Planning for Malicious Activity on Communications Networks

Matthew A. Chapman, Ph.D.
Assistant Professor of Information Technology
University of Hawaiʻi - West Oʻahu

Abstract – **With the rapid advance of malicious activity on communications networks, information security professionals need to determine not if malicious activity is present, but how to plan for this eventuality. Significant phases in planning include a survey of malicious actors, monitoring the cyberspace environment, designing for security, proactive system security, and contingency** planning.

Keywords—Information; Secruity; Cyber; Malicious; Technology

I. Introduction

One does not have to look far in the daily news to discover new accounts of malicious activity in cyberspace of both government and industry networks. The *Washington Post* noted that in the last year, there were two major information security breaches of U.S. Government personnel databases, potentially exposing sensitive information concerning over 22 million people [1]. Additionally, many recent information security breaches of industry have been publicized to include the cyber attack against *Sony Pictures*, the compromise of over 1.1 million credit card accounts from *Staples*, and a similar compromise of *Home Depot* information systems that may have exposed credit information of over 56 million people [2]. Information security professionals and network users alike need to determine not if malicious activity is present, but how to plan for this eventuality. Professional leaders in information security, such as the *International Information System Security Certification Consortium (ISC)^2* have developed detailed, technical certification programs to provide leadership and support in security of information systems [3] [4]. The framework described here is intended to provide a strategic perspective to planning for malicious activity and supplement the growing body of knowledge in information security. Significant phases in planning include a survey of malicious actors, the cyberspace environment, designing for security, proactive system security, and contingency planning.

II. Malicious Actors

To plan for malicious activity on networks, it is first important to assess exactly what actors are involved. Activity to exploit networks and exfiltrate data may come from many different interested parties. This is by no means an all-inclusive list, but many of the major actors are listed here. It is important to not only consider intentional activities, but unintentional activities as well; consider not only external actors, but internal actors as well; consider both trained malicious actors and experimental penetration testers. Malicious actors are categorized here into five main categories, nation state actors, organized crime, political and ideological actors, business stakeholders, and students [5] [6].

A. Nation State Actors

Actors in this category include both recognized and unrecognized governments. These actors have a significant pool of resources in funding, talent, training, and available time. Motivation for nation state actors may include intelligence gathering, political leverage, and military posturing.

B. Organized Crime

This category may include highly organized and trained malicious actors. These criminals may be experts at system penetration, or they may outsource this expertise and hire experts in network penetration. These hired experts are sometimes referred to as hired guns. Organized crime actors may be interested in identity theft, fraud, money laundering, or methods to use cyberspace to leverage physical crimes. Motivation is commonly related to financial gain.

C. Political and Ideological Actors

In addition to the category of nation state actors listed above, other groups may conduct malicious activity in cyberspace or through the Internet to advance their political or ideological objectives. These include both terrorists and hacktivits. Malicious actors involved in terrorist activity are especially important to consider in planning for organizations involved with critical infrastructure including healthcare systems. Motivation for these actors is generally to advance political or ideological views.

D. Business Stakeholders

This category of malicious actors includes disgruntled employees, customers, suppliers, vendors, business partners, contractors, temporary workers, consultants, and employees creating unintentional security incidents. With all of the stakeholders involved in both large and small business, many users with access to information should be considered when planning security. Many of these actors have direct access to information and physical access to networking equipment. Motivation for actors falling into this category may include the potential to gain a larger market share, financial gain, corporate power, and revenge.

E. *Students*

This last category of malicious actors includes both formal and informal students attempting to improve their information security skills, including probing, vulnerability testing, penetration testing, security testing, and network exploitation. There are many tools and scripts available on the Internet for skilled and unskilled students for experimentation. It is very important that all categories of learners understand the ethical and legal implications of testing information systems.

III. The Cyberspace environment

Monitoring developments throughout the cyberspace environment is a continuous process. Two major categories of awareness are highlighted here to emphasize both the strategic and technical aspects of information security - modern cyber conflicts and technical developments.

A. *Modern Cyber Conflict*

The analysis of modern cyber conflict includes the exploration of the participants, the tools, the physical and virtual components of cyberspace, and the techniques used in managing modern cyber conflicts. It is important to observe and adapt to how these conflicts are carried out, how they will continue to evolve, and how to mange both current and future conflict [7]. Many resources are available to observe and research developments in modern cyber conflicts, including public news sources and Internet publications. Examples include resources such as *National Public Radio (NPR) News* [8] and *Security Week – Internet and Enterprise Security News, Insights & Analysis* [9].

