Firewall Hazard Analysis at Manufacturing Organization

Ahmad Rabay'a Muhammad Aamir Khan
Email: {ahmra523, muhkh174}@student.liu.se
Supervisor: Shanai Ardi, {shaar@ida.liu.se}
Project Report for Information Security Course
Linköpings universitetet, Sweden

Abstract

Internet connectivity is truly a necessity for every organization nowadays, but it comes up with a lot of security risks. Firewalls play a significant role in protecting information from unauthorized access and enforce security policies to reduce these kinds of risks. People may think that after installing a firewall, the internal network will be safe and free from hacker attacks. A certain level of security can be achieved only if firewall is properly installed, configured and maintained.

A hazard analysis can be a useful process to identify and potential hazards related to firewall .In our project we intend to perform a hazard analysis of firewall at a manufacturing organization by applying two different methods HAZOP (hazard and operability analysis)and FTA (fault tree analysis).

1. Introduction

"A firewall is a logical object (hardware and/or software) within a network infrastructure which prevents communications forbidden by the security policy of an organization from taking place, analogous to the function of firewalls in building construction" [1].

What do firewalls do? They simply act as a guard to the network and make decisions on whether a particular packet or packet stream can pass through them based on a set of simple rules. In other words, they enforce the organization security policy [2].

Basically Firewall has two interfaces: inside, which is the trusted network side, and outside, which is the un-trusted network side [3]. Its main rule is to protect the inside trusted side from the untrusted outside by filtering the traffic.

As internet business become more complex, the limitation of having two interfaces becomes more apparent [3]. The solution was to have multiple interfaces on the firewall by establishing intermediate zones of trusted either inside or outside, these are referred to as DMZ (from the military term Demilitarized Zone) [3].

Implementing multiple DMZ will raise the problem of how to design the network and where to implement the firewall(s) and how to best configure it to get the perfect security and lowest possible risk [3].

The report is divided into sections; section 2 describes the project background. An introduction about Hazard analysis is introduced in section 3, followed by the methodologies used in the analysis. In section 4 we conduct the analysis, then in section 5 and 6 we introduce the results we found and the project conclusion respectively.

2. Background

The need for information security is constantly increasing as companies are relying so heavily on electronic communication. Without security, a company can incur heavy loss due to unavailability or unreliability of data [3].

Protecting the corporate information is an important issue for an organization having an internal network with connection to internet outside the company. Corporate information may include company's secrets, financial and proprietary information, billing information and claim records. Companies provide their employees computing resources to access information communicate retrieve and distribute the information. It is needed and encouraged to use the internet by the employees of a company to fulfill the requirements of the job. Different studies show that companies are incurring more financial losses due to computer damage and espionage than ever before [4]. So security issue has become a compelling one that cannot be compromised.

In order to protect company's information on the network from unauthorized access, the information is classified usually to three levels; 1) Public, 2) internal and 3) confidential.

Public information can be accessed by anyone connected to the network and is unrestricted for example company news, advertisements and brochures about the products.

Internal information is to be accessed by employees of the company and it is widely distributed throughout the organization. This Information is intended for unrestricted use within and in some cases for business partners as well. It does not need advance permissions. Examples of Internal Information can be personnel directories, internal policies and procedures, most internal electronic mail messages [4].

Confidential or private information is that which is accessible for only authorized users for example higher management. This information is most critical to a company i.e. if it accessed by an un authorized person it may lead to violation of privacy of individuals, cause some serious damages to company or reduce company's competitive advantage. Confidential information may include all proprietary information called trade secrets, key financial information, proprietary information of commercial research sponsors, system access passwords and information file encryption keys, contracts that are considered confidential, employee information (such as personal information, compensation and benefits information, performance, records of disciplinary action, and other similar Information), market conditions and strategies and/or other expertise independently defined by decision makers as a trade secret [5].

Depending on the company's security policy, firewall filters the traffic on the network to ensure security. Having firewall failure can lead to security risks. To reduce the security risks, and to provide awareness about them, it is necessary to identify the possible risks and their results.

