned out, the ABC Datacenter administrators maintained a good patch cycle and the workstation operating systems were patched and up to date. The effectiveness of patching has proven effective against most public exploits when deployed near the release of the patches (Infosecurity Magazine, 2012). Some of the attacker's tools did not work for this reason. There were even application whitelisting and antivirus programs installed on the workstations. However in poor practice, both of these security applications were configured in default or minimal mode and the attackers were able to run their tools on the workstations without being completely blocked or detected (SANS Institute, 2015).

The human susceptibility to deceit has been the cause of about 70% of the data breaches in one extensive study (Verizon Enterprise Solutions, 2014, p. 42). In the case of the ABC Datacenter, some of the marketing employees not only opened the email but also forwarded the email to other coworkers in neighboring departments. One employee that received a forwarded email also had multiple levels of privileges associated with their account. This user also had administrative access to a server in the network. The attackers used common hacker techniques to install a backdoor on the employee's workstation and then used the additional privileges to install another backdoor on the server that the employee had privileges to (Symantec Corporation, 2014, p. 39).

It turned out that this server had less security present than the workstations. The server functioned as a shared repository that belonged to the acquired data warehouse, Tonden File Company, and was in the queue for movement to the ABC Datacenter network. A separate domain administrator account belonging to the acquired company's domain was logged on to this server as well. The attackers were able to steal the privileges of that domain administrator account and install additional backdoors and tools on the Tonden File Company's systems that had not been moved over. Using the same

© 2015 SANS Institute Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

pattern many attackers use, the hackers stole an estimated 11GB of research data and user account information from the ABC Datacenter Corporation and the Tonden File Company systems (Verizon Enterprise Solutions, 2014, p. 30).

The ABC Datacenter security team eventually found out there was a problem when a system that was transferred from the Tonden File Company was observed to consistently use high amounts of bandwidth in the network traffic. After further investigation by the security team, the domains and IPs involved in the suspicious traffic were determined to be malicious. This incident was reported to ABC Datacenter Corporation leadership as part of the incident response and handling procedures. The origin of the compromise was eventually traced back to the marketing department workstations and phishing emails through a backwards analysis of logs.

This case is one of many examples of what hackers have done to networks where management perceived their networks to be secure (Ponemon Institute LLC, 2014). Attention to detail must be given to the application of the critical controls in order to make sure the controls are applied appropriately. Successful implementation is achieved with careful planning and execution of the guidelines provided with the critical controls (SANS Institute, 2015). The critical controls are designed to reduce an organization's attack surface and risk posture against active and relevant threats (SANS Institute, 2015).

In addition to careful implementation, there needs to be active participation by senior technical leadership to accurately understand the state of security of the organization's network. This would be true especially during a time of mergers and acquisitions (El Abed, 2009). Poor communications in the management of the transition project cost the ABC Datacenter Corporation consumer confidence that later translated to tangible revenue losses. The lack of effectiveness of project management also placed the senior leaders in a position of being uninformed and therefore unable to make a knowledgeable decision.

The priority of security awareness for an organization is largely influenced by the importance given to security awareness by senior leaders (Moag & CDS Team, 2011). Leadership sponsored training that is engaging and interactive improves the effectiveness and readiness of the workforce to respond to targeted attacks (Ponemon Institute LLC,

© 2015 The SANS Institute Author retains full rights.

© 2015 SANS Institute, Author retains full rights.

2014). An organization that thoughtfully implements the critical controls and applies best practices for management, will be significantly better positioned to defend and respond to cyber-attacks.

2. Anatomy of the Attack

2.1. Initial Compromise

Email spear phishing attempts were successful in the case of the ABC Datacenter Corporation compromise, despite the existence of security measures. For example, the company had in place an email gateway appliance to control spam and email born threats. The targeted emails to the marketing department were still able to get through the email gateway because the emails were not classified into a threatening category that would block the email. The administrators initially installed the email gateway and left mostly the default recommended settings. They did not revisit the device to tailor the configuration due to competing priorities set by the operations manager. The email gateway blocked many types of spam email, but allowed phishing emails to still get to user inboxes placing the burden of self-reporting a suspicious email on the user.

This strategy may still have worked if there were proper training. Many of the marketing employees did not open the attachment, but 40% of the victims either opened the attachment or forwarded the attachment to other employees. This metric is above the rising trend of 23% of users that open phishing emails in an organization and 11% that open attachments (Verizon Enterprise Solutions, 2015, p. 11). The company had yearly mandatory training on email security that met compliance requirements. However, the email security training consisted of a text-based set of questions and a multiple choice quiz at the end of the training document. This method proved to be less effective than desired by the organization, because it was the forwarding of the email that gave the attackers the additional opportunities to spread out through the network. One of the users that received a forwarded email was an administrator of a server.

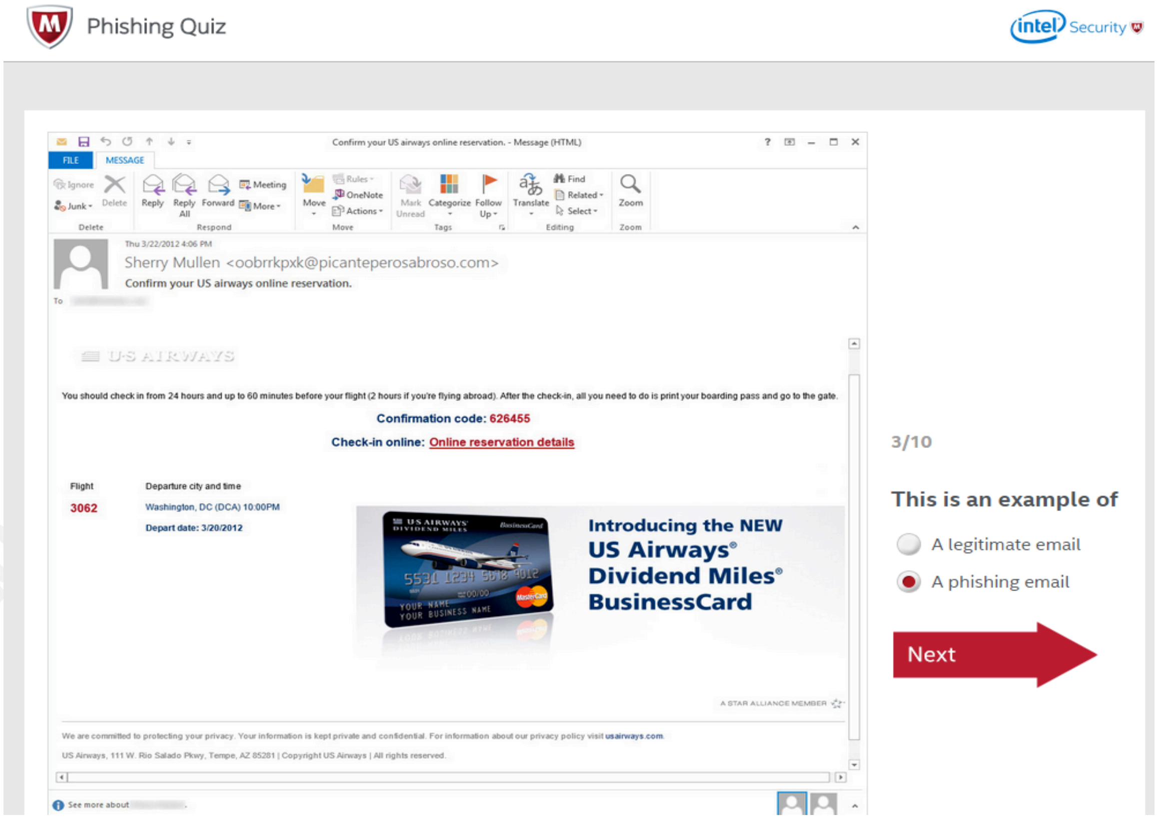
The findings associated with the spear phishing compromise reflect the need to pay close attention to the Secure Configurations for Network Devices (#10) and Security Skills Assessment and Appropriate Training to Fill Gaps (#9) security controls (Council

