Interested in learning more about security?

SANS Institute InfoSec Reading Room

A Perspective on Threats in the Risk Analysis Process

There are many variations and methodologies when it comes to Risk Analysis, however there are fundamental steps that need to be taken no matter what approach is used. In this paper we will take a closer look at one of these initial steps, Threat Analysis, and show why it is important in successfully identifying key assets.

A Perspective on Threats in the Risk Analysis Process

Arthur Nichols

Risk Analysis Overview

Companies are opening their intranet to customers, partners, and suppliers and as companies move their business functions from their local area networks (LANs) to the public and global Internet, the possibility of network intrusion and data theft can grow at a rapid pace. Knowing where and how these intrusions take place can be a daunting task. However, determining key assets and securing these assets from unauthorized intrusion is critical to the operation of any organization. If these assets are left unaccounted for and unprotected, this could affect the mission of the company or organization. As Dr. David Brewer points out in his paper, Easy ways to manage your risk, "The traditional approach to risk management - scope the problem, determine your information security policy, perform the risk assessment and manage the risks - survives in today's technologically advanced world with carefully crafted scoping and security policy statements and the addition of a new feedback loop".
There are many variations and methodologies when it comes to Risk Analysis, however there are fundamental steps that need to be taken no matter what approach is used. In this paper we will take a closer look at one of these initial steps, Threat Analysis, and show why it is important in successfully identifying key assets.

Intrusions or attacks to high-risk assets might not require countermeasures if the potential damage is small. Lower risk attacks will require more attention if the possible loss is great. The estimated loss needs to be integrated into the ranking of the threats. For example, how important is the component of the asset to the operation of the asset or would the loss of a component result in the asset, not being able to perform its mission or reduce its ability to perform its mission. Note that often an asset may have several components that are required for the asset to function.

According to the Decessioneering Company, a company that focuses on Risk Analysis, there are two important points in any risk assessment methodology that should always be kept in mind:

- Where is the risk?
- How significant is the risk

Let's take, for example, an organization that wants to develop a Risk Assessment program. The program presents questions to the asset owner. These questions help determine where the asset fits in the operation of the organization. The program also integrates the responses and determines asset threats and vulnerabilities. If requested, the program will produce an assessment of the results that can help plan for improved protection of the asset. The results will also provide information that can be used for feedback and improving the programs methodology. The responses the asset owner will

supply will help establish the rules needed to support a qualitative approach to the evaluation.
Asking three important questions, or areas of investigation, are at the core of the Risk Management Process:

- Threat profile – what threats or risks will affect the asset?
- Threat probability – what is the likelihood of the threats happening?
- Threat consequence – what impact or effect would the loss of the asset have on the operation of the organization or its personnel?

The relationship between these three questions is essential to the development of a realistic assessment methodology. As Sean Boran points out in his IT Security Cookbook,

Threats + Impact + Likelihood = Risk

The quantitative significance of the areas could change depending on the assets. For example, if an asset is a communication system used for monitoring a controlled area, its loss might be significant while not very likely. On the other hand, if there is theft of property, each loss might be small, yet the total is still significant. In both cases the total impact to the organization could be significant.

A list of asset classes is developed to provide a starting point for the development of the rules that are used in our assessment process. The list is used to identify and group departmental assets by function, by type of ownership, and component ranking (how important is it to the operation of the asset).

Asset function is the main purpose of the asset and how it is being used.

Types of ownership:

- Organization owned and operated
- Organization owned and contractor operated
- Contractor owned and operated; and
- Public owned and operated.

Asset ranking is the importance of the assets to the function of the organization. A high value in the range of 0 to 10 the more significant the component.

Threat Profile

Our methodology not only requires an understanding of the asset, but also a general knowledge of the threats (possible goals of the adversaries), information about classes of adversaries, and methods that could by used by adversaries.
For the purpose of our methodology, threats are defined as events that impact the operation of the asset, or the value of the asset and/or products produced by the asset. Threats may prevent, alter the operation, or corrupt the operation of the asset.

The following table, (derived from Denning, p.26), lists the primary classes of adversaries, the important attributes of the adversaries, the possible goals of the adversaries, and common methods that are used by adversaries.

Adversaries	Attributes	Goals/results	Methods
Insider	Employee Contractor Temporaries Former Employees Student Vendor	Revenge Retaliation Money Ideology Sabotage	Destruction Spoofing Disruption of service Trap doors Virus Trojans
Hacker	Access to sophisticated hardware and software Generally non-violent Technical competence	Distinction-Celebrity Vandalism Revenge Retaliation	Destruction Spoofing Denial of Service Social engineering
Criminals	Some times violent Access to sophisticated hardware and software	Protect of operation Vandalism Arson Blackmail Financial gain	Kidnapping Destruction Spoofing Disruption of service Social engineering
Corporations	Attempts to collect protected information Has support: Technical, Analytical Financial	Corporate Espionage Money Financial gain	Social engineering Spoofing Trap doors
Government Agencies	Trained in espionage Possesses all necessary equipment Has support: Technical, Analytical Financial	Disruption of service Destruction	Destruction Spoofing Disruption of service Kidnapping Social engineering
Terrorist	Technical competence Access to sophisticated hardware and software Violent Politically motivated	Destruction of capability Political statements Sabotage Espionage	Destruction Spoofing Disruption of service Kidnapping Social engineering
Disasters	Natural events	Disruption of service Destruction	Fire, Earthquake, Lighting Storms Utility break downs

