The Nightmare on Cryptville Street: 20 Pills for a Night of Sleep

Oleg Bogomolniy

The Nightmare on Cryptville Street: 20 Pills for a Night of Sleep

GIAC (GSLC) Gold Certification

Author: Student Name, oleg.bogomolniy@gmail.com
Advisor: Toby Gouker
Accepted: 1/1/2016

(Faculty from institutions of higher education wishing to use this case study in class can write to the author at the above email address from their .edu address to request a copy of the case notes that accompany this case.)

Abstract

This paper uses a case study approach to help individuals learn about the Critical Controls for Effective Cyber Defense. By developing a scenario built around a ransomware incident, this case study is intended to be a context for students to use in applying the Critical Security Controls against one of the attack methods progressively used by cybercriminals in the past 5 years.

1. Background

According to Center for Strategic and International Studies, by the year 2014, cybercrime has grown into its own $400+ billion industry and has plenty of room for growing potential (2014). What used to be called "ethical hacking" has now evolved into lucrative hack-hunting business. Uncovering a zero-day vulnerability as part of Google Vulnerability Reward Program, as an example, can result in a reward of up to $20,000. Those, however, who can combine a zero-day vulnerability with an exploit may be selling it on the black market for US$25,000-$500,000 (Sims, 2014).

The influx in business revenue naturally leads to a faster evolution of the tools and infrastructure needed to support that trade. Along with new cybercrime tools aimed at finding and exploiting vulnerabilities, there has been an upsurge of new online services that tremendously ease up cybercrime logistics: Tor, Bitcoin, Russian Business Network, Silk Road (marketplace), TheRealDeal Market, and many others. Underground hacker markets are booming, a conclusion made by Dell SecureWorks research (2014), with counterfeit credentials, premium credit cards, online bank accounts, malware for sale; hacking services for hire, hacker tutorials, and even "100% satisfaction guarantee."

While the cybercrime business is thriving and cybercriminals keep reinventing methods of cashing out, the same cannot be said about the Information Security industry and those who choose the other side. With Advanced Persistent Threats (APT) and Distributed Denial of Services (DDoS) campaigns on one side, and with toughening cyber laws and information security regulations on the other side, has already caused enough nightmares to many Information Security professionals and their organizations. Adding to the mix, new sophisticated methods and tactics used by cybercriminals, nowadays can only add more sleepless nights.

What would it take to get a good, uninterrupted night of sleep? Fighting cybercrime in the virtual world or fighting organized crime in the real world is like eating an elephant. So how and where would we even start eating an elephant? One *bite* at a time, of course! Now let's look into "one *byte* at a time" approach, and how it may effectively help to protect many more *bytes* during just another night of sleep.

tgouker

2. Introduction

Mark Fishman is the leader of Information Security at the Asclepiads Services Corporation (ACS). Leading a team of six, Mark believes he is running a standard information security practice - nothing fancy, but nothing too small either. “Like many other castles,” as he usually likes to describe the concept of perimeter security to his colleagues, “mine is surrounded by the tall brick walls (i.e., Firewalls and IPS’s) with cast iron gates (i.e., Internet Proxy). Even if we are attacked by a million-man army (i.e., DDoS), they would first need to cross a mile-wide water trench that fronts the castle walls (i.e., DDoS Protection and Mitigation).” Inside the “castle”, too, there is hardly any lack of security measures: Endpoint Security suites on laptops, desktops, and servers; monthly cycles for security patches and software updates; Full Disk Encryption (FDE); Mobile Device Management (MDM); vigorous emails scanning for spam and malicious attachments; network segregation; centralized log collection and event correlation (SIEM); ongoing security awareness program, and you name it. However, many of those technologies were only recently deployed in the past few years. Just four years ago there were only two members in Mark’s team, Russell O’Donnell and Daniel Lee, who were crumbling under the workload they had to carry on their shoulders. ASC business management had a reactive approach to information security: it was considered to be more of an insurance policy, than a cost of doing business.

At that time ASC unveiled the plan to transition onto a new Enterprise Resource Planning (ERP) system (e.g., SAP, PeopleSoft, etc.), which was envisioned to be ASC’s segue into new business frontiers. Similar to home improvement projects of completely gutting out and rebuilding the interior of a house, ERP related projects can span over few year and cost millions of dollars. It requires revamping business processes to adhere to a specific ERP system. Mark knew right away: this would be his opportunity to justify much needed investment. First step was getting a buy-in from ASC’s head of IT, Ms. Christine Larkin, and the head of finance, Mr. Richard Czerwinski, both of whom had a great working relationship with Mark. “What do you envision to accomplish, Mark?” Christine asked at the meeting between three of them.