© 2015 The SANS Institute Author retains full rights.

on CyberSecurity, 2015). The ABC Datacenter Corporation did in fact implement Secure Network Engineering by installing an email security gateway to control email attacks. However, administrators should have taken more time to configure the email gateway phishing threshold to a more appropriate threat level. The regular tuning of the email gateway appliance over time would have increased the quality of phishing detection and reduced the absolute dependency on end users to decide.

The company would have benefited from employing scenario based training more frequent than once a year. The human factor has repeatedly proven to be the weakest link in organizations (SANS Securing The Human, 2015). In the case of the ABC Datacenter security breach, more effective workforce training would have significantly reduced the success of the phishing attacks (Moag & CDS Team, 2011, p. 3). This is even more relevant with phishing attacks remaining among the top attack vectors against organizations (TrendLabs APT Research Team, 2012). Diagram 1 shows an example of phishing training designed to help end users become familiar with phishing attacks.

© 20 Author retains full rights.



Confirm your US airways online reservation. - Message (HTML)

Thu 3/22/2012 4:06 PM

Sherry Mullen <oobrrkpxk@picanteperosabroso.com>

Confirm your US airways online reservation.

To [redacted]

You should check in from 24 hours and up to 60 minutes before your flight (2 hours if you're flying abroad). After the check-in, all you need to do is print your boarding pass and go to the gate.

Confirmation code: 626455

Check-in online: Online reservation details

Flight	Departure city and time
3062	Washington, DC (DCA) 10:00PM Depart date: 3/20/2012

Introducing the NEW US Airways® Dividend Miles® BusinessCard

We are committed to protecting your privacy. Your information is kept private and confidential. For information about our privacy policy visit usairways.com.

US Airways, 111 W. Rio Salado Pkwy, Tempe, AZ 85281 | Copyright US Airways | All rights reserved.

See more about [redacted].

3/10

This is an example of

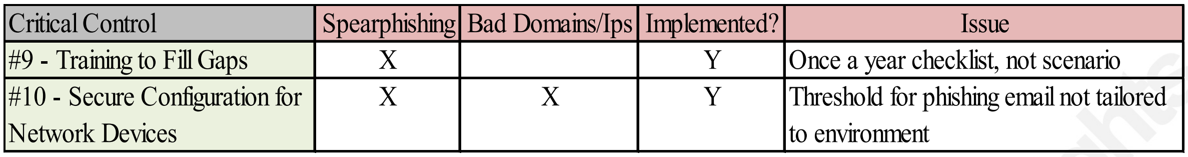
○ A legitimate email

● A phishing email

Diagram 1. Sample phishing training by McAfee (McAfee, 2015)

© 2015 The SANS Institute Author retains full rights.

A list of the security controls that would have helped to prevent and mitigate attacks at the initial stage of compromise are shown in Table 1.



Critical Control	Spearphishing	Bad Domains/Ips	Implemented?	Issue
#9 - Training to Fill Gaps	X		Y	Once a year checklist, not scenario
#10 - Secure Configuration for Network Devices	X	X	Y	Threshold for phishing email not tailored to environment

Table 1. Critical Controls at the Initial Compromise

2.2. Code Execution

Once the phishing victims opened their email attachments, a hidden instance of their browser was launched and directed to the attacker's website. Attackers were able to execute code within the browser. The administrators had the browser and plugins patched and up to date according to vendor patch cycles. However, one browser plugin that was widely used had a publicly available exploit for which the vendor did not yet have a patch. This unfortunate yet common occurrence is similar to a recent Java vulnerability CVE-2015-2590 that was being exploited in the wild for over two months before a patch was released (Constantin, 2015). The hackers used an exploit similar to this one to execute their backdoor on victim computers and connect back to their servers. The company had deployed anti-malware defenses including the Microsoft's Enhanced Mitigations Experience Toolkit (EMET) onto the workstations in the enterprise as part of their default workstation image. However, the administrators relied on the default configuration of EMET to protect the browser and the protection did not work. This is because the browsers that were used by most of the victims were not included in the default configuration of EMET (Hoffman, 2014).

