CHAPTER

11

Computer Network Defense

INFORMATION IN THIS CHAPTER

- What We Protect
- Security Awareness and Training
- Defending Against Cyber Attacks

Computer Network Defense (CND) is defined by the U.S. Department of Defense (DoD) as, "Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks" [1]. The broad scope of these CND activities may very well include components that would be considered Computer Network Exploitation (CNE) and Computer Network Attack (CNA), as we discussed in Chapters 9 and 10, respectively. Additionally, the strategies and tactics developed and utilized in conducting CNE and CNA against our opponents can be used to strengthen our own defenses. CND is also one of the few places in Computer Network Operations (CNO) where we will find military and civilian approaches to be very similar due to the use of the same tactics and equipment.

In the military sense, CND may very well parallel the strategies and tactics that are used for conventional defense. The cyber equivalent of defensive emplacements, listening posts, patrols, and so on can be formulated, and the defensive strategies of conventional warfare can be adapted to cyber warfare by mapping the concepts across. Although this may not always be the most efficient means for us to use the tools of cyber warfare, it does allow time tested concepts to be applied to the new dimension of warfare. Given that the military leadership that is likely to presently be planning and carrying out CNE and CNA will often have been educated in the affairs of war before the advent of cyber warfare, this is the approach that we will most likely find in CND when executed by a nation-state. This may also pose a possible weakness in CNO in general, as it does tend to add a certain element of inflexibility. Although it would be a gross generalization to call this a universal problem, we may find that some portion of military leadership will be hindered by conventional thinking on defense in the area of CND.

http://dx.doi.org/10.1016/B978-0-12-416672-1.00011-8

As we discussed in the introduction to Chapter 10 when we talked about CNA, being able to execute the complete cycle of CND will more than likely require resources similar to those of a nation-state. In a pure cyber attack sense, a non-nation-state can certainly be capable of defending against an attack. In the attacks that occurred against many US financial institutions in early 2013 [2], we can see a number of good examples of large commercial organizations defending against attacks of a purely cyber nature.

The collective financial industry response to these attacks was, in addition to the normal increases in hardening and redundancy in their infrastructure and architecture, highly focused in the area of defense against denial of service [3]. In a pure cyber attack sense, such a response is completely acceptable and likely to be successful in most cases. In the complete form of CNA, as we discussed in the Waging War in the Cyber Era section of Chapter 10, we would likely see a nation-state include elements of conventional warfare. Although many such institutions are very large, they are not operating at the level of even smaller nation-states just yet, and would be ill-prepared to fend off an attack that included physical attacks as a component.

WHAT WE PROTECT

When we look to defend against cyber attacks, it is often useful to examine what exactly it is that we are defending. In a very general sense, we are almost always concerned with the protection of information in one form or another.

Sensitive information, in the eye of the general public, is often categorized as Personally Identifiable Information (PII) or Patient Healthcare Information (PHI), and involves names, addresses, social security numbers, medical records, financial records, and a multitude of similar information. Such information, when compromised can lead to a variety of fraudulent activities, commonly gathered under the umbrella term of identity theft. Such activities can range from credit accounts being opened with stolen credentials to real estate being sold without the authorization of the legitimate owner, to simple theft of funds from bank accounts.

In the world of the military and government, information of a sensitive nature being exposed can have far greater consequences than mere financial loss. Information is categorized as Unclassified (U), Unclassified For Official Use Only (U//FOUO), Confidential (C), Secret (S), and Top Secret (TS). There can also be special clearances above TS. These are sometimes referred to as Sensitive Compartmented Information (SCI) or Special Access Program (SAP). Information housed by such agencies can include Operations Orders (OPORDERS), war plans, troop movements, technical specifications for weapons or intelligence collection systems, identities of undercover intelligence agents, and any number of other items critical to the functioning of military and government. When such information is accessed in an unauthorized fashion, lives can be lost on a large scale and the balance of power can be shifted significantly. The government also worries about data aggregation where multiple lower classified documents when combined produce information that should be at a higher level of classification.

