IST-Africa

IST-Africa 2010 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2010
ISBN: 978-1-905824-15-1

The Community-oriented Computer Security, Advisory and Warning Team

Ian ELLEFSEN, Sebastiaan VON SOLMS
Academy for Information Technology, University of Johannesburg, cnr Kingsway & University Road, Auckland Park, Johannesburg, 2006, South Africa
Tel: +27 11 5592967, Fax: +27 11 5592138, Email: iellefsen@uj.ac.za, basievs@uj.ac.za

Abstract: Critical information infrastructure protection is vital for any nation. Many of a country's critical systems are interconnected via an information infrastructure, such as the Internet. Should the information infrastructure be targeted by remote attacks, it would have a devastating effect on functioning of a country. Developing nations are no exception. As broadband penetration rates increase, and as Internet access speeds increase, developing nations have to implement safeguards to ensure that their information infrastructure is not target or abused by cyber attackers. Many nations implement CSIRT structures to aid in the protection of their information infrastructure. However these structures are expensive to set up and maintain. In this paper we introduce a Community-oriented Advisory, Security and Warning (C-SAW) Team, which aims to be a cost effective alternative to a CSIRT. C-SAW Teams aims to combine cost-effectiveness with the ability to mutate into a full-scale CSIRT structure over time.

Keywords: Critical Information Infrastructure Protection, CSIRT, WARP, C-SAW

1. Introduction

Critical information infrastructure plays a crucial role in modern society. Information infrastructures, such as the Internet, are used to provide interconnection for many different critical systems. Critical systems are interconnected to such an extent that should the information infrastructure fail, the system would cease to function correctly.

Information infrastructures are however vulnerable to attack from a remote location. This is due to the public availability of systems such as the Internet, and the integration of Internet-based technologies in many critical systems. Cyber attacks are becoming more commonplace as broadband rates increase and as more of the world has Internet access.

In order to combat cyber attacks, and prevent information infrastructures from being abused, many developed nations have Computer Security Incident Response Team (CSIRT) structures in place. CSIRTs provide incident handling and incident response facilities for events which may affect a country's national information infrastructure.

A major disadvantage for developing nations wishing to implement a CSIRT structure is that they are expensive to setup and run. In this paper we will address this issue by introducing the theoretical concept of a Community-oriented Security, Advisory and Warning (C-SAW) team.

A C-SAW structure requires that entities needing protection from a CSIRT be divided into a number of communities. These communities are then grouped under a C-SAW team. Over time, as teams grow they are combined to encompass a larger number of communities. This scaling up attribute of C-SAW teams allows a full-scale CSIRT structure to be developed over time, while also harnessing a level of cost-effectiveness and autonomy.

In the following section we will discuss critical information infrastructure protection. We will address why critical information infrastructure protection is required, and then discuss some challenges which developing nations face with regards to providing critical information infrastructure protection.

2. Critical Information Infrastructure Protection

Critical Information Infrastructure Protection (CIIP) plays a vital role in the modern world. All countries rely on a specific set of critical systems, such as electricity distribution, water distribution, telecommunications, and economic systems, in order to function [4, 11]. Should these systems be damaged, or prevented from operating in any way, it would cause a devastating disruption to the county's ability to function.

Many critical systems rely on large interconnected networks, such as the Internet, in order to function effectively. However, this reliance on these information infrastructures creates a point of attack, where a remote attacker can damage, or destroy a critical system.

The infrastructure which is used to provide interconnection for critical systems is generically referred to as Critical Information Infrastructure. Protection of the critical information infrastructure is of vital importance to the effective functioning of critical systems. In the following section we will discuss attacks which can be targeted against the critical information infrastructure.

2.1 Cyber Attacks

Cyber attacks (including cyber warfare and cyber terrorism) are becoming more prevalent as the globe becomes interconnected [1]. Although much of the observed attack traffic (Internet traffic specifically targeted at a software exploit or vulnerability) originates from the developed world, however many developing countries are now appearing as a source for attack traffic [2].