The attackers proceeded to upload their tools to victim's workstations and placed the tools in the user directories that were allowed to store downloads. The hackers unintentionally uploaded tools to whitelisted directories. They only found out after trying to move files into other directories as later evidenced by logs. The administrators had implemented application whitelisting on all workstations. However the method used for whitelisting was solely based on directory path. One of the paths allowed to download and run applications was the user directory where the tools were downloaded to. This misconfiguration existed on all the company systems and was a root catalyst for enabling

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

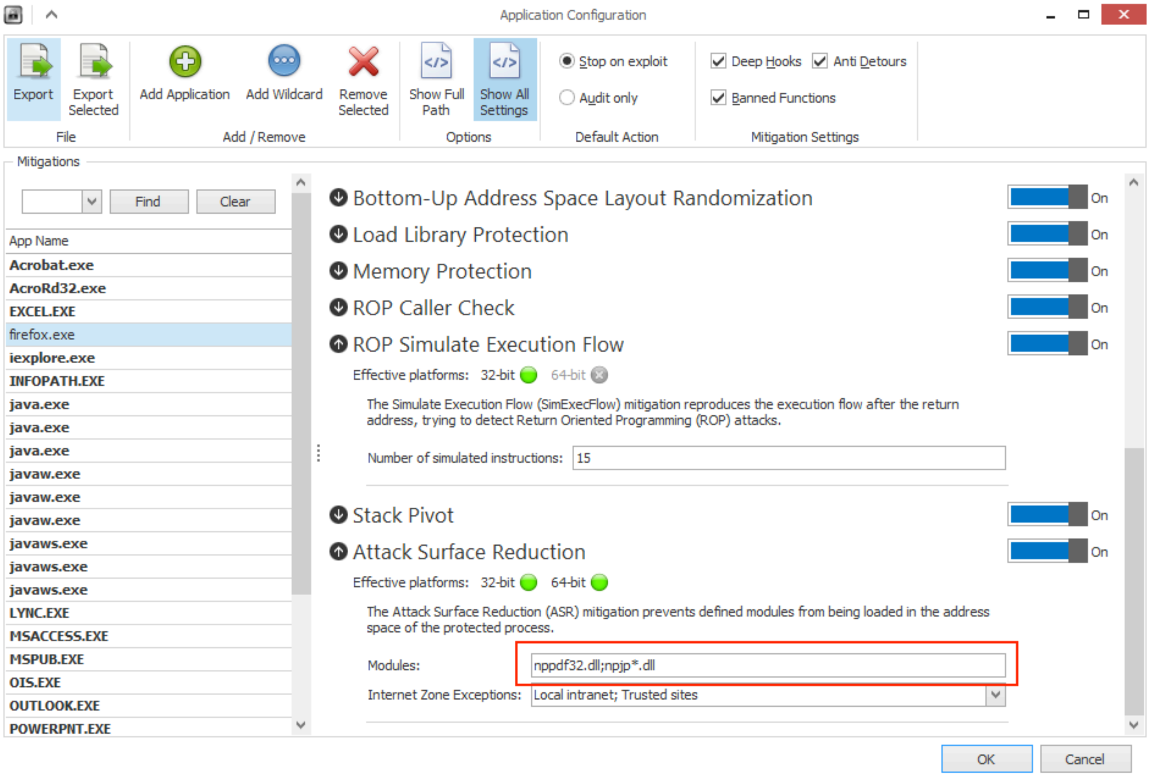
the hackers to compromise the rest of the enterprise and affect the rest of the workstations and servers.

Armed with the ability to run applications, the hackers uploaded privilege escalation tools and executed them. The attackers attempted to execute several privilege escalation tools but were not successful. Remarkably, the workstations did not suffer complete shutdowns or the “blue screens of death” (Hoffman, 2013). However, there were no indications that these escalation attempts were caught by real-time antivirus. The antivirus tools installed on the workstations were up to date, the execution of the tools logged, and yet these tools were not flagged as malicious. The saving grace for this company was the ability for administrators to go back through these logs during the incident response and piece together the events that took place.

The hackers were successful in downloading and executing tools due to inadequately implementing the Malware Defenses (#5), Application Whitelisting in the Inventory of Authorized and Unauthorized Hardware and Software (#2), and Log Alerting in the Maintenance, Monitoring, and Analysis of Audit Logs (#14) security controls (Council on CyberSecurity, 2015). The company installed and deployed EMET across the workstations but the administrators left them in the default configuration. EMET is most effective when its configuration is tailored for an organization’s baseline of applications that need to be protected (Hoffman, 2014). The protections offered by EMET in this case were rendered useless because the user’s browser and plugins were not included in the list of applications protected. The proper configuration could have prevented the technique used to compromise the browser and plugin as seen in diagram 1 (Kirk, 2014).

© 2015 SANS Institute Author retains full rights.

© 2015 The SANS Institute Author retains full rights.



● Stop on exploit
○ Audit only

☑ Deep Hooks ☑ Anti Detours
☑ Banned Functions

App Name
Acrobat.exe
AcroRd32.exe
EXCEL.EXE
firefox.exe
iexplore.exe
INFOPATH.EXE
java.exe
java.exe
java.exe
javaw.exe
javaw.exe
javaw.exe
javaws.exe
javaws.exe
javaws.exe
LYNC.EXE
MSACCESS.EXE
MSPUB.EXE
OIS.EXE
OUTLOOK.EXE
POWERPNT.EXE

Bottom-Up Address Space Layout Randomization — On
Load Library Protection — On
Memory Protection — On
ROP Caller Check — On
ROP Simulate Execution Flow — On

Effective platforms: 32-bit ● 64-bit ⊗

The Simulate Execution Flow (SimExecFlow) mitigation reproduces the execution flow after the return address, trying to detect Return Oriented Programming (ROP) attacks.

Number of simulated instructions: 15

Stack Pivot — On
Attack Surface Reduction — On

Effective platforms: 32-bit ● 64-bit ●

The Attack Surface Reduction (ASR) mitigation prevents defined modules from being loaded in the address space of the protected process.

Modules: nppdf32.dll;npjp*.dll

Internet Zone Exceptions: Local intranet; Trusted sites

Diagram 2. EMET configured to protect Firefox with Adobe and Java Plugins

The ABC Datacenter administrators applied application whitelisting which made some of the work harder for the attackers. However, the administrators configured the whitelisting to allow the user full access to create, modify, and execute all applications in specific folders including the user's download folder. The hackers were not able to write to system directories, but in the end they did not need to. They were able to persist and use backdoors running out of user directories. This pattern of methodology was also used in the Home Depot breach, especially in the early stages of the attack (The Home Depot, 2014).