Laws do exist to protect these types of information, but they are, in many cases, still a work in progress. In the United States, as far as personal data regarding individuals, laws at this point are fairly weak on a federal level. Individual states have gradually begun to enact more stringent data protection and privacy laws, such as SB 1386 in California, in order to compensate for this weakness. Regarding the data held by governments, the military, and some industries, the custodians of such information generally have very strict laws and regulations regarding specifically how the information is handled and controlled, thus putting them in a much better position to protect the data for which they are responsible. We will discuss some of the legal issues surrounding the protection and privacy of data in greater depth in Chapter 13.

Confidentiality, Integrity, Availability

The measures we take to protect our information assets can generally be described in terms of the classic CIA triad of Confidentiality, Integrity and Availability, as shown in Figure 11.1. The confidentiality of data refers to keeping it out of the hands of those that are not authorized to see it. The integrity of data refers to preventing unauthorized modifications to data or system functions. The availability of data refers to being able to access it when needed. These basic principles govern how we go about securing the data with which we are concerned.

Integrity

When protecting the confidentiality of data, we are concerned with keeping it out of the hands of those that should not be seeing it. In terms of specific security implementations, this often means access controls and encryption in order to provide such protections. When

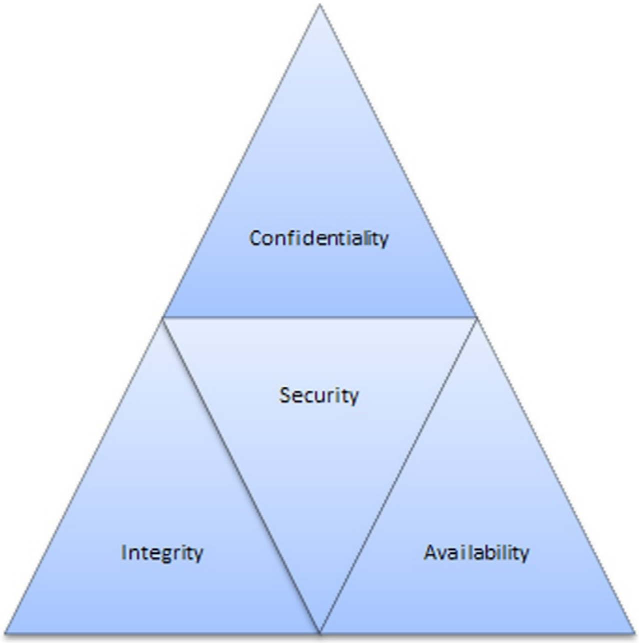

FIGURE 11.1 CIA triad.

applying these measures, we need to consider both data at rest and data in motion. Depending on where the data is at any given point in time, we may need to use different security controls, or different methods within a given control. We can see the results of lapses in confidentiality with the large breaches of PII that seem to occur with disturbing frequency in recent years, such as the breach of the U.S. Department of Energy in February of 2013, resulting in the loss of PII related to several hundred employees and contractors [4].

TIP

A lesser known alternative to the CIA triad, referred to as the Parkerian hexad, exists as well. The Parkerian hexad, developed by Donn Parker, breaks the same general concepts down into the categories of confidentiality, possession, integrity, authenticity, availability, and utility, allowing for a more detailed discussion of the relevant security concepts in a given situation [5]. The use of the Parkerian hexad allows us to be more specific when discussing security scenarios or situations without having to bend the rules of our model.

When we look to protect the integrity of data, or of the party sending the data, we are trying to prevent it from being manipulated in an unauthorized manner. Similarly to the measures that we use to provide confidentiality, we can use encryption to help provide integrity by making the data difficult to successfully manipulate without the proper authorization. In particular, hashes or message digests, such as MD5 and SHA1, are often used to ensure that messages or files have not been altered from the original by creating a fingerprint of the original data that can be tracked over time. Failures in integrity can have serious effects if we are not aware that they have happened, as data in the form of communications or files can be freely altered to reverse their meaning or to alter the outcome of decisions based on the data in question.

Availability

The availability of data simply means that we can access it when we need to do so. Ensuring availability means that we must be resilient in the face of attacks that might corrupt or delete our data or deny us access to it by attacking the environment in which it rests. It also means that we need to have a sufficiently robust environment in order to cope with system outages, communication problems, power issues, and any number of issues that might prevent us from accessing our data. Availability is often accomplished through the use of redundancy and backups for our data and for our environments.