"Christine, you know our current security posture - there is barely any." Mark replied, "I recommend starting with a security risk assessment. We need to benchmark where we stand today vs. where we will need to be for adequately protecting the new ERP system. We can then agree upon a risk matrix as a road map of how we will be getting there."

Christine and Richard looked at each other, "And who will be doing this risk assessment?" Richard asked with grim face, "Please don't tell me you are planning to pitch one of those three-month engagements with $50K price tag."

"And how will we know what 'adequate security protection' will mean in a few years? Your risk matrix may change dramatically by the time the new ERP system is fully implemented?" Christine added.

"Mark, I don't see why we need to spend money to get to spend more money. I don't think the newly formed project management team, in charge of ERP migration, would understand it either," Richard explained his point of view, "Didn't you just say we only had a little security? Why can't we just assume we are ten percent secure? Or, twenty? You can work your way up from there."

"I have to agree with Richard," Christine said to Mark, "Now is not the time to spend money on comprehensive assessments and overwhelming risk matrixes. You can't afford to alienate the project management team. Say, I do remember a while back you presented a plan with security enhancements for IT auditors. Did you do any risk assessments then?"

"No, that was a regulatory audit. So I compiled a list of relative security risk controls from ISO 27000 standard and coupled it with the remediating solutions." Mark answered.

"Oh yes, I remember that one!" Richard agreed excitingly, "Mark, can you revise that plan and use it now? It will look familiar to most decision makers on the project management team."

tgouker

"That's an idea! Not the most optimal one, but definitely an idea." Mark replied.

In fact, the plan did work, and Mark was given the full range of security enhancements to explore. One by one, the ideas from Mark's wish list were finally coming true, including long awaited team expansion. A year later, Heather Grisson and then Richard Diaz joined the team, soon to be dubbed as the "Fantastic Four".

Russ O'Donnell was the original, lone member of the team. Joining ASC off the college over 10 years ago, Russ had been a "go to" person in IT, before he permanently settled into security role. Russ was on his own when a computer virus quickly spread across all user networks and rendered a half of ASC's desktop computers useless. Russ' patience gave way to his frustration. "You have to admit 'I told you so,' again, and again, and again!" Russ yelled at Christine angrily about his warnings of outdated antivirus technology, "Was I not screaming in your ears to upgrade the antivirus and to buy the centralized management console? For how long have I been begging to upgrade network switches and divide our big network into sections? How many more nights do I have to sleep here, in the office, while fixing these viral infections?" Though technically brilliant, Russ' short temper complicated the matter and pushed him further away from IT management. Shortly after the incident, Mark was hired into the management role.

Daniel Lee has been well known for his tough stance against sacrificing security in favor of convenience. "Let me see your key-chain," Daniel usually responds to questions about the necessity of complicated logons, "Do you use the same key for your house, your car, your storage, your safety deposit box, and all of your office drawers? I don't think so. What about the complexity of your keys? Would you settle for a paper clip to open your house locks? No? Why not? It's so much smaller, and it would be so much easier to replace if you lose it," Daniel would passionately argue.

Heather Grisson brought the expertise with the Internet Proxy and Intrusion Prevention System (IPS). Heather believed that most security solutions were reactive, and very little was being done to proactively combat evolving threats. "Look at the bad guys. First, they think with their heads – human intelligence, then they use technology to bring

their ideas to life – artificial intelligence. And what do we do? We use our artificial intelligence to react to their artificial intelligence. What about our human intelligence combating their human intelligence?" Heather reasoned. Consistently with her reasoning, she spearheaded DMZ honeypots and closely followed the Honeynet Project.

Richard Diaz joined the team to revive the security syslogging and monitoring project, which later turned into deployment of a Security Information and Event Management (SIEM) solution. His extensive knowledge of *nix systems made him an invaluable addition to the team.

Ashwani Khan and Samuel Lavner were accepted into ASC's Fellowship Program a year ago. As the newest members in the team, they have been enthusiastically learning from the rest and have been eager to prove their potential. Ashwani likes to compare himself to the 21st century Archimedes, as he often ambitiously shouts "give me a point in the universe and app for that, and I shall move the Earth."

In addition to his amicable team, Mark blatantly relies on a solid relationship with vendors, Value-added Resellers (VAR), or third party integrators within information security industry. Back in the days, Mark was shorthanded and mainly depended on third party contractors to help him with projects and day-to-day problems. Nowadays, Mark dedicates a large chunk of his and his team's time to sort through all the new and crafty solutions to ultimately satisfy his budgetary appetite and to keep the team busy.

