An Information Security Audit for a Finnish Paper Mill

Monica Reinikka

2021 Laurea

Laurea University of Applied Sciences

An Information security audit for a Finnish paper mill

Monica Reinikka

Business Information technology

Thesis

April 2021

Laurea University of Applied Sciences **Abstract**

Bachelor of Business Administration

Business Information Technology

Monica Reinikka

An information security audit for a Finnish paper mill

Year 2021 Number of pages 22

The purpose of this thesis project was to conduct an IT security audit on a paper mill's office systems. This was carried out with a partner company that provides information technology solutions and services. The goal for doing the audit is to develop awareness of the mill's current situation with their office system's security, and to determine the level of protection in order to avoid any production loss or sensitive data breaches. The framework that was followed in the research as a guide is from the Center of Internet Security (CIS). The framework showed how to perform an audit and which parts to focus on in the research. The CIS RAM (Risk Assessment Method) version 1.0. is used to evaluate the possibility and the impact of the vulnerabilities and threats when doing the risk assessment.

The information presented in this report consists of the method of the research, the case study, the security audit, and the risk analysis. The data has been acquired with help of the partner company, through the documents from the system scan, and by interviewing the paper mill's IT personnel. Together we chose to focus on the two controls of version 7.1 of the CIS, and the sections are named "Continuous vulnerability management" and "Controlled use of administrative privileges". The CIS offers a guide chart on how to assess the method from being possibly compromised and which parts have a higher priority to be focused more.

The mill's staff has expertise in the field of information security and some parts were already under implementation during the research. Some of the aspects in the list require enhancing in terms of security since there were a couple of default passwords in use, and there is no regular nor automatic scan running that would keep the software updated with the latest version. In the end, we went through the results about the current state and the client was consulted with proposals on how to enhance their security level – resulting in protection that fulfills the framework's requirements and minimizes the possibility for threats such as unauthorized access into their system.

Keywords: cybersecurity, factory, audit, assessment

Contents

Terminology

CIS (Center for Information Security)

IT (Information Technology)

RAM (Risk Assessment Method)

NNT (New Net Technologies)

SOC (Security Operation Center)

RRM (Remediation Risk Management)

2FA (Two-Factor Authenticator)

BFA (Brute Force Attack)

1 Introduction

This research focuses on paper factory's current situation with their office system's protection level, security awareness, and how to enhance minimizing the risk of getting attacked and the sensitive data from being breached so that they can avoid production loss and grow awareness on how to sustain the protection level. The information was acquired through the system scan and by interviewing the client company's IT department personnel. For the subject being about the company's inner security level, the names and the attachments have been left without mentioning to follow the confidentiality and to avoid security threats.

The research's security audit has been done with a cooperation of a partner company who provides security services and they helped to go through the current situation of the office's systems, and a document of a manual search about the results that could predispose the factory for possible threats e.g. data leaks or a system shut down. The CIS (Central Information Systems) framework has been used as a guide while doing an audit and an assessment, and the analysis shows whether the required parts of the CIS control have been fulfilled or not, what kind of a risk would be as an outcome if the system data is vulnerable for security breaches, and what is the improvement proposal to reach the goal of having an enhanced security. Since the technology keeps evolving and that results in new threats and opportunities, this leads the organizations, as the client of the research, wanting to enhance their systems in a way that they are more protected against any possible data leaks or breaches which could influence their image or the financial business negatively.

A cybersecurity company Gatefy (2021) in their threat research has mentioned some of the famous cyberattack cases and one example from there is a WannaCry in 2017, during this a Windows operating system was being targeted and the data became unreachable for the users till they paid a certain amount of Bitcoin cryptocurrency as a ransom. There are also case examples of a cyber-attack in factories, and Saarilehto (2019) from Nixu had presented one against a Norwegian aluminum manufacturer Norsk Hydro that happened in March 2019. They became a target of a blackmailing attack and therefore had to close part of their facility, which lead running their processes manually for weeks. In Norsk Hydro's case they were able to rely on automated platform which was informing who will react and how on certain parts to minimize the negative outcome, because they had been prepared for such incidents.