Authenticate, Authorize, and Audit

Authentication, authorization, and auditing are commonly known as AAA (shown in Figure 11.2). These are the principles that allow us to practically carry out the securing of data. These are the means through which we can control and track how our data is being accessed, and by who, thus enabling us to enforce the policies that we have created to keep the data secure.

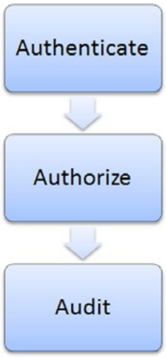

FIGURE 11.2 AAA.

Authentication is the means by which we verify the identity of an individual or system against a presented set of credentials. A very common implementation of an authentication scheme is the combination of login and password. In this particular case, the user's login name is the identity presented, and it is verified against a stored form of the password that the user has given. A common implementation of authentication used by the U.S. DoD is the Common Access Card (CAC). The CAC, sometimes redundantly referred to as a CAC card, has storage areas that can be used to store credentials, such as a certificate, and may also be used with additional forms of authentication such as a Personal Identification Number (PIN). Other hardware-based tokens are now in common use as well, one of the better known being the RSA SecureID. One of the main keys to the future of authentication is the use of biometric identifiers, such as fingerprints, iris scans, and other means based on physical attributes. Such identifiers are ubiquitous, portable, and difficult to forge, given properly designed authentication systems.

Once we have authenticated an identity, we can then check to see what activities that particular identity is allowed to carry out, known as authorization. We can see a common example of authorization in the different levels of account functionality that are defined in many operating systems. Where a root or administrator level account might be authorized to create additional accounts on a system, a general user will likely not be able to do so.

NOTE

The Principle of Least Privilege states that for any given layer in a computing environment, such as a person, process, or a system, that layer be given only the minimum level of privilege that is needed for it to operate properly. Following this principle negates many of the common security issues that we might face.

Auditing gives us the capability to monitor what activities have taken place on a given system or in an environment. While authentication and authorization allow us to control and set limits on user access to our assets, we also need to keep a record of what these authorized individuals have done. This allows us to balance system and network loads properly, as well as monitor for authorized but inappropriate or unwanted activities.

SECURITY AWARENESS AND TRAINING

People pose what is likely the single largest security vulnerability that we have, or will ever have, in any given system or environment. With most other security problems we can apply a patch, change a configuration, or pile on additional security infrastructure in order to fix the problem. With people, we unfortunately cannot do this. People can be lazy, careless, or simply make honest mistakes, all the while circumventing our carefully planned security measures from the inside and leaving us wide open to attack.

Although we can attempt to apply technical measures to keep untoward activity from taking place, and we can create policy that clearly points out correct and incorrect behavior, such measures will be for naught if we do not impress upon people some small measure of awareness regarding the issues surrounding security, and train them in the proper behaviors that will keep them and the organization in which they operate on a better security footing.

Awareness

Security awareness can be a difficult mode of thinking to those that do not already have some acquaintance with the basic concept. Bruce Schneier wrote a piece on this for *Wired* magazine in 2008, and called this sort of awareness the security mind-set. Schneier said "Security requires a particular mindset. Security professionals—at least the good ones—see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it [6]."

This security-aware mind-set is not only critical for security professionals, system administrators, network engineers, and others employed in technical fields, but it is also important for secretaries, doctors, teachers, soldiers, stay-at-home parents, and anyone else who handles information that could in any way be considered important or sensitive. To exacerbate the situation, evaluating which data may or may not be sensitive, and in what situations we need to be aware of the security implications of our actions is a function of security awareness, and needs to be taught as well.

To illustrate the consequences of such failures in both judgment and in the proper mind-set, we need only to look at the near daily security breaches that appear in the media. One good example of such a failure occurred during the time before the 2008 U.S. presidential election. Workers at the U.S. Department of State were discovered to have repeatedly accessed the passport records in an unauthorized fashion for three people who were, at the time, presidential candidates: Barrack Obama, Hillary Clinton, and John McCain. The systems containing this information are configured to alert a supervisor when the record of a high profile individual, such as a presidential candidate, is accessed without a legitimate reason.