Despite the healthy relationship with VAR's, Mark was confronted on a few occasions about weighing more confidence into the decisions made by "outsiders" over those made by his team. There was a concern among the team members about increasing dependency on main stream solutions and the time it was taking to deploy it. At the same time, there were many industry's niche players with innovative approaches. "That's why we need training, Mark!" Heather proposed, "The kind of training when we don't need to waste our time on learning the workarounds for broken product features that should have worked from day one. Such knowledge should come from VAR's."

tgouker

"Heather, you know the deal for justifying any training, and especially now." Mark replied, "You can check with our training provider for available courses. However, it has to be tied to one of your projects and it has to be measurable, as part of the performance management process."

"This conversation feels like a cliché chess game," Heather argued, "White pawn, E2-E4; black pawn, E7-E5. Mark, you know well that our current training provider, though top notch, only offers vendor specific courses."

Just as Mark was ready to respond, Russ took his turn, "Let me guess your next move, Mark. You are going to tell us about overall cost savings ASC realizes by negotiating all of the IT training needs with one training provider. Yes, we get it, but it really does nothing for us."

"We are long overdue for InfoSec specific training. Truly yours, Fantastic Four. Well, plus two, I guess" Daniel quickly summed it up.

"I bet one of you can anticipate my next move. That's when I am going to remind you about travel restrictions for attending training, and that you need to find training courses offered locally." Mark replied with a smile.

"Yes, it helps tremendously!" Russ replied with a sarcasm, "Now we can just zero-in on that one course, which matches all of these requirements."

"Even after the ERP migration is completed, we can't afford to be shorthanded. Would you be willing to attend a training class remotely, from the office?" Mark countered.

Heather swiftly looked at the others and enunciated their silent consensus, "The beggars can't be choosers."

tgouker

3. Fear of the dark

In the past 3 years ASC has invested millions of dollars into the ERP migration project. Dozens of consultants have been working around the clock and hand in hand with ASC's counterparts to make this transition as smooth as possible. With the "go-live" date just a few months away, everyone at ASC is at near boiling point. ASC's business management has made a significant investment into security enhancements: the security team headcount has tripled and the risk controls presented by Mark have been largely addressed. Their commonplace perception, logically, is that the level of financial investment should have drastically minimized the probability of a security breach. Now, without a comprehensive risk assessment, Mark finds few arguments to change this perception.

As the go-live date nears, Mark's mind is getting filled with the fear of a security breach. Noticeably, he starts micromanaging the team – an abnormality to his management style. The weekly team meetings are twice as long as before, because Mark wants to discuss all of the recent vulnerabilities in detail. He spends most of his time on his own, generating more and more reports off the SIEM, IPS, firewall, or antivirus management systems. He is often heard on the phone asking other parties about any recent encounters of unusual security events. Mark does not let his smart phone off his hands, as if it is glued to it, and he jumps to check every email alert. At night, Mark is afraid to fall asleep and to miss a critical alert. Even when asleep, his fears travel into his dreams. When the lights are dim and the moon shines bright, deep into his dreams Mark is haunted by security breach monsters. One night, it may be a nasty malware squid crippling ASC to the ground. Another night, it is a morning newspaper with a front page headline of: "Millions of credit card numbers, personal and health records silently escape ASC, experts confirm." While not certain if there are others who may be haunted by the very same nightmares, Mark is certain about thousands of others for whom security breaches have already become a reality. (Verizon Enterprise Solutions, 2015).

4. It is just a matter of *when*

Day 0 – Thursday, December 5, 2013

8AM. Mark gets to the office and is ready to settle for the morning coffee, when Heather walks into his office. Looking hyped up she says, "Morning Mark! I hope you've already had your coffee, because it may come handy."

"Good morning, Heather! I can tell. What's going on?" Mark replies.

"I just got off the phone with the Help Desk, and you are going to like this. Past Monday there was a viral alert from one of the laptops. It took them a while to get in touch with the user, because he was remotely working from home. When they finally did, he told them not to worry, because it had been taken care of."

"I guess there is more?" Mark asks with increased curiosity.

"Just a tidy bitty more. Last night, at about 9pm, there was another email alert about viral infection, but on a different laptop. Help Desk tried to contact the owner last night and this morning to no avail."

"Ok, do we know what kind of viral infection it was?" Mark asks.

