1dv700-Assignment 3

Group T

Alex Brumen

Fartun Jama

Nour Alasadi

Vilhelm Park

Table of contents

1. Introduction

This chapter should provide an overview of the entire document and a description of the scope of the system and its intended usage.

1.1 Purpose

The goal of this document is to give a description and recommendations of how Loco News's new secure system should be implemented. Additionally, this document is intended to show the organization how security architecture works. The document also gives the system developers an understanding of the security needs that the organization has and how to implement them. The CTO will also get some understanding of what equipment should be bought and how to implement them, while the CEO gets an understanding of what is required to change for the employees.

1.2 Scope

The document provides the guidelines for developing a new and more secure system for Loco News. The purpose of this system is to build a secure, easily maintained, and reliable new system for Loco News to better handle their sources and information. Accompanied are also the encompassing components and network configurations for protecting all devices used by the organization and the employees. The guidance provided in this document constitutes the securing of all devices in the office environment including all connections to and from the server. The document provides the main goal of the new system for Loco News and also the overall security precautions which are supposed to be implemented and followed by all the management team and the employees of the company. The new system should implement the following guidelines:

- The new system will have two-factor authentication implemented and used by every employee that will be logging into the system and using the company’s devices. This is to protect who gets access to the organization’s data.
- The system will have two separate networks, a private one that will be only used by the company-related matters and a public one that the company's guests will use.
- The data of the company will be encrypted and backed up on the cloud.

2. System overview

The guidelines that we are going to create are based on principles and strategies that will be showcased with a bullet list. They will be essential in the new system that we are suggesting Loco news implement.

- Every employee is bound to professional secrecy which will be a requirement to work in Loco news. The employees can't leak any secret information while working in the company and will be running into legal problems if they do.
- The company will have a policy that the employees need to follow, the policy will only be related to the security of Loco news.
- Every computer related to work should have two-factor authentication (2FA), this will be done with a Universal 2nd Factor (U2F) which is a specialized USB [1].
- In the new system, there is a requirement for Loco News to hire another CTO that will specialize in computer security, there is currently no one knowledgeable about computer security in the company.
- The security for the wi-fi should be upgraded from the current WPA PSK to WPA2 PSK [2] and create a password that is 15-25 characters long as well as the characters should be mixed between letters and numbers.
- The server can contain all sensitive information for the company but needs to either be relocated to a new building with limited access or the other company needs to stop having access to the server room. The sensitive information will be encrypted using the application Pretty Good Privacy (PGP). PGP is an application that uses the scheme of public-key encryption [3].
- The information that is deemed essential for the company should be put in a remote cloud backup such as google drive [4]. The information that is stored in google drive should also be encrypted using the application PGP and to access the information in the backup there will be a 2FA that will be connected to the work phone with the Google application [5]. This will be given to the employees which responsibilities are handling the backup.
- The computers will be protected by the antivirus software Malwarebytes or Kaspersky Anti-Virus, the versions of the antivirus that will be used in the system will be the version you pay for [6][7][8][9].

2.1 General overview

The new system will keep the two physical Dell servers, it will be either relocated to a room in the current building, stop giving access to the server room for the neighboring company, or moved to another building. The server room will have some kind of authentication outside so that only the employees working with the server will have access to it. The servers will contain the vulnerable information, but this information will be encrypted using the application PGP which is a scheme using public-key encryption. The sensitive and essential information to run Loco news will be stored in the cloud-based backup system Google Drive, this information will also be encrypted using PGP [5].

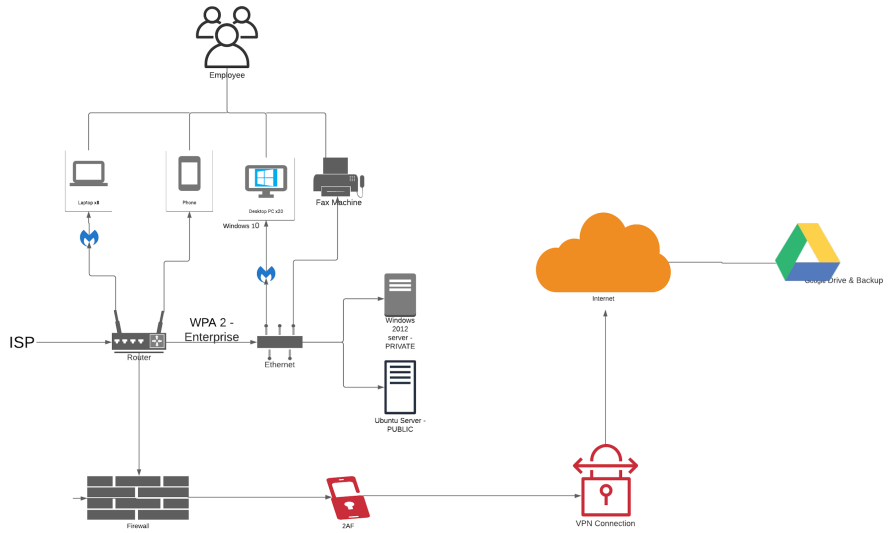
In the new system, there should be some sort of system to suppress fires in the building, the suggestions would be to implement a fire alarm system and a fire sprinkler system. The fire sprinklers

should be positioned where it's deemed necessary. Outside there will be authentication to access the building and there will be cameras to monitor who accesses the Loco News building.

The computers that are related to work will be using 2FA and every computer will be connected to its U2F which is a USB that you insert when you log in to the computer. Only the employees that are responsible for the backup will need to make their Google accounts 2FA. The wif-fi will be upgraded from WPA PSK to WPA2 PSK [2]. The password to access the wi-fi will be changed from default to a more secure password. The computers in the company will also have new antivirus software installed. The company can choose between Malwarebytes premium or Kaspersky Anti-Virus, both of which costs money.

Related to personal security the personnel will be required to sign a professional secrecy contract. They will also be required to sign a contract where they will follow a new policy for the company. The policy is regarding security and it will include details such as what the employees are and aren't allowed to do while at work or handling work devices.

When the consulting company designs the system they need to keep in mind that there should be some features that are for the admin and some for the regular users. The admin should be able to create passwords, reset passwords, and delete passwords. The admin who will handle the server will be allowed to access sensitive data, while a regular user will have access to data from the server, but never the vulnerable information. To access the sensitive information there will be a 2FA that is connected between the server and the computer the admin is working on, when the Admin wants to access sensitive information they need to insert a U2F. The new system will store data in the Loco news server and the application that we suggest creating will have a way to search for data inside it.



The new systems software architecture

2.2 Assumptions

We will assume that the company will implement the changes they can currently and that we are not limited to a budget. If the budget makes it impossible to implement all the changes we believe that the company will make the changes when their budget allows it. Another assumption is that currently, no one is an expert in the company regarding security and all the risks that we find are not known. We assume this is based on the information that has been provided and how the company currently looks. Another assumption is that no dependency between the companies computers will be affected by changing OS and limiting the software that is allowed for employees to use. Another assumption that will be made is that if a source is reliable it will be up to Loco news employees since they are professionals in the news field and should be able to tell if a source is reliable or not. In the document regarding what Loco news wants from our consulting company, they describe that we should discuss the cost associated, but not really what exactly that cost is. So we assume that it's regarding the cost associated with the new system.

2.3 Constraints

For the new system, there will be a couple of constraints that will be listed.

- Another constraint is that it will not be possible to access the backup if it's protected with 2FA and the phones related to Google Drive are lost for unforeseen reasons at the same time.
- A constraint that was given from Loco news was that they can't relocate the server to another room in the building.
- One constraint that we have is that we require that all the computers for the company will use the operating system Windows and nothing else besides that. This means that Loco news will not get help with computers that do not use Windows, which means that you may still have some security issues with computers using Linux or Mac after using our new system.

2.4 Risks

There are always security risks in every system. Therefore our system does have security risks as well. The risks in our system are mostly depending on the users who handle our new system.

Network infrastructure
The local area network (WLAN) has now WPA2 Enterprise [10]. The Enterprise version makes every user unique with their own password and username for authentication to the network.
The users who are connected to the network now need to set up a password that meets the default password security policies (Eight characters long, upper and lowercase, and symbol).

Operating system
When all desktops and laptops now move to Windows 10 operating system. The biggest risk appears when users do not upgrade the system that runs Windows 10. If a system uses an old version the system possibly has known vulnerabilities that haven't been patched [11].

