

Incident Response Checklist

Discuss in Forums {mos_smf_discuss:/root}By Axel Tillmann

Most Fortune 1000 companies have established security departments with clearly defined duties, separate from the traditional Network Operations groups. Typically "Security" is, among many other tasks, responsible for accessing and identifying threats to the corporate network infrastructure and endpoints. Therefore several technologies have been either investigated or deployed. Among those are: Firewalls, IDS, IPS, SIM/SEM, Antivirus, NAC. All these categories belong to either of two functions: Prevention or Detection.

I. PreambleIt is the painful experience for most customers that while prevention and detection may have reduced impacts to the infrastructure, threats still appear. It is the overwhelming consensus of leaders in the security industry that those threats will intensify and will be more intelligent in bypassing prevention. This belief is founded in the detailed understanding of our vulnerabilities and the knowledge that future attacks will be more often done with criminal intent, versus past attacks, which were devised as a "sport" by high-school/university "kids."These facts now force companies to take a hard look at responding to threats. The response splits into two groups, quarantining and remediation. Both are manual processes with response taking some organizations hours even days just to be able to identify individual nodes on the network. Remediation is a manual process, which unlike response, can't easily be automated. Due to the multifaceted nature of attacks, the individual "cleanup" process requires human intervention.With the help of proper technology the response process can be strengthened and have a staged roll-out from semi-automatic to full automation.II. Automating Response with a Response System

A response technology needs to address every single aspect of the response. The following graph highlights all necessary functions of response.

Response technology needs to ease the process for the following levels:

Layer 2 Response – quarantining individual nodes on the network
 Layer 3 Response – quarantining IP traffic types anywhere in the network
 Layer 8 Response – quarantining users from accessing the network

In order to be effective, a deployed technology will have to have the combined knowledge of the best network engineers in the company. Following is a checklist of requirements that a system needs to be able to handle.

Vendor Agnostic

The technology system needs to be vendor agnostic in order to give corporations the freedom to choose infrastructure equipment which is the best fit for a given project rather than worrying about a homogenous infrastructure, just to ease the task of managing it.

Manual and Automatic Inputs

Due to the complexity and the nature of the potential threats a response system cannot rely solely on automatic input from security sensor technology. It is the experience from large customers that information about problems may come from many sources such as, directly from users who experience network problems, deployed protocol analyzers (e.g. distributed sniffers), antivirus servers, HP Openview/IBM Tivoli, modern firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, Security Information Management Systems, or load monitors. In order to utilize all information sources the response technology needs to offer input in either automated fashion or manually for direct user access. The automated input needs to accommodate the various control desires of corporations through giving them the option of engaging into a controlled process with human intervention or fully automated. If a review of events is required the system needs to offer a managed process, which allows them to review quarantining events in so called authorization queues before they are deployed in the network.

Variety of Quarantine Options

Simply turning off switch ports is not the most appropriate way. A good response system needs to offer distinguished actions based on circumstance or supplied rules. For example if VoIP is deployed in a corporation, many switch ports have more than one MAC address active on a given switch port (PCs are typically cascaded off of a VoIP phone). In these cases applying a MAC filter is the more appropriate action to take, which terminates access for the infected station and keeps the VoIP connection going. Move to VLAN is another desired action option. This allows the quarantining of systems to specialized VLAN offering either limited access or special scanning technology on the VLAN for further remote assessment, forensics, or remediation of the situation.

Granular User Access Control

A response system represents the most powerful network engineer in any corporation. Therefore it is required to create users with various degrees of access and execution rights. A system needs to differentiate between three different rights:

Yes - a user is allowed access to the task

No - a user is not granted access to the task

Authorization - a user requires authorization from someone else for a given task

These rights need to be separated for the different quarantining actions in the network:

- quarantine nodes
- quarantine subnets
- quarantine IP traffic
- quarantine users
- change global threat/disaster levels

In addition the user access control needs to be able to differentiate between various parts of the network, so that users can be created who have only rights to execute on certain parts of the network (CIDR range control).