"Well, that's where it gets interesting." Heather says, while trying to contain her calm, "Help Desk called me this morning, because both email alerts from Monday and Wednesday had to do with the same type of infection, but on two different laptops. Both instances were detected by our AV, but neither could be automatically remediated."

"Did they tell you what kind of infection it was? Anything to worry about?" Mark asks in anticipation of some bad news.

"Yes, it was Trojan.Ransomcrypt. I checked the AV management console to confirm."

"Hmm, doesn't ring a bell. Did you research it? How bad is it?"

"Yes, I had started researching it 15 minutes before you came in! And that's where the fun begins. It is a brand new ransomware; yes, another fancy 'ware' term. This one is called CryptoLocker and it stands for its name, because it encrypts the files on your hard drive. You want the decryption key? It could be yours for a mere $300, though the prices fluctuate. Not bad, ha? From what I've read so far, the initial infection vector is via email phishing. Luckily, it is not viral and is contained on the infected host. The amount of infections on the net, though, has been actively increasing for the past month."

"How many infected systems are there that have been reported so far? Only two laptops?"

"Yes, so far we know of only two infected laptops. Well, one laptop was supposedly fixed by the user, who's been working remotely from home this week; not sure how he fixed it, though. The other laptop is with its owner at the ERP meeting that started at 8am."

"If he is not screaming at us yet, it means he is working!" Mark interrupts.

"That's why I need you to talk to his manager, who can help me to get the infected laptop ASAP." Heather requests, "I tried to IM him, but he hasn't responded yet. I was planning to warn him about the possibility of losing his data. Then I realized he could cause unnecessary commotion. I will let you handle it through your channels."

"Yes, let me try his manager, first. You know how sensitive it gets if anyone assigned to the ERP project can't function. I have to run! I have back-to-back meetings this morning until 2pm, so let's have a follow-up meeting in my office right after. Meanwhile, please let the rest of the team know about this CryptoLocker, as soon as they get in. Ask Ashwani and Sam to get on the phone with AV support. Russ and Dee should start emailing other vendors' support engineers to see what they can do for us. Would be interesting to see if Rich can find anything in the logs. Please try to get to 'patient zero' - that user who's

working from home. We need to find out if it was CryptoLocker and what he did to get rid of it. I'm going to start drafting an awareness email we can broadcast to all users. Good thing I will be with Christine at my next meeting. It will save me some time by giving her a verbal update. Oh, and let the Messaging team know about that phishing email, that infects computers with CryptoLocker."

2PM. Mark comes back into his office, where his whole team has gathered to discuss the morning events. Right away, he senses something is not right. "I have to say I didn't expect to see everyone in here. What is the latest update?" Mark immediately gets to the point, "Did you retrieve the second infected laptop?

"Yes, we did get that laptop," Heather says, "but there is a bigger issue at hand here."

"What's the matter now? Do we have more infected system?" Mark asks in suspicion of the viral outbreak.

"We dug deeper into CryptoLocker," Russ chimes in, "and we are afraid it is much worse than we thought. It appears that many files on our shared network drive are also encrypted."

"What?" Mark exclaims, but tries to contain his anger, "How did that happen?" Mark asks more calmly.

"From what we've read so far, CryptoLocker only targets user files: pictures, Office docs, PDF's, that sort of stuff; it doesn't touch the Operating System." Heather explains, "All the CryptoLocker needs is the administrative access on the infected computer. It will then crawl through anything it can access from it: local drives, USB's, network drives… everything!"

"And how did we find out about the files on the network drive being encrypted?" Mark asks intently.

"We were overheard by the Data Storage team, when we were on the phone with AV support." Ashwani answers, "They have been trying to find the cause of the mysteriously sporadic data corruptions on Storage Attached Network (SAN) since past Monday."

"Since MONDAY?" Mark screams, as his patience is running out, "Holly…" he tries to outburst, but stops at the last moment and covers his face with his hands, "And they didn't bother engaging anyone from our team? Are we sure this is CryptoLocker related?"

"We asked them to check the user ID's, which were last used to modify those supposedly corrupted files. It matched the user ID's of the infected laptops' owners. So those mysterious corruptions were most probably encrypted files." Rich explains.

"Do we know how bad it is?" Mark asks anxiously.

"We are not certain, but preliminary we estimate terabytes." Rich adds, "I started running the audit report from all of the logs collected in the past 7 days. We should see what files on the shared drive have been modified by either of user ID's. The Data Storage team is running their scripts to accomplish the same."

"What about the backup SAN? Can we failover to it?" Mark proposes.