Cyber attacks need not require a high level of technical ability. Tools such as Metasploit [10] allow users with relatively limited technical abilities to make use of software exploits. This problem is compounded by higher broadband rates and higher broadband penetration in developing countries, where security mechanisms and policies are not adequate or are unenforceable.

In the following section we will discuss Computer Security Incident Response Teams as a mechanism used in many developed countries to provide support for critical information infrastructure protection.

2.2 Computer Security Incident Response Teams (CSIRTs)

Many developed countries have mature CIIP systems in place, to aid with, and to help prevent attacks against their national critical information infrastructures. This allows them to quickly respond to events, to provide warnings, and to handle incidents.

Computer Security Incident Response Teams (CSIRTs) are organisations within a national critical information infrastructure protection structure, which are tasked with the providing support for cyber events [7, 13]. They are further responsible for the dissemination of computer security information, such as vulnerability reports, to relevant parties, called the constituency of the CSIRT.

CSIRTs have a hierarchical nature [7]; a National CSIRT (sometimes called a Coordinating CSIRT) will coordinate the efforts of Regional CSIRTS. Regional CSIRTs will in turn coordinate with security teams inside companies, and private entities.

CSIRTs will often have links to their international counterparts which allows information concerning current cyber events to be distributed quickly. Cyber events can be

handled quickly, and the effect of these events can be limited. Figure 1 shows the relationship between different components within a classic CSIRT hierarchy. Coordinating CSIRTs have relationships with Regional CSIRTS, which in turn have relationships with end users (the constituency). The Coordinating CSIRT will also have relationships with international CSIRTs; this allows for efficient communication of security related events.

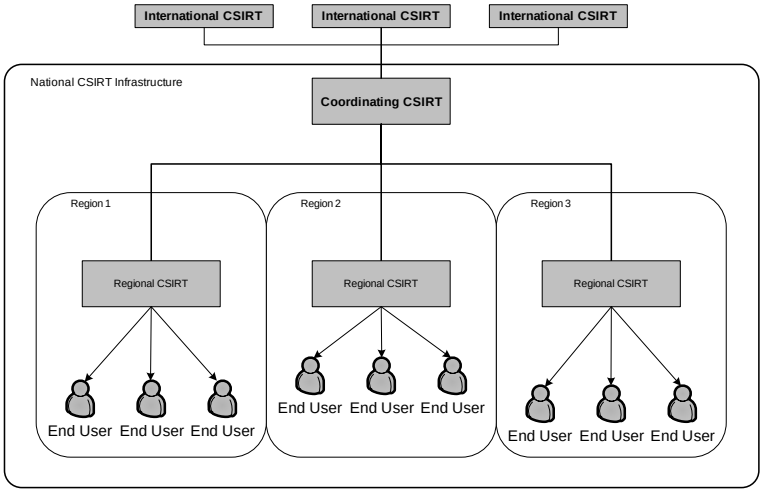

Figure 1: Overview of a CSIRT Structure

The primary focus of a CSIRT structure is to provide incident handling and advisory services to their constituency [13]. CSIRTs provide two main types of services; these are reactive services, and proactive services [13]. Reactive services are those services which a CSIRT provides when there is an incident; as the name implies, the CSIRT will react to these event. Proactive services are services aimed at preventing future events; these normally take the form of education, and information exchange.

CSIRT structures require personnel with expert knowledge and large amounts of equipment to manage. Developing nations that wish to implement a CSIRT structure will be required to invest heavily in outside knowledge and experience. However, development of a national CSIRT structure is vital for these nations, and to protect their information infrastructure from being abused. In the following section we will discuss why the creation of a CSIRT structure is of vital importance for the developing world.

3. The Need for Protection in the Developing World

As the demand for Internet-based services increases, and the integration of information infrastructures into critical systems becomes common place, the capacity of the network links to developing nations will increase. This can be seen by the number of new fibre optic cables which are being laid in Sub-Saharan Africa, and throughout the developing world.

This increase in available Internet connectivity will allow Internet-based service to be available to a larger percentage of the population in these areas. However, the lack of adequate protection mechanisms in many of these countries will allow them to become a launch pad for cyber criminals.