As a result of this incident, several workers were fired or reprimanded, and those that remained had limitations placed on their access [7]. A modicum of security awareness might have alerted these individuals to the idea that unauthorized access to records containing the personal information of presidential candidates including name, address, date of birth, social security number, travel records, and a variety of other information, might have unwanted consequences for them on a personal level. The unintended consequence of accessing senior government officials' personal data could have a national impact.

Our example, while an apt illustration of lack of security awareness, unfortunately falls toward the relatively tame end of the spectrum, as far as incidents of this type can end. Numerous such cases, such as the VA laptop loss that we mentioned when we discussed CIA earlier in this chapter, can be found;from PII, such as social security numbers, being broadcast to large email distribution lists to unencrypted medical records of U.S. military veterans being lost, and virtually limitless other cases. While technical security measures can be put in place to help prevent such occurrences, as long as we continue to fail in the aspect of security awareness we will continue to have these issues.

When we attempt to teach these concepts to our users, the main point is simple: try to think like an attacker. In any given situation, whether it is a phishing email, social engineering attack, policy violation, or most any other issue that we may be confronted with, such guidance will usually steer us to the proper path. If we are able to instill a certain amount of constructive suspicion in our user base, we will often find ourselves on the proper side of such incidents. The training must result in changes to attitude and behavior to be effective. Although we may find that we tend to receive the occasional false positive from training our users in such a fashion, this is a far more desirable result than dealing with the security breaches that come from lack of care in such matters.

Training

In addition to the concepts of security awareness that we wish to instill, there is also the matter of general security training. In most organizations, such training for end users will consist of more specific direction to accompany our general security awareness efforts. In many governmental organizations, such training is mandatory on a reoccurring basis. Such training will often consist of instruction in properly secure behavior for use of various means of communication such as email, Instant Messenger (IM), and phone. These communications media are often used to scam or attempt to elicit information through social engineering, and are an important focus of our security training efforts. Additionally, depending on the environment in question, we may also wish to add additional items to our security training efforts, such as physical security, proper handling of sensitive information, and so on. For those who work in secure facilities these physical security measures often give a false sense of security—they are a key part of CND; however, they often are not funded to the same levels depending on the culture of the organization or experience of the leadership.

When conducting training for the more technical members of an organization, such as system administrators, network engineers, developers, security personnel, and the like, it is still important to go over the basics of our security training program, but we will likely need to compose additional training to address the specifics of such categories of specialization. For our system administrators and network engineers we will need to address the security of our operating systems and network infrastructure, for our developers we will need to address secure coding standards and practices, and for our security personnel we will need to make them aware of both the internal and external security practices of the organization. For all of these members, we need to stress the appropriate use and safeguarding of any privileged accounts to which they may have access.

DEFENDING AGAINST CYBER ATTACKS

When defending against cyber attacks, many of the steps that we will take will be proactive in nature and involve hardening our environments and monitoring the activities that take place in them. This is an easy statement to make, and is relatively simple to accomplish in a small- or medium-sized network environment, relatively speaking, such as what we might find in a business or corporation. When we look to perform such activities in the much larger environment that we might find when operating on a national or a global scale, this becomes a considerably more difficult prospect.

At present, we have the capability to perform a certain amount of monitoring on a large scale, as we discussed in the Surveillance section of Chapter 9. When we begin to look to more specific activities, such as intrusion detection or vulnerability assessment, the scale of environment within which we can cope shrinks to a much smaller set due to the sheer mass of data to be monitored. Presently, strategies are being developed in an attempt to monitor and address large-scale cyber attacks, but these are still in their infancy. Currently, much of the effort being put into CND is in the areas of policy and compliance, particularly in governmental circles.

In July of 2012, President Obama signed an executive order that many say constitutes, among other items, the long-discussed Internet kill-switch for the United States [8]. In the face of a concerted attack on critical infrastructure, some say that such measures may be preferable to potential destruction and loss of life that could accompany an attack on Supervisory Control and Data Acquisition (SCADA) systems and the environments they control. This may not be an ideal solution and will likely be exceedingly difficult to carry out. Although not necessarily a viable plan, this does serve as a good indicator of the present state of nationwide CND in the United States.

