SECURITY

Computer Incident Response and Product Security

The practical guide to building and running incident response and product security teams

ciscopress.com

Damir Rajnović

Computer Incident Response and Product Security

Damir Rajnović

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing December 2010

Library of Congress Cataloging-in-Publication Data:

Rajnović, Damir, 1965-
Computer incident response and product security / Damir Rajnović.
p. cm.
Includes bibliographical references.
ISBN 978-1-58705-264-4 (pbk.)
1. Computer networks—Security measures. 2. Computer crimes—Risk assessment.
3. Data recovery (Computer science) I. Title.

TK5105.59.R35 2011

005.8—dc22

2010045607

ISBN-13: 978-1-58705-264-4

ISBN-10: 1-58705-264-4

Warning and Disclaimer

This book is designed to provide information about computer incident response and product security. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The author, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:
U.S. Corporate and Government Sales 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States, please contact: **International Sales** international@pearsoned.com

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Brett Bartow

Managing Editor: Sandra Schroeder

Development Editor: Andrew Cupp

Senior Project Editor: Tonya Simpson

Book Designer: Louisa Adair

Composition: Mark Shirar

Manager, Global Certification: Erik Ullanderson

Business Operation Manager, Cisco Press: Anand Sundaram

Technical Editors: Yurie Ito, Derrick Scholl

Copy Editor: Apostrophe Editing Services

Proofreader: Water Crest Publishing, Inc.

Editorial Assistant: Vanessa Evans

Cover Designer: Sandra Schroeder

Indexer: Tim Wright

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Contents at a Glance

Contents

Introduction

This book is actually two books in one. The first six chapters are about forming and running a computer incident response team. Starting with Chapter 7, "Product Security Vulnerabilities," the book is devoted to managing product security vulnerabilities. The reason these two subjects are combined into a single book is that they are connected. Attackers use security vulnerabilities to compromise a device. Remove vulnerabilities from the product and it becomes so much more resilient to attacks.

For many companies, incident response is new territory. Some companies do not have incident response teams (IRT). Some would like to have them but need guidance to start, and others would like to improve existing practices. Today, only a handful of companies have mature and experienced teams. For that reason, this book provides guidance in both creating and running an effective incident response team. Organizations that are evaluating whether to invest in an IRT, or that are starting to build one, will find the information in this book to be invaluable in helping them understand the nature of the threats, justifying resources, and building effective IRTs. Established IRTs will also benefit from the best practices highlighted in building IRTs and information on the current state of incident response handling, incident coordination, and legal issues. In an ideal world, this book can provide all the right answers for how to handle every incident; however, because every situation is unique, this book strives instead to help you ask the right questions.

Similarly for managing product security vulnerabilities, the sad truth is that many vendors prefer to live in denial rather than face the truth—vendors who would rather cover up information about vulnerabilities than remove the problem. Only a handful of responsible vendors do the right thing and face the problem and not hide from it. Other vendors should follow their lead and establish their product security teams, join the community, and start making a difference. This is especially important because the protocols underpinning the Internet are starting to show their age. We are now witnessing a rise in the number of vulnerabilities that affect these basic protocols (such as DNS, TLS, and TCP), and these vulnerabilities affect virtually every device that can be connected to the Internet. Vendors without product security teams cannot react properly, or at all, on these vulnerabilities and leave their customers exposed. Ultimately, vendors ignore product security at their own peril, as customers will move away from them and go to vendors who know how to manage vulnerabilities.

Goals and Methods

This book has several goals; the two main ones follow:

- To help you establish computer incident response teams, if you do not have them, and give you ideas how to improve operation of the existing ones.
- To help vendors in understanding that their products will contain security vulnerabilities no matter how hard they try to avoid them and to form a team and processes to manage these vulnerabilities.

Accepting problems might not be easy, and other factors, such as organization culture, can make this acceptance even more difficult, but it must be done. Interestingly, when the organization accepts the existence of the problems, it can benefit, as some examples in the book show.

When talking about a particular aspect of either an incident response or vulnerability management, this book always tries to formulate a problem, present options, and discuss relative merits of the options. This presents a balanced view on the matter. In some instances, the book offers suggestions on how things should be done. Apart from a few cases in which these actions may be dictated by laws, these suggestions are mine. Both of the areas (incident response and vulnerability management) are largely unregulated, so you are not forced to act according to these suggestions. Finally, there are cases in which there is no right or wrong answer and you are free to explore. In such instances, the book offers hints, usually in the form of questions, on how to define boundaries and parameters of the action or requirement.

Topics Not Covered

In the incident response part of the book, the biggest area not covered is forensics. Despite the fact that forensics is a large part of daily routine of many teams, I refrained from covering that topic. There is a plethora of good sources on forensics, so this book will not try to replace those. Other major topics not covered are malware analysis and operating system (OS) hardening for the same reason.

In the products security part of the book, areas that are not covered are secure (defensive) programming, product development lifecycle, negative (robustness) testing, and other development-related topics. Each of these areas deserves a book unto itself, and in many cases there already are several published books, so it is better to focus on an area that has not received as much exposure.

Who Should Read This Book?

In the same way both subjects are multifaceted, so is the target audience. Some chapters contain more technical information, whereas others deal with legal or managerial issues. Although the overall tone is closer to team managers and the level or two above, I strongly believe that each team member must be cognizant of all issues described in this book. Because security touches organization at so many points and deals with many intertwined things, it is impossible to perform a good job from a narrow view. Only by having full awareness of as many aspects of incident handling and product security (as the case might be) will the team be able to deliver outstanding performance.

There is no prerequisite knowledge for understanding this book apart from general knowledge about computers, operating systems, networks, and network protocols. In parts that demand deeper technical knowledge, sufficient information is provided to aid understanding to make the book as accessible to nontechnical decision makers as it is to security professionals.

How This Book Is Organized

Although this book can be read cover-to-cover, it is designed to be flexible and enable you to easily move between chapters and sections of chapters to cover just the material of interest.

Chapters 1 through 6 deal with computer incident response and cover the following topics:

- **Chapter 1, "Why Care About Incident Response?"**—This chapter covers the various reasons an organization should set up an incident response team (IRT). Some of the reasons are simply to protect the organization, but others are legal in nature.
- **Chapter 2, "Forming an IRT"**—If you want to form an IRT, this chapter provides ideas on how to go about it: how to make your case to upper management, how to defend your budget, where to place the team within the organizational hierarchy, and what policies you might want to put in place.
- **Chapter 3, "Operating an IRT"**—This chapter provides ideas about how to operate a successful IRT. It does not discuss technical details about how to address a particular incident but instead covers how to prepare the team for effective incident handling. It also gives information on what other groups within the organization should be involved and when and why.
- **Chapter 4, "Dealing with an Attack"**—After an attack has been detected, how do you handle it effectively? That is the question this chapter answers. Again, it does not provides concrete answers on how to deal with compromised passwords, for example, but what process to follow to manage an attack situation well.
- **Chapter 5, "Incident Coordination"**—Rarely, an incident is limited to only a single organization. Miscreants routinely use compromised computers to mount further attacks. This chapter deals with the issues of incident coordination. What are the important issues when working jointly with other IRTs? And what about when law enforcement gets involved?
- **Chapter 6, "Getting to Know Your Peers: Teams and Organizations Around the World"**—Sometimes it might feel that you alone are fighting all the badness in the world, but that is not the case. There are many IRTs around the globe, and they work with each other. This chapter presents some of them and some more significant forums where various teams are coming together. This knowledge helps greatly when dealing with an incident that involves someone from the other side of the globe or to understand the latest attacks that you have discovered in your network.

