شركة شبكة الخدمات الآلية
Automated Services Network Co.

Application Security Policy

Version: 1.6
Date: 16-11-2025

Approved by:

Sabah Al-Ghunaim
Chairman

شركة شبكة الخدمات الآلية
Automated Services Network Co.

Contents

Purpose:

The purpose of this policy is to define web application security assessments within Automated Services Network Company (eNet). Web application security assessments are performed to identify potential or realized weaknesses because of inadvertent misconfigurations, weak authentication, insufficient error handling, sensitive information leakage, etc. Discovery and subsequent mitigation of these issues will limit the attack surface of eNet services available both internally and externally as well as satisfy compliance with any relevant policies in place.

Scope:

This policy applies to all eNet web application security assessments requested by any individual, group, or department for the purpose of maintaining the security posture, compliance, risk management, and change control of technologies in use at eNet.

All web application security assessments will be performed by Information Security Staff, under the direction of the General manager. All findings are considered confidential and are to be distributed to persons on a "need to know" basis. Distribution of any findings outside of the eNet is strictly prohibited unless approved by the Chief Information Officer.

Any relationships within multi-tiered applications found during the scoping phase will be included in the assessment unless explicitly limited. Limitations and subsequent justification will be documented prior to thestart of the assessment.

Definitions:

The following definitions apply to the Web Application Security Policy:

Risk Level: Information Security Staff will assign a level of risk in accordance with the following definitions:

- **High** – Any high-risk issue must be fixed immediately, or other mitigation strategies must be putin place to limit exposure before deployment. Applications with high-risk issues are subject to being taken off-line or denied release into the live environment.
- **Medium** – Medium risk issues should be reviewed to determine what is required to mitigate and scheduled accordingly. Applications with medium risk issues may be taken off-line or denied release into the live environment based on the number of issues and if multiple issues increase the risk to an unacceptable level. Issues should be fixed in a patch/point release unless other mitigation strategies will limit exposure.
- **Low** – Issue should be reviewed to determine what is required to correct the issue and scheduled accordingly.

OWASP Risk Rating Methodology: Open Web Application Security Project (OWASP) is an unbiased source of information on the best practices for improving the security of

software.

Policy Statements:

The following policy statements apply to the Web Application Security Policy:

Web applications are subject to security assessments based on the following criteria:

- **New or Major Application Release** – will be subject to a full assessment prior to approval of the change control documentation and/or release into the live environment.
- **Third Party or Acquired Web Application** – will be subject to full assessment after which it will be bound to policy requirements.
- **Point Releases** – will be subject to an appropriate assessment level based on the risk of the changes in the application functionality and/or architecture.
- **Patch Releases** – will be subject to an appropriate assessment level based on the risk of the changes to the application functionality and/or architecture.
- **Emergency Releases** – An emergency release will be allowed to forgo security assessments and carry the assumed risk until such time that a proper assessment can be carried out. Emergency release will be designated as such by the Chief Information Officer or an appropriate manager who has been delegated this authority.

All security issues that are discovered during assessments must be mitigated based upon the Risk Level assigned. The Risk Levels are based on the OWASP Risk Rating Methodology. Remediation validation testing will be required to validate fix and/or mitigation strategies for any discovered issues of medium risk level or greater. The following security assessment levels shall be established by the Information Security Branch:

- **Full** – A full assessment is comprised of tests for all known web application vulnerabilities using both automated and manual tools based on the OWASP Testing Guide. A full assessment will use manual penetration testing techniques to validate discovered vulnerabilities to determine the overall risk of all discovered.
- **Quick** – A quick assessment will typically consist of an automated scan of an application for the OWASP Top Ten web application security risks at a minimum.
- **Targeted** – A targeted assessment is performed to verify vulnerability remediation changes or new application functionality.

Other techniques and tools may be used depending upon what is found in the default assessment and the need to determine validity and risk are subject to the discretion of the Security Engineering team.