Asset Protection

The information source of cyber security breaches does not "discriminate" any special system and therefore does not distinguish between the importances of the system. Neither does the manual response process. Users can easily shut down the DNS server(s) without being told by the switch "you are shutting down the DNS server port. A response system needs to provide so called Deny and Quarantine rules which allow the upfront definition of asset protection as well a predetermined quarantining action. The Deny rules need to be able to receive input based on CIDR, MAC address, and Hostname. Quarantine rules need to offer influence on the taken action: Turn off switch port, Apply MAC filter to switch port, Move station to VLAN. In addition individual systems should be able to require authorization for the quarantining action, independent from the user account settings.

Network Communication

In order to work with all network infrastructures in a reliable way there should not be a requirement for the deployment of any special protocols nor should SNMP be used for the execution of commands. A system needs to represent the best practices used by the best network engineers, hence it should use the standard access control protocols Telnet or SSH, as used by the network engineers.

A response system should never sit inline, because impacting traffic through inline devices is never a good idea. For one, typical network speeds and loads do not allow for an in depth analysis of the entire data packet. A rule of thumb: one needs at least 10x the network speed to rip the packet into its individual pieces and then about another 5x for analysis of the content. This translates that a 1GB Ethernet link needed to be analyzed by a processor of at least 16GHz (consequently a 10GB link would require 160GHz). Those processors don't exist on the market today. Any system that would attempt to do so will either drop packets or go into bypass mode. More information on this topic can be supplied on request.

Reporting Requirements

A multitude of federal regulations (e.g. Sarbanes Oxley) require detailed reports on actions taken in the event of responding to cyber security breaches. Any response technology needs to record all interactions with the system and offer the details in the form of audits and reports to provide the required reports of events.

Threat/Disaster Support

Companies need to be able to put plans for worst-case scenarios in place. Without automating the process those scenarios may have been too time consuming in the past in order to be considered for a successful deployment. A good Response technology, however, should also take advantage of an intelligent network engine and offer configurable worst case scenarios, configured ahead of time and ready for execution within seconds of a recognized impact. A reasonable number of levels should accommodate the multiplicity of the various events. The ability to define threat/disaster levels will now enable organizations to prioritize their business environments and close doors on non-mission critical operations. A manufacturing company will be able to shut the network link between manufacturing and the normal corporate network, ensuring that the manufacturing process stays undisturbed. III. Implementing the Plan and the System

In preparation for installing a response system the following audits need to be done:

1. Access the number of systems used (e.g. 1 system per major country location, 1 lab system, backup system(s)).
2. Define user groups (by territory, access rights, administrative rights, reporting rights), including user groups for security

devices.

3. Define users and associate them with the predefined user groups. Add also user definitions for security devices (typically to a user ID’s per sensor).
4. Define default message formats for notification procedure.
5. Define potential integration with Trouble Ticket system.
6. Audit important host systems and assign rules for them (Deny and Quarantine rules).
7. Define emergency procedures and prioritize network operations. Based on this upfront work, define the number of Threat and Disaster levels (e.g. 1-256). Implement the disaster procedures (quarantine nodes, subnets, and IP traffic) for each individual level.
8. Audit type and number of security devices (Central Antivirus server, IDS, IPS, SIM) that should have some form of integration with the response system. Determine which monitored activities should have an immediate quarantining action associated with them, and which activities should only lead to entries into the authorization queue. Configure the necessary templates and roll them out to all devices.
9. Discuss and consider other network elements to feed into the response system (HP Openview/IBM Tivoli, Protocol Analyzers, Load and traffic monitors).
10. Define procedures to update the infrastructure definitions within the response system.
11. Train people on access and functionality of the response system. IV. Additional Considerations

A response system drastically cuts down on the time it takes to identify a location of any specific node, determining the necessary quarantining action, and implementing it. Therefore the exposure to vulnerabilities is drastically reduced and the impact is minimal.

Remediation could also become, to a degree, part of that response technology, by pointing questionable stations to a specialized VLAN where scanners can evaluate the level of problems and could in conjunction with a response system, bring nodes back to the network if no problems have been found.

Such a procedure can be easily achieved from a remote help desk, minimizing onsite support requirements.

Under network connections we also discussed the technical difficulty of inline operation. Security sensors should therefore be only deployed as sensors and not as inline devices. Many corporate customers experienced the need to open up the security setting on inline devices because either valuable traffic was blocked or the performance became unreasonable.

For more information, visit Enira's web site at <http://www.enira.com/> or email axel.tillmann@enira.com.