Chapters 7 through 13 deal with managing product security vulnerabilities and cover the following topics:

- **Chapter 7, "Product Security Vulnerabilities"**—This chapter introduces the theme of product security vulnerability. It talks about defining what vulnerability is, differences between a vulnerability and a feature, and their severity.

- **Chapter 8, "Creating a Product Security Team"**—Discusses details pertinent to the creation of a product security team. Issues common to forming the IRT, such as budget considerations, are not discussed again here because they are covered in detail in Chapter 2, "Forming an IRT." This chapter deals only with issues specific to forming the product security team.
- **Chapter 9, "Operating a Product Security Team"**—Gives details on what is needed to operate a successful product security team. Irrespective of a vendor, every product security team must have resources to test reports and record the information. It also must establish a relationship with key partners, such as third parties that provide components for the products. This chapter describes some of the issues that will be encountered in this process.
- **Chapter 10, "Actors in Vulnerability Handling"**—No single team or vendor exists in isolation. This chapter provides an overview on who can be involved in the whole product vulnerability space and what their motivations might be. This chapter also lists key forums that vendors can use as a vehicle to establish contact with each other.
- **Chapter 11, "Security Vulnerability Handling by Vendors"**—This chapter describes in detail steps to deal with a vulnerability—starting from receiving a report on potential vulnerability all the way to publishing a notification. Even though the exact steps each vendor will make while dealing with the vulnerability are unique for that vendor, the overall process is common for everyone. This common process is the focus of this chapter.
- **Chapter 12, "Security Vulnerability Notification"**—After a remedy is produced, a vendor wants to notify its customers about the vulnerability and its remedy. This seemingly simple document requires much more effort than many initially assume. This chapter discusses various issues related to the notification, from what types a vendor may need and why, to language and dissemination, and finishes with the document maintenance.
- **Chapter 13, "Vulnerability Coordination"**—More and more, a vulnerability can affect multiple vendors. This chapter talks about issues related to vulnerability coordination. Why would a vendor consent to be coordinated by an external party? Who can be a coordinator and what would be required to be a good one? These and other questions are covered in this chapter.

Chapter 3

Operating an IRT

After an IRT is established, your next concern is how to successfully operate your team. This chapter covers the following topics to help you improve the operation of your IRT:

- Team size and working hours
- New team member profile
- Advertising team's existence
- Acknowledging incoming messages
- Cooperation with internal groups
- Prepare for the incidents
- Measure of success

Team Size and Working Hours

One of the more common questions that organizations setting up their incident response team ask is, "How large should an IRT be?" Providing that budget is not a constraint, the team's size is a function of what services the IRT wants to provide, the size and the distribution of the constituency, and planned working hours. (That is, will the IRT operate only during office hours or around the clock?) In practice, if you are starting from scratch and the IRT's task is defined as "go and deal with the incidents," a small team should be sufficient for the start. The first 12 to 18 months of the IRT's operation can show whether you need more people on the team.

Many teams after their formation operate only during the office hours. (For example, if you are in western Europe, that would be Monday through Friday from 09:00 to 17:00.) For this kind of coverage a two-person team should suffice. Although office-hours coverage is fine for the start, the IRT should look into extending its working hours to be active around the clock.

The main reason for extending the working hours is that some services (for example, a public website) are available at all times. If someone compromises computers providing these services, the IRT must be able to respond swiftly and not two days later after the weekend is over. Miscreants do not work standard office hours, so the IRT must do the same.

One of the standard ways to extend working hours is to have someone who is on-call. This person can answer telephone calls and check incoming emails after hours and over the weekend. This setup can be augmented by cooperating with other teams. If, for example, the IT has someone who is on-site outside office hours, the IT person might be the one who will accept telephone calls, monitor emails, and alarm the IRT only when needed.

From a technical perspective, it is easy to have someone on-call. It is not necessary to have someone in the office because modern, smart mobile telephones can receive and send emails, surf the Internet, and you can even use them to talk. Smart telephones generally cannot do encryption, so you would need to devise a way to decrypt and encrypt messages. From a staffing perspective, if you want around-the-clock and weekend coverage, the number of the people in IRT would depend on whether the duties can be shared with other teams in the organization. If the duties can be shared, you might not need to increase the size of the IRT. If not, increasing the team size should be considered. A three-member team might be a good size given that one person might be on vacation and another might be sick, which would leave only one active person. Although two people can also provide around-the-clock coverage, it would be a stretch and might burn them out if they would operate that way for a prolonged period of time.

If the host organization is within the EU, it must pay attention to the European Working Time Directive (Council Directive 93/104/EC and subsequent amendments), which regulates that the working week must not be longer than 48 hours, which also includes overtime. On the other hand, people might opt-out from the directive and work as long as required. The host's human resources department must investigate this and set up proper guidelines.

Irrespective of what hours the IRT operates, that fact must be clearly stated and communicated to other teams and the constituency. Do not bury it somewhere deep in the documentation but state it prominently close to the place containing the team's contact details. Setting the right expectations is important.

When the IRT operates only during office working hours, the team must not forget that it is living in a round and multicultural world. Living in a round world means that the team must state its time zone. Do not assume that people will automatically know in which time zone the team operates based just on the city and the country. It is possible that the constituency, or larger part of it, is actually situated in a different time zone from the one in which the IRT physically operates.

A multicultural world means that people in one country have different customs from people in other countries. We do not necessarily have weekends or holidays on the same days. Take an example of an IRT that operates from Israel and a large part of its constituency is in Europe. Will it operate on Saturdays? What are its office hours? Will it work on December 25th? The people who report an incident to the team might not know these details in advance. It might be the first time they are reporting something to the

team, and they do not know what to expect. The point is that all the information related to your working hours must be visibly and clearly stated on your team's website.

Digression on Date and Time

While on the topic of a multicultural world, we must mention date and time formats. You always must use an unambiguous format for the date and time. To that end, ISO 8601 is strongly recommended to be adopted by the IRT. In short, according to the ISO 8601, a date should be written in YYYY-MM-DD and time in hh:mm:ss format. ISO format is suitable when the data is automatically processed. Because not all people are familiar with the ISO 8601 standard, it is highly recommended to use the month's name (for example, October or Oct) instead of its number in all correspondence. That way, you can eliminate any possible ambiguity on a date. When sending data that is a result of some automated process or that will be processed, you should also add a note that all dates are in the ISO format so that recipients know how to interpret them.