We have chosen a firewall at a manufacturing company for hazard analysis. We have assumed a sample manufacturing company with 50 employees. It consists of 6 different departments including production, marketing & sales, accounts & finance, administration, IT, and procurement department. The company has more than 50 computers connected through an internal network. For each department there is a separate switch which makes this network as a metropolitan network. For its daily operations, the company relies on various kinds of information resources including data processing systems, emails, voicemails, copiers, fax machines and other information generation and exchange methods. It is very important to make these resources available to meet the company's goals and objectives [5]. The company works gets orders from customers, arranges the requirements accordingly, manufacture the product and then supply the product to the customers. Having a good understanding of current market trends the company also works on stock basis and continues production if there are no orders. It also accepts orders online via its website, and updates the status of current orders as well.

In order to stay well reputed in the market and to fulfill the needs of customers efficiently the company wants its internal information to be secured. It cannot allow competitors to get information about its strategies, financial data, contracts, pricing, suppliers, customers, product or marketing plans. But at the same time it wants all these type of information available for use. Unauthorized access or non-availability to any such contents can make an adverse Impact on the company's competitive position, tarnish its reputation or cause a severe loss of market share.

3. Hazard Analysis

"A hazard is a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object) will lead inevitably to an accident (loss event)" [6].

Hazards have to be assessed and analyzed for their potential severity and probability, then make the appropriate treatment to control the hazard before cause any further accidents [6].

Risk is the hazard level combined with (1) the likelihood of the hazard leading to an accident (sometimes called danger) and (2) hazard exposure or duration (sometimes called latency) [7]. The combination result of the likelihood with the exposure called the risk evaluation matrix that indicates which risk is acceptable and which need an immediate treatment.

There are number of different hazard analysis methodologies that are in use today such as HAZOP, FMEA, HACCP, ETA and FTA. Each of these methodologies has specific properties in term of resource and scope that make it more applicable in some cases more than others, and some of these methodologies identify the hazards while others identify the trigger for the hazard.

We used two different methodologies (HAZOP and FTA) that work in two different ways.

HAZOP is forward looking – inductive – technique that identifies hazards, causes, consequences, and provide recommendations to reduce the occurrence of the hazard, or mitigate its consequences [8].

FTA is backward looking – deductive technique that shows us in visual way the interrelationship (cause-consequence) of events leading to the root event, also determines parallel and sequential events combinations [9].

The two methodologies also lead to two different results. HAZOP concentrate in identifying the hazard causes and how to reduce the consequences. While FTA identify the hierarchy of the fault until each single event (see section 5).

3.1 Hazard and Operability (HAZOP)

"A Hazard and Operability (HAZOP) study is a structured examination of an operation in order to identify and evaluate problems that may represent risks to personnel or equipment" [10].

The HAZOP technique was initially developed to analyze chemical process systems, but has later been extended to other types of systems and also to complex operations and to software systems.

A HAZOP is a qualitative technique based on guide-words and is carried out by a multi-disciplinary team (HAZOP team) during a set of meetings [10].

HAZOP procedure:

1. Divide the system into sections (i.e., reactor, storage)
2. Choose a study node (i.e., line, vessel, pump, operating instruction)
3. Describe the design intent
4. Select a process parameter. Process parameter is the relevant parameter for the conditions of the process. (e.g.
5. Apply a guideword. A guideword is a short word to create the imagination of a deviation of the design/process intent. (e.g. no, less, more, reverse, also, other, early, late, step unsuccessful etc.)
6. Determine cause(s), why the deviation could occur.
7. Evaluate consequences/problems resulted of the deviation.
8. Recommend action: What? When? Who?
9. Record information, by recording consequences, causes and suggested remedies.
10. Repeat procedure (from step 2)

Figure 1 illustrates The HAZOP procedure [8].

3.2 Fault tree analysis (FTA)

"Fault tree analysis (FTA) is a graphical technique that provides a systematic description of the combinations of possible occurrences in a system which can result in a risk" [11].

This method can combine hardware failures and human failures.

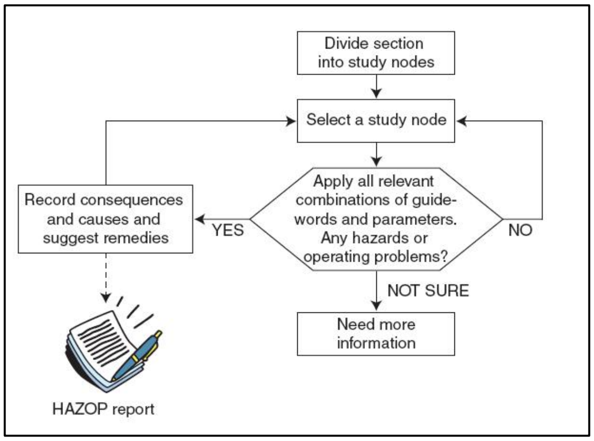
Divide section into study nodes
Select a study node
Apply all relevant combinations of guide-words and parameters. Any hazards or operating problems?
YES
NO
NOT SURE
Record consequences and causes and suggest remedies
Need more information
HAZOP report

Figure 1. The HAZOP procedure

Fault tree analysis (FTA) is a top-down approach to failure analysis, starting with a potential undesirable event (accident) called a TOP event, and then determining all the ways it can happen.

The analysis proceeds by determining how the TOP event can be caused by individual or combined lower level events, until we reach an appropriate level where events either independent basic events, which represent a basic equipment failure, or undeveloped events, which represent an event that didn't examine further because information is unavailable.

The causes of the TOP event are "connected" through logic gates

FTA is the most commonly used technique for causal analysis in risk and reliability studies [12].

FTA main steps:

1- Definition of the system, the TOP event (the potential accident), and the boundary conditions which is the operational stat of the system when the TOP event occurs.

2- Construction of the fault tree, by identifying the main events causing the top event and connect them by logic gates.

3- Identification of the minimal cut sets, which is a set of basic events whose occurrence ensures that the TOP event occurs.

4- Qualitative analysis of the fault tree, by investigating the minimal cut sets order and ranking.

5- Quantitative analysis of the fault tree, to investigate the probable time the minimal cut set may occur.

6- Reporting of results, by describing the findings of conducting the FTA in a brief report [12].

Fault trees are developed using gate and events symbols. A gate may have only one input and one or more outputs.

Figure 2 shows the common gate and event symbols for use in FTA [13].

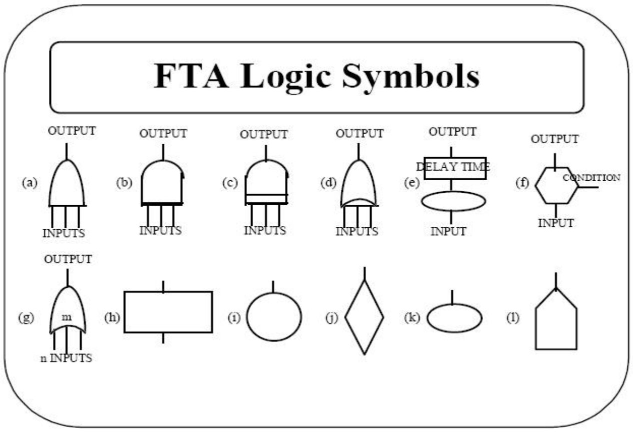

Figure 2. FTA Logic Symbols

a - OR Gate

b - AND Gate

c - Priority AND Gate

d - Exclusive OR Gate

e - Delay Gate

f - Inhibit Gate

g - M-out-of-N Gate

h - Resultant Event

i - Basic Fault Event

j - Incomplete Event

k - Conditional Event

l - Trigger or Switch Event

4. Analysis

Below is the analysis performed by using the two methodologies, HAZOP and FTA.

4.1 HAZOP of firewall

Figure 3 (appendix) presents the HAZOP analysis for firewall of a manufacturing company. At the first step we divide the system into sections physical structure, configuration and physical location of the firewall.

As the first study node, we choose the physical structure of firewall. It can consist of a computer on which it is installed, or a purpose-built appliance. We select the process parameter firewall failure. Selected guideword for this parameter is “No” because firewall is shutdown. The other alternatives like less, more or reverse are not suitable for this situation. The cause of failure can be the hardware failure or power failure. As a consequence of this failure protected network stops communicating to the public network because all the traffic passes through the firewall. It may cause work delay for the company because website and mail service stop responding. Recommended action for this problem is to check the power supply and hardware. If hardware is damaged replace it with other already configured firewall or use core router with maximum possible protection. If the problem is found with power supply the recommended action will be arrangement of power supply or UPS. As a safeguard, the responsible should see the instructions and recommendations on product manual and also check the warranty of the product to replace it before the time. Incase of power supply failure, the safeguard is to always run the system on UPS.