In this section we will discuss the effects of increased broadband penetration to developing nations, specifically in Sub-Saharan Africa. We will then discuss how a lack of a national computer security effort may affect these developing nations. Finally we will introduce the concept of a Warning, Advice, and Reporting Point as a starting point for addressing these issues.

3.1 Increasing Broadband Penetration

Developing nations are becoming ever more interconnected. This is due to the high demand for Internet-based services and content. Large interconnectivity projects, such as the SEACOM marine cable, will allow developing nations in Sub-Saharan Africa to have access to vastly more bandwidth in the coming years. For example, the SEACOM cable [12] will provide a large amount of bandwidth to Sub-Saharan Africa.

The available bandwidth to developing nations is set to increase even further in the coming years. By 2011, a number of new marine fibre optic cables will be become active [2, 9]. Developing nations are not the only countries to benefit from increased Internet connectivity. Many developed nations are implementing high speed Internet technologies, such as WiMAX, 4G mobile networks, and "Fibre-to-the-home" solutions, which will allow users to connect to the Internet at higher speeds [2].

Increases in bandwidth will allow cyber attackers to utilise developing nations for more complex attacks. National structures have to be put in place to insure that the newly available information infrastructure does not get abused by cyber attackers. In the following section we will discuss the lack of national computer security efforts in many developing nations. This lack of security coordination allows developing nations to be seen as a "safe haven" for cyber criminals.

3.2 Lack of a National Computer Security Effort

In many developing nations there is a lack of a coordinated computer security, or cyber security, effort. Cyber criminals will use developing nations as a staging point to launch cyber attacks [3, 8].

Some developing nations do have teams which focus on computer-related crime, such as computer forensic investigation units or computer security efforts within private organisations [5]. However, these groups are focused on the forensic investigation of computer crime or the protection of national information infrastructure, and do not constitute a national coordinated cyber security effort.

CSIRTs on the other hand provide support and monitoring for computer security related events. As a national CSIRT structure grows, they could possibly provide computer forensic services, however this is not their primary focus. The lack of a CSIRT structure in developing nations creates a "gap" in the protection of the information infrastructure. It is this gap which cyber criminals are abusing in order to launch cyber attacks from developing countries.

"Full-blown" CSIRTs are an attractive solution to provide computer security incident handling; however the initial setup cost can be prohibitively expensive. This may prevent developing nations from setting up CSIRT structures.

In the following section we will discuss some of the limitations of a CSIRT. We will then discuss the concept of a Warning, Advice and Reporting Point (WARP), which is a smaller team, focused on providing computer security incident handling services to a small group.

3.3 Warning, Advice, and Reporting Point (WARP)

CSIRTs by their very nature are large and complex organisations which provide excellent protection for national information infrastructure. However, as Harrison and Towsend [6] explain, CSIRTs are limited in two ways; they are expensive, and they are reactive. CSIRTs are expensive in terms of setup, maintenance, personnel requirements, and technical requirements. CSIRTs are reactive in terms of the primary service they provide. Only once an event has occurred can the CSIRT relay the relevant information to their constituency in order to limit the effect.

A third limitation which can be identified is the complexity of knowledge which a CSIRT will pass on to their constituency. Many smaller businesses, those without dedicated computer security personnel, or simply the "man on the street", will not be able to decipher vulnerability reports which are passed on by the CSIRT. Although attempts are made by the CSIRT to make this information accessible to everybody, there will be a large number of cases where the information will not be acted upon. This will result in large number of businesses not benefiting from the CSIRTs services.

In order to address some of these concerns, some countries have implemented Warning, Advice, and Reporting Points (WARPs). WARPs are not meant to replace CSIRTs, they are meant to complement each other [6], by allowing information from a CSIRT to be accessible to a much broader range of constituents.

WARPs have a small number of members, analogous to the constituency of a CSIRT; these members will generally be operated by one or two individuals this allows them to provide member-specific support. The focused nature of a WARP allows them to be highly cost-effective, and provide protection to a larger number of individuals [6]. The small number of members of a WARP allows it to remain focused on the needs of the groups [14]. This encourages member participation in computer security matters.

