5/11/2014

Applying Defensive Cyber Operations (DCO) Lessons Learned to Critical Infrastructure Operations Management

Ken Foster, CISSP, DCO Ops Manager

Contents

Cyberspace has become a dangerous place. In the not so distant past, a firewall and good anti-virus was all that was required to keep most bad actors at bay. Today, highly sophisticated malware engines allow bad actors with reduced skill sets the ability to custom blend exploit code into targeted attacks that signature-based anti-malware solutions rarely detect upon initial deployment. This has lead to a security subculture where a constant battle exists between Whitehat's and Blackhat's. While there is no official scoreboard, most security professionals will privately acknowledge the dark forces have the upper hand. This is exacerbated by the applicable truism that "the bad guys only have to be lucky once, but the good guys have to be lucky every time". These are daunting odds in the cat and mouse game of cyber defense.

Issue:

Cyber Defensive Operations (DCO) can be defined in general terms as the management of cyberspace risks through enhanced situational awareness, application of Information Assurance measures, and increased resiliency of critical network operations. DCO is implemented as a holistic approach to knowing what is happening at the packet level on a defended network and taking a Defense-in-Depth layered approach to inhibiting suspicious activities. This approach consists of people, processes, and technologies that must be dedicated to these efforts. An event log, never reviewed is a waste of bits as evidenced in the 2013 Target data breach. As long as Zero-day exploits exist and users continue to open emails from untrusted sources, the risk can never truly be prevented (figure 1). Implementing true DCO measures are often expensive and complicated to implement. Senior management often applies risk modeling and transference measures (e.g. insurance policies and outsourcing) as a method of risk avoidance. This process appears cost effective on paper but far too often fails to factor the true and sometimes intangible cost related to lost confidence, public relations efforts, legal fees, and lost customers that result from an actual manifestation of those risks. According to the 2013 Ponemon Institute Data Breach study, the average cost in the United State for a data breach is $188 per record and assumes the per records losses at reduced costs due to cost averaging and bulk purchases of mitigation related actions, artificially lowering the per record cost [1].

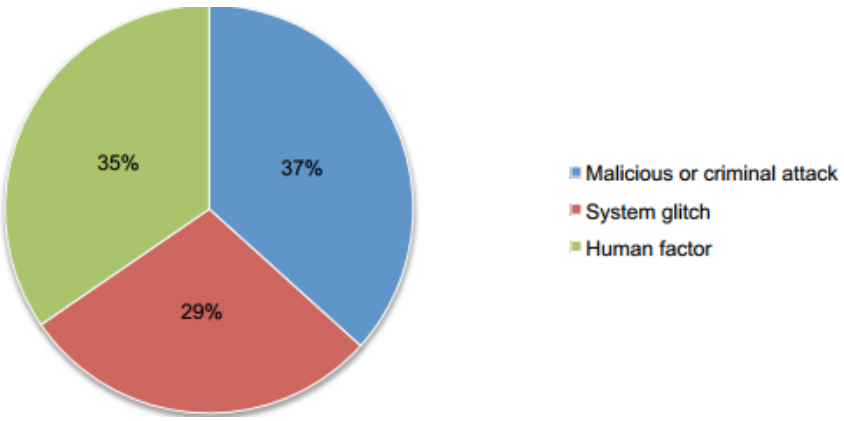

Figure 1. Ponemon Institute 2012 Data Breach Root Cause Distribution [1]

Risk:

One method to gage risk is to benchmark previous trends as future indicators. According to the 2014 Symantec Internet Security Threat Report, Issue 19 [2], there are some very sobering statistics to consider. One in eight websites (many legitimate) on the internet have at least one critical vulnerability. One in every 392 emails received is characterized by some sort of phishing attack indicator. Finally, the most chilling of these statistics is a 91% uptick in targeted attacks were reported in 2013. Spear phishing remains the top means of network initial entry, with Government and Professional Service providers holding the highest rates in 2013 (figure 2).