The more effective implementation would have been to use hash based whitelisting in addition to path based. Using hash based whitelisting does come with some initial administrative overhead, but can be very effective in blocking unauthorized applications that are not part of the organizational baseline (Sedgewick, Souppaya, & Scarfone, 2014, p. 2). As applications are baselined for an organization in "learning mode", the upkeep for applications becomes easier to manage over time. The benefits

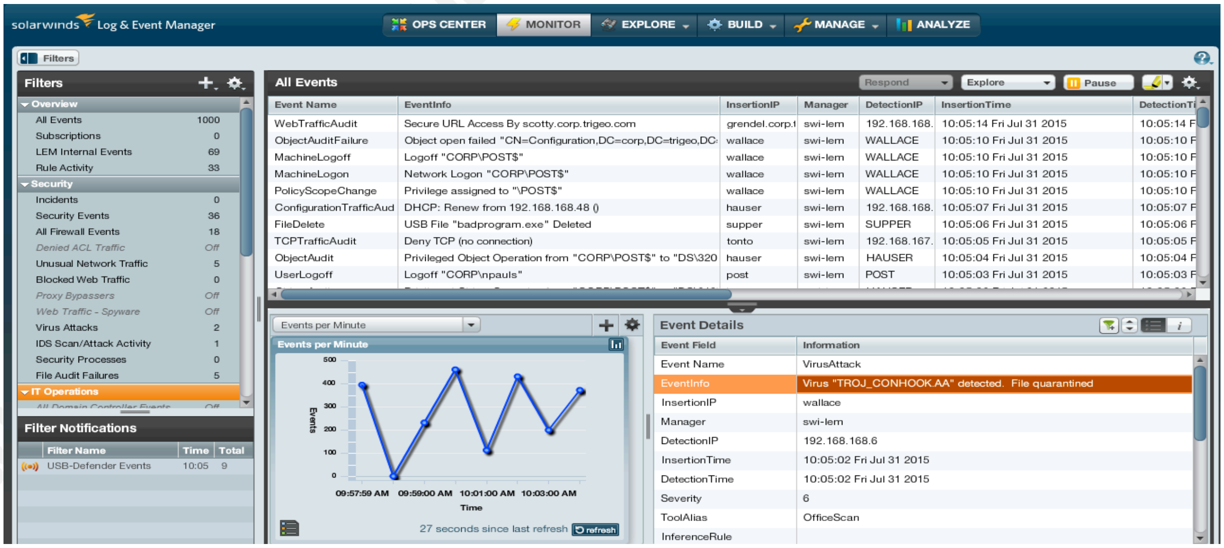
© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

outweigh the initial effort to properly apply application whitelisting and would have been a significant deterrent to these attackers.

The hackers failed to execute privilege escalation tools successfully. This was due in part to the workstations being patched and up to date. There was also no evidence that the attackers employed zero day attacks against the operating system of the workstation. One concerning aspect of these events is the failure of antivirus to detect the malicious executables. Antivirus alone will not prevent more advanced attacks against a network (Brink, 2012). A significant mitigation to this attack would have been to install and configure a host intrusion prevention system, also known as HIPS (Brink, 2012). HIPS can be configured at a granular level to allow, prevent, and log details of execution of certain types of files.

In addition to granular configuration capabilities, detailed logging and alerting are available in most enterprise HIPS products. Enterprise HIPS products also facilitate the aggregation of logs and alerts across an enterprise in user friendly dashboards. Many HIPS products integrate with Security Information and Event Managers (SIEM). Examples are provided below of events reported in a demo network.



Filters

Overview	
All Events	1000
Subscriptions	0
LEM Internal Events	69
Rule Activity	33
Security	
Incidents	0
Security Events	36
All Firewall Events	18
Denied ACL Traffic	*Off*
Unusual Network Traffic	5
Blocked Web Traffic	0
Proxy Bypassers	*Off*
Web Traffic - Spyware	*Off*
Virus Attacks	2
IDS Scan/Attack Activity	1
Security Processes	0
File Audit Failures	5
IT Operations	

Filter Notifications

Filter Name	Time	Total
USB-Defender Events	10:05	9

All Events

Event Name	EventInfo	InsertionIP	Manager	DetectionIP	InsertionTime	DetectionTi
WebTrafficAudit	Secure URL Access By scotty.corp.trigeo.com	grendel.corp.t	swi-lem	192.168.168.	10:05:14 Fri Jul 31 2015	10:05:14 F
ObjectAuditFailure	Object open failed "CN=Configuration,DC=corp,DC=trigeo,DC=	wallace	swi-lem	WALLACE	10:05:10 Fri Jul 31 2015	10:05:10 F
MachineLogoff	Logoff "CORP\POST$"	wallace	swi-lem	WALLACE	10:05:10 Fri Jul 31 2015	10:05:10 F
MachineLogon	Network Logon "CORP\POST$"	wallace	swi-lem	WALLACE	10:05:10 Fri Jul 31 2015	10:05:10 F
PolicyScopeChange	Privilege assigned to "\POST$"	wallace	swi-lem	WALLACE	10:05:10 Fri Jul 31 2015	10:05:10 F
ConfigurationTrafficAud	DHCP: Renew from 192.168.168.48 ()	hauser	swi-lem	192.168.168.	10:05:07 Fri Jul 31 2015	10:05:07 F
FileDelete	USB File "badprogram.exe" Deleted	supper	swi-lem	SUPPER	10:05:06 Fri Jul 31 2015	10:05:06 F
TCPTrafficAudit	Deny TCP (no connection)	tonto	swi-lem	192.168.167.	10:05:05 Fri Jul 31 2015	10:05:05 F
ObjectAudit	Privileged Object Operation from "CORP\POST$" to "DS\320	hauser	swi-lem	HAUSER	10:05:04 Fri Jul 31 2015	10:05:04 F
UserLogoff	Logoff "CORP\npauls"	post	swi-lem	POST	10:05:03 Fri Jul 31 2015	10:05:03 F

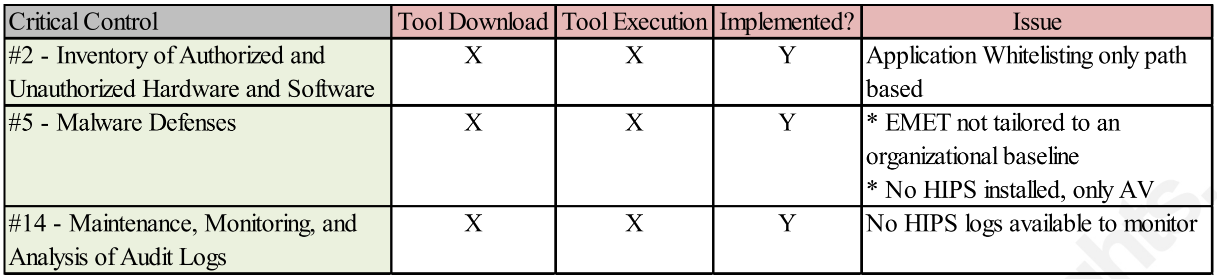
Event Details

Event Field	Information
Event Name	VirusAttack
EventInfo	Virus "TROJ_CONHOOK.AA" detected. File quarantined
InsertionIP	wallace
Manager	swi-lem
DetectionIP	192.168.168.6
InsertionTime	10:05:02 Fri Jul 31 2015
DetectionTime	10:05:02 Fri Jul 31 2015
Severity	6
ToolAlias	OfficeScan
InferenceRule	

Diagram 3. Solarwinds SIEM reporting real time security events (SolarWinds, n.d.)