Policy and Compliance

One of the major keys to a successful defense lies in the area of security policy. Through the use of policies we can set the expectations for those that develop and use the environments that we expect to keep secured. Security policy defines the behavior of our users, the configuration of our software, systems, and networks, and innumerable other items. Ultimately our security policies define what exactly we mean when we say secure. Additionally, it is important to note that policy implemented without the proper authority to enforce it is utterly useless and often ignored.

In addition to defining our security through policy, we also need to ensure that the policy is followed, this being done through our compliance efforts. In government, compliance is verified against such bodies such as the Federal Information Security Management Act (FISMA), the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), the National Industrial Security Program Operating Manual (NISPOM), Director of Central Intelligence Directive (DCID) 6/3, and innumerable others. In the civilian world, we find the focus more in the direction of the Health Insurance Portability and Accountability Act (HIPAA), North American Electric Reliability Corporation's (NERC) Critical Infrastructure Protection (CIP) regulations, the Payment Card Industry Data Security Standard (PCI DSS), Sarbanes-Oxley (SOX), and many others. Without compliance, our policies are not worth the paper on which they are printed, or the bits in which they are stored.

Surveillance, Data Mining, and Pattern Matching

As we discussed in the Surveillance section of Chapter 9 many large governments presently have some sort of monitoring on the various means of communications moving in and out of their borders. While this is by no means a complete coverage, and gaps in such monitoring can, in many cases, be found or created, it does provide a measure of security. The ability to track communications with those in other countries can potentially give us a warning when coordinated activities, such as attacks may be taking place in the immediate future, possibly including cyber attacks, through data mining and pattern matching performed on the communications records we collect.

WARNING

Surveillance and reconnaissance activities, if not conducted properly, can often violate the relevant wiretap laws of the country in which they are carried out. It is important to secure the proper legal advice before proceeding with such efforts.

If we examine the systems that are used to perform large-scale communications monitoring, we can see many parallels to the familiar Intrusion Detection Systems (IDS) that we can commonly find in operation on smaller networks. In essence, these systems are IDS operating on a much more gross scale. Such systems may very well serve as the basis or technological precursors for large-scale IDS that is capable of the detailed examination of electronic communications that we are familiar with on a small scale. Although the level of technical sophistication needed to perform such activities is lacking at present, we are almost certain to see such capabilities in the near future.

Intrusion Detection and Prevention

Intrusion detection and intrusion prevention on a nationwide scale, as we discussed in the previous section, is a difficult prospect. At present, the networks that comprise the Internet are not segmented along national boundaries, for the most part. Additionally, we have a wide variety of media that can be used to carry network communications, including: copper and fiber optic cables, satellite communications, purpose-built wireless networks, packet radio, and any number of other means. This lack of network segmentation along physical borders and wide variety of communications methods makes IDS/IPS a technically challenging prospect to implement.

Two main strategies exist for accomplishing intrusion detection and/or prevention on this scale; we can either structure networks to provide a limited number of connections outside of the area that we wish to protect and monitor, or we implement massively distributed IDS/IPS; either method has its inherent issues. Restructuring our networks to provide only a few choke points is most certainly the cleanest route to take, and may be workable when building new networks, but would likely be prohibitively expensive for existing networks. Likewise, massively distributed IDS/IPS, although having the benefit of not requiring us to alter our networks, is likely to miss some of the traffic entering and exiting said networks. In either case, at present, conducting such operations is likely to prove difficult in a variety of ways.

An example where this has been deployed as part of national defense in the Department of Homeland security Network Security Deployment National Cybersecurity Protection System (operationally known as EINSTIEN). EINSTEIN was deployed in accordance with Comprehensive National Cybersecurity Initiative directive 5—Connect current cyber ops centers to enhance situational awareness. There are multiple blocks but the first was built around IDS [9].

Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and Penetration Testing are two of the main tools of CND. These methods allow us to discover the weaknesses in our systems and networks that allow attackers to conduct reconnaissance and surveillance, gain entry, or other attacks. Vulnerability assessment and pen testing are just a few aspects of something called a Red Team assessment. Red teaming is used by both government and commercial entities alike.

