Computer security incident response team

ASSIGN BUSTER

Copies were kept in a “ file” in a “ file” drawer off “ file cabinet”. The file cabinets were pet in vaults, if they kept any type of personal information, or they could be locked in a safe. They may be guarded by a security company, or even the US Armed Forces. Fast forward to the digital age—now people hardly know what a piece of “ carbon paper is. They know how to work a tablet, a laptop, a desktop. Along with learning how to use computer, we have found a way to commit crimes, Just as before computers, only this time won’t even need to leave home to do most of the work. Isn’t paper and pencil safer??

With the Internet and e-commerce becoming the way of purchasing for many people, security got much more complicated”. (Barr, Building Cross-Enterprise Security Teams, 2010) The purpose of this paper is to show how and why a Computer Security Incident Response Team (aka SKIRTS) is established. By explaining the “ how’ and “ why,” people will be able to see that going to back to paper and pencil is not a step they want to take. Computer Security Incident Response Teams (SKIRTS) are made up of not only Individuals that are specially trained In handling an Incident, but there are also others that are on the team with them.

Before we get to the makeup of the team let’s look at the reasons for forming a Computer Incident Security Response Team. It mess that we hear on the news almost dally of security breaches where attackers have broken Into computer systems and stolen financial Information, social security numbers, birthrates, Just about any type of Information that someone could need to commit a crime with the information gotten. “ Organizations are

learning firsthand efficiently, and if it was from a vulnerability either see that a “ patch” is in place, or try to figure a “ fix” around the vulnerability’.

Depending on the “ needs” of the company, this will decide who will be part of the response team along with if the team will be in-house, a hired professional security many, or an on an as-needed-basis. There are “ motivators that will drive establishment of a SKIRTS that include: A general increase in the number of computer security incidents being reported A general increase in the number and type of organizations being affected by computer security incidents. A more focused awareness by organizations on the need for security policies and practices as part of their over-all risk management strategies.

New laws and regulations that impact how organizations are required to protect information assets. The realization that systems and network administrators alone cannot protect organizational system sets” (University, 2014). Now we have some motivations for designing the teams. But, “ many questions need to be answered in designing the team, such as: What are the basic requirements for establishing a SKIRTS? What type of SKIRTS will be needed? What type of services should be offered? How big should the SKIRTS be?

Where should the SKIRTS be located in the organization? How much will it cost to implement and support the team? What are the initial steps to follow to create a SKIRTS? All good questions however, there is not a standard set of answers to these questions” (University, 2014). The main goal of establishment of a “ SKIRTS is to minimize and control the damage resulting

from incidents, provide effective guidance for response and recover activities, and to work to prevent future incidents from happening" (Barr, 2012).

When establishing a SIR the following actions should be included: Creating an incident response policy and plan Developing procedures for performing incident handling and reporting Setting guidelines for communicating with outside parties regarding incidents Selecting a team structure and staffing model Establishing relationships and lines of communication between the indecent response team and other groups both internal (I. E. Gal department) and external (I. E. Law enforcement agencies).

Determining what services the incident response team should provide Staffing and training the incident freestones team" (Paul Coonskin, 2012) Now we have a good idea of what we need, so let's try to get a concrete list of people that would actually make-up a SKIRTS: 1. " Management – this is essential to have a member of upper level management, not only for the decision making, but to add support that will more likely make the team be effective. 2. Information Security- these are the employees who are trained in the area of handling electronic incidents. . IT / MIS – Many companies have a separate security and IT department 4. IT Auditor – May companies are beginning to use auditors that are specially trained in the area of computer technology. 5. Security – This is the people that are responsible for physical security. 6. Attorney – useful for supplying 8. Public Relations – A company's image is an asset of considerable value, especially if the company is publicly traded. 9. Financial Auditor – How do you put a monetary figurer n the damage that has occurred as a result of an incident? 10.

You may also choose to include professionals such as law enforcement, vendors and/or technical peccaries (University, 2014). Now we have a concrete list of people from different parts of the organization that should be involved. However, this is only a guideline, it is up to each organization to tailor the team to fit their organization. Along with naming the makeup of the SKIRTS, it is important to define the role of each of the people that maybe on the team. Everyone will have a definition of what their role is in the team. Here are basic roles for each team member: 1 . Management – Besides giving the team the authority they need to operate, is to make the big decisions based on input from the other members of the team. . Information Security – assessing the extent of the damage, containment, basic forensics, and recovery. 3. IT / MIS – to ease the effects to system end users, and to assist the Information Security team with technical matters as required. 4. IT Auditor – to observe, learn why the incident happened, ensure procedures are being followed and work with IT security to avoid problems in the future. 5.

Security – may include assessment of any physical damage, investigation of physical evidence, and guarding evidence during a forensics investigation to maintain a chain of evidence. . Attorney – to ensure the usability of any evidence collected during an investigation in the event that the company chooses to take legal action. Can also provide advice regarding liability issues in the even that an incident affects customers, vendors, and/ or the general public. 7. Human Resources – to provide advice as to how best to handle situations involving employees.

HRS will usually not be called upon until after an investigation has begun, and usually only in the even that an employee is discovered to be involved. 8. Public Relations – communicate with team leaders, insuring an accurate understanding of the issue and the company’s status, and to communicate with the press and/or informing the stockholders of the current situation. 9. Financial Auditor – A monetary figure on the damage that has occurred as a result of the incident, is usually required for insurance companies.

Also an accurate figure will be needed in the event the organization chooses to press charges under the National Information Infrastructure Protection Act; It is required that you are able to document at least $5, 000. 00 worth of damage. ” (Broking, 2001) Next the team must sit down and define the words “ event” and “ incident. ” Once he team has been formed and everyone knows what their role will be on the team, the team must sit down and define the words “ event” and “ incident. ” Start with defining an event. An “ event is any observable occurrence in a system or network.

Events include a user connecting to a file share, a server receiving a request for a web page, a user sending an e-mail, and a firewall blocking a connection attempt” (Paul Coonskin, 2012) are all examples of events, these don’t cause the SKIRTS a lot of worries. However, adverse events do, as these are events with a negative consequence, such as system crashes, packet floods, unauthorized use of yester privileges, unauthorized access to sensitive data, and execution of mallard violation of computer security policies, acceptable use policies or standard security practices.

Examples of an incident would be an attacker commanding a bootee to send high volumes of connection request to a web server, users are tricked into opening mallard as an attachment to e-mail, files held for ransom” (Paul Coonskin, 2012) It is important that the team practices for the inevitable security breach to happen. As the team works together, the procedure will become learned and followed step-by-step as if there is a real security incident to be handled.

By working as a team, when the real incident happens, the team will be ready, know exactly how to handle the incident using the policy and procedures that have already been set up and learned by the team. Security of networks is not something that should be taken lightly by anyone that works for the organization. Human Resources by being on the SKIRTS team will have a large responsibility in seeing that employees understand and adhere to the Policies and Procedures governing computers. By educating, and bringing to every employee’s attention the need to keep the network safe and secure for the data that has been entrusted to them.