As the second study node we choose the configuration of firewall. Configuration of firewall depends on the security policy of the company. We select the process parameter poor configuration of firewall. Selected guideword for this parameter is “Less” because in this case it is providing less security than required. The other alternative is more which will be used in next part. The cause of this problem can be the inadequate security policy (e.g. default accept-all policy). As a consequence the attackers can access the confidential data of the company and company can incur serious loss. The contracts with different companies, proprietary information and financial statements can be available for competitors and company can lose its competitive advantage. Recommended action for this problem is to immediately block all communication and allow only known and trusted networks. A safeguard for this problem is to maintain and check the firewall log and make a good security policy and reconfigure the firewall.

Poor configuration can have another form also. With the guideword “More” it is selected for poor configuration caused by an inadequate policy which is stricter than required (e.g. default deny-all). As a consequence the company can suffer from work of marketing and sales, who want high speed and more freedom to work. This can result in a decrease in sales. Recommended action for this problem is to allow web requests and emails from outside, and emails from inside to outside. The safeguard for this problem is to define a good security policy which can give enough security and full speed access to internal and external resources.

We repeat the steps for next study node which is physical location of the firewall. The process parameter selected is “firewall bypassed”. The guideword is “step unsuccessful”. The alternatives like no, more less etc. are not found suitable here. The cause for this problem can be wrong location of the firewall. There can be some other access points which are not passing through the firewall. As a consequence the protected network is at risk. Company may lose its confidential information.

Recommended action for this problem is to disconnect all of unprotected access points and split them from protected network. A safeguard can be an appropriate location for the firewall from where every request must pass through the firewall. Also management should prohibit use of dialup modems and personal laptops in the premises of the organization.

Firewall can be bypassed if a security hole is found in the operating system or network design. We select the guideword "step unsuccessful" because other alternatives like no, more, less etc can not be used here. As a consequence the company's internal and external work can suffer because a hacker can get access inside the network. The recommended action for this problem is to disconnect the main gateway and after checking the log block the involved source. A safeguard is to stay updated with security updates and constantly monitor (or subscribe to) firewall vendor's security bulletins.

The next process parameter is "firewall can't work". We select the guideword "step unsuccessful" for this parameter. No other suitable guideword matches with the selected parameter. A cause can be the new types of threats e.g. web server attacks. As a result website of company can be defaced and attacker may launch attacks from web server, which may affect company's reputation. Recommended action is to check the log and block the source. And a safe guard is to use the web application firewall to protect the web server from attack.

4.2 FTA of firewall

Figure 4 (see appendix 1) presents the FTA analysis for firewall of a manufacturing company, as stated in section 3.2, the first step in the FTA analysis is to identify the top event, which is the firewall failure in a manufacturing organization, during the normal operation as a boundaries condition. The next step is to construct the fault tree. To perform this step we start by identifying the main events and conditions causing the top event "firewall failure".

Three main events found that may directly cause a firewall failure, are: First, firewall shutdown, and in this case firewall isn't working at all. Second, wrong access policy, in this case the firewall is working but cause wrong accessibility configuration. Third, firewall bypassed, and this event differ from the previous two events since it's mainly raised as a result of some external attack efforts, so the firewall is working well but an attacker can find a vulnerable in the system to bypass it.

In order to construct the fault tree, we proceed by identifying all sub-events until we reach an appropriate level that is either independent basic event or undeveloped event (see section 3.2). Firewall shutdown can be caused by three events: Circuit problem is a basic event that represent a basic equipment failure and lead the firewall to stop working. Power supply failure also represents a basic equipment failure – basic event – and lead firewall to shutdown. Firewall license expired that makes firewall not working anymore, and this event has a basic sub-event cause it that the firewall license is not up to date.