Physical
The physical security has been improved. The only risk remaining is to make sure the employers that work for Loco news take care of the RFID tags. These RFID tags are used to prevent misleading improper access control to different departments.

Suppression system
The risk with a fire alarm that has a water trigger is that it can damage the electronics in the building. The fire alarm will trigger when it does detect a potential fire threat.

Backup within the cloud
The risk of sharing all backup data to google drive in the cloud is that it will be stored on the public internet, even if the data is not an audience itself. It is still stored in the cloud.

Password policy
Weak passwords are always the number one security issue for authentication systems. If a password does not meet the requirements it often leads to a compromised system within a matter of seconds [12].

Device handling 2FA
There is a risk regarding 2FA that the computers that will use a physical U2F to log in to the computers, and the 2FA for Google Drive when it comes to the fact that it's connected to a work-related mobile device. If all mobile phones that are connected to Google Drive are lost at the same time there is a chance that the backup will be lost forever. If an employee loses their U2F it will cause an inconvenience for the company since they can't access their computer.

Human error
Since the employees are not that knowledgeable about technology and computer security there is a chance that they forget their passwords and don't have them archived anywhere. If the employees also forgot their security questions that you are required to input in Windows 10, they will need to reset the computer and lose all data that they had to get a new password and regain access to the computer. If there is no backup to the information the data will be permanently lost.

Electricity loss
Another risk for the system is that it can't function if there is no electricity. Everything in the system relies on having electricity currently so if the company runs into unforeseen circumstances where they lose all electricity the company will not be able to function. If the server crashes in the middle of processes due to loss of power there is a chance that data gets corrupted. If the data is for example in relation to an update it can hurt the OS for example [13].

2.4.1 Mitigations

Network security

Every system benefits from the network therefore the network security is the priority.

To make the network secure and close as many security flaws as possible. There should be high AES encryption with unique authentication on the network. The network should then be set up with Wi-Fi protected access 2 enterprises, even known as WPA2 enterprise. This makes sure the AES encryption within all systems has secure communication [14]. The WPA2 enterprise makes sure every user does have a unique authentication to the network. All users will therefore leave a track and information about the session. This makes it easier to track down malicious actions. If an account is compromised an attacker can have access to one single account inside the network. Therefore all other accounts will stay safe.

Every user inside the network should have a different privilege. Administrators should have their own accounts with the privileges to do what they are supposed to.
While regular employers who work at the office or at home with their laptops should have low privileges access to the infrastructure and only access to the needed resources. This makes the scope for administrator access smaller and the risk of privileges escalation harder [15].

Physical security

Physical security will use secure locks with a good pin mechanism [16]. Cameras should be used outside the building to monitor every entry. To protect against robbery and improper access. The entries inside the building should be using an RFID authentication system [17]. This future makes every employer's card unique and with the right privileges and gives the correct access to different departments inside the building.

All entries are then adjusted to open depending on the employee’s configuration inside the card. For example, an employee and an administrator should have different access to different departments inside the building. This makes sure no unauthorized employer gets access to wrong information or room access.

Operating systems
The chosen operating system is Windows 10 for the laptops and Desktop at the office. To prevent common vulnerabilities and exposures (CVE) [18]. All computers owned by an employee should configure their computers to automatically update to the latest version every week on Tuesday. Because Microsoft, the owner of Windows 10, path their security vulnerability every week on Tuesday [19]. With this configuration, the systems should always be up and running at the latest version. This makes every computer as secure as possible.

Backup within the cloud
To protect data breach from a backup stored in the cloud. The security employee that handles the backup should set up an extremely strong password with all symbols and around 15+ characters long. The authentication system should also have a 2AF setup. Google Drive should have been configured to log authentications and notice when a login has failed to have the data storage under full monitor control to detect brute force attacks or authentication bypass techniques from attackers outside the network.

Password policy
Passwords should be 8+ characters long with all symbols embedded in them. The password should not contain any personal information or keywords related to the Loco company. The password should be

tested and confirmed before putting it into the real authentication system. This is to prevent leaked passwords from being reused [20].