WARPs will not exist in isolation, as discussed above, WARPs and CSIRTs are meant to complement each other. CSIRTs service larger constituencies, and WARPs act as a bridge between smaller groups and the larger CSIRT.

The cost effective nature of a WARP is very attractive to developing nations where the outline of a full CSIRT is prohibitively expensive. However, WARPs cannot be simply transplanted into a system without CSIRT support, due to the symbiotic nature of the two organisations. In the following section, we will introduce the Community-oriented Security Advisory and Warning Team, which is aimed at combining WARP-like cost-effectiveness and CSIRT-like services in a dynamic structure which can be tailored for developing nations.

4. Community-oriented Security Advisory and Warning Team

Developing nations may not have the resources available to implement a full-scale CSIRT. As discussed above, CSIRTs are expensive and reactive; they also service a very large constituency and may not be able to effectively filter information for its constituents. WARPs on the other hand are very small in comparison (up to 100 members). They are highly cost-effective, and provide highly focused information for its members. WARPs by nature are loosely coupled within the environment, where as CSIRTs are highly integrated into the national information infrastructure protection effort.

What is required by developing nations is a hybrid approach which is both cost-effective and can be scaled over time to meet increasing requirements. In this section we aim to introduce such a theoretical model, which we call a Community-oriented Security, Advisory and Warning Team. Such an approach aims to be both cost-effective and loosely coupled in nature, but can be expand over time to gradually operate as a full CSIRT. In the following section we will discuss the requirements of such a model.

4.1 Requirements

A Community-oriented Security Advisory and Warning (C-SAW) Team will aim to fill the gap between a WARP and a CSIRT. This can be achieved by initially having a WARP-like structure which over time will serve as a full CSIRT.

A C-SAW Team must be cost-effective and community-oriented. Communities should be of a moderate size, which are slightly larger than that of a WARP. C-SAW Teams should maintain and encourage communication between other teams, which will allow for a

greater level of information exchange. They should also provide filtered information to their members which will maximise effectiveness. C-SAW Teams should be loosly-coupled, in that they sould not be dependent on other teams in order to function optimally. Lastly, they should be able to provide more complex services over time, as the size of the community increases.

In the following section we will discuss the structure of a C-SAW Team. We will discuss how the loosely coupled nature will allow C-SAW Teams to gradually combine into a full-scale national CSIRT structure.

4.2 Structure

C-SAW Teams will initially resemble a WARP-like structure; however it will differ in a number of aspects. Community-oriented Security, Advisory and Warning Teams will service a relatively large number of organisations, for example, “all businesses in the west of a city”. This will allow for a focus on a specific community of organisations. Ideally a C-SAW Team will service at most 250 organisations; however this would depend on the community.

A key aspect of a C-SAW Team is that of cooperation through communication with other teams. This will allow for a “net of protection” to develop across a number of communities. As communities grow, teams will need to expand in order to service them. This can result in a number of C-SAW Teams merging to adequately service this larger community. Figure 2 conceptually shows how a C-SAW Team will gradually provide an increasing number of services and more complex information to members of the community over time. Eventually, merged C-SAW Teams can be all integrated into a national CSIRT structure.

In the following section we will discuss the eventual migration of a C-SAW Team to a full national CSIRT structure.

4.3 Migration to a CSIRT

The migration to a full-scale CSIRT structure is demonstrated in Figure 3. Initially, protection is provided through a number of small C-SAW Team. Over time, as communities increase in size, C-SAW Teams will merge to form a single, larger, C-SAW Team. This merging process will repeat until a CSIRT structure develops.