Second main event is wrong access policy, it has two sub-events are unauthorized access or no access. The unauthorized access is caused because three wrong firewall configurations sub-events:

All access that allows all the incoming traffic to access the network, it has two sub-events even the firewall left as its default configuration or it's configured to allow all configuration option that is a basic event raised by the person who is responsible for security configuration.

Unwanted access because of wrong configuration rules that left a hole in the firewall system. Finally Un-trusted access is result of firewall trusting un-trusted networks.

No access is result because firewall is configured to deny all the incoming traffic, and this sub-event disallows all the traffic to pass to the network.

The third main event for firewall failure is to be bypassed through exploiting vulnerability, it has three main categories:

Backdoors is hardware or software secret entrance into a computer system that bypasses security controls [14], it divided into two sub-categories: Operating system backdoors or applications backdoors, both are undeveloped events because information is unavailable.

Attacks can be divided into two event types:

Find vulnerability by port scanning using special software, or using browser attacks through the browser holes.

Making the firewall device inaccessible by using DoS attack as event that will exhaust the computer resources, all these sub-events are undeveloped events.

Finally, the wrong firewall location may result of firewall to be bypassed and have an insecure network.

Identifying the minimal cut sets step will help us to assess the qualitative and quantitative analysis steps of the fault tree, but we don't conduct this analysis because we don't rely on our project on a real manufacturing organization, and this kind of information are very confidential, it will not be available on internet and firms refuse to provide it.

The final step on the FTA analysis is to report the results, which are mentioned in the next section.

5. Results

By applying HAZOP on firewall we found the following results:

Firewall should be physically placed on such a point where every access request from a public network to the protected network must pass through it. Firewall must be purchased from a well known manufacturer so that the risk of circuit failure can be reduced. As well as warranty of the firewall should be concerned more, so that it can be replaced before time. A firewall is practically useless without a strong corporate security policy. So the performance of firewall is based on the strength of the security policy. A firewall cannot prevent against users with modems that reside in the same network. Policies about dialup modems and wireless devices must be defined and strictly enforced by management of the organization.

By analyzing the firewall hazards using the FTA methodology we found that some of the reasons are from un-human forced errors like power and circuit problems that lead the firewall to stop working.

Some of the hazards are because of leak of knowledge on firewall configurations, like accepting wrong IP address in the firewall rules, or have a wrong network trust relationship, in both cases the firewall don't work in the desired manner by allowing some unwanted traffic to pass or block the wanted traffic.

The other type of hazards mostly caused by an external intruder who try to pass through the firewall using exist holes in the system using some kind of port scanning software like nmap, or create ones by specific kind of attacks like DoS or Nat penetration attacks.

6. Conclusion

HAZOP is based on the principle that in a hazard analysis a team identifies more problems than individual work. HAZOP session brings new ideas and deep reviews of the process by brainstorming. It covers safety, operational aspect and covers human errors as well. It focuses to identify both hazards and operability problems. But there are some problems with HAZOP. It focuses more on the solutions. By applying this method on IT systems we can find more problems, so we can have a good defense against expected problems.

FTA is a Top-down approach start from the undesired event to the cause that require a skilled analyst to do, also it's suitable for single event, multi event that may lead to the Top event, and human errors that was the main cause of the most firewall hazards according to the previously conducted analysis.

The FTA methodology helps the organization to carry out some improvement to the system by knowing all the possible causes of undesirable hazards and know exactly where the hazards are in the current system.

We find that HAZOP is a better technique than FTA because it focuses more on safeguards and recommendations. Whereas FTA gives a visual representation of the events interrelationships until the least single event without any suggested remedies. In HAZOP every thing like causes, consequences, safeguards, and appropriate actions for each deviation is documented so it provides a systematic examination. HAZOP chart provides complete details for a single failure its causes, consequences and recommendations so it facilitates the analysis process in a better way.