B. *Technical Developments*

The technical developments in the information security field move at an extraordinarily fast pace. The idea of keeping up with new software, hardware, networking equipment, vulnerabilities, exploits, patches, emerging threats, policies, and legal statutes is daunting. For malicious actors, these rapid changes offer opportunity. For those tasked with information security, it is a herculean challenge, especially considering personnel constraints, budgetary constraints, and the technical training required. Examples of resources to monitor technical developments include the *United States Computer Emergency Readiness Team (US-CERT)* website [10] and the *National Vulnerability Database* available from the *National Institute of Standards and Technology (NIST)* [11].

IV. Designing for security

Certainly a major aspect of planning for malicious activity on communications networks is implementing a secure design that is robust and able to adapt to the numerous cyber actors and the evolving cyber environment. Designs and their implementation require attention to the technical aspects of network security, the physical environment that houses the network hardware, personnel and corporate policies, and laws that govern the use and distribution of digital information.

The vendor neutral *Security+* credential of the *Computing Technology Industry Association (CompTIA)* is internationally recognized and provides one of the foundational certifications for information technology professionals. Domains covered include network security; compliance and operations security; threats and vulnerabilities; applications, data, and host security; access control and identity management, and cryptography [12].

The *ISC^2 Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK)* currently organizes many of these aspects into eight domains; security and risk management, asset security, security engineering, communication and network security, identity and access management, security assessment and testing, security operations, and software development security. Although some components of these domains overlap with other phases, the topics relating to each domain area are technically robust and continuously updated as the requirements evolve [3] [4].

Inside of the various domains and categories identified by professional organizations as mentioned above and practiced in security planning, there are many common principles to consider for technical planning and implementation [3] [12].

A. *Defense in Depth or Layering*

For a defense to be viable, it is important for a malicious actor to be faced with a series of obstacles and defenses. Even a single-flawless defense has the potential of being overwhelmed, avoided, removed, or destroyed. A layered defensive architecture has the potential to greatly increase the complexity faced by a malicious actor. This includes perimeter defense, network defense, and host based defenses.

B. *Diversity of Defenses*

A diverse defense forces a malicious actor to solve multiple problems. Ideally, each of the information protection systems will use a different technique to secure information. This can greatly complicate the challenge for the adversary. In partnership with defense in depth, defenses should be designed to protect from the outside-in and from the inside-out.

C. *Agility*

It may be difficult to plan a network that is agile or manage critical information systems that do not remain static. However, the ability for a network to vary configurations and for data to be stored and processed in an unpredictable fashion will make the cyber environment more difficult and less predictable for the malicious actor.

D. *Simplicity of Design*

Simplicity of design is directly in conflict with the first three principles above. A layered, diverse, and agile network may easily become overly complex. A network may be too complex for the defenders to understand and manage, which could result in introducing unknown vulnerabilities.

E. Physical Defenses

It is certainly much easier to pick up a computer and walk out the door with the device than it is to access the system remotely, through a layered, diverse, and agile defense. Physical considerations cannot be overlooked. Access to network components, network data, and even key personnel needs to be considered and included in the security design.

V. PROACTIVE SYSTEM SECURITY

After the completion of network design and implementation, or if planning for malicious activity on an established communication system, the information security professional has the continuous task of maintaining a secure environment. This task can be overwhelming and should not be given to a single individual. As much as the financial situation will allow, it is recommended to build a diverse, trained, and experienced team.

A proactive system security approach supports the concept of taking on the mindset of a malicious actor, in order to test and attempt to penetrate your own network. This is a hands-on approach where the penetration tester uses knowledge of the cyber environment to analyze and attempt various types of attacks, in order to understand how to defend against them. Of course, there are significant legal implications to this approach, and written permission describing the penetration test in detail is paramount [13] [7]. This fact is worth repeating. Written permission is absolutely necessary.

The list of available tools to support both vulnerability and penetration testing is quite long. One of the most common, free, open source tools is the *Open Vulnerability Assessment System (OpenVAS)*. This software offers a set of tools and services for vulnerability scanning and management [14]. One of the popular commercial solutions is the *Nessus Vulnerability Scanning and Vulnerability Management System*, which supports over 60,000 plugins, or small pieces of code, to test for specific known vulnerabilities [15]. Perhaps the most significant toolkit is the open source distribution of *Kali Linux*. Kali provides a robust and continually updated set of penetration tools to support proactive system security [16].