As far as the time is concerned, do not forget to include the time zone. This is especially important if recipients are in different time zones. You can either use the time zone's name (for example, "GMT" or "Greenwich Mean Time") or the offset from the GMT (for example, GMT + 0530—GMT plus 5 hours and 30 minutes). The preference should be to include the offset rather than the time zone's name because the names can be ambiguous. For example, EST can mean either Eastern Summer Time or Eastern Standard Time. Eastern Summer Time is used in Australia during the summer, and its offset from GMT is 11 hours (GMT + 1100). On the other hand, Eastern Standard Time can be in either Australia or North America. The Eastern Standard Time in Australia is used during the winter and is 10 hours ahead of GMT (GMT + 1000), whereas the same Eastern Standard Time in North America has an offset of –5 hours from GMT (GMT – 0500).

One good website related to time zones is time and date.com, owned and operated by Time and Date AS. It is at http://www.timeanddate.com and is useful when dealing with multiple time zones.

New Team Member Profile

There was a time when requirements for becoming a member of the Cisco PSIRT team included, apart from sound security acumen and knowledge, things such as "works 24 hours a day, leaps over tall buildings, and is capable of stopping a running train." Shirts with the letter "S" were given when you joined the team, but we had to bring our own cape. That was the humorous side of the requirements, but reality, as everyone knows, is much stranger than fiction.

Computer security is not just a job; it is a way of life and a special state of mind. When most people see a new device or an application, they think: "Nice features. How can I use them?" Security-inclined people think: "How can protection be circumvented, and how can someone misuse a feature?" That is what immediately separate security-oriented people from others. Working in the computer security arena requires dedication, an open mind, and knowledge. One comforting thing for people who would like to work in an IRT

but are afraid they would not be given the chance because they lack knowledge and experience is that these things are important but are not paramount. You can learn facts, but you cannot "learn" lateral thinking and security acumen.

When hiring, the IRT should look at the way a candidate thinks about problems, the way the problem is approached, and how quickly new information is used to reevaluate it. Often a candidate might be asked some trick questions that are completely unrelated to security, or even computers, just to assess how the candidate thinks. If candidates have the right qualities, they can learn the details afterward. It is always much easier to memorize simple facts such as "/etc/shadow file contains passwords" than to understand reasons why passwords have been moved from /etc/password and placed in this other file.

Obviously, having the knowledge is good and, all things being equal, candidates with more knowledge and experience will probably have an advantage over inexperienced ones. Therefore, for all prospective IRT members, keep on learning and be curious.

Apart from security acumen, a good candidate must also posses the following skills:

- Good technical skills. Understand operating systems, networks, cryptography, a few programming languages (for example, Perl, C, and Java), and how all these elements interoperate.
- Have good interpersonal skills.
- Do not panic easily.
- Form a mental image of an incident based on sketchy information and make decisions.

Strong Technical Skills

Good understanding does not mean knowing all the details, but it does mean knowing salient details, why things are set up that way, and where to look for full details. Here are two examples of what would be a minimum of knowledge on two topics:

- **Microsoft Windows configuration parameters:** Microsoft Windows stores configuration details in the Registry, which is divided into hives. Each Registry hive is further divided into keys, subkeys, and values. A tool Reg.exe is used to edit the Registry. Further details are on the Microsoft website.
- **Border Gateway Protocol (BGP):** Transfers routing information in the Internet. The routing information is used by individual routers to make decision where to route a particular packet given its destination. More information about BGP can be found on the Internet Engineering Task Force (IETF) and Cisco websites.

In both examples, it is sufficient to know the basic principles about how things are related and what their function is in the overall scheme. Knowing where to look for more information, or who to ask, is also required. Good team members must be able to learn new things fast, and "fast" means in a matter of a few hours. Understanding malware written in a programming language that you never have seen before should slow you down only for how long it takes to locate and download a reference manual for that language.

Effective Interpersonal Skills

Handling incidents requires good interpersonal skills. Electronic mail is used a lot in the communication with other teams, but it is not known for its capability to transfer subtleties. People can interpret the same sentence differently depending on the way it is said and the tone that was used, but none of that can be conveyed by email. Often people who exchange emails are using a common language (English, most of the time) that is not the native tongue for either of them. Adding cultural differences into the mix can make the communication challenges even more demanding. To improve the understanding of the case, you should always consider picking up the telephone and calling the other party.

There are, however, some potential drawbacks when talking to a member of the other IRT. When non-native speakers are involved, there may be disparity on how well the other party mastered the spoken versus written language. Some people might have an excellent command of a written language but a mediocre, if not bad, command of the spoken language. That can happen if the person does not have a sufficient opportunity to practice talking and listening to a foreign language but spends a lot of time reading it. Even if a person is good at speaking a foreign language, it is still a question of the accent. That can occasionally cause problems even for native speakers when one, or both, sides have a heavy local accent. As you can see, there are ample opportunities for misunderstanding, so the members of an IRT must be able to handle the situation well.

One situation that can arise when handling a live incident is that a person reporting the incident says offensive things or becomes abusive. In most cases, when that happens, that kind of behavior is not normal for the reporter but is the consequence of the attack. The attacked person might feel that he is not understood and that the IRT member is taking the situation too lightly, so the reporter might become agitated. The IRT member must be able to recognize when such a behavior is the result of panic and when it is not and adjust the approach accordingly.

Does Not Panic Easily

Occasionally a team needs to handle an ongoing incident. The party from the other side is being attacked right now, its business is disrupted, and it is losing money or sensitive information is being siphoned off. It is understandable if that person is not calm but agitated and panicked. For IRT members, it is important to know how to handle that situation. First, the team members must not be easily agitated herself but have a steady temper. They also must work to calm the person on the phone to get the information on what is happening.

Forms an Incident's Image

When handling live incidents, the IRT member must be able to quickly form a picture of what is going on. To assess the situation, decide on possible ways to deal with the situation and recommend actions, which must be done in real time with only partial information. Sometimes the information is partial because the person reporting the incident forgot to provide it, and sometimes because she genuinely does not know it.

Apart from creating a picture, the IRT member must be able to make decisions autonomously and confidently. Someone who is indecisive cannot provide effective help during an ongoing incident.

Advertising the IRT's Existence

It is not sufficient only to have a team; other people must know about it. The team's existence must be announced internally within the constituency and externally to other teams. Only when people know about the team will they ask the IRT for help. One of the more obvious things is to set up a website that explains what the team does and how it can be reached. But that should not be the end of the effort. A website is passive. The team must invest energy and actively introduce itself. That advertising can take many forms and not be limited to the following:

- Attend and present at conferences and meetings.
- Send letters to appropriate people within and outside the constituency.
- Print posters and place them at visible places within the organization.
- Print and give away mugs, pens, stationery, or similar giveaway items.
- Include information about the team in new hire documentation packets, sales material, or a service offering prospectus.
- Meet with key people within and outside the constituency, and talk to them about the team and its purpose.
- Print an advertisement in a magazine or newspaper. Give interviews.
- Broadcast an advertisement on the radio or TV.
- Publish research papers or books.