Probability of Threat Occurrence

The practical value of a risk analysis on key assets depends on the knowledge and completeness with which the risks are identified. A good analysis requires that the all aspects of the asset be examined to isolate those conditions, circumstances, activities, and relationships that affect the asset. To effectively analyze threats against key assets, it is necessary to consider as many of the potential threats as possible. This requires some in depth knowledge of the asset.
Below are a few factors that are important to organizational assets:

- Physical environment of the asset
- Numbers and capabilities of the attackers
- Telecommunications associated with the asset
- Business Contingency and Disaster Recovery plans for the asset
- Attractiveness of the asset to attack

Experience has taught us that once an attack is publicized, more people will try the same or similar attacks. With more avenues of attacks against an asset there is a greater the potential that the attack will happen at some time.

According to the Sans Institute "Most of the systems compromised in the Solar Sunrise Pentagon hacking incident were attacked through a single vulnerability. A related flaw was exploited to break into many of the computers later used in massive distributed denial of service attacks. Recent compromises of Windows NT-based web servers are typically traced to entry via a well-known vulnerability."

Consider the case where there is one avenue attack of against a given asset. This will result in a "potential" that the attack will happen. Now consider the case where the same asset has two avenues for an attack. In this case the potential will be greater than the case where there is only one avenue of attack. To carry the analysis one step farther, consider the same case but with more than two avenues of attack. This will result in even a greater relative potential that an attack will happen.

Threat Consequence

Knowing that threats can occur within an organization and its many environments and disciplines will help in determining what threats will affect the asset and what is the likelihood of an attack occurring. It will also help in determining the consequence or impact of a threat.

To help understand threats and their impact on assets, a mapping of threats with impact is necessary. The following four impact categories lists threats, both direct and indirect, and indicates areas where a given threat may have an impact.

Economic
A direct economic impact, for example, would be the loss or misdirection of organizational funds related to the purchase of goods or services that are used by the organization or an organizational contractor. An indirect impact, in this case, might result in the improper analysis of a chemical sample because improper chemical reagents were ordered or improperly labeled.

Safety
A direct safety impact, for example, would be the release of a hazard to the environment as a result of an attack. An unauthorized change to a manual or automated procedure that could result in an incident might be an indirect example.

Operational
A direct operational impact, for example, could be the shutdown of an organization due to a virus infecting the main servers. Indirect impact might be economic in nature such as failure to meet a deadline due to funds transfer failure.

Security
A security impact, for example, would be the release of confidential or proprietary information. The security effect would be direct if the released information is passwords and indirect if the released information was of some economic value.

General Risk Factors

After evaluating the answers gathered from our analysis program and applying them to our three areas of investigation, threat profile, threat occurrence and threat consequence, general risk factors are assigned to the asset or the components of the asset. When all the available data about each identified risk has been collected, each risk will be rated without consideration to any countermeasures. This produces a list of ranked risks. A separate list will be produced taking in account current countermeasures. This will help show how current countermeasures are impacting the asset by reducing the risks.

General risk factors that might be used in the initial approach could be:

Certain
The event will happen. For example, not using passwords on an unattended system in an open area will at sometime allow an unauthorized user access to the system.

High
The potential for the event occurring is much greater than that the potential for the event not occurring. For example, known and reported bugs in a system where available patches have not been installed and the system is easily accessible to a large number of users.

Moderate
The event is more likely to occur than not to occur. For example, unauthorized access to a system on a network even with the use of a password may present a problem.

Limited
The event is less likely to occur than not to occur. For example, unauthorized assess to a system on a network protected by passwords and a firewall.

Unknown
Not enough information is available to evaluate. For example, a network with a new type of firewall or a new operating system that has not been fully tested.

Economic Risk Factors

We also need to take in account economic risk factors in our investigation. There are several economic factors that should be considered in the threat analysis. These factors include:

- Would one group gain an unfair advantage over another if asset information were provided? An example might be customer privacy information?
- Would the loss of access to an asset cause an economic loss to a group? For example a firewall that fails closed.
- Would the loss of the asset effect the production of commercial products. Example: an asset that is required to insure the safety of a process, service, or product.
- Would an attack on an asset indirectly cause the loss of organization facilities, for example, cutting electric power to a facility?
- Would an attack have an effect on the image of the organization or other organizations around the globe, for example, not being able to account for all confidential customer data?