"They checked the backup SAN, but the replication process had already overwritten the original files with the encrypted ones. The backup tapes are our only viable option." Richard dismisses Mark's hopes for a quick solution.

"Beautiful… Anything from the vendors' support? What did the AV support say? How can we fix this?" Mark asks.

"AV support is doing their regular routine." Sam explains, "We tried to escalate the case, but still we need to do the whole nine yards of submitting the viral sample … blah, blah, blah. They are not treating CryptoLocker with any higher

priority than other infections. Or, maybe they are scared themselves and don't have the fix. We got more information about CryptoLocker form searching the net." Sam starts reading out loud:

We're very sorry to hear this happened… Of course, there is never any guarantee whatsoever that paying the ransom will unlock anything. More likely than not, paying the ransom won't accomplish anything other than fattening the pockets of the jerk or jerks that developed or deployed the malware. (Donohue, 2013).

Losing files completely is a terrible blow, but you can lose data in lots of other ways: a dropped hard disk, a stolen laptop or just plain old electronic failure… Here are five "top tips" for keeping safe against malware in general, and cyberblackmailers in particular: keep regular backups of your important files; use an anti-virus, and keep it up to date; keep your operating system and software up to date with patches; review the access control settings on any network shares you have, whether at home or at work; don't grant yourself or anyone else write access to files that you only need to read; don't give administrative privileges to your user accounts. (Ducklin, CryptoLocker ransomware - see how it works, learn about prevention, cleanup and recovery, 2013).

The encrypted files can essentially be considered damaged beyond repair. But if you have properly prepared your system, it is really nothing more than a nuisance… Here are a few tips that will help you keep ransomware from wrecking your day: back up your data…, filter EXEs in email…, disable files running from AppData/LocalAppData folders…, patch or update your software… (Myers, 2013).

"So it seems as everyone is scrambling to find a solution." Ashwani added, "Even if there is someone claiming to have the fix, there is someone else who has unsuccessfully tried it. Like Sam said, there may be no fix. Not for a while, at least. Here…" Ashwani reads out loud:

tgouker

Once the malware encrypts the data, although not impossible to decrypt, it is not practical given that the keys for each infection are different. Given that the malware signatures continually change; antivirus products have done little to mitigate the threat until it is already wide spread. (Westin, 2014).

"On a positive note," Daniel gets his turn to speak, "we did find some information about CryptoLocker logistics. Supposedly, the infected host needs to talk to CryptoLocker's mothership – their Command & Control servers, a.k.a. C2. That's how it acquires the encryption keys, which are unique for each infected computer. Ashwani and Sam found some posts on the Internet with a bunch of C2 IP's, and we blocked those inbound and outbound. It is far from a permanent fix, as there are probably more C2 servers out there. I am waiting for a call back from our Proxy support engineer. Hopefully, there is something in the CryptoLocker message to the C2 servers that we can permanently block in our Internet Proxy. I wish I could do this on my own."

"Good, good!" Mark replies to acknowledge he was paying attention. Although, it is clear to all that his mind is somewhere else, "Heather, were you able to get in touch with the 'patient zero'? We need to find what he did to fix his laptop."

"We suspect he may have paid the ransom." Heather answers, "I tried all means possible, except for physically going to his house and knocking on his door." At the same moment she catches the look on Mark's face, as if he may actually consider it as an option. She continues, "We should be more concerned about making sure that laptop is not connected to our network. What if it is still infected? Maybe we should disable his VPN credentials."

"That's good, that's good." Mark replies, as everyone is now staring at him and trying to determine what he is thinking about. He momentarily snaps out, "Yes, let's do that, let's disable his VPN. I will email his manager that I have authorized it." Mark says assertively to everyone's relief. He then continues, "Ok, let's regroup. Please escalate this case with all of our vendors to see if there

is any assistance they can offer. Let's keep our eyes on AV management console for any alerts. I will speak to the Help Desk manager to escalate anything unknown directly to me. I have to brainstorm this situation and start updating IT and business management. Christine gets off her meeting at 3PM, and must catch her in her office before she leaves for the next one."

3PM. Mark goes to talk to Christine Larkin in her office. He finds Christine there with Richard Czerwinski. "Come on in, Mark! I was just telling Richard about our morning meeting with the ERP vendor. I have a few minutes and then Richard and I need to be on another conference call. What's going on?"

"We have a situation on our hands," Mark then goes on to explain the situation.

