Incident Response Capacity Building in the Americas

FIRST | **Forum of Incident Response and Security Teams**
Maarten Van Horenbeeck, Cristine Hoepers and Peter Allor

"A Computer Security Incident Response Team (CSIRT) is defined as a team or an entity within an agency that provides services and support to a particular group1 (target community) in order to prevent, manage and respond to information security incidents. These teams are usually comprised of multidisciplinary specialists who act according to predefined procedures and policies in order to respond quickly and effectively to security incidents and to mitigate the risk of cyberattacks. There are hundreds of CSIRTs in the world that vary in mission and scope. One of the chief ways to classify CSIRTs is to group them by the sector or community they serve. Below are some of the national CSIRTs within OAS member states."

Introduction

The Forum of Incident Response and Security Teams (FIRST) is a global association of incident response teams members in over 70 countries, that enables them to respond more effectively to security incidents by providing access to best practices, organizing events and providing computer security incident response team (CSIRT) education. This paper explores some of the experiences FIRST has had catering to such a wide constituency, our view on incident response capability, and what organizations can do to improve the overall state of cybersecurity in the region.

An ever more complex world

When we look back at 1989, when FIRST was originally established, the world was quite a different place from today. In those early years, our member incident response teams already dealt with complex incidents, but the scope and amount of systems they affected were almost universally less than they are today. The Morris worm, which started affecting the burgeoning network in 1988, was rumored to affect about 10% of the Internet, some 6,000 machines in total.[1]

Today, a large number of complex issues include the following:

- Large botnets of malicious software, such as Citadel, which Microsoft Corporation assessed to have infected over 1.9 million clients.[2]
- Large distributed denial-of-service (DDoS) attacks of up to 500 Gbps,[3] which risk affecting Internet exchange points (IXPs).[4] In addition, these DDoS attacks are enabled through misconfiguration of thousands of endpoints, making the issue impossible to resolve for a single nation or organization.
- Complex malicious code attacks leveraging 0-day vulnerabilities, increasing highly targeted attacks and in cybercrime activity.

These changes require incident responders to adjust rapidly. Incident response teams on a national level are increasingly providing a more diverse set of services, including both the ability to provide reliable information about security threats to constituents, work with service providers and vendors to ensure a healthier Internet ecosystem and have strong investigative skills to analyze attacks that are less well understood. For smaller incident response teams, this can be a tremendous challenge.

Meeting these challenges

As such, it is important for the incident response community to acknowledge these differences, and work on ways of addressing them. Within FIRST, we see success in this area as follows.

- Responding CSIRTs are able to contact others to mitigate attacks.
- When working with another team on an incident, both CSIRTs speak the same operational language and have accurate expectations on the use of the information provided.
- The community has the tools and techniques to enable automated information sharing. Analysts leverage the information to truly understand the ramifications of the incident and make the right choices to reduce risk while mitigating the attack.

The CSIRT community cannot be successful in isolation

In order to get to this point, we see the need for development of a strong, inclusive community of CSIRTs, the availability of training and education to community members, and the need for standardized practices within this community.

The CSIRT community cannot be successful in isolation. One of the interesting aspects of Latin America and the Caribbean is that there are wide discrepancies between countries' awareness of cybersecurity issues, both in government and in the general population. This is only expected to continue as more new users come online, evidenced by impressive user growth rates across the continent. Security efforts must include the development of a culture of cybersecurity, such as that proposed by OAS,[5] which creates a fertile environment within which CERTs operate.

Efforts should include awareness training of Internet users and operators, fostering close public-private partnerships with the private sector, and the development of appropriate cybercrime policies that take into account and support privacy. In addition, security really starts with awareness and the use of best practices in technology. In this regard, an important role exists for academia to teach non-security professionals how to build secure technology.

Rooted in the community

Ideally, the CSIRT community should scale up to the point where each organization has a well-equipped incident response capability. This may be a single individual, or a small team, but every organization should be able to take responsibility for the traffic it emanates. However, given the large number of networks and their respective growth, this could be considered wishful thinking. An alternative is for each country to develop its "CSIRT of last resort"[6]—a CSIRT that can be a point of coordination for those networks that may not have a directly reachable, well trained incident response team. It should be well understood that each organization is ultimately responsible for its own security—a national team can only assist in the coordination, but will not be able to "pull the plug" or investigate every compromised machine.

In 2014, FIRST and CERT.br led an effort within the Internet Governance Forum to develop best practices for the CSIRT community. One thing which was universally stated within the community of participants was the need for a "CSIRT of last resort" to be developed outside of the community, rather than be "top down" through a government decision. For a CSIRT to be effective, trust is an incredibly important requirement, and the only way trust can develop is through a history of collaboration and participation in the security community. Whether the CSIRT is operated by the government, a network provider, a commercial entity or academia matters less, as long as it is developed in partnership with the entire security and networking community within the region.