1.1 Objective of the research

The objective for this thesis was to gather the information about the office system's current state and by that acquire the knowledge if there is a possiblity for the security threats and how to minimize them for happening. Reasoning for the research was to use the results as a guidance to show in which parts to focus to maintain the goal - avoid any production loss, because that will effect the manufacturer financially. The paper mill does not have any prior experience of system breaches or data leakages, and the goal of the research is to have an enhanced preparedness to avoid it from happening in the future as well. To strengthen the whole company's security, the framework will possibly be used as an example within the organization's other units too to align the same protection level.

Using the CIS framework as a guiding tool which helps to focus on certain area while doing the audit. It has different controls and the most suitable ones for the area that has been focused on in this research are control 3. "Continuous Vulnerability Management" which is mainly focused on applications that are being used in the office systems, and control 4. "Continuous Vulnerability Management" is about the personnel who has an account access into the system at the paper mill. The results will be used as a list of the aspects that will be followed and changed.

Questions that answering in this research:

1. Why is this research important for the paper factor?
2. How the security assessment has been done?
3. What is the outcome and how to improve?

2 Research methodology

The method that was used in this research was a case study and aiming to analyze the specific issues and tasks that are presented in this thesis paper. A case study is one of the methods in a qualitative research and it contains observations, analysis and interviews visually and by text. The case was to gather the information of the paper factory's current situation within their office IT systems, which areas need enhancing and how to do it. This project included remote meetings with the participants, and since there is confidential information involved that could cause a possible security threat for the company's data and systems - the names are not being published. Together we discussed on the time schedule, the areas that are being focused on and then lastly presented the results and consulted on how to continue. The information has been gathered through the documents provided by the security service partner company who has access to the systems, and by interviewing the client company's IT personnel at the factory taking part in this project.

3 Research framework

There are many cyber security frameworks and instructions available on how to enhance the organization's cyber security level. Together with the client and the partner company we had chosen the newest CIS framework version's two controls: "Continuous Vulnerability Management" and "Controlled Use of Administrative Privileges", because they fit and provided the wanted information in this audit. For the result evaluation of the sub-controls that are being presented in this thesis are performed by the CIS RAM (Risk Assessment Method). The framework helps the company to get a stronger security as a main goal, and it has been described to be suitable for different kind of users in the field, such as for experts and novices for its simplicity, and for these reasons it has been chosen to be utilized in this research.

There are three different groups from where the organizations can recognize their unit's needs so that they can get more suitable instructions to meet their goals. This research follows the implementation group 2., which means the factory has personnel with a cyber security expertise and knowledge in order to implement the sub-controls that are introduced in chapters 3.3 and 3.4.