"This is not good." Christine responds, "In fact, this is bad. This is really, really bad. Tomorrow will be the meeting of the Board of Directors. I can only imagine how far this breach may resonate. And it doesn't even seem to be a DDoS attack or an APT. Two incidentally infected laptops bring the multimillion-dollar project down on its knees. How can we possibly relay something like this to the business? I am surprised they haven't started calling us, yet."

"I don't get it," Richard engages in the conversation, "how could this possibly happen? You have the firewall, you have the antivirus, you have the monitoring systems, and you have all of that other security stuff you've always wanted. Are you telling me there was nothing that could have prevented this problem?"

"Mark, it is after 3PM and the clock is ticking. What is the plan?" Christine interjects.

"Based on the last DR exercise, it will take about 12 hours to restore the SAN from the backup tapes. That's in-line with our Recovery Time Objective (RTO). If we start tonight, the restore should be done by early morning." Mark proposes, "Since the first CryptoLocker alert came on Monday, it would the safest and

least risky to restore SAN from last Friday's backup. Unfortunately, today's work will be lost, too."

"That's a WEEK worth of ERP project!?" Richard exclaims, "We could have told business this morning not to save onto shared drive, couldn't we?"

"Mark, a week of data could be too drastic. Any 'Plan B'?" Christine counters.

"My team is working with the Storage to get the exact numbers of affected files." Mark explained, "The first infection occurred on Monday, following by the second infection on Wednesday. Since we haven't heard ERP team complaining, we can restore from Tuesday tapes. Then, tomorrow morning we will run the new reports and fish out any delta of infected files. Of course, we will need a crew from selective IT and business teams to work through the weekend and confirm this incident is completely contained."

"That plan sounds a lot more realistic!" Christine approved, "I will also need the postmortem from you by tonight. Please include recommendations of what needs to be done addressed for this problem not to repeat itself."

5. Conclusion

Mark Fishman, the Asclepiads Services Corporation, along with other characters in this story, are fictional. Nonetheless, the case study describes real-life events that took place in two unrelated organizations from dissimilar industries. Mark Fishman represents hundreds of thousands of others who came face to face with the gruesome reality of ransomware. Over half a million encryption keys were recovered, that had been used by CryptoLocker to hold victims' data for ransom. According to the U.S Department of Justice (2014), the Operation Tovar "disrupted a global botnet that had stolen millions from businesses and consumers as well as a complex ransomware scheme." The mastermind behind CryptoLocker, however, is at large (The FBI, 2015). CryptoLocker may be "dead", but its legacy is lived with CryptoWall – another generation of an evolutionary ransomware (The FBI, 2015a).

tgouker

Cybercrime businesses are thriving and cybercriminals keep reinventing new methods of cashing out. None of us can, singlehandedly, defeat an army of those who spread the evil across our cyber space. Nor a plethora of the technical solutions, on its own, can prevent a growing number of computer hacks: Target, Sony, White House, and many others. How can this evident gap be closed? This case study is going to look into a solution originally proposed by The Council on Cyber Security - a community (both, individuals and institutions) of independent information security experts committed to protect the open Internet. The Council created and adopted twenty critical security controls, which are now being supported and enhanced by the Center for Internet Security (CIS, 2015). These controls immensely help to prevent and to combat ransomware. If these controls had been adopted prior to CryptoLocker incident:

1. It would have helped Mark to justify for adequate investment into security enhancements;
2. It could have prevented the viral infection of two ACS laptops by CryptoLocker;
3. It would have drastically minimized the magnitude with which CryptoLocker encrypted the data on the ASC's shared network drive.

All you have to do, dear boys and girls, is to believe! Sweet, dreams…

tgouker

References

CIS. (2015, October 15). *The CIS Critical Security Controls for Effective Cyber Defense.* Retrieved from The Center for Internet Security: https://www.cisecurity.org/critical--controls.cfm

CSIS, McAfee. (2014, June). *Net Losses: Estimating the Global Cost of cybercrime.* Retrieved from Center for Strategic & International Studies: http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

Dela Cruz, J. (2013, October 11). *Threat Refinement Ensues with CryptoLocker, SHOTODOR Backdoor*. Retrieved from Trend Labs, Security Intelligence Blog, Thret News and Information Direct from the Experts: http://blog.trendmicro.com/trendlabs-security-intelligence/threat-refinement-ensues-with-crypto-locker-shotodor-backdoor/

Dell SecureWorks. (2013). *CryptoLocker Ransomware*.