All these actions can announce the team's existence, its goals and missions, and publicize its achievements. Another goal, when possible, is to seek feedback on the team. How it is fulfilling its mission and how to improve. Nobody is that good that there is no room for improvement.

Acknowledging Incoming Messages

Receiving an email about a compromised device is usually how work on a new incident starts. The first step in this process is for the IRT to acknowledge receiving this initial notification. The acknowledgment must fulfill several goals:

- Ensure the sender that the report is received and given attention.
- Communicate the incident tracking number back to the sender (if assigned).
- Set the expectations on what will happen next.

- Provide information about the IRT and how it can be contacted.
- The acknowledgment reflects team image, so it must look professional and be courteous.

Giving Attention to the Report

Some teams might opt for an automatic response to the sender, but that, albeit providing a quick response, might be viewed as too impersonal. This autoresponse mechanism is easy to set up, so many groups and organizations (not necessarily related to handling security incidents) use it. Unfortunately, a majority of these groups and organizations never follow up on these reports—or it appears that way, so most of the people now mistrust these automated responses. Mistrust in a sense that the sender does not have confidence that his report will ever be worked on. Some people mistrust these automated responses so much that they do not even consider them as a real acknowledgment.

Most people prefer communicating with another human being than an impersonal machine. Having someone who can compose a reply is much better, even if the confirmation is not as instantaneous as it would have been if it were automatic. It is perfectly fine to have a template answer that will be used to acknowledge the receipt of a report, but it is also acceptable to modify it for the added "human touch."

Following are some examples of varying the template text:

- Use the sender's name in the response.
- Ask for additional details.
- Add seasonal greetings (for example, "Happy New Year") but only if you know the sender. Not all people celebrate the same holidays, and some might get offended if they are wished well for a "wrong" (in their eyes) holiday or occasion.

Incident Tracking Number

If the report represents an incident, it must be assigned a tracking number. That number must be told to the sender so that she can use it in subsequent emails. That way, both parties will always know which incident they are talking about. When exchanging encrypted email, the Subject line should contain only the incident number and nothing else. That way, it gives away the minimum details to whoever intercepts the message.

Setting the Expectations

You must set the right expectations on what will happen next and how long it might take. If the report is not an incident, state so clearly with the explanation on what to do if the sender does not agree with the assessment. If the report is an incident, state whether it is being handled right now, and if not, when it might be taken into the process.

Making sure that the other party knows exactly what is happening now, what will follow, why, and when is important to prevent misunderstandings. It is always better to include more information than to leave the other party guessing what is going on, because most of the time, these guesses will be wrong. In this context, more information means where

you are in the process of handing that incident and not more information as in personal information from other compromised sites.

Information About the IRT

Where can more information about the IRT be found and how can it be contacted? This is usually only a pointer to the IRT's website that contains all the details. There will always be people for whom this is the first time they communicate with the IRT. They obtained your email address from someone but they do not know what the IR team does and how. Adding a pointer to where people can learn more about the team is easy and can help first-time reporters a lot.

Looking Professional and Courteous

To make your responses more professional, you can prepare some template text in advance so that whoever will be composing the actual response can cut and paste parts of the template. The template adds to the uniformity of the acknowledgments that, in turn, helps people who are reading them as they get to know what information will be in the acknowledgment and where. This does not mean that people will now send a prepacked response instead of leaving that to auto-responder software. The template is there so that all relevant elements are included in the acknowledgment, and each team member can add their own touch to the response.

Sample Acknowledgment

An example of an acknowledgment can look like this:

> Subject: Your report [IRT-1845249561249]
>
> Reply-to: irt@example.org
>
> Dear Miyamoto-san,
>
> We received your report, and it is assigned tracking number IRT-1845249561249. Please keep this number in the subject line of all subsequent emails related to this incident.
>
> This incident will be taken by one of our incident managers within the next 48 hours. You should receive a further email from the incident owner around that time. In the case that you are not contacted within 4 working days after you receive this email, please contact us again so that we can investigate the problem.
>
> Our contact details, as our incident handling policy and other information about the IRT, can be found at http://www.example.org/security.
>
> Regards,
>
> Adela
>
> ——-
>
> IRT http://www.example.org/security
>
> Emergency telephone: (+1) 234 5678 9012

Cooperation with Internal Groups

In the same way the IRT cannot operate in isolation from the other IRTs, it also cannot operate without support and cooperation from various internal groups and departments. Depending on the particular case, not all departments or functions might be present in the host organization, but if they are, the IRT should consider liaising with them. The groups and departments are as follows:

- Physical security
- Legal department
- Press relation
- Internal IT security
- Executives
- Product security teams
- Internal IT and network operation center (NOC)

Physical Security

Without good old-fashioned physical security, many state-of-the-art security mechanisms would not properly work. There are examples where hardware keyloggers have been installed on computers. That was possible only if someone had physical access to computers. Equipment theft is also possible only if someone can physically grab the equipment.

This group usually operates, or has access to, Closed Circuit TV (CCTV) cameras, if they are installed on the premises. Therefore, their cooperation is invaluable in cases where identity of a person must be confirmed.

Occasionally, it is these people who have power to arrest and detain. So, if the IRT is sure that they identified the culprit within the organization, someone from the physical security group would make an arrest.

Legal Department

Many of us have made some joking remarks on lawyers' accounts, but joking aside, they exist to protect the organization and to protect you. They can be an invaluable asset. The IRT must work to identify whom, from the legal side, would support the team in its job. The best results can be achieved if someone, or a few people, are given an extra task to support the IRT on a long-term basis.

You must expect to invest a considerable effort at the beginning while the legal team learns about the security world and the IRT learns about the legal challenges. Only after both sides understand each other's positions can real cooperation begin.

The IRT should bring all new or different incidents to the attention of the legal team. In the majority of cases, the legal team might decide that the new case falls under one of the previously encountered issues. It is a remaining few that will prompt the legal team to look deeper into the matter to see how the organization can better protect itself from the legal perspective. These improvements might range from the way the IRT approaches similar incidents to modified contracts that the organization will use in the future.

It is also a good idea that lawyers from different organizations reach out to each other and start a dialogue. This area is relatively young, and there are many interesting challenges ahead. It is much easier if they are approached collectively than individually. One such attempt is underway as a part of the Vendor Special Interest Group forum under FIRST. Interested parties can visit http://www.first.org/vendor-sig/index.html and contact moderators.

Press Relations

Sooner or later, the IRT might be involved in a big, or interesting, case, and the press might approach the team to give a statement. Talking to the press can be tricky. Usually the journalists would like to receive as much information as possible, whereas the IRT might not want to disclose all the information, at least not at that particular moment.