A list of the security controls that would have helped to prevent and mitigate attacks at the code execution stage of compromise are shown in Table 2.

© 2015 The SANS Institute Author retains full rights.



Critical Control	Tool Download	Tool Execution	Implemented?	Issue
#2 - Inventory of Authorized and Unauthorized Hardware and Software	X	X	Y	Application Whitelisting only path based
#5 - Malware Defenses	X	X	Y	* EMET not tailored to an organizational baseline * No HIPS installed, only AV
#14 - Maintenance, Monitoring, and Analysis of Audit Logs	X	X	Y	No HIPS logs available to monitor

Table 2. Critical Controls at Code Execution

2.3. Contagion

One of the users caught in the phishing attack had multiple privileges assigned to their account. The lack of separating roles for user accounts is poor practice and opens up a network to vulnerabilities that can otherwise be prevented (Symantec Corporation, 2014). The victim in focus was one of the users shifted from the acquired company to the new parent company ABC Datacenter. The user was forwarded a copy of the email as a courtesy by one of the marketing personnel. This user was also one of the developers of an enterprise communications and collaboration application that was just acquired from the Tonden File Company. The enterprise application was used to store and share information related to company projects. The server hosting the application was scheduled to be transitioned from the Tonden File Company's datacenter to the ABC Datacenter Corporation's datacenter warehouse.

The developer's account in the new parent company's domain was recently assigned administrative privileges to manage the application server. The set of events that followed were the unfortunate results of providing too much privilege to the developer much like in the case of the New York Times breach (CyberSheath Services International, LLC, 2014, p. 10). After the developer's workstation had been compromised, the multi-privileged account was used to remotely survey the application server and install hacker tools. Subsequently, the hacker's backdoor was installed with root privileges because the install was done with administrative privileges. The attackers proceeded to collect the hashes and credentials of users on the server. The server itself had antivirus but did not have application whitelisting installed. The hacker tools were not identified or logged as malicious on this server either by antivirus (Brink, 2012).

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

The hackers harvested credentials on this server and were able to acquire the credentials of a domain administrator from the Tonden File Company that was logged on to the server. When the security team retraced the attacker's steps, it was determined that the domain administrator account was idle and not in use. The attackers used their newly acquired credentials to survey the trusted systems in the acquired company. The attackers repeated the process of compromising systems and installed backdoors and tools on the Tonden File Company's systems. The hackers were eventually able to gather more credentials and installed backdoors on other user workstations and connected them to the attacker's infrastructure as is done by many hacker groups (Mandiant, 2014).

The attackers were successful in compromising systems in this stage due to the improper implementation of the Controlled Use of Administrative Privileges (#12), Account Monitoring and Control (#16), Malware Defenses (#5), and Secure Configurations for Hardware and Software (#3) critical controls (Council on CyberSecurity, 2015). The effect of improper critical control implementation became cumulative over time. Improper application whitelisting and malware defense configurations enabled the attacker's ability to execute tools. The developer's regular user account was assigned administrative privileges to the application server for convenience. This decision proved to be a costly one by having made it easier for the hackers to compromise systems further in the network.

The appropriate action would have been to create a separate administrative account for the developer to use for administering the application on the server and not the server itself (SANS Institute, 2015). The administrators would have benefitted from determining the minimum privileges required on the server to manage the application and assigning those permissions. Utilizing a separate account would have at least raised the cost and effort for the hackers to compromise further systems. The use of separate accounts per role also increases the effectiveness of accountability for privileged use of accounts (Symantec Corporation, 2014).

An additional open door was presented to the attackers through the presence of a privileged account from the Tonden File Company logged on to the server. Upon further investigation, it was determined that a domain administrator account was not necessary

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

for administering the server. Appropriate role-based access employs the principle of least privilege for users and roles (Symantec Corporation, 2014). The server administrator role did not include the rights for managing Active Directory. The correct action would have been to use a less privileged account for administering the server. Careful planning should have taken place in the development of the transition project plan. This would have minimized the overlap of privileged access and made it easier to monitor exceptions (El Abed, 2009).

The transfer of company systems certainly complicated the daily operations and monitoring of normal activity. It would have been beneficial for the company to consider the security status of each system (El Abed, 2009). Requirements for the implementation of security controls should have been placed on servers and group permissions before servers were allowed to have trusted connections to the parent company. The implementation of properly configured application whitelisting and malware defenses on this particular server would have served as deterrents to the actions that the attackers took on the server (US-CERT, 2015).

A list of the security controls that would have helped to prevent and mitigate attacks at the contagion stage of compromise are shown in Table 3.

Critical Control	Privilege Escalation	Lateral Movement	Installing Software	Implemented?	Issue
#3 - Secure Configuration of Hardware and Software	X	X	X	Y	* Too much privilege given to developer on server * Server configuration changes were not monitored closely
#5 - Malware Defenses	X	X	X	Y	Servers less protected than workstations
#12 - Controlled Used of Administrative Privileges	X	X	X	Y	Administrators made an exception for convenience of migration
#16 - Account Monitoring and Control	X	X	X	Y	Administrative use of account was not closely monitored

Table 3. Critical Controls at Contagion

2.4. Theft of Data

When the attackers gained administrative access to both networks, they also gained privileged access to all the files and data on both companies' workstations and file servers. The hackers used the previously acquired credentials to access files in the main

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

data repository with file server administrator credentials. The hard drives of the file servers had full disk encryption enabled, but the files themselves remained unencrypted while the servers were powered on. The attackers began to pilfer data from the repository related to research. The attackers downloaded several backups of organizational data belonging to an organization's financial records. It was assumed that the hackers were unsuccessful at making use of them because the backups had an additional layer of encryption provided by the backup software used. The frequency at which data was downloaded from the network was recorded to be a few times a week in the parent company.