Dell SecureWorks. (2014, December). *Underground hacker markets are booming.* Retrieved from Dell SecureWorks: http://www.secureworks.com/assets/pdf-store/white-papers/wp-underground-hacking-report.pdf

Donohue, B. (2013, November 11). *CryptoLocker is Bad News*. Retrieved from Kaspersky Lab Daily: https://blog.kaspersky.com/cryptolocker-is-bad-news/3122/

Ducklin, P. (2013, October 18). *CryptoLocker ransomware - see how it works, learn about prevention, cleanup and recovery*. Retrieved from Naked Security, Award-winning computer security news from Sophos: https://nakedsecurity.sophos.com/2013/10/18/cryptolocker-ransomware-see-how-it-works-learn-about-prevention-cleanup-and-recovery/

Ducklin, P. (2013a, Ocober 12). *Destructive malware "CryptoLocker" on the loose – here's what to do*. Retrieved from https://nakedsecurity.sophos.com/2013/10/12/destructive-malware-cryptolocker-on-the-loose/

Dunn, J. E. (2014, February 7). *Cryptolocker scrambles US law firm's entire cache of legal files*. Retrieved from TechWorld: http://www.techworld.com/news/security/cryptolocker-scrambles-us-law-firms-entire-cache-of-legal-files-3501017/

FBI. (2011). Department of Justice Disrupts International Cyber Crime Rings Distributing Scareware.

Goodin, D. (2013, October 17). *You're infected—if you want to see your data again, pay us $300 in Bitcoins*. Retrieved from Ars Technica:

tgouker

http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/

Google Vulnerability Reward Program (VRP) Rules. (n.d.). Retrieved from Google Application Security: https://www.google.com/about/appsecurity/reward-program/

Honeynet Project. (n.d.). Retrieved from The Honeynet Project: https://www.honeynet.org/

International Organization for Standardization. (n.d.). *ISO/IEC 27002:2013 Information technology -- Security techniques -- Code of practice for information security controls*. Retrieved from http://www.iso.org

Jarvis, K. (2013, December 18). *Dell SecureWorks*. Retrieved from CryptoLocker Ransomware: http://www.secureworks.com/cyber-threat-intelligence/threats/cryptolocker-ransomware/

Krebs, B. (2014, June 2). *'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge*. Retrieved from Krebs on Security. In-deapth security news and investigation: http://krebsonsecurity.com/2014/06/operation-tovar-targets-gameover-zeus-botnet-cryptolocker-scourge/

Longstaff, T. (1989). *Information about the PC CYBORG (AIDS) trojan horse.* Retrieved from THE COMPUTER INCIDENT ADVISORY CAPABILITY: http://www.securityfocus.com/advisories/700

Merriam-Webster Dictionary. (n.d.). *Definition of ransomware*. Retrieved from Merriam-Webster Dictionary: http://www.merriam-webster.com/dictionary/ransom

Myers, L. (2013, December 12). *11 things you can do to protect against ransomware, including Cryptolocker*. Retrieved from We Live Security, Security news, views and insight from the ESET experts: http://www.welivesecurity.com/2013/12/12/11-things-you-can-do-to-protect-against-ransomware-including-cryptolocker/

Nachreiner, C. (2013, November 4). *Everything You Wanted to Know About Cryptolocker*…. Retrieved from WatchGuard Security Center Everything you need to take threats head on : http://watchguardsecuritycenter.com/2013/11/04/everything-you-wanted-to-know-about-cryptolocker/

Ransom:Win32/Crilock.A. (2014, August 14). Retrieved from Malware Protection Center: http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Trojan%3AWin32%2FCrilock.A&ThreatID=-2147284168

tgouker

Russinovich, M. (2013, 01 07). *Hunting Down and Killing Ransomware*. Retrieved from Mark Russinovh's Blog: http://blogs.technet.com/b/markrussinovich/archive/2013/01/07/3543763.aspx

Sims, S. (2014). Introduction to IDA Pro and Debugging. *Cyber Defense Initiative.* Washington, D.C.: SANS.

The Critical Security Controls for Effective Cyber Defense. (2014). Retrieved from Council on Cybersecurity: www.counciloncybersecurity.org

The FBI. (2015, August). *Cyber's Most Wanted, Wanted by the FBI*. Retrieved from The FBI: https://www.fbi.gov/wanted/cyber/evgeniy-mikhailovich-bogachev/view

The FBI. (2015a, June 23). *Criminals Continue to Defraud and Extort Funds from Victims Using CryptoWall Ransomware Schemes*. Retrieved from Federal Bureau of Investigation, Public Service Announcement: http://www.ic3.gov/media/2015/150623.aspx