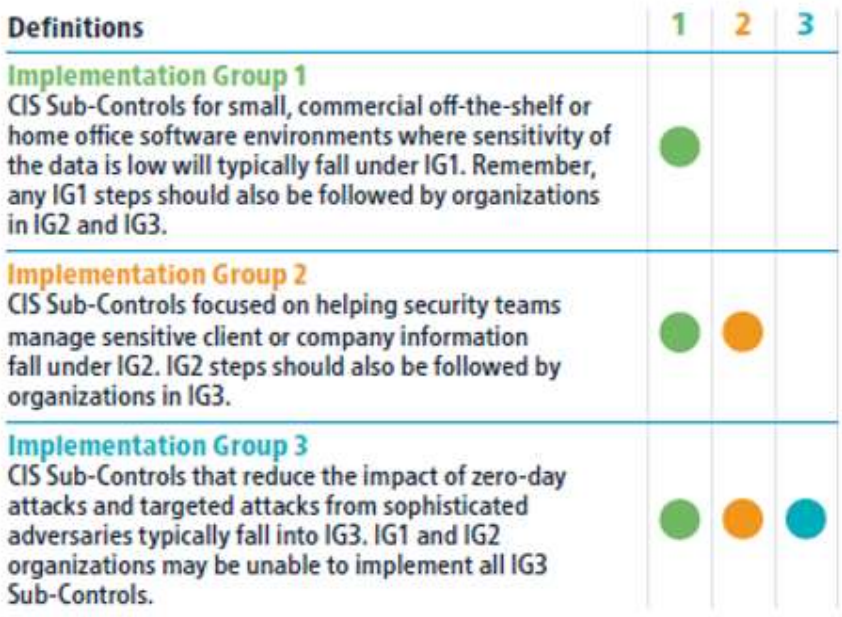

Figure 1. Implementation groups presented (the CIS framework 7.1, 2019)

The whole framework's focus has been created to help the organizations improvement with their cyber security defenses. The controls are developed by a cyber security community that have worked as a volunteer and the main things they do are based on feedbacks from people who use the controls, and it helps to create and maintain it even further. The control is downloaded free since the community wants to give any organization a chance to adapt the control within their own views (the CIS 2020).

3.1 Introducing the security audit

Being aware of the company's security level helps to understand the current situation of which areas could use some more enhancing and which areas are up to date. The security audit checks are recommended to be done regularly, so there will be less chance for a breach to go unnoticed. A specialist Petters (2020) from a software company named Varonis, has listed some of the benefits of the audit on the blog, such as it giving an image of how adequate the security strategy is that currently is being used, and then an ability to see if the efforts of the security training are progressing to the next area of the audit.

Performing an audit check has different steps, and Petters (2020) also introduced the workflow starting with defining the assessment criteria - the goals of the whole audit. The objects will now then be divided into different categories that are classifying the priorities. Second step is to be choosing the tool which will be used and ran within the office systems to achieve the wanted results. Conducting the security audit comes as a third step and it is about documenting and monitoring the findings, and possibly using previous audit as an addition for a comparison. A final stage comes when everything is completed, and it is a time to share the results with the included parties within the project. Listing the findings of an audit helps to prioritize the parts that require immediate fixing with rest that is not as alarming.

The process of the audit in the research had started with a remote meeting with personnel from the paper factory and the security service provider company. Together we had discussed about the aspects and areas that are desired to have a focus, the goals were to enhance the security to avoid a production and a financial loss, choosing the tools that will be used, such as the CIS framework with its controls, the schedule for the project was planned, and at the final meeting the results were gathered from the documents and the interviews were presented for the client, and the meeting ended with the improvement proposals presented in this research.

3.2 Risk assessment

The criteria while evaluating the risks of the controls that do and do not meet the requirements in this research are done by following a CIS RAM version 1.0. Decision to pair both of the services from the same organization was to limit the amount of variations in the results to be consistent in the evaluation of risk, and align to the same main goal pattern:" Identify, develop, validate, promote, and sustain best practice solutions for cyber defense." – the Center for Information Security.

The assessment method has been divided into two tables where the impact and likelihood criteria's have a score and marked as 1-3. The meaning of the scores has been explained in the table and starting from the number 1. meaning a minimal or a zero harm as a result. 2. meaning the incident is not being tolerable, and the 3. is about recovering from the attack, and it might be something that cannot be recoverable. The scores of the research assessment are shown in the table 3. and 4.

Impact score	**Impact score defined**	**Likelihood score**	**Likelihood score defined**
1	No or minimal harm would result	1	Not foreseeable
2	Harm would not be tolerable	2	Expected to occur
3	Harm may not be recoverable	3	Regular occurence

Table 1. Simplified Impact and Likelihood Criteria (CIS RAM 1.0, 2018)

Getting the final risk score result from evaluation happens by calculating the impact score x likelihood score. For the simplified score list the CIS gives the organization using the RAM to define their own risk that what will be in the line of acceptance and it is presented in table 2.