The easiest way to handle the press is to have a dedicated PR person assigned to the team to work closely with it. Failing that, the next option is to have someone from the IRT receive PR training and act as the team's spokesperson. The last, and the least desirable option, is to have somebody, without any training, step in front of the journalists. Whatever your case happens to be, following are a few simple tips on what to do when talking to the press:

- There is no such thing as "off the record." Whatever you say can end up being printed. If something is not to be mentioned at the time, do not mention it under any circumstances.
- Be prepared. If possible, ask for questions in advance and prepare the answers.
- Ask to review the final article before it will be published.
- Do not lie. Sooner or later, people will find the truth, and then your credibility is gone—not only your personal credibility, but also the credibility of your team and the organization.
- Do not speculate. Know the facts and stick to them. It is better to say that something is not known than to speculate.
- Know what can be said. Always keep within safe limits. When necessary, a "no comments" phrase can be handy to use.

- Have a message to pass to journalists.
- Do not always answer a question that was asked but one that you would like to be asked (thank Alan Greenspan for this one). If used judiciously, this can help with getting your points to journalists.

Listed like that, it does not sound like much, but it might not be easy to accomplish every time.

If your team is lucky to have a dedicated PR person, she can help you with promoting your team. The PR person can also proactively work with journalists and help them understand what the IRT is doing, why, and how. This all can help you greatly in the time of crisis because informed journalists can present the facts in a more accurate light.

If you judge that an incident might generate inquiries from the press, you should prepare a holding statement that can be used if a journalist contacts the organization and asks for a statement. An example of such an event might be an incident that affects many other companies or has especially significant and severe consequences for your organization.

In virtually all cases, there is not much benefit from proactively contacting the press and offering information about an incident. If an incident occurs, the organization has the IRT that can handle the situation. The business continues as usual. The exception to this rule might be a situation in which someone else will publicize the situation, and you want your version of the events to be heard first.

Internal IT Security

Some organizations might have a separate group that handles only internal security cases, cases pertaining to the host organization. This setup can occur when, for business reasons, all customers' incidents are handled by one team and internal cases by another.

In that case, the internal IT security group is a natural an ally of the IRT. Having a close relationship can be mutually beneficial. Both teams can organize regular meetings to exchange information on what kind of attacks they are seeing and observe trends. The group handling customers' incidents should provide information only on types of attacks but not who has been attacked. In addition to the regular information exchange, both teams should enable members from one team to rotate into another team and spend some time working with the other group.

Despite all this synergy between the teams, some functions will be duplicated. If business reasons dictate the existence of two teams, duplication is natural.

Executives

It was mentioned previously that the IRT should have an executive sponsor. Apart from having a sponsor, the IRT must have the means to reach other executives. There must be an arrangement for the IRT to brief the executives on a regular basis and when emergencies occur.

Regular briefings are important so that the executives can learn about the organization's exposure to the newest security threats. They can also learn about the IRT's challenges to address the threats and make appropriate decisions. This communication is even more important during the crisis. Additionally, because of the exposure the team will get, the executives will know whom to talk to when they need more information. This way, executives will not waste time asking around and receiving nonauthoritative or plainly wrong information. For executives, it is vital to be informed whether their part of the organization is affected by the incident and, if it is, how and to what extent.

Direct communication with the executives is important for the IRT because it provides a visibility opportunity for the team. The security of the organization and the IRT will gain in stature in the eyes of the executives. Visibility and consistent good performance will transform the IRT into a trusted adviser to the executives on matters related to information security.

A consistent and constant information flow from the IRT to the executives is important. For executives to rely on the team's messages, they must follow a fixed pattern. Even if the message is "nothing to report," it must be delivered when expected. In a crisis, the messaging period will change and will be delivered when required instead of waiting for the next scheduled time slot. It is not necessary that the message is always delivered in person. Often an email or voice message will suffice.

The format of the message must be suitable for the purpose. Executives are busy people with little time to waste, so the communication must be specifically tailored to fit the purpose. That encompasses not only the graphical layout but also the file format and media. Big Microsoft Word files are not useful if received on a Blackberry. Voice mail can be a more noticeable event than receiving yet another email. On the other hand, it is easier to reread a mail message multiple times than listen to the same voice mail, especially if the interesting part of the message is close to its end. The teams must know what it wants to accomplish and tailor the messaging accordingly.

Here are few tips when communicating with the executives:

- **Frequency:** Not more often that every two weeks but not less than once a month for regular updates. During a crisis, the first message should be sent as soon as the severity of an incident reaches a certain criteria. (For example, the number of compromised hosts, certain key hosts, or what services are compromised.) After that point, the frequency should be a function of the incident, and reporting can be done from every hour to once a day.
- **Content:** Keep it short and simple. Provide pointers to where all details are being kept. Order information chronologically so that the most recent information is presented first. Background information can be added at the end. Do not forget to include the impact to the organization—why this communication is important to the executives. The next steps and the time of the next communication also must be presented, together with actions that executives must undertake.

When sending both an email and a voice message, they should not be identical. The email can contain more background information, whereas the voice message should focus only on the most recent developments.

- **Format:** Between two slides to four slides for regular face-to-face meetings. For all other regular updates, text email (no Microsoft Word or Adobe PDF documents) together with a voice message should be used. Text email is preferred over all other formats because it can be quickly downloaded even over a slow connection (for example, a 2400-baud modem line in a hotel) and easily read on any device.

  A web page must be created where executives can find all the information. That must be a single top-level page that gives an overall view of all current events. This top-level page must then contain links for each individual incident and to all other communications to the executives.

- **Length:** Optimally, approximately 2 and not longer than 3 minutes for a voice mail and a one-page email (approximately 200 words to 300 words). Everything else should be given as additional information on a web page.

Here are examples of a voice message and an accompanying email that provide an update on an ongoing incident. We will assume that the update is provided once daily. The voice mail is given first:

> This is Joe Smith with an update regarding the incident that occurred on January 30, 2009. This voice mail is sent to the emergency executive council. The full list of the recipients is given at the end of this message. All information in this message is confidential.
>
> On January 30th, unknown attackers used an unpatched vulnerability to gain access to servers in accounting and engineering. The unauthorized access was discovered when attackers were transferring files to an external server. There is no PR coverage of the incident.
>
> The status on February 3rd is that 60% of all servers in the organization have been patched. All servers in accounting are patched and are all back online. 80% of servers in engineering are patched. The help desk is the most exposed part of the organization, with only 20% of servers patched. Our IRT report web page contains full details of the patching progress.
>
> In addition to patching, our intrusion prevention systems are updated with the new signature, and all firewalls are configured to make exploitation of the vulnerability harder.
>
> We expect to patch all servers in the organization by February 10th. Determining the extent of leaked personal information will be finished by February 5th. After the scope of the leak is determined, the Legal and HR department will be engaged to asses our legal exposure.
>
> No actions are required from the executive council at this time.
>
> The next regular update is on February 4th at 14:00.
>
> This message is sent to: name_1, name_2, ...
>
> Regards,
>
> Joe Smith

The accompanying email can look like this:

From: IRT@example.com

Subject: Status on the security compromise on 2009-Feb-03

—— CONFIDENTIAL – DO NOT DISTRIBUTE ——

Hello,

This is Joe Smith with an update about the incident that occurred on January 30, 2009. This email is sent to the emergency executive council.