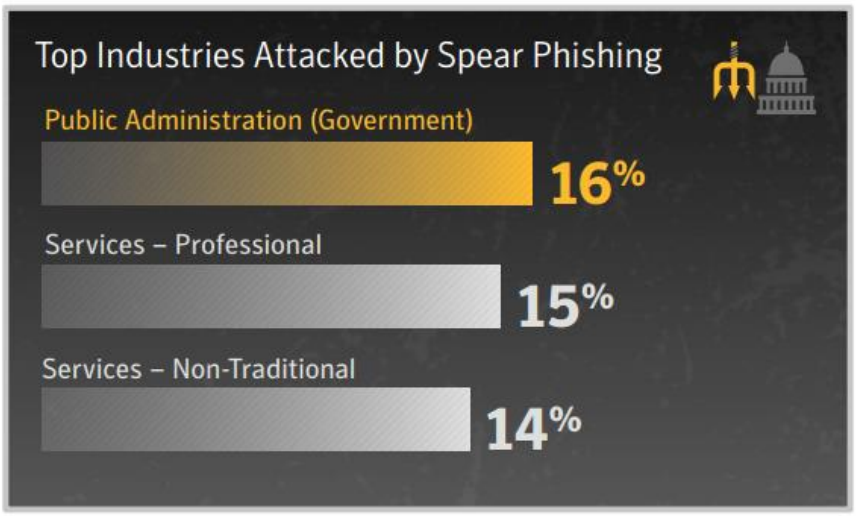

Figure 2. Symantec 2014 Internet Security Report – Spear Phishing Target Leaders [2]

The picture gets bleaker when considering that only nine percent of cybercrime and one percent of cyber Hacktivist breaches were discovered by internal network security personnel [3]. Of those breaches discovered, 85% were discovered in less than a week while the remaining took months or more to detect. By using the lens of hindsight, it become apparent that many of these breaches could have been detected earlier or possible prevented if the proper application of a Defense-in-Depth approach coupled with better monitoring of network logs and artifacts had been implemented.

Mitigation:

A sound mitigation strategy must consider 3 core facets as part of a complete and mutually supportive solution:

- People:
  - Users: Users represent the single largest target for compromise on networks. Organizations must train users' on proper cyber hygiene. This training must be developed to be both engaging and deeply integrated into the organizational culture. If training is viewed as a box to check annually, then change is required.

- C-Level Executives: These organizational members must understand they are a constant target, have access to highly sensitive materials, and must receive additional training. C-Level members must know how to rapidly spot potential threats, know what to do, and how to report these attempts to cyber security.
- Administrators / Privileged Users: We must develop a culture of knowing what 'Right' looks like. These staffers must enforce a separation between their privileged credentials and user identity's. These users should always logon as standard users and only privilege escalate to perform specific approved functions, thus inhibiting the ability of malware and exploits to gain root / administrative level access over compromised systems. Performing functions such as recreational web surfing or checking email (internal or external) should never be accomplished while logged on with privileged credentials.
- Cyber Security Professionals: These personnel must receive constant, relevant training and be afforded the opportunity to attend lectures, conferences, and training sessions both virtually and in person in an effort to stay up to date on trends, techniques, and practices for defending the organizations network and resources. Whenever possible organizations should encourage these personnel to participate in table top exercises, provide support to other organizations during an incident, and participate in working groups related to cyber security. Practice and experience are crucial elements to an effective response. These types of opportunities increase the organizations incident response personnel's ability to performing more efficiently.

- Technologies:
  - Firewalls: No organization should be without a firewall. Many smaller organizations have outsourced their firewall management. Regardless of who manages these resources, when was the last time a best practices audit was conducted on the rules? Are insecure protocols or ports allowed; can they be migrated to secure versions? Who requested the rule; are they still required? These important questions should be address no less than annually.
  - Intrusion Detection System (IDS) / Intrusion Prevention Systems (IPS): It is a best business practice to monitor the organization's internal network with some sort of intrusion analysis process. There are two key difference between and IDS and an IPS. The first is an IPS allows for the automation of mitigation measures upon anomaly detection, while and IDS logs and reports the incident for human review and follow-up. The second is cost; quality IPS's are orders of magnitude more expensive when compared to an IDS. This primarily has to do with the processing power necessary to inspect, analyze, and apply an action algorithm to each packet passing through the device in near real-time. If the organization cannot afford a robust IPS implementation, do not underestimate the value of a well-placed IDS sensor array.
  - Proxies: Every point of ingress and egress is a potential avenue for network penetration by an attacker. Proxies provide application specific protections, increasing both the organizations ability to protect their users, but also as a method to logically enforce policies. Consider a web proxy. This device can obviewscate internal user IP

addresses while preventing web access to undesirable sites, known malicious pages, and potential drive-by malware.

- Security Information and Event Management (SIEM): In organizations that have deployed a Defense-in-Depth architecture, one of the greatest difficulties is event correlation. For instance, if an apache web server exploit is received by a Microsoft Exchange server, the impact is likely negligible. However, if it's received by an HP Printer, then there may be cause for concern since the device hosts an internal web server. With so many log sources, dashboards, and alerts to comb through, this is often a daunting task for cyber security professionals. One way to get the most from these tools is through the integration of a Security Information and Event Management (SIEM) appliance. A SIEM uses artificial intelligence to analyze the organizations connected logs, alerts, and tools and weights the collected events, allowing the security administrators to focus on the most critical issues first.
- Anti-Malware: This classification of software includes anti-virus, host-based firewalls, ad/spyware detection, and root kit detection. It is a best practice to ensure an organization implements an enterprise anti-malware solution. This provides a centrally managed console to collect infection information, detect outbreaks, and ensure signature and base application updates are accomplished. It is also recommended you deploy a different anti-virus solution on your servers than is on your clients. While more costly and complicated to manage, this practice increases the chances of an outbreak detection by applying two different signature engines to your network.

- Policies:
  - Governance: This topic is broad reaching and includes regulatory and organizational imparities designed to protect the network and its resources. Most U.S. government agencies and many states have adopted the National Institute of Standards and Technology (NIST) guidelines. It is important to remember, they these guidelines are a one size fits all solution; additional guidance from the C-level staffs are required to achieve true security and compliance.
  - Best Business Practices (BBP): It goes without saying that those institutions known in the cybersecurity community as leaders are generally qualified to publish industry best practices. Examples of BBP's to consider as core tenants of an organizational cybersecurity solution include the SAN's Top 20; Microsoft Enterprise Security Best Practices; and NIST 800-14.
  - Resilience Auditing: There is a significant gap between theory and practice. In military jargon the saying goes "No good plan survives initial contact". Just like in battle, SOP's and Recovery Plans need to be tested, even if only incrementally. Far too often SOP's and plans are developed based on best case scenarios and almost always require multiple test and review cycles until a solid product is produced. Ensure you attempt to build flexibility into the plan wherever possible. The best plans include provisions for multiple shifts. An exhausted administrator configuring a critical server is a whole new disaster waiting to happen. Another factor to consider is where are your resiliency plans and resources located? Would they truly be accessible if the entire regions telecommunication network when down or a natural disaster caused

your facility to become physically unreachable? What about personnel; does the plan assume a percentage of key staff may be unable to response to the incident because they are adversely affected by the same event? The time to find out the plan doesn't work is not in the middle of a disaster response.

- Incident Response: Organizations should embrace incident response as an opportunity to take back the control of their data and resources lost to the incident. However, it's most important that cool heads prevail. Considerations pertaining to evidence, data breach, liability, recovery, reporting and disclosure, and executive briefings must be addressed in every phase of this operation. Rushing to recovery can cause clean back-up tapes to become infected or critical evidence of a breach and its impacts to be lost. Ensure everyone knows their role, boundaries, and works a step by step checklist to ensure nothing is missed. Separate C-Level staffs from the incident responders; they only add stress to an already stressful situation. Ensure an IR counsel if formed as soon as the incident is verified. Don't forget to include your Legal, Public Relations, and Operations Manager in the counsel. Decisions are often made on the fly. Ensure a scribe is present at all meetings to document when new details are first discovered, any decisions made, whom authorize the decision, and establish a general time line for the incident. This information will become critical once the incident is under control.

Applying Incident Response Lessons Learned:

Without going into too much detail, I recently attended a large scale Incident Response (IR) exercise. In this exercise, each team was allowed to use a host of tools to detect the attempted and successful presence of rouge devices on internal networks, unexpected processes on servers, data exfiltration attempts, and theft of administrative credentials through the presence of key loggers and backdoor malware exploits. Each evening, the team conducted an informal session to identify lessons learned. Provided below is a summary of exercise lessons that can be applied universally:

- Documented Baselines are Crucial: Its orders of magnitude more difficult to detect anomalous behaviors if you don't know what normal looks like. Document processes, user accounts, and approved applications on systems; archive them for later referral. It's also helpful to hash system directories in case suspect binaries are later detected. This will help you identify suspect files renamed to hide their true malicious intent.
- Tool Familiarity: Ensure organizational incident responders are familiar with the tools they are expected to use, ensure them access to known good installation media and licenses, have a well-documented SOP in hard copy, and ensure they have experience with the tools deployment and reconfiguration. To ensure the team's success, cross-train personnel on the use of these tools should sustained operations or the loss of a key team member occur during the incident. At a minimum be prepared to review logs (e.g. syslog and local system / device), review processes on systems in real-time, hash files, monitor IDS/IPS events in real-time, monitor for rouge devices, collect live memory dumps from systems, and detect changes in user accounts / permissions on hosts and domains controllers.
- Incident Response Leader: There is only one Incident Response Leader! They must be empowered to execute and not unduly influenced or distracted by management. Management

must be kept separate from the incident response cell, they were selected and training to perform this role; distractions add to stress and missed events.

- Robust Communications: Incident responders need to operate as a team. This team must communicate dynamically with each other to identify indicators of inter-related events. When a potential event is detected, it should be called out to the other team members and the leader. This type of dynamic real-time information collaboration is key to the response. The team must train to work in this type of dynamic environment.
- Document Everything: One individual on the response team must be dedicated to documentation. This establishes a time line of events, documents possible attacking IP addresses, and identifies anomalous binaries located on systems. Without this documentation, responders will duplicate efforts, lose valuable time, and remediation's will be incomplete.
- Well-Placed Sensors: During an incident, situational awareness of the network and potential anomalies is important. It can mean the difference between detection and a missed indicator. Have hardware and network tap capabilities either in place or available to deploy to critical network segments. Becoming familiar with open source IDS and SIEMS tools such as Security Onion [4] can make all the difference in your response.
- Collaboration is Critical: The situational awareness collected by the Incident Response Team must be shared with the Operations staff, C-Level management, 3rd party vendors (when appropriate), Regulators, and Law Enforcement. It would be arrogant to assume your network is the only one who is / has sustained this type of incident. Prior lessons learned and providing appropriate situational awareness to others can prevent larger attacks from manifesting. Assign someone the role of cyber intelligence coordinator. Have them establish relationships in advance with the State Information Security Office, MS-ISAC, US CERT, local/State Law Enforcement cybercrimes, FBI, and DHS cyber to ensure open lines of communications can be established if needed.
- Evidence Collection Trumps Remediation: Often in the heat of an incident, a responder will power off a suspect computer or block an IP in the firewall before collecting any artifacts for later law enforcement analysis. This is a mistake! Forensics analysis of the packets, RAM, and deposited files are crucial in determining the motives, methods, and potentially the identities of the intruders. Failing to properly collect this evidence almost certainly ensures an intruders methods and intent will never truly be known, nor their identities ever determined.

References:

[1] Ponemon Institute, "2013 Cost of Data Breach Study," May 2013. [Online]. Available: https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf. [Accessed 11 May 2014].

[2] Symantec Inc., "Internet Security Threat Report 2014," April 2014. [Online]. Available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. [Accessed 11 May 2014].

[3] Verizon Inc., "2014 Data Breach Investigations Report," 2014. [Online]. Available: file:///C:/Users/Ken/Downloads/rp_Verizon-DBIR-2014_en_xg.pdf. [Accessed 11 May 2014].

[4] D. Burks, "Security Onion," nd. [Online]. Available: http://blog.securityonion.net/p/securityonion.html. [Accessed 11 May 2014].