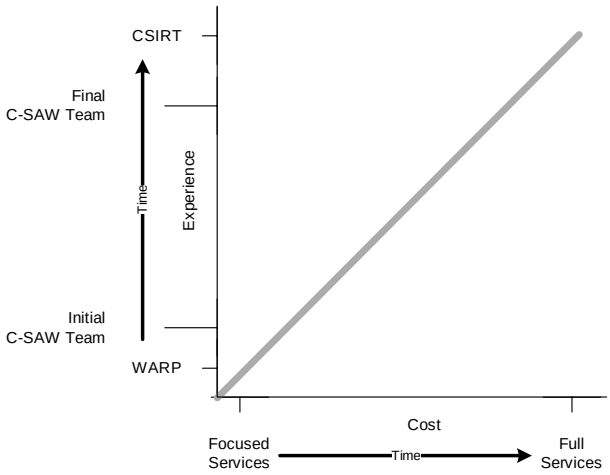

Figure 2: Services Provided by a WARP, C-SAW Team, and a CSIRT Over Time

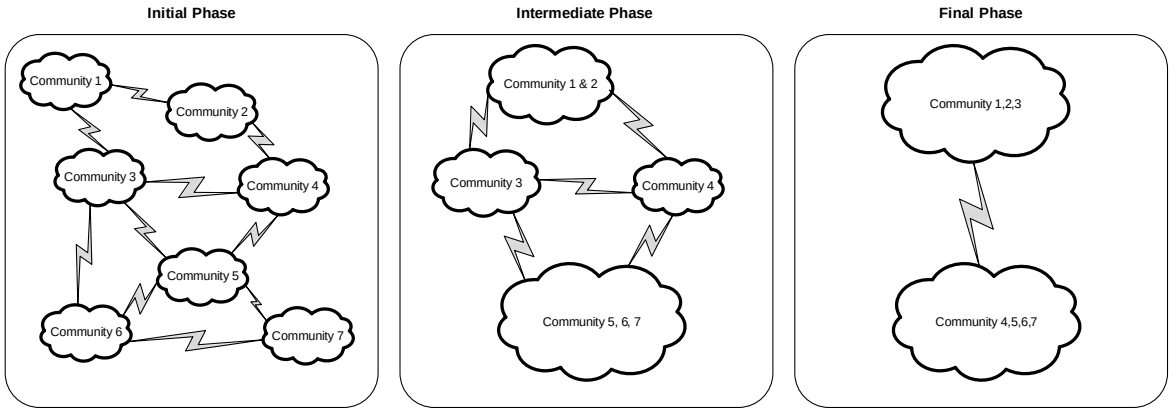

Figure 3: Migration and Mutation of a C-SAW Team Over Time

This migration process has a number of benefits over implementing a full CSIRT directly. Firstly, the cost-effectiveness of a WARP-like structure is harnessed for the initial phase. Secondly, a larger community of individuals will be able to receive protection from a CSIRT-like structure in the intermediate and final phase. Thirdly, the loosely coupled nature will allow C-SAW Teams to act in isolation, or share knowledge with other C-SAW Teams. Finally, the cost of implementing a CSIRT-like structure will be spread over time, while initially providing protection to a large number of communities. In the following section we will discuss the differences between a C-SAW Team and a WARP.

4.4 Differences Between a C-SAW Team and a WARP

In the initial phases, a C-SAW Team will closely resemble a WARP. However, there are a number of important differences between a C-SAW Team and a WARP. WARPs exist within an existing CSIRT structure, they from a bridge between a CSIRT and the "man on the street". C-SAW Teams will be designed to operate independently, until there is sufficient infrastructure in place to merge existing C-SAW Teams into a more comprehensive structure.

WARPs by their very nature are designed to service a very small community. As discussed above, this allows them to remain focused. C-SAW Teams will be designed to service a mid-sized community, constituting of various types of originations. This attribute a C-SAW Team will allow for interaction with a wide variety of organisations, with the aim of maximising information exchange, and minimising initial costs. WARPs are also not designed to scale up to service larger communities, whereas a C-SAW Team can be designed from to satisfy this requirement.

These differences are sufficient to warrant the creation of C-SAW Teams to effectively create a national CSIRT structure from the bottom up. In the following section we will discuss our future work and then we will present a conclusion to the concepts which were discussed in this paper.

5. Future Work

In this paper we introduced the concept of a C-SAW Team, as a dynamically expanding alternative to a CSIRT, which should prove to be more cost-effective over time than a full-scale CSIRT. Future work on this topic involves expanding and evolving the concept of a C-SAW Team. We plan to investigate the effectiveness of a C-SAW structure, compared to a traditional CSIRT structure. Furthermore we plan to outline services which a C-SAW team will provide, and we also plan to outline the generic interactions between a C-SAW team and an associated community.