Background

On January 30th, unknown attackers used an unpatched vulnerability to gain access to servers in accounting and engineering. The unauthorized access was discovered when attackers were transferring files to an external server. There is no PR coverage of the incident.

All details related to this incident can be found at http://www.example.com/IRT/incident web page.

Current status

Patching is in progress across all the organization. The following table provides status per individual parts of the organizations:

Accounting: 100%

Engineering: 80%

Manufacturing: 40%

Web-farm and mail servers: 70%

Help desk: 20%

Overall: 62%

In addition to patching, our intrusion prevention systems are updated with the new signature, and all firewalls are configured to make exploitation of the vulnerability harder.

The next update will be sent on Feb 04 at 14:00.

Next milestones

Feb 05—Determine the scope of personal information leak.

Feb 06—Engage Legal and HR to determine legal exposure due to personal information leak.

Feb 10—100% of servers to be patched.

Pending executive actions

No actions were required from the executive council at this time.

Regards,

Joe Smith

—— CONFIDENTIAL – DO NOT DISTRIBUTE ——

Product Security Team

If the host organization is a vendor that is responsible for developing and maintenance of a product or service, it should have a dedicated team that deals with security vulnerabilities in the products. Similarly, like with the situation with IT, both teams, product security and IRT, can benefit from having close ties. The product security team can provide information on different vulnerabilities so that the IRT can start looking at whether it is being exploited. Information on vulnerabilities can also be used to reevaluate some old data. What was previously seen as only noise or random attempts might suddenly be seen as focused efforts to exploit a particular vulnerability.

The product security team can benefit from receiving information on new attacks, analyzing how the attacks affect its products, and passing the knowledge to the group responsible for maintenance and product design.

Even if the organization is not a vendor, the team should establish ties with vendors' product security teams. At least, the IRT must know how to contact them. Vendors always appreciate when they receive notification on a new vulnerability or other suspicious behavior of their products.

Internal IT and NOC

Depending on the organization's size and complexity, you may have a separate IT group that maintains and monitors the internal network. If you are an Internet service provider (ISP), you probably would have a separate network operation center (NOC) that maintains a network used by your customers. These two groups are your partners. They can provide the IRT with the current information on what is happening in the network (internal or external). They can also provide early warnings about new attacks while they are being tested[1]. NOC, in particular, can add network-centric view on attacks and contribute methods how to combat attacks using network infrastructure.

Be Prepared!

An IRT, by its nature, deals with emergencies and exceptions. As such, it is hard to be prepared for something that cannot be foreseen. Although nobody can be prepared for

[1] Occasionally, you can capture early samples of new exploits while they are tested by miscreants before deploying them on a large scale.

the exact incarnation of the next worm—because we do not know what it will look like—you can be prepared for a general threat of worms. The new worm is expected to have some general characteristics common with previously seen worms. It is known how previous worms affected the organization, so the IRT can prepare to handle future outbreaks similar to the previous ones. Following are some steps that can be taken to prepare to handle incidents:

- Know current attacks and techniques.
- Know the system the IRT is responsible for.
- Identify critical resources.
- Formulate response strategy.
- Create a list of scenarios and practice handling them.

Know Current Attacks and Techniques

It is imperative for the IRT to possess an intimate knowledge of current attack techniques and attacks themselves. Without that knowledge, the IRT would not know how to distinguish an attack from some legitimate activity. Obviously, the knowledge must not be limited only to the attacking side. It must also cover the defense. How can you protect your organization from various attacks and what are the potential drawbacks of different methods? This also encompasses features and capabilities of installed equipment. And last, but not least, know the network's topology and characteristics.

The next question is, How should you gather that knowledge? Unfortunately, there is no easy way to accomplish that. It must be done the hard way. Reading public lists like Bugtraq, full-disclosure, and others is standard for every team. Attending conferences and learning new issues is also important. Analyzing what is going on in the team's constituency is obligatory. Monitoring, as much as possible, underground is necessary. Setting up honeypots and honeynets and analyzing the activity is also an option. But, above all, talk to your peers and exchange experiences. That is something that cannot be substituted with anything else. All evidence points to the fact that miscreants do exchange information and that they do it rather efficiently. Good guys, on the other hand, tend to lag behind in sharing the information. Chapter 6, "Getting to Know Your Peers: Teams and Organizations Around the World," talks more about some of the main forums that IRTs can use to interact with peers.

It is not necessary for each IRT member to monitor all the sources. There are simply so many potential sources to collect the information that it is almost impossible for a single person to track them all. One workaround is to contract out this task to an external company or, if it is done internally, share the task among team members so that not all of them are monitoring the same sources.

When monitoring sources is contracted out, you need to make sure that the received information is relevant to the IRT. For example, if your constituency is predominately using the Solaris operating system, the information on vulnerabilities in Microsoft

Windows is not that useful to you. The positive side of contracting out this task is that you are freeing your resources. The potential negative side is that you might need to renegotiate your contract if you want to change the scope of the information you are receiving.

If the information collection is done internally, you can include other groups or individuals to help you with that task, even if they are not part of the IRT. This help can be either formal or informal. If your organization has a group that monitors external information sources, you can make a formal arrangement with them to receive only the information that might interest the IRT. If you do not have such a group in your organization, you might find security-conscious individuals who are monitoring some of the sources that might also interest the IRT. If there are such individuals, you can ask them to forward all potentially interesting information to the IRT. This would be an informal arrangement that, in some cases, can be reliable and function quite well. If you have such arrangement, do make sure to nurture that relationship. Commend these people for what they are doing and try to make them feel appreciated. You can give them some small awards or take them out for a dinner. People like to see that their work is appreciated, so an occasional meal together will pay for itself many times over by the work these other people will do.

If your IRT decides to operate a honeypot or honeynet, you must make sure that you will have sufficient resources to do so. A honeypot is a nonproduction service exposed to the Internet with the purpose of being (mis)used by an attacker. The IRT can then capture malware and gain firsthand knowledge about how it infects devices and propagates. The service can be emulated with special software or it can be a real service. A honeynet is a network of honeypots. One way to arrange a honeynet is to assign an unused (either by your organization or in general) portion of IP addresses to a group of computers and monitor all traffic going in and out of that network. Computers can be either real hardware or virtual. If they are virtual computers, you should know that some malware can detect whether it is executed on a virtual platform and, if it is, the malware will not behave maliciously.

Although installing a honeypot and honeynet is relatively quick, monitoring and analyzing what is going on requires a considerable effort. You also must make sure that your honeypot is not used to attack someone else. Overall, honeypots can be valuable sources of information, but they also require significant effort to properly use them.