References

[1] R. Niederberger, "Firewall Issues overview", Research Center Jülich, August 16, 2006, April 3, 2009

[2] J. Broderick, "Firewalls: Are they enough protection for current networks? ", Strategic Consulting, Symantec Corporation, San Antonio, USA, April 3, 2009

[3] C. Amon, T. Shinder, A. Carasik-Henmi, "The Best Damn Firewall Book Period", Syngress, 2003

[4] L. Janczewski "Internet and Intranet Security Management: Risks and Solutions", Idea Group Publishing, 2003

[5] www.nchica.org/HIPAAResources/Security/GeneralPolicy.doc (accessed at Saturday, April 11, 2009)

[6] N. Leveson, "Safeware: System Safety and Computers", Reading, MA, Addison-Wesley, 1995, March 24, 2009

[7] B. Frakes, "Safety and Reuse", Computer Science Department, Virginia Tech, http://www.favaro.net/john/RESAFE2006/papers/Frakes.pdf, March 24, 2009

[8] M. Rausand, "HAZOP Hazard and Operability Study", October 7, 2005, http://www.ntnu.no/ross/srt/slides/hazop.pdf, March 25, 2009

[9] C. Ericson "Fault Tree Analysis", Sept 2000, http://www.fault-tree.net/papers/ericson-fta-tutorial.pdf, May 18, 2009

[10] M. Lihou, "HAZARD & OPERABILITY STUDIES (HAZOPS) ", Lihou Technical & Software Services, http://www.lihoutech.com/hazop.htm, March 24, 2009

[11] Health & Safety Briefing, "Quantified Risk Assessment Techniques - Part 3, Fault Tree Analysis – FTA", No. 26c, December 2006, www.theiet.org/factfiles/health/hsb26c.cfm?type=pdf , March 25, 2009

[12] M. Rausand, "Chapter 3 System Analysis Fault Tree Analysis", October 7, 2005, http://www.ntnu.no/ross/srt/slides/fta.pdf, March 25, 2009

[13] B. Dhillon, "Reliability Engineering in Systems Design and Operation", New York, Van Nostrand, Reinhold, Co., 1983 http://smaplab.ri.uah.edu/ipd/2_3_1.pdf, March 25, 2009

[14] D. Byers, "Practical Network Security", http://www.ida.liu.se/~TDDD17/lectures/slides/tddd17_lec03_net.pdf.

Appendix 1:

Guide word	**Deviation**	**Cause**	**Consequence**	**Safeguard**	**Action**
No	Failure	Hardware Failure	No communication outside the company. Marketing and sales suffered due to non connectivity. Web site down. Mail server down.	Check product guide and warranty to replace it before time. Arrange for a backup alternate firewall configured as per company's security policy.	Use the alternate firewall or use core router with maximum possible security according to company's defined policies.
No	Failure	Power Supply Failure	No communication outside the company. Marketing and sales suffered due to non connectivity. Web site down. Mail server down.	Make sure availability of urgent power supply.	Arrange power supply or use urgent power supply.
Less	Poor configuration (less strict)	Inadequate security policy (less security)	Confidential data accessible for attackers (contracts with different companies, proprietary information, financial statements disclosed to competitors)	Maintain and check the access log and make a good the access policy. Block the involved or doubtful destination.	Deny all requests from outside except known and trusted networks.
More	Poor configuration (more strict)	Inadequate security policy (less communication)	Marketing and sales efficiency suffered due to less communication.	Revise policy and re-configure the firewall	Allow web requests and emails from outside, and emails from inside to outside.

Step unsuccessful	Firewall bypassed	Wrong location of firewall	Security compromised. Corporate secrets disclosed. Details of contracts made accessible to competitors. Network open for attacks	Relocate the firewall and chose a point where every access request from a public network to the protected network must pass through the firewall	Disconnect unsecured access points and separate the protected network from compromised networks.
Step unsuccessful	Firewall bypassed	Lack of security updates / found security holes	Server(s) down. No electronic communication at all. Internal and external work suffered. Production loss, marketing loss, reputation at risk. Loss of important records	Make sure to stay updated with the latest security trends and standards.	Disconnect the main gateway. Start inner network and communication. Check the log and block the involved source.
Step unsuccessful	Firewall bypassed	Dialup modems and wireless devices	Security compromised. Confidential information disclosed. Details of contracts made accessible to competitors.	Dialup modems and wireless equipment should be prohibited and disconnected as a serious risk when they are found	Prohibit use of dialup modems. Discourage the use of laptop with wireless cards for official work.
Step unsuccessful	Firewall can't work	New types of threats e.g. Web server and web application attacks	Web server attacked, website defaced, company reputation and goodwill damaged.	Use web application firewall to identify attacks to protect the web server.	Check the log and block the involved source.