6. Conclusion

Critical information infrastructure protection is of vital important to the functioning of a country. Many critical systems, and information based systems, rely on information infrastructures in order to operate. Should these infrastructures come under attack, or be disabled, it would seriously hamper a country's ability to function.

Computer Security Incident Response Teams (CSIRTs) are tasked with providing protection for a country's information infrastructure, through a system of incident handling services. CSIRTs are complex structures which aim to provide a holistic approach to information infrastructure through a system of warnings. CSIRTs will warn their constituents (the group of organisations which they serve) when an incident is ongoing.

CSIRTs are limited in that they are expensive to start up and maintain, and the information which they distribute many not be relevant to all constituents. To address these shortcomings Warning, Advice, and Reporting Points (WARPs) can be created. WARPs are formed by loosely coupled groups of members, all with a common interest. WARPs are highly cost effective and simple to set up and maintain. WARPs never act in isolation; rather they act in combination with CSIRTs to service its members.

Developing nations may not have the resources available to set up a full scale CSIRT structure, and the classic WARP model is too simple to provide overall protection. The aim of this paper was to introduce a Community-oriented Security, Advisory and Warning (C-SAW) Team, which can combine the cost-effective, simple nature, of a WARP, with the ability to mutate over time to a full scale CSIRT.

C-SAW Teams will allow critical information infrastructure protection to be set up quickly, with limited cost overheads. Gradually by combining C-SAW Teams; a full-scale national critical information infrastructure system can be realised.

References

[1] Akamai Technologies Inc. The state of the internet - volume 2 number 1. Electronic, July 2009. URL http://www.akamai.com/stateoftheinternet/.

[2] Akamai Technologies Inc. The state of the internet - volume 2 number 2. Electronic, October 2009. URL http://www.akamai.com/stateoftheinternet/.

[3] BBC. What makes a cyber criminal? Electronic. URL http://news.bbc.co.uk/2/hi/americas/7403472.stm.

[4] R. F. Dacey. GAO-04-628T Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems. United States General Accounting Office, March 2004. URL http://www.gao.gov/new.items/d04354.pdf.

[5] J. Fick. Cyber Crime in South Africa: Investigating and Prosecuting Cyber Crime and the Benefits of Public-Private Partnerships. Technical report, PriceWaterhouseCoopers, March 2009.

[6] J. Harrison and K. Towsend. An Update on WARPs. ENISA Quarterly Review, 4(4):13–14, December 2008. URL http://www.warp.gov.uk/Marketing/enisa_quarterly_12_08.pdf.

[7] G. Killcrece. Steps for Creating National CSIRTs. CERT®; Coordination Center, August 2004. URL www.cert.org/archive/pdf/NationalCSIRTs.pdf.

[8] O.B Longe and S.C Chiemeke. Cyber Crime and Criminality in Nigeria - What Roles are Internet Access Pointes in Playing. European Journal of Social Sciences, 4, 2008. URL http://www.eurojournals.com/ejss_6_4_12.pdf.

[9] manypossibilities.net. African undersea cables. Electronic. URL http://manypossibilities.net/african-undersea-cables.

[10] Metasploit. Future of metasploit. Electronic, Metasploit 2009. URL http://www.metasploit.com/data/confs/sanspt2009/msfuture.pdf.

[11] J. Moteff, C. Copeland, and J. Fischer. Critical infrastructures: What makes an infrastructure critical?, January 2003. URL http://www.fas.org/irp/crs/RL31556.pdf.

[12] Seacom. Seacom Brochure. Electronic. URL http://www.seacom.mu/.

[13] M.J. West-Brown, D. Stikvoort, K. Kossakowski, G. Killcrece, R. Ruefle, and M. Zajicek. Handbook for Computer Security Response Teams (CSIRTs). Carnegie Mellon Software Engineering Institute, Pittsburgh, PA, 15213-3890, 2nd edition, April 2003.

[14] D. Winder. Little green idol. Electronic, December 2008. URL http://www.warp.gov.uk/Marketing/Online Security.pdf.