VI. CONTINGENCY PLANNING

If the technical defenses, physical defenses, training, and policies fail to protect the communications network from exploitation, contingency plans should be available in order to take immediate action. This phase of planning requires the participation of a number of stakeholders including technical experts, operations directors, legal experts, and decision makers.

According to the *International Federation of the Red Cross and Red Crescent Societies (IFRC)*, the purpose of contingency planning is to prepare an organization to respond in the event of an emergency. The IFRC suggests that contingency planning should address three main questions: “What is going to happen?”, “What are we going to do about it?”, and “What can we do ahead of time to get prepared?” [17].

Contingency planning for communications networks in military doctrine includes categories of procedures to direct the defensive posture of networks, when they are suspected to be under attack from malicious actors. These categories range from defending networks under normal conditions, to the implementation of very restrictive procedures. These plans also come in the form of specific actions tailored to respond to projected events, or tailored readiness options (TROs). These are supplemental measures that are narrowly focused to respond to specific intrusions [18].

Additionally, contingency plans may be robust documents providing strategy, goals, objectives, activation procedures, management concerns, coordination requirements, and quality control standards as described by the IFRC [17].

VII. CONCLUSION

Information security professionals should no longer simply prepare for the possibility of malicious activity on communications networks, but plan as if these penetrations were inevitable. Significant phases of planning for malicious activity include a survey of malicious actors, an understanding of both the strategic and technical cyber environment, designing for security, proactive system security, and contingency planning. The framework described here is intended to provide a strategic perspective to planning and contribute to the growing body of knowledge in information security.

ACKNOWLEDGMENT

Thank you to the faculty and staff of the University of Hawai‘i - West O‘ahu for your support and Aloha.

REFERENCES

[1] E. Nakashima (2015, July 9). “Hacks of OPM databases compromised 22.1 million people, federal authorities say”. The Washington Post [online]. Available from www.washingtonpost.com [Accessed 10 09 2015].

[2] K. Granville (2015, February 5). “9 Recent cyberattacks against big business”. The New Your Times [online]. Available from www.nytimes.com [Accessed 10 09 2015].

[3] H. Topton (Ed.). Official (ISC)2 Guide to the CISSP CBK, Second Edition. Boca Raton, FL: Auerbach Publications, 2010.

[4] International Information Security Certification Consortium, Inc. Available from www.isc2.org [Accessed 10 09 2015].

[5] E. Skoudis and T. Liston. Counter Hack Reloaded, Second Edition. Boston, MA: Pearson Eduction Inc., 2006.

[6] M. T. Simpson, K. Backman, & J. E. Corley. Hands-on Ethical Hacking and Netowrk Defense, Second Edition. Boston, MA: Cengage Learning, 2011.

[7] University of Hawaii. General Catalog 2014-2015 [online]. Kapolei, HI: Univerity of Hawaii West Oahu, 2015. Available from www.uhwo.hawaii.edu/general-catalog/ [Accessed 07 04 2015].

[8] NPR News. “Overview and history”. Available from www.npr.org [Accessed 11 09 2015].

[9] Security Week. “Security Week, Internet and enterprise security news, insights & analysis”. Available from www.securityweek.com [Accessed 01 09 2015].

[10] US-CERT. “National Cyber Awareness System”. Available from www.us-cert.gov/ncas [Accessed 11 09 2015].

[11] National Institue of Standards and Technolgoy. “National vulnerability database”. Available from nvd.nist.gov [Accessed 11 09 2015].

[12] M. Ciampa. CompTIA Security+ Guide to Network Security Fundamentals, Fifth Edition. Boston, MA: Cengage Learning, 2015

[13] P. Engebretson. The Basics of Hacking and Penetration Testing, Second Edition. Waltham, MA: Syngress, 2013.

[14] Open VAS. "About OpenVAS". Available from www.openvas.org [Accessed 12 09 2015].

[15] Tenable Network Security. "Nessus vulnerabilty scanner". Available from www.tenable.com [Accessed 12 09 2015].

[16] Kali by Offensive Security. "About Kali Linux." Available from www.kali.org [Accessed 12 09 2015].

[17] Internatinal Federation of the Red Cross and Red Crescent Societies. Continency Planing Guide [online]. Geneva, Switzerland: IFRC, 2012. Available from www.ifrc.org [Accessed 16 09 2015].

[18] S. Winterfeld & J. Andress. The Basics of Cyber Warfare: Understanding the Fundamentals of Cyber Warfare. Waltham, MA: Syngress, 2012.