Compliance and disciplinary action

In cases where it is determined that a breach or violation of eNet policies has occurred, the

Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent.

Exceptions

In certain circumstances, exceptions to this policy may be allowed based on demonstrated business need. Exceptions to this policy must be formally documented and approved by the Chief Information Officer, under the guidance of the Information Security Office. Policy exceptions will be reviewed on a periodic basis for appropriateness.

Review and Revision

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 12 months.

Acknowledgment of Application Security Policy

This form is used to acknowledge receipt of, and compliance with, the Automated Services Network Co. Application Security Policy.

Signature

By signing below, I agree to the following terms:
I have received and read a copy of the "Application Security Policy" and understand the same.
I confirm that the above have read and received and read a copy of the "Application Security Policy" and agree to comply to it.

Full Name	Designation	Signature
Akhilesh Pokkanchery	Senior Network Administrator	
Fahim Mahamud Parkar	Mobile Developer	
Linto Lawrance Neelamkavil	Application Support Manager	
Medhat Merzk Zaki	Web Developer	
Emad Genidy	Network Administrator	
Omar Mahmoud Hagras	Project Manager	
Rama Krishna Uddarraju	Information Security Manager	
Syed Imran	Web Developer	
Shahad Abdulwahab Sawas	Software Tester	

Annex - OWASP Risk Rating Methodology

DISCLAIMER

Over the years there has been lots of debate about the OWASP Risk Rating Methodology and the weighting of Threat Actor Skill levels. There are other more mature, popular, or well-established Risk Rating Methodologies that can be followed:

- NIST 800-30 - Guide for Conducting Risk Assessments
- Government of Canada - Harmonized TRA Methodology
- Mozilla resources:
    - Risk Assessment Summary
    - Rapid Risk Assessment (RRA)

Alternatively you may with the review information about Threat Modelling, as that may be a better fit for your app or organization:

- https://owasp.org/www-community/Threat_Modeling
- https://owasp.org/www-community/Application_Threat_Modeling
- OWASP Threat Dragon

Lastly you might want to refer to the references below.

Note: Edits/Pull Requests to the content below that deal with changes to Threat Actor Skill will not be accepted.

Author: Jeff Williams

Introduction

Discovering vulnerabilities is important, but being able to estimate the associated risk to the business is just as important. Early in the life cycle, one may identify security concerns in the architecture or design by using threat modelling. Later, one may find security issues using code review or penetration testing. Or problems may not be discovered until the application is in production and is actually compromised.

By following the approach here, it is possible to estimate the severity of all of these risks to the business and make an informed decision about what to do about those risks. Having a system in place for rating risks will save time and eliminate arguing about priorities. This system will help to ensure that the business doesn't get distracted by minor risks while ignoring more serious risks that are less well understood.

Ideally, there would be a universal risk rating system that would accurately estimate all risks for all

organizations. But a vulnerability that is critical to one organization may not be very important to another. So a basic framework is presented here that should be "customized" for the particular organization.

The authors have tried hard to make this model simple to use, while keeping enough detail for accurate risk estimates to be made. Please reference the section below on customization for more information about tailoring the model for use in a specific organization.

Approach

There are many different approaches to risk analysis. See the reference section below for some of the most common ones. The OWASP approach presented here is based on these standard methodologies and is customized for application security.

Let's start with the standard risk model:

- **Risk = Likelihood * Impact**

In the sections below, the factors that make up "likelihood" and "impact" for application security are broken down. The tester is shown how to combine them to determine the overall severity for the risk.

Step 1: Identifying a Risk

The first step is to identify a security risk that needs to be rated. The tester needs to gather information about the threat agent involved, the attack that will be used, the vulnerability involved, and the impact of a successful exploit on the business. There may be multiple possible groups of attackers, or even multiple possible business impacts. In general, it's best to err on the side of caution by using the worst-case option, as that will result in the highest overall risk.