Know the System IRT Is Responsible For

The IRT must know what it is protecting, the location of the boundaries of the systems for which it is responsible, and the functions of different parts of the system. After defining boundaries, the next step is to identify the groups (or people) that can be contacted when the IRT must cross the boundaries. All this is only the start. These steps just define the area of the IRT's responsibility. The next task is to determine what is "normal" within that area. This is important because the incident is something that is not expected. It is an activity that is not standard. Most of the malware would initiate actions that are not usual for an average user (for example, starts mass mailing or connects to an IRC channel). If the

IRT knows what is normal for the given system, it will be easier to spot deviations and start investigating them. This is also known as determining the baseline. Depending on the organization, some of the tasks to determine the baseline can be done by IT or some other department and not the IRT. Irrespective of who is doing it, the IRT must be able to receive and use that information to spot anomalies.

The baseline means different things for different aspects of the overall system. On the highest level, it can consist of the following things:

- Number of remote users
- Number of internal users
- Total consumed network bandwidth, inbound and outbound, at all links (for example, between branch offices, toward the Internet)
- Traffic breakdown per protocol and application (TCP, UDP, mail, web, backup, and so on) and bandwidth utilization per protocol

Each of the categories can then be further refined and a more detailed picture can be formed. For remote users, remote IP addresses can be recorded. A traffic model of a user can be formed by recording how much traffic (packets) is generated inbound and outbound and what protocols and applications have generated it. For some protocols, what types of packets are being generated can even be recorded. If we take TCP as an example, the ratio of SYN packets versus ACK packets can be recorded. How many fragmented packets are in the mix? That information can then be used to identify the presence of anomalous traffic because different types of packets are used by different attack programs. Another type of information that can be recorded is the direction of the traffic. That is important because the site can be the target or source of an attack.

Information used to build the baseline should come from multiple sources to build a better picture. Traffic snapshots (or full captures for small sites), Netflow data, syslog logs, logs from intrusion prevention/detection systems, and application logs of all of these sources should be used to build the baseline.

Collecting data to form the baseline can be illuminating. On occasions that can give an interesting picture and reveal all sorts of things that are being done without the knowledge of appropriate groups. It does not always have to be in the negative sense. It is common to find some servers still offering services and being used, even though they were officially decommissioned several years ago. Various cases of network or system misconfigurations can also be detected (for example, traffic being routed down the suboptimal path). Unofficial web servers and wireless access points are also likely to be discovered during the process.

Taking only a single snapshot might not be sufficient to establish a credible baseline. Traffic and usage patterns change over time. They are different depending on the hour within a day, a day in a week, and month in a year. During lunch time, it is expected to see less traffic than in the middle of the morning. Around holidays, traffic will be again

lower than during the normal working days. Adding or removing a significant number of computers will affect the baseline, too. The message is that information should be constantly updated with the latest measurements.

The baseline does not need to be precise to the byte and must not be used rigidly. If, for example, 40 percent of incoming traffic on the main Internet link is TCP, the times when that ratio increases to 45 percent do not need to be immediately considered as a sign of an attack. But if it suddenly jumps to 60 percent or more, it is probably suspicious. There will always be some variation in each of the baseline components, and the IRT must be aware of what the expected variation is. That can be determined only with prolonged and continuous inspection.

Identify Critical Resources

The next step in the process is to identify critical resources. What resources are critical for the business and in what way? What will happen if a resource is unavailable? If the company website is used only to present what the organization is about, it being unavailable might not have severe consequences. If the website is also used for ordering, you need to keep the period of not being available as short as possible. The billing system might be more critical than email infrastructure, and so on.

This part of the process must be done with help from different groups and departments within the organization. Each of them should identify what resources are critical for their business. All that information then must be taken to a higher level of management and looked at from the global organization's perspective. Although something might be critical for a given department, it might not play a significant role from the overall business perspective. The criticality of services should be reviewed periodically and after significant change in the business model is introduced.

Formulate Response Strategy

After completing the inventory of critical resources, an appropriate response strategy can be formulated. This strategy is supposed to answer questions such as: If a service, or server, is compromised, what can and should be done? Here are few examples that illustrate this point:

- If a company's website is defaced or compromised, what needs to be done? If the website is used only for general information, it can be simply rebuilt, and no effort will be spent trying to identify how the compromise happened or who did it.
- If a host used for collecting billing information is compromised and the attacker is siphoning credit card information from it, can you simply shut off the computer to prevent further damages? Although that can prevent data theft, it might also prevent collecting billing information, and the organization will lose some money as a consequence.

- What level of compromise needs to happen before a decision to attempt to identify a culprit for possible prosecution will be made versus just shutting him out? This can possibly mean that the attacker will be left to (mis)use the compromised system for some time while the investigation is going on. What is the point when the business might seriously suffer as the consequence of the compromise and the investigation has to be stopped?

Answers to some of the questions can also lead to rethink the way the system is organized or services are offered. In the case of a website, maybe it can be made static and burned on a DVD so that the possibility of defacement is reduced if not eliminated. Maybe some critical services can be split across multiple computers, so if one is compromised, it can be shut down without affecting the other service.

Why is this important? When the attack is ongoing, there might not be sufficient time to think about what the various actions of the attacker and defenders can cause to the organization. At that time, the IRT must react as quickly as possible to minimize the impact to the organization. Knowing how different computers and services depend on each other and how important they are to the organization enable the team to respond quickly and accurately while minimizing the impact and disruptions to the business.

Create a List of Scenarios

Instead of waiting for incidents to happen and then learning how to respond, the IRT should have regular practice drills. Some most common scenarios should be created, and the team must practice how to respond to them. This is especially important after new members join the team. Even if they are experienced in incident handling, each organization will have some processes slightly different, and practice drills are the right time and place to learn them. The main purpose of these exercises is that people gain practice and confidence in handling incidents. They also serve to test how effective the current response might be given changes in the network (added new devices or software features) and to accordingly modify the way to respond. These exercises do not need to be limited only to IRT but can involve other parts of the organization. In such joint exercises, all involved participants must know when the exercise is active. This is to prevent confusion so that people will not panic or take wrong actions thinking that the real compromise is happening.

What can these scenarios look like? For a start, they must cover the main aspects of all handled incidents. If these incidents happened once, there is the possibility that they will happen again. Here are some suggestions of what can be covered:

- Virus or worm outbreaks
- External and internal routing hijacked
- DNS-related attacks (for example, the organization DNS entry gets changed and points to a bogus site)
- Computer compromise

- Network sniffer installed on several computers
- Website defacement or compromise
- Phishing attacks
- DoS attacks
- Emergency software upgrade

These may be the most common scenarios that one organization might encounter. Depending on the organization's role and technical capabilities, some additional scenarios can be created. Also, some of the scenarios might not be applicable to the team because of job separation (for example, software upgrade is done by the IT department).

These practice drills can be only a paper exercise, or they can be conducted on an isolated network segment. Instead of using physical devices, it also might be possible to either simulate them or to use virtual devices (for example, virtual computers in VMware). What method and technology will be used depends on the goals and capabilities.

Devices we can simulate are computers, routers, and networks of devices. In these simulations, devices can be either targets of simulated attacks or used to observe how malicious software behaves. Some of the software for creating virtual computers are VMware, Parallels, Xen, and QEMU. A more comprehensive list of different software is posted at the Wikipedia web page at http://en.wikipedia.org/wiki/Comparison_of_platform_virtual_machines. Some of the software for creating virtual computers can also be used to connect virtual computers creating virtual networks. Dynamips, Dynagen, and Simics are some of the software that can be used for simulating routers and network of routers.

A paper exercise is good for formulating the initial response on an attack that has not been encountered yet and to modify an existing response after the system changed because the equipment changed or software was upgraded. Testing the response, on the other hand, is best done on the actual equipment. At that time, all the previously invested work to determine the baseline and what is the normal state for the network pays off. Having this information, the team can send (or simulate) the right amount and the mix of traffic and then superimpose attacking traffic on top of it. In some instances, that might not be relevant, but in others, such as DoS attacks, it can be relevant. The instances when the baseline is not that important are in the presence of single-packet attacks. In that case, it is sufficient to send only a single packet to compromise or reset a device or a process on the device. You need to use real devices for the verification to make sure that the simulator reflects the real device's behavior. It can take some time for the simulator to be updated with the newest features present on the devices.

Use simulators and emulators to practice the response once when you are sure that it actually reflects how the real device will behave and when it is known what the response is. After the response is established and practiced, new elements should be added to it.

Some unexpected or unusual elements should be introduced. They can be various things, such as the following:

- The telephone network is down; at the same time, team members cannot use fixed telephony or mobile phones to communicate.
- It is impossible to physically reach the affected device (for example, a computer is locked in a room and the room key is lost).
- A new device is introduced into the network without anyone's knowledge (for example, a load-balancing device inserted in front of the web farm) or the network topology is changed.

Introducing these elements should prevent people from trying to fit the problem into the solution instead of the other way around. Each new case should be like the first one and should be handled with a mind open to any eventuality.

The last things to practice are, seemingly, impossible scenarios. You must accept that, occasionally, the research community does come up with a revolutionary new attack technique, and things that were considered impossible suddenly become routine. Here are a few examples:

- A scenario that contains a logical paradox. That would be the trick case to verify that the handler can notice the paradox. An example might be to invent a device under attack that is not connected to the network or withhold information about an intermediate device.
- A feature suddenly stops working (for example, packet filters do not block packets; rate limiters do not limit packet rate).
- Significant improvement in attack techniques (for example, a complete compromise of MD5 and SHA-1 hash functions, an AES crypto system is broken, and the number factoring becomes trivial).

For some of these scenarios, there may be no valid, or possible, responses, so their value lies in forcing people to think out of the the-box. Some of the scenarios might one day become reality—a collision in MD5, a number factoring using quantum computers—so thinking about them today might give the organization an edge.

Measure of Success

How can you measure whether the IRT is successful? Executives always like to know whether the budget given to the IRT is well spent and whether the organization is more secure now than it was before. There is no universal answer to these questions. Instead of trying to provide partial answers, it is better to describe a framework on how to create metrics that will be used to measure the team's success.

At the start, it must be said that, by itself, counting the number of incidents the team has handled in a given time period is not a good measure of how the team is doing. It can

certainly be a component of the measure, but that number by itself is not informative, and there are good reasons why. After the team starts operating, it will initially see only a few incidents. Quickly that number will start to rise rapidly, and the more the team is working on them, the more incidents will come to light—and the number of incidents will just keep on growing. From that perspective, it might appear that the team is not doing things right because before it started working, there were only a few incidents, and now they never stop. In reality, the reason for seeing an increased number of incidents is because the IRT is actively looking for them while before nobody took notice of them, even when the signs were obvious.

The way to approach creating the metrics to measure the team's success is to start from who is the team's constituency and what is the team's goal, and what it tries to do for the constituency. That will provide the starting point of defining what can be measured. Additionally, you can try to measure changes in the risk the organization faces from a compromise. Part of that risk assessment is the speed of recovery and limiting the damage after the incident. The final part of the metrics is the team's influence and standing with the community. A good guide on how to define what to measure, how, and why is the ISO 27004 standard. Let's now look at some examples of how metrics for measuring the team's success can be defined.

One of the goals for most of the IRTs is to increase security awareness within the constituency. This goal can be aligned with specific policies such as "All users will receive basic security training" or "All users' passwords will be longer than six characters." Data on a number of users receiving security training and the results of checking users' password can be easily obtained, so you can calculate where you are in meeting the policy goals. This then directly feeds into one of the measures of the team's success.

Assessing changes in the risk the organization faces from computer attacks is harder to accomplish. You cannot directly measure the attacker's willingness to attack your organization, but you can use the fact that attackers are mostly opportunistic creatures to your advantage. If you are a hard target, attackers will go after others who are easier targets. What you can measure here is what is happening to your organization relative to your peers and the industry. Reliable data on attacks is hard to come by. CSI and BERR surveys (mentioned in Chapter 1) can serve as guides, but the numbers must be taken with caution. Attacks do not have to be targeted; you can also compare the number and severity of virus outbreaks within the organization versus the industry. One example that illustrates this very well was an outbreak of a particular worm a few years ago. Most of the other organizations were infected, but Cisco was not because of the measures the Cisco InfoSec team implemented.

Being a leader in the field is also a sign of the team's success. This can be measured by looking at the number of talks the team was invited to give, the number of interviews the IRT members gave, and how many of the team's ideas were incorporated into best practices and international standards.

Summary

Running a successful IRT involves many aspects. The team must have the right people and do the right thing. Not only must you pay attention to major things, but you also must not lose sight of the small details. Although all these details might look overwhelming, with dedication from the entire team, they can be achieved, and you will have a successful and respected IRT.

References

Comparison of platform virtual machines, Wikipedia. January 19, 2009. http://en.wikipedia.org/wiki/Comparison_of_platform_virtual_machines.

Computer Security Incident Handling Guide, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-61 Revision 1. Tim Grance, Karen Kent, and Brian Kim, March 2008. http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf.

Council Directive 93/104/EC of November 23, 1993 concerning certain aspects of the organization of working time, Council of the European Union, November 23, 1993. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1993L0104: 20000801:EN:PDF.

Data elements and interchange formats—Information interchange—Representation of dates and times, ISO 8601:2004, 2004-12-03.

Directive 2003/88/EC of the European Parliament and of the Council of 4 November 2003 concerning certain aspects of the organization of working time, Official Journal L 299, 18/11/2003, p. 0009—0019. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003L0088:EN:HTML.

Dynagen, http://dynagen.org/.

Dynamips, http://www.ipflow.utc.fr/index.php/Cisco_7200_Simulator.

Forum of Incident and Response Security Teams, http://www.first.org/.

The GNU Privacy Guard, http://www.gnupg.org/.

The International PGP Home Page, http://www.pgpi.com/.

ISO (2009), Information security management measurements, ISO/IEC 27004:2009. http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=40874&ICS1=1&ICS2=140&ICS3=30.

PGP Corporation, http://www.pgp.com/.

Virtutech Simics, Simics, http://www.virtutech.com/.

Index

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W