The need for robust CSIRT in enterprise, academia and government cannot be underestimated. Governments have an important role to play in motivating the development of these teams, but they also need to realize that they cannot "enforce" trust—they must identify who have gained it, foster its growth for the country at large, and work with everyone to enable them to achieve their goals. Trust is also tied to the services a CSIRT offers. When a CSIRT is correctly focused on responding and mitigating an incident, foreign corporations and organizations will often trust them more, and provide more information to support their mission. This information may be limited when the CSIRT has a role in criminal prosecution, or is part of an intelligence service. The types of information provided to either organization tend to be different, and hence the roles should be properly segregated.

Developing capacity

When a network of CSIRTs exists, it is important for them to continuously build up their capability. We see three different levels for improving the delivery of CSIRT services:

Capability – Can you do it? A capability defines a measurable activity that may be performed as part of an organization's roles and responsibilities. For the purpose of the CSIRT services framework, the capabilities can either be defined as the broader services or as the requisite tasks, sub-tasks or functions.

Capacity – How much can you do? Capacity defines the number of simultaneous occurrences of a particular capability that an organization can execute before they achieve some form of resource exhaustion.

Maturity – How well can you do it? Maturity defines how effectively an organization executes a particular capability within the mission and authorities of the organization.

In order to be successful at increasing the effectiveness of a CSIRT program, there will need to be a focus on each of these three elements.

In 2014, FIRST launched an effort to develop a community-driven education program,[7] which is in the process of publishing an authoritative list of services offered by a CSIRT, and will make available at no cost, a detailed curriculum for each service. This effort is supported by several national CSIRTs, including CERT.br as well as several international organizations, including the OAS, and is expected to deliver initial training materials by late 2015.

Standards and Standardization

An additional area of investment for the incident response community is in standardizing procedures and working on open standards. There is a strong need for standards to enable incident response teams to exchange data during an incident, or agree on appropriate methods to deal with a particular type

of incident. Standards enable teams to capitalize on the trust they have built with each other and allocate their analysts on solving difficult problems.

Here we see a strong need for the community to evaluate the adoption of information exchange standards such as Structured Threat Information eXpression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII), as well as standards to properly define the risk of a particular vulnerability, such as the Common Vulnerability Scoring System. FIRST has supported these and other useful standards through sponsoring their development,[8] as is the case with CVSS, or by working with our members to organize training in teaching standardized practices.

Next steps for the community

There is a lot of work to be done to ensure the further development of a secure Internet for users in Latin America and the Caribbean, and this work is becoming more crucial every day as Internet adoption continues to grow at high rates. Governments have an opportunity to work with the private sector, civil society and academia to help motivate them to develop incident response capabilities within their sector, and within individual organizations. In addition, governments should ensure that among the teams with national responsibility, a "CSIRT of last resort" exists for their country, which actively builds trust with each of these organizations and has the ability to not decide on their behalf, but coordinate across sectors when an incident occurs.

The OAS has a unique role to play in its ability to convene governments within the region to come together and discuss these topics. In 2015, FIRST signed a Memorandum of Understanding with the OAS,[9] in which we endorsed the OAS's strong role in helping build incident response capability in the region. FIRST looks forward to providing the OAS with support from the technical community, in addition to our education efforts, in achieving these goals.

Organizations that are in the unique position where they can provide funding for these efforts, such as the Inter-American Development Bank (IDB) are highly encouraged to consider supporting these incident response projects. CSIRTs in the end will limit the losses the local economy will suffer from cybercrime, and they be a great force for good in a developing community. We encourage these organizations to become proficient at understanding the type of services that are truly valuable—supporting the core incident response capability, rather than more expensive and less effective efforts such as wide-scale monitoring of end-user networks. FIRST hopes to contribute to these assessments through the publication of our updated CSIRT services list in late 2015.

Conclusions

The Incident Response community is undergoing significant changes, in response to changes in the types and complexity of attacks it needs to respond to. Within the Americas, maturity of their capabilities is not very uniform, and in need of improvement. This paper outlined a number of core areas of focus for governments in the region, and hopes to inform how the community is currently in process of addressing these, and where they are in need of support. It identifies how governments can most benefit the community by identifying where gaps exist, and motivating existing mechanisms to improve their capability, or add additional goals and services to meet their economy's strategic security requirements. ■

Notes

1. Denning (1999) in Marchette, David J. "Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint". New York: Springer-Verlag.

2. Microsoft on the Issues (2013). Initial revelations and results of the Citadel botnet operation. Retrieved, July 15th from **http://blogs.microsoft.com/on-the-issues/2013/06/21/initial-revelations-and-results-of-the-citadel-botnet-operation/**.