Step 2: Factors for Estimating Likelihood

Once the tester has identified a potential risk and wants to figure out how serious it is, the first step is to estimate the "likelihood". At the highest level, this is a rough measure of how likely this particular vulnerability is to be uncovered and exploited by an attacker. It is not necessary to be over-precise in this estimate. Generally, identifying whether the likelihood is low, medium, or high is sufficient.

There are a number of factors that can help determine the likelihood. The first set of factors are related to the threat agent involved. The goal is to estimate the likelihood of a successful attack from a group of possible attackers. Note that there may be multiple threat agents that can exploit a particular vulnerability, so it's usually best to use the worst-case scenario. For example, an insider may be a much more likely attacker than an anonymous outsider, but it depends on a number of factors.

Note that each factor has a set of options, and each option has a likelihood rating from 0 to 9 associated with it. These numbers will be used later to estimate the overall likelihood.

Threat Agent Factors

The first set of factors are related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

- **Skill Level** - How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)
- **Motive** - How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
- **Opportunity** - What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)
- **Size** - How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

Vulnerability Factors

The next set of factors are related to the vulnerability involved. The goal here is to estimate the likelihood of the particular vulnerability involved being discovered and exploited. Assume the threat agent selected above.

- **Ease of Discovery** - How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)
- **Ease of Exploit** - How easy is it for this group of threat agents to actually exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)
- **Awareness** - How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)
- **Intrusion Detection** - How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

Step 3: Factors for Estimating Impact

When considering the impact of a successful attack, it's important to realize that there are two kinds of impacts. The first is the "technical impact" on the application, the data it uses, and the functions it provides. The other is the "business impact" on the business and company operating the application.

Ultimately, the business impact is more important. However, you may not have access to all the information required to figure out the business consequences of a successful exploit. In this case, providing as much detail about the technical risk will enable the appropriate business representative to make a decision about the business risk.

Again, each factor has a set of options, and each option has an impact rating from 0 to 9 associated with it. We'll use these numbers later to estimate the overall impact.

Technical Impact Factors

Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

- **Loss of Confidentiality** - How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
- **Loss of Integrity** - How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)
- **Loss of Availability** - How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
- **Loss of Accountability** - Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9)

Business Impact Factors

The business impact stems from the technical impact, but requires a deep understanding of what is important to the company running the application. In general, you should be aiming to support your risks with business impact, particularly if your audience is executive level. The business risk is what justifies investment in fixing security problems.

Many companies have an asset classification guide and/or a business impact reference to help formalize what is important to their business. These standards can help you focus on what's truly important for security. If these aren't available, then it is necessary to talk with people who understand the business

to get their take on what's important.

The factors below are common areas for many businesses, but this area is even more unique to a company than the factors related to threat agent, vulnerability, and technical impact.

- **Financial damage** - How much financial damage will result from an exploit? Less than the cost to fix the vulnerability (1), minor effect on annual profit (3), significant effect on annual profit (7), bankruptcy (9)
- **Reputation damage** - Would an exploit result in reputation damage that would harm the business? Minimal damage (1), Loss of major accounts (4), loss of goodwill (5), brand damage (9)
- **Non-compliance** - How much exposure does non-compliance introduce? Minor violation (2), clear violation (5), high profile violation (7)
- **Privacy violation** - How much personally identifiable information could be disclosed? One individual (3), hundreds of people (5), thousands of people (7), millions of people (9)

Step 4: Determining the Severity of the Risk

In this step, the likelihood estimate and the impact estimate are put together to calculate an overall severity for this risk. This is done by figuring out whether the likelihood is low, medium, or high and then do the same for impact. The 0 to 9 scale is split into three parts:

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Informal Method

In many environments, there is nothing wrong with reviewing the factors and simply capturing the answers. The tester should think through the factors and identify the key "driving" factors that are controlling the result. The tester may discover that their initial impression was wrong by considering aspects of the risk that weren't obvious.