Vulnerability Assessment allows us to, generally using scanning tools such as those that we discussed in Chapter 6, discover surface vulnerabilities in our systems. Typically such assessments involve iterating through the complete catalog of our systems and scanning for vulnerabilities on each, using known signatures for those vulnerabilities. Although this can indeed expose some of the means of entry that attackers can use, it is not a complete picture of how our systems might be vulnerable. In order to get a more complete picture of the holes in our systems, we need to be much more thorough in our efforts and conduct penetration tests.

Penetration Testing, when conducted properly, can much more closely mirror the activities of an attacker attempting to compromise our environment. Penetration Testing can be performed from a white box perspective, in which we are provided with information on the environment to be attacked, or can be done from a black box perspective, in which we have no additional information that an attacker would normally have. Many arguments can be made for either approach, but generally white box testing is less costly and black box testing more closely represents an outside attack. We may also wish to consider additional elements in our Penetration Testing efforts, such as social engineering, which we discussed in Chapter 8, and physical security, which we discussed in Chapter 7.

One of the dangers in planning and in trusting the results of penetration tests is to insure that the tests are not hampered to the point of not being useful. If we put restrictions on our penetration tests that disallow specific attacks, environments, or even legacy systems, then we are no longer accomplishing the goal of using the same methods that potential attackers will be using. Such restrictions are all too common in penetration testing scenarios and can not only render our efforts useless, but can provide us with a false sense of security.

Disaster Recovery Planning

Disaster Recovery Planning (DRP), as a defensive measure, can allow us to withstand or recover from the attacks, outages, and disasters that we were not able to prevent outright. Such measures are usually accomplished through the use of backups for our data and through the use of varying degrees of redundant systems and infrastructure. Although, in the case of CND, properly stored backups will certainly allow us to recover in the case of an attack, it is more likely that we will find greater utility in redundant infrastructure to resist an attack. DRP differs from Continuity of Operations planning in that it focuses on the IT infrastructure vs sustaining business operations.

In the case of a large-scale cyber attack, it is entirely possible that we will find ourselves unable to operate from certain network blocks, domains, systems, and so on. Unlike the disaster recover planning that most organizations undertake, when undertaking such planning for CND, it will more than likely pay to ensure that our backup locations from which we can operate are distributed widely in both a geographical and a logical sense. In this way, when we are under attack or need to operate from a logically separated location, we are likely to have one which has not been affected by the attack.

Defense in Depth

One of the more important principles of a successful defensive strategy is defense in depth. Defense in depth proposes a layered approach to security, as shown in Figure 11.3. In this

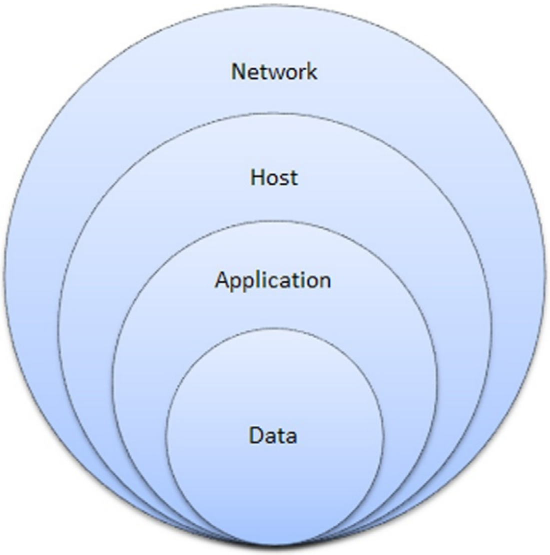

FIGURE 11.3 Defense in depth.

particular case we have defenses at the network level, the host level, the application level, and the data level. We might have, as an example, firewalls and IDS/IPS at the network level, software firewalls and antimalware tools at the host level, access controls at the application level, and encryption at the data level. In addition, the user awareness training we talked about in the security awareness section of this chapter, as well as physical security layers like badge access control, checkpoints, and guards, could easily be integrated into our layers of security. At the center of all these layers of defense lies our critical information. The layers and security measures at each layer may vary according to the environment in question, but the basic principles will remain the same.

NOTE

Defense in depth is actually an ancient military concept. One of the first recorded uses of such a strategy was carried out by Hannibal against the Romans during the Battle of Cannae in 216 B.C [10].

The principle behind defense in depth is, through the multiple layers of security measures, to hinder our attackers sufficiently so that our elements of detection will discover their activities or so that they will decide that our security measures are too great and give up on their attacks.

