Cyber Security: Update

www.staysafeonline.org

1

Case Study 1… SC lessons learned

- On August 13 2012 a spam email was sent out to a number of entity employees, and someone clicked on the email to open it
- Once opened and clicked upon the embedded link the malware loaded unbeknownst to the reader
- The users credentials were then compromised and sent back to the hacker
- Hacker using the citrix portal for the state, used the stolen credentials to remote login
- Hacker probed and meandered around the network loading more malware and password monitoring and grabbing programs
- Mapping and discovering the network the hacker learned all the users and servers in domain
- On Sept. 12th 2012 he stubble onto the backup databases for the Dept. of Revenue
- Using user credentials and machines inside the state's network the hacker took 2 days to copy the entire tax databases, over 73 GB!
- The assault was over at this point, but the damage was yet to begin.

2

Case Study 1… The Attack on SC Dept. of Revenue

- ~ 4,000,000 individual records; over 700,000 Business records and over $45,000,000 spent and counting
- On October 10th The Secret Service Notified the state of the breach through detections of identity breach activities
- Lesson one: DOR only invested in perimeter breach protections, firewalls… nothing was monitoring activity within their domain and across there networks
- Lesson two: Attacker was accessing servers and databases and files from weird and arbitrary access point, moving and manipulating data
- Lesson three: Sarbanes-Oxley (SOX) Act requires and holds top officials and senior management directly responsible for accountability for data and financial information, the axe fell on the director of DOR
- Lesson four: Staff needs to be trained on Cyber security and management needs to appropriate funding to properly protect the enterprise with an "onion affect" security architecture.
- Lesson five: Rigid password policy enforcement, Role based access control

3

Case Study 2…
City of Conway Breach

- On 9/11/2013 the City of Conway was hit by a intrusion into their network.
- Someone in the public utilities opened a malicious email and clicked on a Google ad link inside the email, loading and launching the Zeus Trojan virus
- The Zeus Trojan is a particularly aggressive virus that used for numerous intrusion tasks including: form and file grabbing, keystroke logging and to install cryptoLocker ransomware
- The Trojan began pushing itself out and causing a alert through the ISP provider to black list the City (Turn off internet services because of malicious activity)
- The State security Office who manages the City's IDS detected the activity and it looked like it infected the City's Domain Controller server
- Alerts were sent out and all city services were suspect, SLED was notified and began CJIS investigation which was then turned over to the FBI for investigation
- The next day the FBI arrived at the City and confiscated all city servers and removed them back to Columba for forensic analysis
- The entire city was without Computers, no electronic control system, no records --- they had to roll back to a manual paper system to conduct any city business!

4

Case Study 2…
City of Conway Breach

- The IT department had to deal with all the turmoil of the investigation and disruption of all city services, and had payroll to get out within 5 days!
- There was an amazing effort to rebuild the payroll servers from scratch and backup records so the city would not miss payroll
- 5 days after confiscation the FBI returned all the equipment to the City for them to put back together and into service; it took IT 4 days to reassemble the mess created
- The end results were that only the laptop was infected and had to be rebuild and cleaned; the city's infrastructure and security measures worked, even though the initial view was a false positive and disrupted all city services for over two weeks.

5

Case Study 2…
City of Conway Breach

- Lesson one: have your cyber insurance policy and know how to enact it; without it the City of Conway would have been much worst for the wear
- Lesson two: Make sure your backups are up to date and not stored on the same machines they are backing up!
- Lesson three: Make sure your organization understands how single sign-on manifests itself inside your organization and document that for the forensics teams
- Lesson four: Have provisions for backup/ redundant servers and especially the domain server
- Lesson five: Have redundant security layers (remember the onion philosophy)
- Lesson six: Help your IT department champion the necessary security funding, redundancy funding and spares funding; you will save money if you have an even like this one!

6

Thank You.

And remember

STOP, THINK and CONNECT!

Vince.Simonowicz@CityofRockHill.com

7