Repeatable Method

If it is necessary to defend the ratings or make them repeatable, then it is necessary to go through a

more formal process of rating the factors and calculating the result. Remember that there is quite a lot of uncertainty in these estimates and that these factors are intended to help the tester arrive at a sensible result. This process can be supported by automated tools to make the calculation easier.

The first step is to select one of the options associated with each factor and enter the associated number in the table. Then simply take the average of the scores to calculate the overall likelihood. For example:

'''Threat agent factors'''					'''Vulnerability factors'''			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1		3	6	9	2
Overall likelihood=4.375 (MEDIUM)								

Next, the tester needs to figure out the overall impact. The process is similar here. In many cases the answer will be obvious, but the tester can make an estimate based on the factors, or they can average the scores for each of the factors. Again, less than 3 is low, 3 to less than 6 is medium, and 6 to 9 is high. For example:

Technical Impact					**Business Impact**			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8		1	2	1	5
Overall technical impact=7.25 (HIGH)					Overall business impact=2.25 (LOW)			

Determining Severity

However the tester arrives at the likelihood and impact estimates, they can now combine them to get a final severity rating for this risk. Note that if they have good business impact information, they should use that instead of the technical impact information. But if they have no information about the business, then technical impact is the next best thing.

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

In the example above, the likelihood is medium and the technical impact is high, so from a purely technical perspective it appears that the overall severity is high. However, note that the business impact is actually low, so the overall severity is best described as low as well. This is why understanding the business context of the vulnerabilities you are evaluating is so critical to making good risk decisions. Failure to understand this context can lead to the lack of trust between the business and security teams that is present in many organizations.

Step 5: Deciding What to Fix

After the risks to the application have been classified, there will be a prioritized list of what to fix. As a general rule, the most severe risks should be fixed first. It simply doesn't help the overall risk profile to fix less important risks, even if they're easy or cheap to fix.

Remember that not all risks are worth fixing, and some loss is not only expected, but justifiable based upon the cost of fixing the issue. For example, if it would cost $100,000 to implement controls to stem $2,000 of fraud per year, it would take 50 years return on investment to stamp out the loss. But remember there may be reputation damage from the fraud that could cost the organization much

more.

Step 6: Customizing the Risk Rating Model

Having a risk ranking framework that is customizable for a business is critical for adoption. A tailored model is much more likely to produce results that match people's perceptions about what is a serious risk. A lot of time can be wasted arguing about the risk ratings if they are not supported by a model like this. There are several ways to tailor this model for the organization.

Adding factors

The tester can choose different factors that better represent what's important for the specific organization. For example, a military application might add impact factors related to loss of human life or classified information. The tester might also add likelihood factors, such as the window of opportunity for an attacker or encryption algorithm strength.

Customizing options

There are some sample options associated with each factor, but the model will be much more effective if the tester customizes these options to the business. For example, use the names of the different teams and the company names for different classifications of information. The tester can also change the scores associated with the options. The best way to identify the right scores is to compare the ratings produced by the model with ratings produced by a team of experts. You can tune the model by carefully adjusting the scores to match.

Weighting factors

The model above assumes that all the factors are equally important. You can weight the factors to emphasize the factors that are more significant for the specific business. This makes the model a bit more complex, as the tester needs to use a weighted average. But otherwise everything works the same. Again it is possible to tune the model by matching it against risk ratings the business agrees are accurate.

References

- Managing Information Security Risk: Organization, Mission, and Information System View
- Industry standard vulnerability severity and risk rankings (CVSS)
- Threat Modelling Web Applications
- Threat Modelling
- Practical Threat Analysis
- A Platform for Risk Analysis of Security Critical Systems

- Model-driven Development and Analysis of Secure Information Systems
- Value Driven Security Threat Modelling Based on Attack Path Analysis
- Risk Rating Template Example in MS Excel