TrendMicro. (2006, March 14). *Ransomware! Ransomware! Ransomware!* Retrieved from Security Intelligence Blog, Thret news and Information Direct from the Experts: http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware21-ransomware21-ransomware21/

TrendMicro. (2012). *Ransomware*. Retrieved from Definition: http://www.trendmicro.com/vinfo/us/security/definition/ransomware

U.S. Department of Justice. (2014, June 2). *U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator*. Retrieved from The Federal Bureau of Investigation: https://www.fbi.gov/news/pressrel/press-releases/u.s.-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware-charges-botnet-administrator

Verizon Enterprise Solutions. (2015). *2015 Data Breach Investigations Report.*

Westin, K. (2014, January 24). *New CryptoLocker Ransomware Variant Spread Through Yahoo Messenger*. Retrieved from TripWire, The State of Security: http://www.tripwire.com/state-of-security/vulnerability-management/new-cryptolocker-variant-spread-yahoo-messenger/

Yung, A. (1996). Cryptovirology: extortion-based security threats and countermeasures. *Security and Privacy, 1996. Proceedings., 1996 IEEE Symposium on* (pp. 129-140). Oakland, CA: IEEE.

Zeltser, L. (2015, March 17). *Scammers Prescreen Victims for Tech Support Scams via Twitter and Phone*. Retrieved from Information Security in Business: https://zeltser.com/prescreening-tech-support-scam/

tgouker

Last Updated: February 23rd, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Zurich February 2020	Zurich, CH	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Jacksonville 2020	Jacksonville, FLUS	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Manchester February 2020	Manchester, GB	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS Secure Japan 2020	Tokyo, JP	Mar 02, 2020 - Mar 14, 2020	Live Event
Blue Team Summit & Training 2020	Louisville, KYUS	Mar 02, 2020 - Mar 09, 2020	Live Event
ICS Security Summit & Training 2020	Orlando, FLUS	Mar 02, 2020 - Mar 09, 2020	Live Event
SANS Northern VA - Reston Spring 2020	Reston, VAUS	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Munich March 2020	Munich, DE	Mar 02, 2020 - Mar 07, 2020	Live Event
SANS Jeddah March 2020	Jeddah, SA	Mar 07, 2020 - Mar 12, 2020	Live Event
SANS St. Louis 2020	St. Louis, MOUS	Mar 08, 2020 - Mar 13, 2020	Live Event
SANS Paris March 2020	Paris, FR	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Dallas 2020	Dallas, TXUS	Mar 09, 2020 - Mar 14, 2020	Live Event
SANS Prague March 2020	Prague, CZ	Mar 09, 2020 - Mar 14, 2020	Live Event
Wild West Hackin Fest 2020	San Diego, CAUS	Mar 10, 2020 - Mar 11, 2020	Live Event
SANS Doha March 2020	Doha, QA	Mar 14, 2020 - Mar 19, 2020	Live Event
SANS Norfolk 2020	Norfolk, VAUS	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS SEC504 Nantes March 2020 (in French)	Nantes, FR	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS San Francisco Spring 2020	San Francisco, CAUS	Mar 16, 2020 - Mar 27, 2020	Live Event
SANS Secure Singapore 2020	Singapore, SG	Mar 16, 2020 - Mar 28, 2020	Live Event
SANS London March 2020	London, GB	Mar 16, 2020 - Mar 21, 2020	Live Event
SANS Kuwait March 2020	Salmiya, KW	Mar 21, 2020 - Mar 26, 2020	Live Event
SEC588 Beta One 2020	Arlington, VAUS	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS SEC560 Lyon March 2020 (In French)	Lyon, FR	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Oslo March 2020	Oslo, NO	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Madrid March 2020	Madrid, ES	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Seattle Spring 2020	Seattle, WAUS	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Secure Canberra 2020	Canberra, AU	Mar 23, 2020 - Mar 28, 2020	Live Event
SANS Abu Dhabi March 2020	Abu Dhabi, AE	Mar 28, 2020 - Apr 02, 2020	Live Event
SANS Philadelphia 2020	Philadelphia, PAUS	Mar 30, 2020 - Apr 04, 2020	Live Event
SANS FOR585 Rome March 2020 (In Italian)	Rome, IT	Mar 30, 2020 - Apr 04, 2020	Live Event
SANS Frankfurt March 2020	Frankfurt, DE	Mar 30, 2020 - Apr 04, 2020	Live Event
SANS 2020	Orlando, FLUS	Apr 03, 2020 - Apr 10, 2020	Live Event
SANS Secure India 2020	OnlineIN	Feb 24, 2020 - Feb 29, 2020	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced