UNDERSTANDING AND ANALYSIS OF CYBER THREATS

MARCHENKO M.V.
National Aviation University, Kyiv
Supervisor – Martyniuk H.V., PhD, Associate Professor

A threat could be anything that leads to interruption, meddling or destruction of any valuable service or item existing in the firm's repertoire. Whether of "human" or "nonhuman" origin, the analysis must scrutinize each element that may bring about conceivable security risk.

Cyber threat analysis is a process in which the knowledge of internal and external information vulnerabilities pertinent to a particular organization is matched against real-world cyber attacks [1]. With respect to cyber security, this threat-oriented approach to combating cyber attacks represents a smooth transition from a state of reactive security to a state of proactive one. Moreover, the desired result of a threat assessment is to give best practices on how to maximize the protective instruments with respect to availability, confidentiality and integrity, without turning back to usability and functionality conditions.

For today threat analysis is viewed as a process with some components: scope, data collection, threat/vulnerability analysis of acceptable risks, mitigation and anticipation.

Scope. Scope gives info on what is included and what is not in the analysis. In terms of cyber security, items under consideration are those that must be protected [2].

Data Collection. Amassing detailed information about real cyber incidents (e.g., URLs to malicious links, phishing email header and content, and uncovered hostile Command and Control (C2) infrastructure of domain names and IP addresses) is the first step. The focus should fall on targeted threats existing in reality, and scope settings need to filter out those perceived as such but not real, which can merely distract your attention from other ongoing security affairs [3].

Threat/Vulnerability Analysis of Acceptable Risks. Here is being gathered to determine the level of current exposure — most of all — whether the current defenses are solid enough to neutralize information threats in terms of availability, confidentiality and integrity. This part should include as well an evaluation of whether the existing procedures, policies and security measures are adequate. Vulnerability analysis also encompasses penetration testing, which in turn seeks to acquire something valuable from the adversary's arsenal like a classified document, code or password [4].

Mitigation & Anticipation. When all previous steps are completed, a competent security analyst can use this corpus of threat data to arrange in groups activity patterns of close similarity, and promptly implement mitigation measures, and anticipate the emergence of similar cyber attacks in the future[5].

During the first power outage related to the cyber attack, Russian hackers caused power disconnections in several regions of Ukraine. The actors used spear phishing to plant BlackEnergy3 malware, which was used to disable control system computers. As a result, the utilities relied on manual efforts to restore power.

Ukrainian power companies are not unique in their control systems technology or vulnerability to cyber attack.

How can Ukraine protect itself? Author think, that Ukraine can protect itself using following steps.

Review security architecture. Experienced and qualified security professionals should regularly review network architecture including VPN configuration, firewall placement and rules, and router access control lists[6].

Enhance network security monitoring capability. Robust log collection and network traffic monitoring are the foundational components of a defensible network. Failure to perform these essential security functions prevents timely detection, pre-emptive response, and accurate incident investigation[7].

Search for Indicators of Compromise. With network security monitoring capability in place, automated tools can alert security analysts and process operators when anomalous behavior or malware is identified in your environment[8].

Review Incident Response Plans. The plans should cover response protocols for realistic scenarios such as the wiper malware seen the Ukraine attacks[9].

Most of all, organizations should remember that not performing a threat and risk analysis will leave them open to cyber pests that can damage their business for good.

References:

1.Apple Inc. Risk Assessment and Threat Modeling. Retrieved on 07/08/2014 from https://developer.apple.com/library/ios/documentation/Security/Conceptual/Security_Overview/ThreatModeling/ThreatModeling.html

2.Cyber Squared Inc. Cyber Threat Analysis, not just for the Military. Retrieved on 07/08/2014 from http://www.cybersquared.com/2012/02/cyber-threat-analysis-not-just-for-the-military/

3.Goel, S. & Chen, V. (2005). Information Security Risk Analysis – A Matrix-based Approach. Retrieved on 07/08/2014 from http://www.albany.edu/~GOEL/publications/goelchen2005.pdf

4.Hughe, J. & Cybenko, G. (2013). Quantitative Metrics and Risk Assessment: The Three Tenets Model of Cybersecurity. Retrieved on 07/08/2014 from http://timreview.ca/article/712

5.Hulme, G. (2014). CSOs need to more precisely understand the actual threats facing their organization. The fix? Threat modeling. Retrieved on 07/08/2014 from http://www.csoonline.com/article/2134353/strategic-planning-erm/can-threat-modeling-keep-security-a-step-ahead-of-the-risks-.html

6.Mateski, M., Trevino, C., Veitch, C., Michalski, J., Harris, J., Maruoka, S., Frye, J. (2012). Cyber Threat Metrics. Retrieved on 07/08/2014 from http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-065.pdf

7.Microsoft. Threat Modeling Principles. Retrieved on 07/08/2014 from http://msdn.microsoft.com/en-us/library/ff648644.aspx

8.MSM. Cyber Intelligence Threat Analysis. Retrieved on 07/08/2014 from http://measurablesecurity.mitre.org/directory/areas/threatanalysis.html

9.Richards, K. (2014). RSA 2014: HP exec says security threat analysis should guide strategy.