The reduced security posture of the acquired company afforded the hackers a more relaxed network for conducting the exfiltration of data. The attackers showed a particular interest in the data residing in the acquired company's file servers. The information consisted of research information on sensitive projects by wealthy organizations. Attackers siphoned research data at a similar frequency as the parent company. Over the course of three months the hackers continued to steal data with increasing frequency and use of bandwidth over time as is the pattern with data loss trends (Verizon Enterprise Solutions, 2015).

The theft of data was possible due to a lack of proper implementation of the Data Protection (#17), Controlled Access Based on the Need to Know (#15), and Maintenance, Monitoring, and Analysis of Audit Logs (#14) critical controls (Council on CyberSecurity, 2015). The parent company servers had full disk encryption, but the files were not encrypted at rest while the servers were on. This grievous oversight cost the company dearly in the form of customer data being compromised, consumer confidence lost, and loss of revenue from customers that went to competitors. If it had not been for the backups having an additional layer of encryption, the consequences would have even been worse as it has been for many other victims (Verizon Enterprise Solutions, 2015, p. 29).

One appropriate prevention would have been to apply encryption to all files on the file servers with the use of client certificates owned by the customer. Encrypting the files would have protected the data cryptographically and raised the cost to the attackers.

© 2015 The SANS Institute Author retains full rights.

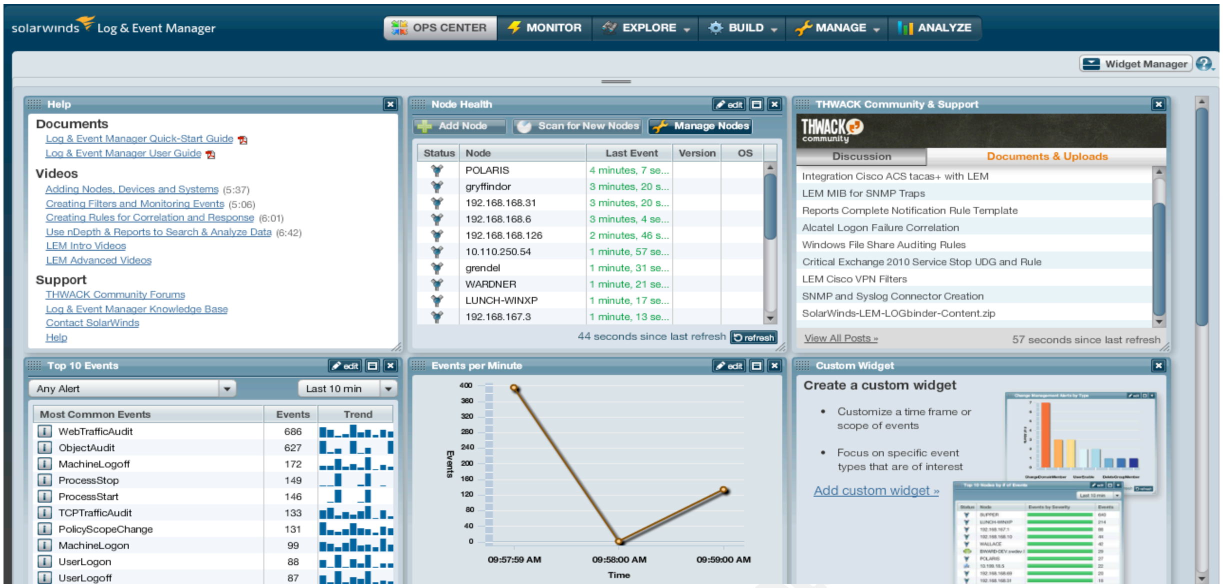
This would have had the additional benefit of limiting exposure of the data to even internal employees to ABC Datacenter Corporation that did not have a need to know of the customer information. This data protection mechanism alone would have rendered the data that the attackers stole useless without the private keys to the data owned by the customers.

The Tonden File Company had a mixed environment consisting of encrypted and non-encrypted files stored on their servers. There were more files were unencrypted than encrypted and most of the data stored by Tonden File was related to research. The attackers focused in on this data in their attack. The same data protection controls that applied to ABC Datacenter, would have been beneficial for protecting data on Tonden File servers. Additional considerations should have been given to the encryption of the data at rest during the development of the data changeover plan.

A great concern that arose from this incident was the lack of the detection of this activity as malicious. The absence of network-based data loss prevention (DLP) devices served to the detriment of the security team and the organizations. A properly installed, configured, and tuned network-based DLP solution would have alerted the security team much sooner on the potential compromise of data and data leakage. The security team needed better alert definitions in their network analysis security information and event management (SIEM) to detect the use of unauthorized encryption channels to unfamiliar websites. Both of these solutions together would have aided the security team in catching and responding to the exfiltration of customer data. Diagram 4 shows a sample dashboard with the types of alerts that would have helped the security team (SolarWinds, n.d.).

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.



Documents

- Log & Event Manager Quick-Start Guide
- Log & Event Manager User Guide

Videos

- Adding Nodes, Devices and Systems (5:37)
- Creating Filters and Monitoring Events (5:06)
- Creating Rules for Correlation and Response (6:01)
- Use nDepth & Reports to Search & Analyze Data (6:42)
- LEM Intro Videos
- LEM Advanced Videos

Support

- THWACK Community Forums
- Log & Event Manager Knowledge Base
- Contact SolarWinds
- Help

Status	Node	Last Event	Version	OS
	POLARIS	4 minutes, 7 se...		
	gryffindor	3 minutes, 20 s...		
	192.168.168.31	3 minutes, 20 s...		
	192.168.168.6	3 minutes, 4 se...		
	192.168.168.126	2 minutes, 46 s...		
	10.110.250.54	1 minute, 57 se...		
	grendel	1 minute, 31 se...		
	WARDNER	1 minute, 21 se...		
	LUNCH-WINXP	1 minute, 17 se...		
	192.168.167.3	1 minute, 13 se...		

44 seconds since last refresh

- Integration Cisco ACS tacas+ with LEM
- LEM MIB for SNMP Traps
- Reports Complete Notification Rule Template
- Alcatel Logon Failure Correlation
- Windows File Share Auditing Rules
- Critical Exchange 2010 Service Stop UDG and Rule
- LEM Cisco VPN Filters
- SNMP and Syslog Connector Creation
- SolarWinds-LEM-LOGbinder-Content.zip

57 seconds since last refresh

Most Common Events	Events	Trend
WebTrafficAudit	686	
ObjectAudit	627	
MachineLogoff	172	
ProcessStop	149	
ProcessStart	146	
TCPTrafficAudit	133	
PolicyScopeChange	131	
MachineLogon	99	
UserLogon	88	
UserLogoff	87	

Create a custom widget

- Customize a time frame or scope of events
- Focus on specific event types that are of interest

Diagram 4. Solarwinds SIEM reporting aggregate events across an Enterprise (SolarWinds, n.d.)