Device handling 2FA
Some ways to mitigate the risk of losing the U2F would be to have a secure location where it can be stored in the company building. Have a brief introduction to U2F where you get some information on how to acquire the computer again if you can't 2FA due to the U2F being lost. There is a way to remove the 2FA from your windows 10 as long as there is something else that is logged into it from another device [21]. So by removing the authentication, it is possible to access the computer, but there will be a need to redo the connection to a new U2F to get 2FA again. One way to mitigate the risk of losing the work-related mobile which will be used to connect to the cloud backup would be to store them in a safe location in the company building such as a safe. Basically not allow those devices to leave the company building.

Human error
To mitigate human error the main thing that can be done is to have some sort of course for the employees where they learn basic computer security and also basic conduct such as how to archive their password safely. Also, make sure that the security question they chose is easy to remember while also archiving it just in case.

Electricity loss
One way to mitigate the electricity loss issue would be to connect the server with an uninterruptible power supply (UPS). UPS will keep the server running even if the power is lost, but only for a somewhat short amount of time. The purpose of UPS is to keep the server running long enough so that the server can shutdown cleanly and therefore not damage any of the contents of the server. [13].

3. System design

The system we provide should be an easy-to-use system with protection that does use the best possible solution for Loco news. Therefore we have divided all sections into their own.

Policy / Professional secrecy
Related to personal security the personnel will be required to sign a professional secrecy contract. which specifies that they can't leak any vulnerable information while working for Loco news. If they leak any vulnerable information they will be met with legal consequences. They will also be required to sign a contract where they will follow a new policy for the company. The policy is regarding security and it will include details such as what the employees are and aren't allowed to do while at work or handling work devices. to download any software to their personal work computers if the software has not been controlled and accepted by the CTO. The policy will also contain that the work computers need to have secure passwords which means that the passwords are required to be between 10-20 characters long and needs to use numbers, letters, and special characters. There is currently no requirement for the password to be secure so technically the password could be only a few characters long and be easy to crack if the work computers come into the wrong hands [22].

Two-factor authentication (2FA)
2FA will be used in all authentication systems. Authentication systems do offer 2FA on almost every service at the moment Google drive and other accounts do use 2FA to make sure the employer is the owner of the account. 2FA is used as an added security feature after an authentication has been done [23]. 2FA uses another device that receives a code that is used to login to the authentication system the employer tries to access. Loco news will have 2FA in their Google drive system for the backup. We will also suggest that you use U2F that has been discussed earlier in the document for the work-related computers. If it's possible to use 2FA for other accounts in the work it's highly recommended to add 2FA to these accounts as well.

Physical
For physical security measures, Loco News will have to invest in instruments/ tools.
RFID - (or Radio Frequency Identification Device) is a good example for establishing better physical security. RFID is basically a card that transmits electromagnetic fields to identify objects [24]. Every employee should have an RFID in order to enter a room.

This will minimize the risks of having unauthorized individuals in a room where sensitive information is being kept. This will increase the confidentiality of the information and sensitive documents. Original locks will also be used. These locks will be used in all entries to get inside the building itself. The locks should use high secure pins [16] to prevent lock picking [25] and improper access.

Suppression system
Basic fire alarms should be in place inside the building to prevent the company from taking fire damage. The alarms should have a built-in water system that triggers when it comes in contact with smoke. The alarms should be placed inside the office room, server room, and in the main entry. This will prevent the fire from spreading.

Server room
At the moment the servers are located in the basement and are publicly available to every employer in the company. The servers can stay in the basement as long as it is isolated from other users. Only the authenticated employees should be able to have access to the servers.
Therefore any privileges should be in place to make sure only authorized employees get access to the department where the servers are located. To make the servers even more secure it is a great idea to add an enclosed to the servers. This is a budget-friendly solution that makes sure the servers are safe. The system will also include a UPS that is connected to the server so that in the worst-case scenario the server won't get damaged by the loss of power. The UPS we recommend are Nedis ups 2000va which is regarded as a high-quality UPS.

Network
The Network infrastructure at the moment has a basic configuration in the security overall. The *Wi-Fi protected access* (WPA) is not set as an enterprise version. This makes the wireless area network (WAN) only use one single key for its network access.
To improve this a *WPA 2 Enterprise* [11] should be set up instead to make every employer have it's own username and password for the WAN. This also makes sure that the employers do have access to the system and makes it easier to monitor and log user activity on the network. Since every user is unique the monitoring for the malicious activity will be improved.