We may like to think that we can create an environment that is impenetrable to attack and can successfully fend off any attacker for an indefinite period of time, but this is an unrealistic expectation. Instead, we should configure our layered defenses so that we can slow an attacker as much as we can in order to have time to detect and deal with their attacks. Additionally, if we segment the information on the network, and restrict access to each segment based on need, we can help mitigate some of the risk of an attacker being able to get in, get everything, and get back out again.

SUMMARY

In this chapter, we discussed CND. CND is the defensive and largely proactive component of CNO. We discussed how CND fits into the overall category of defensive actions and how non-nation-states might not have sufficient resources to be able to defend against a complete attack by a nation-state.

We covered what exactly it is that we attempt to secure, in the sense of data and information. We also covered some of the key principles of security such as the CIA triad of confidentiality, integrity, and availability, as well as AAA, covering authentication, authorization, and auditing. These basic principles are the foundations on which we base the defense of our information assets.

We talked about security awareness and training efforts in order to secure what is likely to be the weakest link in our defenses: people. We covered the security mind-set, and what we can try to do to impart some of this mind-set to the users for which we are responsible. We also covered security training for our users, so that we might educate them as to the proper responses for some of the situations in which they might potentially damage our security footing. We also discussed the need for differing security training for the different levels of technical ability that we might need to address.

In defending against cyber attacks, we talked about some of the different strategies that we might use to defend ourselves against attack. We covered some of the uses that surveillance tactics from CNE might be used and how data mining and pattern matching might be used on such collected data. We also covered intrusion detection and intrusion prevention and how implementing these on a very large scale might be difficult. We discussed the uses of vulnerability assessment and penetration testing in discovering the security holes in our environments, and some of the ways in which such tactics might provide us a false sense of security. We went over DRP and how we might need to customize such plans to cope with the realities of cyber warfare. Lastly, we covered defense in depth and discussed how we might employ many layered security measures in our defensive implementations.

In CND we have to be successful all the time and every time. Our opponents can attack at any time, using any method at their disposal, and only need to be successful once. We have to be alert and react to every attack. This applies to every system, network, and organization equally. As a part of the military, critical infrastructure or even corporate systems, we are part of the ongoing fight.

References

[1] Director for Joint Force Development. Joint Publication 1-02 Department of Defense Dictionary of Military and Associated Terms, http://ra.defense.gov/documents/rtm/jp1_02.pdf; 2011 [accessed 05.05.13].

[2] Perlroth N, Sanger D. Cyberattacks seem meant to destroy, not just disrupt. The New York Times 2013; http://www.nytimes.com/2013/03/29/technology/corporate-cyberattackers-possibly-state-backed-now-seek-to-destroy-data.html?pagewanted=all&_r=0 [accessed 05.05.2013].

[3] Smith G. Banks fight cyber attacks by hiring outside help. Huff Post 2013; http://www.huffingtonpost.com/2013/01/10/bank-cyber-attacks_n_2441870.html [accessed 18.03.13].

[4] Schwartz M. Department of Energy Confirms Data Breach. Information Week 2013; http://www.informationweek.com/security/attacks/department-of-energy-confirms-data-breac/240147877 [accessed 18.03.13].

[5] Parker D. Fighting computer crime. s.l. New York: Wiley; 1998.

[6] Schneier B. Inside the twisted mind of the security professional. Wired.com, http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0320; 2008 [accessed 18.03.13].

[7] Associated Press. Passport files of candidates breached. MSNBC.com, http://www.msnbc.msn.com/id/23736254/; 2008 [accessed 18.03.13].

[8] Obama B. Executive Order – Assignment of National Security and Emergency Preparedness Communications Functions. The White House, http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness; 2013 [accessed 18.03.13].

[9] U.S. Department of Homeland Security. Network Security Deployment. Homeland Security, http://www.dhs.gov/network-security-deployment; 2013 [accessed 05.05.2013].

[10] Flaherty K. Verifying your defense in depth strategy: from Hannibal to today. BreakingPoint, http://www.breakingpointsystems.com/community/blog/verifying-your-defense-in-depth-strategy-from-hannibal-to-today/; 2009 [accessed 18.03.13].