A list of the security controls that would have helped to prevent and mitigate attacks at the theft of data stage of compromise are shown in Table 4.

Critical Control	Unencrypted Data	Data Leakage	Implemented?	Issue
#14 - Maintenance, Monitoring, and Analysis of Audit Logs	X	X	Y	Unauthorized traffic not monitored closely in acquired company
#15 - Controlled Access Based on the Need to Know	X	X	Y	File ACLs not enforced on workstations or admin users
#17 - Data Protection	X	X	Y	No network-based Data Loss Prevention capability employed

Table 4. Critical Controls at Theft of Data

3. Lessons Learned

3.1. Proper Critical Control Usage Guidelines

The consistent theme throughout this unfortunate chain of events has been the lack of attention to detail in the implementation of the critical controls in the ABC Datacenter Corporation. The negative effects of these improper implementations were cumulative. At every stage of the attacker's infiltration, the company's implementation of the critical controls worked to either thwart or enable the attacks. Attackers were unsuccessful at installing tools in certain directories due to whitelisting and some of the

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

data that was taken was confirmed as encrypted. However, the hackers were able to upload tools, install backdoors, and steal data while remaining largely undetected by the security team.

The prioritization of the critical controls established by the Council on CyberSecurity truly stands out as relevant when analyzing this scenario (Council on CyberSecurity, 2015). A proper implementation of the Inventory of Authorized and Unauthorized Software (#2), Secure Configuration of Hardware and Software (#3), Malware Defenses (#5), Security Skills Assessment and Appropriate Training to Fill Gaps (#9), issues around privileged account and roles (#'s 12, 16), and log alerting and monitoring (#14) would have helped the company be positioned to defend against the types of attacks used against the company (Council on CyberSecurity, 2015). In addition to this, the company would have greatly benefitted from having regular Penetration Tests and Red Team Exercises (#20) to test the effectiveness of their security and security team's incident response.

Specifically, the critical controls contain sub-controls grouped into four categories that list specific actions this company could have taken to implement, automate, and measure the effectiveness of the controls (Council on CyberSecurity, 2015). The quick-wins, visibility and attribution, hygiene and configuration, and advanced sub-controls should have been paid closer attention to. The technical leadership in the engineering and security teams acknowledged the need to go through these sub-controls in detail and was tasked to develop a detailed roadmap that aligns with the gaps listed here and the business priorities of the company.

3.2. Management Controls

It was later determined that aggressive timelines for the transition of the systems from the acquired company to the parent company was a factor in the decreased attention to procedures and monitoring. Transferring systems from different networks can be a tumultuous time for administrators (El Abed, 2009). The delicate balance of keeping users content while making necessary system changes that bring downtime is an art at best and can get discouraging at times. Applying best practice principles of project management to ensure stakeholder communications, project tracking, and measuring risk

© 2015 The SANS Institute Author retains full rights.

© 2015 SANS Institute, Author retains full rights.

would have helped the organization make better decisions based on better information (Ponemon Institute LLC, 2014). This would have increased the company's likelihood of a smoother transition and reduced the occurrences of overlooking important details.

Along of the lines of project management best practices, one of the more serious issues identified was the poor translation of technical information to a senior leadership level in stakeholder communications. The leadership team had the impression that customer data was encrypted at rest because the hard drives were encrypted. This technical misunderstanding led several individuals in the leadership team to be under a false sense of security which is very dangerous for a company (Ponemon Institute LLC, 2015). This impact this revelation was expected to have on customers was not something the leadership team delayed in addressing. The leadership staff immediately decreed that all data would be encrypted at rest as their highest priority.

Another finding that was identified was the lack of appropriate training of the workforce. The training for the workforce consisted of yearly text based training with a short quiz included in the training. This requirement satisfied the legal and compliance department but was not effective at preparing the employees for responding to the phishing attacks. The Security Skills Assessment and Appropriate Training to Fill Gaps (#9) critical control recommends as a quick win to deliver part of the training in person with the use of scenarios (Council on CyberSecurity, 2015). This format of training is interactive and effective at helping employees remember how to respond to relevant threats (Ponemon Institute LLC, 2014). This would have helped the ABC Datacenter Corporation employees to be more prepared to report the phishing attack instead of opening the attachment.

In addition to this, an online security awareness program sponsored by senior leadership should have been used to supplement or even replace the once a year training. This type of training consists of a set of online modules that is convenient for employees to take and easier to track from a technical perspective (SANS Securing The Human, 2015). The training could be given more than once a year and measured in terms of successful and unsuccessful responses to simulated attacks in the online modules. The endorsement of the security awareness program by senior leadership sets security

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

awareness as a priority for the organization as a whole. In the wake of the discovery of workforce susceptibility to the phishing attack, the leadership staff motioned to revamp security awareness training program as a high priority. Unfortunately, it took this bad experience to get the attention of senior executive leadership as is the case with many companies (Ponemon Institute LLC, 2015).

4. Conclusion

The critical controls have proven to be effective for organizations to defend and respond to cyber-attacks. This is evidenced by the continual reports, case studies, and successes reported by companies (SANS Institute, 2015). The ABC Datacenter Corporation began on the path to implement these controls but did so haphazardly. A more thoughtful and methodical approach was necessary to ensure that the critical controls would be properly planned for and implemented.

Careful planning and execution is possible by using the guidelines included in the Critical Controls (Council on CyberSecurity, 2015). The subcategories of each critical control contain specific guidelines that provide more than just installing security products, but instructions for administrators for implementing the critical controls the effective way. This would have been effective for the ABC Datacenter in reducing the attack surface area significantly and reduced the likelihood that attacks would have been successful.

The situation for the compromise of ABC Datacenter was even more challenging because the breach took place during a merger and transition of systems. Sub-par communications practiced at the project management level falsely set expectations that all customer data was protected. This facilitated the eventual creation of vulnerabilities that were used to compromise the network. These vulnerabilities were a main factor in the compromise of customer data cost the ABC Datacenter a loss of consumer confidence and revenue. Effective project management practices would have ensured accurate information was communicated to all stakeholders, appropriate risk decisions made and helped to prevent the attack vectors used to compromise valuable customer data.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Senior leadership needed to be more closely involved with the support and monitoring of the security awareness program of the workforce. The yearly paper exercise that ABC Datacenter employed was ineffective at preparing the workforce for the spear phishing attack. Relevant and interactive training that was tailored to the workforce, required on a more frequent basis and publically endorsed by senior leadership would have had a more significant effect at preparing employees to respond properly to the email attacks.