3. Olson, Parmy (2014). "The Largest Cyberattack in History Has Been Hitting Hong Kong Sites". New York: Forbes. Retrieved, July 15th from **http://www.forbes.com/sites/parmyolson/2014/11/20/the-largest-cyber-attack-in-history-has-been-hitting-hong-kong-sites/**.

4. Prince, Matthew (2013). "The DDoS That Almost Broke The Internet". Retrieved, July 12th from **https://blog.cloudflare.com/the-ddos-that-almost-broke-the-Internet/**.

5. Organization of American States (2014). "A comprehensive Inter-American Cybersecurity strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity". Retrieved, July 12th from **http://www.oas.org/juridico/english/cyb_pry_strategy.pdf**.

6. Internet Governance Forum (2014). "Best Practice Forum on Establishing and Supporting Computer Security Incident Response Teams (CSIRT) for Internet Security". Retrieved, July 12th from **http://www.intgovforum.org/cms/documents/best-practice-forums/establishing-and-supporting-computer-emergency-response-teams-certs-for-Internet-security/409-bpf-2014-outcome-document-computer-security-incident-response-teams/file**

7. FIRST (2015). FIRST develops framework for education curriculum for global Computer Security Incident Response Teams (CSIRTs). Retrieved, July 10th from **https://www.first.org/global/education**.

8. FIRST (2015). Common Vulnerability Scoring System v3. Retrieved, July 16th from **https://www.first.org/cvss**.

9. OAS (2015). OAS and FIRST Sign Agreement to Improve Hemispheric Response to Cyber Incidents. Retrieved, July 15th from **http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-190/15**.

Cristine Hoepers

General Manager of CERT.br, the Brazilian National CERT, maintained by NIC.br, from the Brazilian Internet Steering Committee. She has a degree in Computer Science and a PhD in Applied Computing. She has been working with Incident Management at CERT.br since 1999, where she supports the establishment of new CSIRTs in the country, provides training in information security and incident handling, and develops best practices for systems administration and user awareness materials. She is the Chair of the FIRST Botnet SIG and a Member of the Advisory Board of the LACNIC AMPARO Project. In the past, she served as a member of the FIRST Steering Committee, was a member of the ITU HLEG (High Level Experts Group), and was one of the Brazilian representatives at the OAS Hemispheric Network of CSIRTs.

She is an authorized instructor to deliver CERT Program courses, from the SEI/Carnegic Meyon University, and has been a speaker and moderator at several forums such as International Telecommunication Union (ITU), Organization of American States (OAS), Anti-Phishing Working Group (APWG), the Internet Governance Forum (IGF), the Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG), Latin America and Caribbean Network Information Centre (LACNIC), Forum of Incident Response and Security Teams (FIRST), and AusCERT conferences on the topics of incident handling, Internet fraud and spam, and CSIRT development and use of honeypots to identify Internet infrastructure abuse.

Peter Allor

Director on the FIRST (Forum of Incident and Security Teams) Board. He has served within this premier global organization and is a recognized leader for incident since 2006. For the past five years he was the Chief Financial Officer and Treasurer, working the business aspects of FIRST.org, Inc. He is now serving as the CSIRT Services Education Framework Co-Chair, driving global participation from National CSIRTs, Critical Infrastructures, Enterprises and Non-Government Training or University Programs. Peter works for IBM Security as their Chief Security Strategist for Product Management and on disclosure coordination issues for IBM X-Force Researchers. He is responsible for aligning IBM's Products and Services for customer needs globally to include government, IoT and SCADA, as well as medical devices. Peter is a member of the Information Technology Sector Coordinating Council (IT-SCC) Executive Committee, which works within the private sector on policy and strategy input to the U.S. Government. Peter is also a Board Member of the Industry Consortium for Advancement of Security on the Internet (ICASI.org). He serves on the OASIS Cyber Threat Intelligence standard for upgrading STIX/TAXII and CyBox. He is also on the Steering Committee for the Diabetes Technology Society Cybersecurity Standard for Connected Diabetes Devices.

Maarten Van Horenbeeck

Director of the Forum of Incident Response and Security Teams (FIRST), the premier organization and recognized global leader in incident response. He has served as a member of the Board of Directors since 2011, and was Chairman of the organization from 2013 through 2015. Outside of his work for FIRST, he is Director of Security for Fastly, a content delivery network that speeds up web sites and application program interfaces. Maarten has 14 years of professional experience in information security, and has worked on the security teams at Amazon, Google and Microsoft. He focused much of his career on building threat intelligence and incident response programs, particularly focused on the investigation and response to targeted attacks. Originally from Belgium, Maarten lives in San Francisco, California, and holds a Masters degree in Information security from Edith Cowan University in Western Australia.

FIRST | Forum of Incident Response and Security Teams
www.first.org
first-sec@first.org