These considerations will be ranked initially as:

Significant
The loss of the asset would impact the loss of production and the asset would require immediate replacement or the temporary use of other assets.

Moderate
Possible economic loss of production and the asset may require rapid replacement.

Low
The loss of the asset may require replacement.

Value not known
The loss of the asset has not been evaluated for economic impact or not enough information is known to evaluate the economic impact.

After evaluating answers from the associated asset(s), economic risk factors are assigned. The risk factors are assigned to the assets or the components of the assets and are compiled to form a composite economic risk factor. The economic risks will be used to help develop an overall risk factor.
The overall ranking factor for an asset includes both the general risk factor and the economic risk factor. Risk factors can be modified by organizational priorities that will affect the overall risk factors for assets.

Once the threats, impacts and corresponding risks have been listed and the constraints have been analyzed, the significant business risks (or weaknesses) will be more evident, allowing a counter strategy to be developed. (Boran, 2.4.2.6)

Feedback

The methodology can be evaluated by working with the owner of the assets to answer the questions. The results will be reviewed with the owner of the asset to make the results easier to use and understand. The rankings of the risks will be evaluated with the owners to insure that important risks were not omitted and that unimportant information is not included in the questions. The final results will be also be reviewed with the owners and with the organization in insure that reasonable factors are assigned to assets. The methodology will be modified as needed, based on results of the reviews.

Conclusion

We have looked at one of the fundamental building blocks in the Risk Analysis process. Asking these key questions, what threats or risks will affect the asset, what is the likelihood of the threats happening, and what impact or effect would the loss of the asset have on the operation of the organization or its personnel, can determine if the risk analysis process will be a success or failure. We have also shown that applying general and economic risk factors can also aid in ranking key assets. We need to keep in mind that these are only the first steps that are taken in the risk analysis process, however by applying this methodology we can help insure that assets that critical to the organization and vulnerable to threats will be identified.

References:

Denning, Dorothy E. “Information Warfare and Security.” Addison Wesley 1999

Krause, Micki, Tipton, Harold. “Handbook of Information Security Management.” Auerbach 1998

The Experts’ Consensus. “How To Eliminate The Ten Most Critical Internet Security Threats.” Version. 1.33, June 25, 2001. URL: http://www.sans.org/topten.htm (Aug. 25, 2001)

Brewer, David. “Easy ways to manage your risk”. Gamma Secure Systems Limited. URL: http://www.gammassl.co.uk/topics/hot10.html (Aug. 13, 2001)

C&A Security Risk Analysis Group. “Introduction to Risk Analysis.” URL: http://www.security-risk-analysis.com/introduction.htm (Aug. 5, 2001)

Decessioneering Company. “Risk Analysis Overview” URL: http://www.decisioneering.com/risk-analysis-start.html (Aug. 28, 2001)

Boran, Sean. “IT Security Cookbook.” 2000. URL: http://www.boran.com/security (Aug. 29, 2001)

Last Updated: June 29th, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Cyber Defence Japan 2017	**Tokyo, JP**	**Jul 05, 2017 - Jul 15, 2017**	**Live Event**
SANS Cyber Defence Singapore 2017	**Singapore, SG**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS ICS & Energy-Houston 2017	**Houston, TXUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Los Angeles - Long Beach 2017	**Long Beach, CAUS**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANS Munich Summer 2017	**Munich, DE**	**Jul 10, 2017 - Jul 15, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DCUS**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
Security Awareness Summit & Training 2017	**Nashville, TNUS**	**Jul 31, 2017 - Aug 09, 2017**	**Live Event**
SANS San Antonio 2017	**San Antonio, TXUS**	**Aug 06, 2017 - Aug 11, 2017**	**Live Event**
SANS Boston 2017	**Boston, MAUS**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Prague 2017	**Prague, CZ**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Hyderabad 2017	**Hyderabad, IN**	**Aug 07, 2017 - Aug 12, 2017**	**Live Event**
SANS Salt Lake City 2017	**Salt Lake City, UTUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS New York City 2017	**New York City, NYUS**	**Aug 14, 2017 - Aug 19, 2017**	**Live Event**
SANS Adelaide 2017	**Adelaide, AU**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Chicago 2017	**Chicago, ILUS**	**Aug 21, 2017 - Aug 26, 2017**	**Live Event**
SANS Virginia Beach 2017	**Virginia Beach, VAUS**	**Aug 21, 2017 - Sep 01, 2017**	**Live Event**
SANS San Francisco Fall 2017	**San Francisco, CAUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Tampa - Clearwater 2017	**Clearwater, FLUS**	**Sep 05, 2017 - Sep 10, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NVUS**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS Dublin 2017	**Dublin, IE**	**Sep 11, 2017 - Sep 16, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, ILUS**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
Rocky Mountain Fall 2017	**Denver, COUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MDUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, GB**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, DK**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS SEC504 at Cyber Security Week 2017	**The Hague, NL**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London July 2017	**OnlineGB**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**