Companies must heed the guidelines for implementing the critical controls and ensure all levels of leadership have the appropriate level of engagement in awareness of risk posture of the network and employees in order to avoid the pitfalls that the ABC Datacenter Corporation fell into. The more organizations do to thoughtfully implement controls and enable the workforce with resources to be prepared against targeted attacks, the better the organization will be at defending their employees, customers, and valuable information from compromise.

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

References

Brink, D. E. (2012). *Endpoint Security: Anti-Virus Alone is Not Enough*. Boston, MA: Aberdeen Group.

Constantin, L. (2015). *Oracle patches already-exploited Java zero-day flaw, over 190 other vulnerabilities*. Retrieved from PCWorld website: http://www.pcworld.com/article/2948592/security/oracle-fixes-zeroday-java-flaw-and-over-190-other-vulnerabilities.html

Council on CyberSecurity. (2015). *The Critical Security Controls for Effective Cyber Defense v5.1*. Retrieved from http://www.counciloncybersecurity.org/critical-controls/

CyberSheath Services International, LLC. (2014). *The Role of Privileged Accounts In High Profile Breaches*. Retrieved from http://www.cybersheath.com/SiteMedia/CyberSheath/Whitepapers/CyberSheath_Privileged_Breaches.pdf

El Abed, W. (2009). *Mergers and Acquisitions: The Data Dimension*. Retrieved from Global Data Excellence Ltd. website: https://community.informatica.com/mpresources/docs/M&A_DataDimension_FINAL.pdf

Guerra, J., & Andrews, D. (2013). *Why You Need a Data Warehouse*. Retrieved from RapidDecision website: http://datalyticstechnologies.com/wp-content/uploads/2014/01/2013-03-Why-You-Need-a-Data-Warehouse.pdf

Hoffman, C. (2013). *Everything You Need To Know About the Blue Screen of Death*. Retrieved from How-To Geek, LLC website: http://www.howtogeek.com/163452/everything-you-need-to-know-about-the-blue-screen-of-death/

Hoffman, C. (2014). *Quickly Secure Your Computer With Microsoft's Enhanced Mitigation Experience Toolkit (EMET)*. Retrieved from How-To Geek, LLC website: http://www.howtogeek.com/190590/quickly-secure-your-computer-with-microsofts-enhanced-mitigation-experience-toolkit-emet/

© 2015 SANS Institute Author retains full rights.

© 2015 The SANS Institute Author retains full rights.

Infosecurity Magazine. (2012, June 28). 99% of attacks could be stopped by patching.*News*. Retrieved from http://www.infosecurity-magazine.com/news/99-of-attacks-could-be-stopped-by-patching/

Kirk, J. (2014, August 1). Microsoft security tool EMET 5.0 puts a leash on plugins. *PCWorld*. Retrieved from http://www.pcworld.com/article/2460640/microsoft-security-tool-emet-50-puts-a-leash-on-plugins.html

Mandiant. (2014). *Mandiant M-Trends Beyond the Breach* (2014 Threat Report). Retrieved from https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

McAfee. (2015). Email Phishing Awareness Quiz – McAfee. Retrieved from https://phishingquiz.mcafee.com/

Microsoft. (2014). Microsoft Support. Retrieved from https://support.microsoft.com/en-us/kb/2458544

Moag, J., & CDS Team. (2011). *Human Behavior and Security Culture*. Retrieved from Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth website: http://exec.tuck.dartmouth.edu/downloads/623/human_behavior_and_security_culture_ciso_workshop_overview.pdf

Ponemon Institute LLC. (2014). *Is Your Company Ready for a Big Data Breach? The Second Annual Study on Data Breach Preparedness*. Retrieved from https://www.experian.com/assets/data-breach/brochures/2014-ponemon-2nd-annual-preparedness.pdf

Ponemon Institute LLC. (2015). *2014: A Year of Mega Breaches*. Retrieved from http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf

SANS Institute. (2015). SANS Institute - Critical Security Controls: Guidelines. Retrieved from https://www.sans.org/critical-security-controls/guidelines

SANS Institute. (2015). SANS Institute - What Works Case Studies. Retrieved from https://www.sans.org/critical-security-controls/case-studies

SANS Securing The Human. (2015). Information Security Awareness Training | Metrics Resources. Retrieved from https://www.securingthehuman.org/resources/metrics

© 2015 The SANS Institute Author retains full rights.

© 2015 SANS Institute, Author retains full rights.

Sedgewick, A., Souppaya, M., & Scarfone, K. (2014). *Guide to Application Whitelisting* (SP 800-167 Draft). Retrieved from National Institute of Standards and Technology website: http://csrc.nist.gov/publications/drafts/800-167/sp800_167_draft.pdf

SolarWinds. (n.d.). SolarWinds Log & Event Manager. Retrieved from http://lem.demo.solarwinds.com/lem/

Symantec Corporation. (2014). *Internet Security Threat Report 2014* (Vol. 19). Retrieved from https://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf

The Home Depot. (2014). *The Home Depot Reports Findings in Payment Data Breach Investigation*. Retrieved from https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf

TrendLabs APT Research Team. (2012). *Spear-Phishing Email: Most Favored APT Attack Bait*. Retrieved from Trend Micro Incorporated website: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-spear-phishing-email-most-favored-apt-attack-bait.pdf

US-CERT. (2015). *Top 30 Targeted High Risk Vulnerabilities* (Alert (TA15-119A)). Retrieved from https://www.us-cert.gov/ncas/alerts/TA15-119A

Verizon Enterprise Solutions. (2014). *Verizon 2014 PCI Compliance Report*. Retrieved from Verizon website: http://www.verizonenterprise.com/resources/reports/rp_pci-report-2014_en_xg.pdf

Verizon Enterprise Solutions. (2015). *2015 DATA BREACH INVESTIGATIONS REPORT*. Retrieved from Verizon website: http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

Vijayan, J. (2014). *In rare move, banks sue Target's security auditor*. Retrieved from Computerworld website: http://www.computerworld.com/article/2489063/data-security/in-rare-move--banks-sue-target-s-security-auditor.html

© 2015 SANS Institute, Author retains full rights.

© 2015 The SANS Institute Author retains full rights.