Version	Definitions of acceptable risk
Plain language	The risks need to be reduced and the parts are being prioritized by following the risk score.
Mathematical	Acceptable risk < 3 x 2; or acceptable risk < 6

Table 2. Risk acceptance criteria (CIS RAM 1.0, 2018)

This case includes the calculations that are as maximum 3 x 3 = 9 – resulting it as not acceptable. Risk score 6 has been set to be still at the acceptable limit, because the parts are currently under work to be implemented.

The CIS tells that they have wanted to create the assessment method to help and justify organization's plans and implementations when using the scoring with the current control version 7.1. And the given examples in the RAM 1.0 can be used amongst cyber security experts and novices, resulting in no specialization requirements. The CIS RAM helps the organizations to meet the legal requirements related to the security, e.g. regulations, laws and standards. One burden associated can be another security program that is already existing and it will make it layer on top of another or possible tradeoffs with other priorities and constraints they meet - such as lack the funding for a certain high level cyber security.

3.3 Continuous vulnerability management – CIS control 3

This is the third control of the CIS framework and it is described by the CIS community themselves to be focusing on continuously to take an effort against the attackers by minimizing, remediating, and identifying the vulnerabilities. Attackers are constantly trying to find security breaches, and through those they can get access to a data that is not meant to be seen for unauthorized people. It will be helpful in the long term to take care of the system security updates and situations, since getting the data compromised can be a costly situation.

Bluth (2020) at Ivanti has written the longer it will last to do the patching and getting the updates, the longer there is an opportunity to be vulnerable against possible exploits. The third control has its main focus on having automated software update tools deployed, so the scan can be done continually to recognize the possible breaches well before it could be done manually.

The NNT has opened more about each sub control section that is included in the implementation group, and in this control all of them are included. The audit results for this research are found in chapter 4. Analysis.

3.1 ”*Run automated vulnerability scanning tools*” having a main focus on the automated tools to scan the network and systems on a weekly basis, or possibly even more often since the more scans are being done – the faster the vulnerabilities are possibly being found.
3.2 ”*Perform authenticated vulnerability scanning*” is similar to the previous where it also highlights the importance of the system scan where the information is gotten from all scopes, inside and outside. Combining the gathered data gives a better picture of current state of vulnerabilities.
3.3 ”*Protect dedicated assessment accounts*” is a recommendation for having an account for vulnerability scans that is especially dedicated for it, and preferably one that does not have a privileged access to the system e.g. as an admin – as a reasoning the NNT mentioned a lower credential theft risk.
3.4 ”*Deploy automated operating system patch management tools*”, to assure that the security system providers newest security updates are in use.
3.5 ”*Deploy automated software patch management tools*”, similar with the previous sub control, both are advising companies to implement the tools that work as automated, because they are more reliable than manual updates, reasoning for this is a faster security flaw patch fix once it is available.
3.6 ”*Compare back-to-back vulnerability scans*” gives more insight about the current situation by comparing the results of the current and previous results of the scan, giving an opportunity to spot an exception that is documented, or patch a vulnerability.
3.7 ”*Utilize a risk-rating process*” as a last sub control that is for vulnerabilities which are discovered for a remediation. The RRM (remediation risk management) is a process to manage circumstances that might have been included unwanted results.

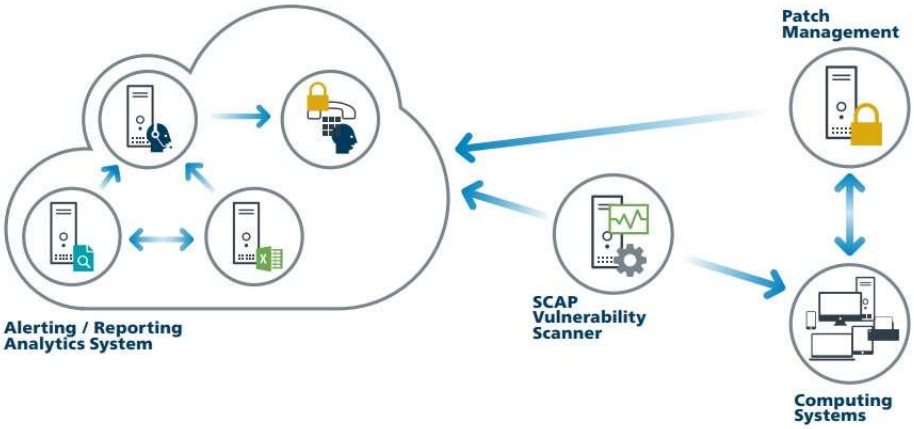

Figure 2. NNT. System Entity Relationship Diagram (CIS framework Control 3, 2019)

3.4 Controlled use of administrative privileges – CIS control 4

Importance in training the employees about maintaining the security is important in the sake of personal and business's data, since there are different techniques that the attacker can use to gain the access to the administrative account. The user being attacked can be fooled to open an email that has a malicious attachment or a link, that by pressing or opening it can result in running a malware in to the system. There are different options on how the control can be taken over, e.g. by installing a remote-control software or keystroke loggers that records everything the person types are one of the many ways.

The attacker can gain access by contacting both the unprivileged and privileged account user. Since the trust between workers' messaging connection is higher than from an unknown person, people are less alarmed when getting an email from a person you work with since the ingenuine reaching out can be disguised as a real one - making it more difficult to distinguish a genuine message from a malicious one. One of the sub controls is not included in the implementation group resulting the sub-control 4.6 without mentioning. The NNT has summarized the sub-controls as followed:

4.1 "*Maintain inventory of administrative accounts*", have a list of the accounts that have administrative rights, resulting awareness of the individuals who are privileged and have access to sensitive data.
4.2 "*Change default passwords*" , one of the first steps to make something more secure is to be changing the passwords that are given once taken into use. Attackers can run a brute force attack method, which means trying to get inside the system with guessing the passwords.

Default passwords can be found on the internet which gives a free entry into the system making the data vulnerable and accessible.

4.3 ”*Ensure the use of dedicated administrative accounts*”, phishing is a widely used method in order to get access into the user’s account. By clicking links or downloading files e.g. from an email is a threat and by using different account for things outside the professional data account lowers the risk.

4.4 ”*Use unique passwords*”, using different passwords on different platforms will keep other devices and systems safer, because then the attacker won’t be able to gain access for the network or system information while using this one same password that was used in the previous try.

4.5 ”*Use multi-factor authentication for all administrative access*”, enhances the security level when required to authenticate the logging with administrative accounts, e.g. 2FA (Two-Factor Authenticator) is a widely used method to add more security when logging in to the account, lowering the chance for other’s using the account without the owner of it being aware.

4.7 ”*Limit access to scripting tools*”, Only authenticated users should be able to have access in the scripting tools, e.g. PowerShell or Python. The risk for an attacker to have access to cause harm in the system is reduced when the rights are only for admins.

4.8 ”*Log and alert on changes to administrative group membership*”, having the information of who is authorized to gain access for some certain data helps the management to see if there is any malicious action and by whose account.

4.9 ”*Log and alert on unsuccessful administrative account login*”, too many wrong password attempts for an admin account should be alarmed and notified, so it can be inspected and confirmed if the user is being the owner of that account or if it is someone else.

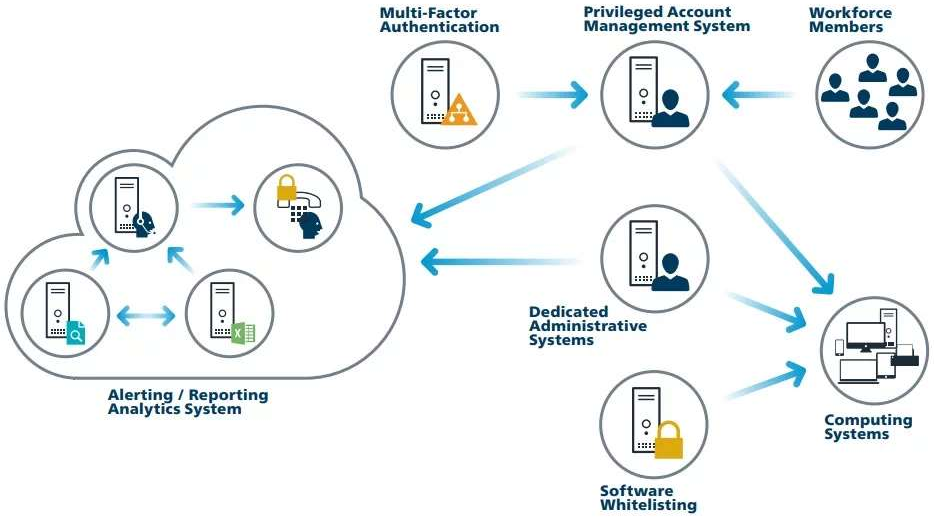

Figure 3. NNT. System Entity Relationship Diagram (CIS framework 7.1 control 4, 2019)

4 Analysis and the auditing process

The CIS control framework was used as a guideline where the steps were shown in a certain order and the areas were divided in different sections. It was performed by going one sub-control in a time, making it easier to focus on certain parts, and then continue to the next once the current asset was completed. The data for the research was gathered by going through the documents provided by the partner company since they have access to the mill's systems, and by interviewing the mill's IT personnel included in the project. All of the interviews and the meetings were held remotely because of the current pandemic.

Together with the mill's IT manager we evaluated their unit to fit the implementation group 2. The groups were first introduced with a figure 1 in the third chapter.

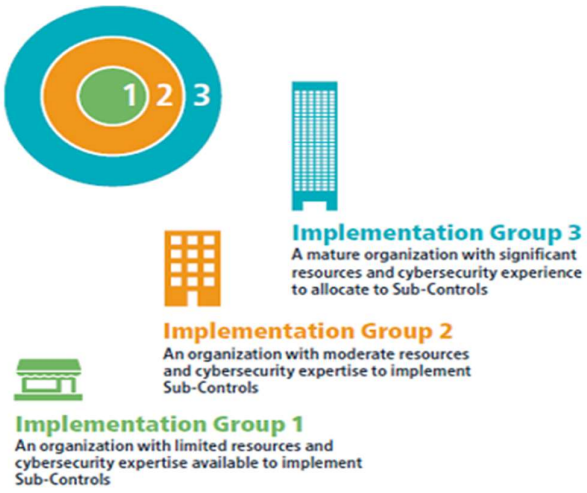

Figure 4. Implementation groups presented (CIS framework 7.1, 2019)

The mill suited the group's description since they have a dedicated group to secure and protect their IT systems. Group 1 would be a small company with a limited cybersecurity knowledge, and the third group is about the whole organization where now during this audit we had focused only in one of the factory units.

The audit has been done for the office systems and the assessment's meaning is to be aware of the company's current state, which areas need enhancing and how to reduce the risks from being compromised. Having the latest version of the updates results the company to be less prone for vulnerabilities and breaching.

At the final meeting, all the information had been gathered and presented that what needs to be fixed and implemented, and lastly a consultation on how and why to do it. With the results

that had been gotten after following the used guideline, the company knows which parts to pay attention and what has possibly been missing.

4.1 Results of the CIS control 3 audit

The attackers often take an advantage of the situations where a user or a company does not have the highest protection applied. Prioritizing the focus areas help to sort out the data's importance in order, and classifying the vulnerabilities will make the recovery process after being attacked faster.

During the audit, there were no automated nor authenticated tools that would do a regular scans, since the tool that was used in this project was for one time only. The security audit scans are recommended to be done regularly, so there will be less chance for a breach to go unnoticed. The automation would keep the software updated with the latest version and be regularly finding possible threats, by not having the automated scanning tool, the system will stay vulnerable till the next scan is done manually.

The sub-control that is being fulfilled in this control is the part 3.3. which requires an account dedicated only for the vulnerability scans, and in this research the partner company had their own account without administrative rights for the audit checks. The client was currently using a manual software that scans once it is installed, and to have an improved security level it would require to deploy an automated tool that makes sure there is a latest security update version in use. There was no access in all of the parts because some of the data was highly restricted and only accessible by the mill's employees, so was not able to compare the data results from the previous security scan.

A risk rating process in this research is done by following the CIS RAM, that is presented with the sub-control list in the table below where the framework and the risk assessment method has been combined. During this audit, the paper mill fulfills only one of the sub-controls out of seven overall.

The color scheme represents the fulfillment state, and the risk score has been calculated by multiplying the impact score with the likelihood score.

CIS sub-control	Asset type	Security function	Title	Fulfillment	Impact score	Likelihood score	Risk score
3.1	Applications	Detect	Run automated vulnerability scanning tools	No	3	3	9
3.2	Applications	Detect	Perform authenticated vulnerability scanning	No	2	2	4
3.3	Users	Protect	Protect dedicated assessment accounts	Yes	2	1	2
3.4	Applications	Protect	Deploy automated operating system patch management tools	No	3	3	9
3.5	Applications	Protect	Deploy automated software patch management tools	No	3	3	9
3.6	Applications	Respond	Compare back-to-back vulnerability scans	No	2	1	2
3.7	Application	Respond	Utilize a risk-rating process	No	2	1	2

Table 3. The assessment of the control 3

4.2 Results of the CIS control 4 audit

With the second control followed by the framework, the first section was about having an automated admin account inventory instead of a manual. The automated version will keep the inventory list of authorized rights within the systems up to date - resulting more visibility for possible disruption tries when knowing who currently has the access with the administrative privileges. Then there was an observation of default passwords in use that were found during the system scan, and they were changed during the check resulting a fulfillment of the requirements. The password changes are recommended to do before a new asset is being deployed, since it can give the attacker an opportunity to continue in compromising the domain systems through one of the accounts by using a default password. As required in the control, the mill's IT system blocks the internet access for an

administration account, because the employees have a secondary account that is dedicated for internet and email use to avoid vulnerability risks, such as phishing attacks.

There was an observation of non-expiring passwords and they are recommended to be configured as expiring after a certain time, resulting a decreased exposure probability for the password to be discovered or cracked. The office system administrative accounts do not yet have encrypted channels nor an authenticator while logging. 2FA is a widely used method to minimize the chances for an unauthorized access and the feature is currently under work to be applied. A user without administrative rights is not able to run scripts nor has access to PowerShell, making it to fulfill the security requirement that only authorized users are able to use them.

The SOC (Security Operation Center) informs and gives an alert to the office's IT personnel whenever administrative rights are given or removed and they also require a reason for these actions, more visibility when the access rights have changed so it will not go as unnoticed. There currently are no notifications whenever a wrong password has been entered while trying to login to an admin account, to improve the protection level, it is advised to implement an alert that informs when an administrative account has too many unsuccessful password entries.

One other security partner company is providing services for the mill, in area where they are using their own systems from their side to see the situations of the accounts at the paper mill's office. Consulting the client company of this research to have access to the inventory also on their own because it would raise the knowledge if there has been something abnormal, and possibly start an investigation of the malicious behavior tracking faster.

CIS sub-control	Asset type	Security function	Title	Fulfillment	Impact score	Likelihood score	Risk score
4.1	Users	Detect	Maintain inventory of administrative accounts	No	2	2	4
4.2	Users	Protect	Change default passwords	Yes	3	3	9
4.3	Users	Protect	Ensure the use of dedicated administrative accounts	Yes	3	3	9
4.4	Users	Protect	Use unique passwords	No	3	3	9

4.5	Users	Protect	Use multi-factor authentication for all administrative access	No	3	2	6
4.7	Users	Protect	Limit access to script tools	Yes	3	2	6
4.8	Users	Detect	Log and alert on changes to administrative group membership	Yes	2	2	4
4.9	Users	Detect	Log and alert on unsuccessful administrative account login	No	3	2	6

Table 4. The assessment of the control 4

5 Conclusions

The meetings and the interviews provided an insight of the mill's current situation and it was clear that the IT personnel is aware of how important it is to maintain security, since they had some of the things under implementation during the audit, and they had been expecting to hear that not all of the aspects are being fulfilled. The used framework provided a list that could be followed by steps, and it helped to see which areas are meeting the requirements, and which parts are not.

The conclusion after doing the project and audit, is that not having the latest advanced security features implemented in the systems were the important findings, because it predisposes the mill's data to be vulnerable for attackers from the outside.

The management of the vulnerability preparation requires enhancing and the control lacks the most fulfillment in this framework. The client has been informed of their current situation and consulted on how to continue with an enhanced protection with all the different parts having a different priority. Only one part out of seven is being fulfilled, meaning the mill does not meet the conditions of implementation group 2 requirements within this control. The main focus has to be on applying automated and authenticated scan tools, which

will lead to be informed about the current state regularly – resulting more awareness if there has been any changes. To fulfill the requirements for the control and fit in the current implementation group, the company must get automated tools for the systems and use them regularly. Now the chances of being compromised are high when having only manual and one-time vulnerability scans.

The control 4 it was significantly differerent, since there were more parts fulfilled, but the situation is still critical for having only four sub-controls out of eight. Organizations must prioritize the information security in their businesses, since it is a big factor when the financial gain is depending on it. Changing the personnel's default and already used passwords regularly will lower the chances for the intruder to succeed with the BFA attack in the office systems. Shankdhar (2020) at Infosec states that the BFA is one of the common methods to crack passwords still in the end of 2020, even though there are many different tools for it and they constantly become more popular. To lower the chance of this incident from happening at the client's systems, there should be a limit for unsuccessful login attempts for their accounts with a wrongly typed password.

It would have been interesting to see how the proposed ideas will be in use since further research is needed to compare the results from this project and with the next to see how the proposed ideas will be in use, and if the other units are going to follow the same framework in their future security audits and the assessments.

References

Electronic

Bluth, B. 2020. Ivanti. Continuous vulnerability management is a must
https://www.ivanti.com/blog/continuous-vulnerability-management-is-a-must#:~:text=The%20third%20control%20is%20continuous,window%20of%20opportunities%20for%20attackers.%E2%80%9D

CIS, Center of Internet Security. 2018. CIS RAM launch event
https://www.cisecurity.org/webinar/cis-ram-risk-assessment-method-launch-event/

Center of Internet Security. 2019. CIS framework control 3: Continuous vulnerability management
https://www.cisecurity.org/controls/continuous-vulnerability-management/

Center of Internet Security. 2019. CIS Control 4: Controlled use of administrative privileges
https://www.cisecurity.org/controls/controlled-use-of-administrative-privileges/#:~:text=CIS%20Control%204This%20is%20a,computers%2C%20networks%2C%20and%20applications

Gatefy. 2021. 11 real and famous cases of malware attacks
https://gatefy.com/blog/real-and-famous-cases-malware-attacks/

New Net Technology. 2019. CIS Control 3: Continuous vulnerability management
https://www.newnettechnologies.com/cis-control-3.html

New Net Technology. 2019. CIS Control 4: Controlled use of administrative privileges
https://www.newnettechnologies.com/cis-control-4.html

Petters, J. 2020. Varonis. Security audit
https://www.varonis.com/blog/security-audit/

Saarilehto, S-M. 2019. Nixu. Norsk Hydro otti kolauksen, mutta heillä todennäköisesti oli suunnitelma
https://www.nixu.com/fi/blog/norsk-hydro-otti-kolauksen-mutta-heilla-todennakoisesti-oli-suunnitelma

Shankdhar, P. 2020. Infosec. Popular tools for brute-force attacks
https://resources.infosecinstitute.com/topic/popular-tools-for-brute-force-attacks/

Figures

Tables