Figure 3. HAZOP analysis for firewall in a manufacturing company

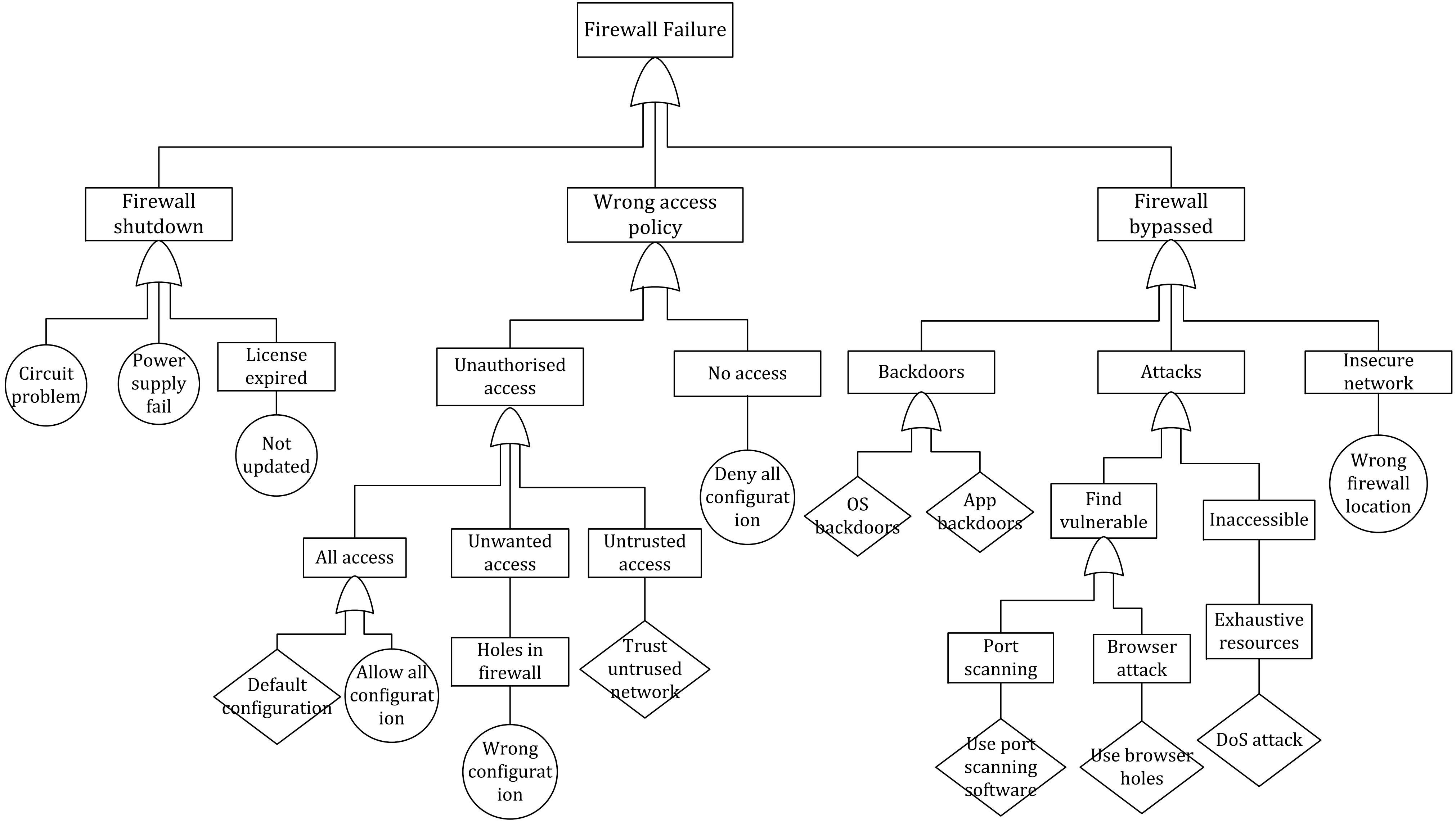

Figure 4. FTA for firewall at manufacturing company