The WPA 2 offers AES [14] encryption and makes the network connection more secure inside the WAN when connecting and accessing systems. This prevents network analysis from unauthorized users outside the network. System devices such as printers, office desktops, and servers should be connected with an ethernet cable instead of the WAN to prevent device hijacking and death attacks [26] leading to a denial of service (DOS). Invest in a switch that can prevent this attack technique and also keep the printers, office desktops, and servers separate from the WAN.

Monitor physical
Investing in cameras and in security alarms makes all entries to the building more secure.
Cameras should be located outside the entries and monitor the employers who enter the building and all camera data should be stored in a hard drive to keep all the logs. The logs can then, later on, be reviewed to get information about who entered the building during a certain time. This type of technology makes it easier to have control over the building and watch every entry and also have a view if someone tries to break into the building.

Backup storage
A backup with all the storage should be used to save data in an isolated location that the backup data takes from the original infrastructure and storage. The storage should collect data from the original system and make sure to always back up the data. If the original system takes damage or gets infected by any malicious software the backup should be a last resort to restore the system again.

The backup storage should be manually viewed from time to time to make sure everything is working correctly and to make sure the backed-up data is not corrupted. When the backup data hits the isolated hard drive with storage it should be encrypted using the AES algorithm

3.1 Software design

Windows 10 will be the operating system that all software components will use. They will be installed on each desktop and laptop owned by Loco News. All systems shall be up to date and all Loco News personnel that work from home (using laptops) shall update the Windows 10 operating system frequently for better performance, new patches, better security, and improved features.
All software components should use google drive cloud. Authorized personnel could configure and replace the cloud. Other recommendations are Malwarebytes and Bitlocker. To establish a secure connection between a user and server an Secure Shell (SSH) protocol should be used. SSH protocol provides different authentication methods that focus on protecting the integrity and security of communication using strong encryption algorithms. [27]

Laptops should use Virtual Private Network (VPN). VPN creates a data tunnel that sends encrypted (unreadable) data to the Wireless Fidelity network (Wi-Fi network) that has another endpoint located elsewhere. A VPN can be used to enhance privacy by replacing the user IP address with the VPN provider IP address. This privacy will minimize the chances of employees being targeted by unauthorized individuals. [28]

3.2 Security Software design

The security software design for Loco News company was designed to provide the company with the highest protection and security level possible. The goal of the security software design is to provide protection for all of the different parts of the company such as the company's devices, networks. These include anti-virus, intrusion prevention systems, and also firewalls.

The Sys but still budget-friendly virus protection software. Our consulting company recommends Malwarebyte or Kaspersky anti-virus for the Loco news technical systems. Malwarebyte and Kaspersky anti-virus isn't too expensive and does have a live scan that can run regularly. The benefit of this software is that it does check the memory for the malware activity and more deeply scans inside the system than just the file storage [9][29].

The configuration of the computers and servers is the most important part. Most security configurations are left as the default in the old design. This is a security problem when it comes to passwords, firewall protection, and information storage. All settings should be changed manually and configured well to meet the highest possible security.

The system's main operating system is Windows 10 and to prevent unknown flaws there should be regular scanning for updates within all windows 10 systems to prevent unauthorized access from an attacker. This can be configured inside the Windows 10 operating system itself and with Microsoft's own tools that come within Windows 10.

The secure shell (SSH) will be located inside the server to have access when working from home. To make this secure and strong passwords should be set up and employers should use a virtual private network (VPN) when connecting to the server. The VPN will make sure the communication is secure to the server and has strong encryption [28].

The key for decoding the backup data should be saved to a USB flash drive or written down on paper and locked into another isolated location. This is to prevent improper access control and data exposure.

Backup with google drive cloud storage

To back up the data inside Loco news. Google offers a budget-friendly future that allows companies to back up their data directly to their server into the cloud. Therefore a company is able to buy the storage space that is required for the backup at Google drive. This prevents companies from buying their own Network-attached storage (NAS) to store backup data which can be expensive. Google Drive can be accessed easily from everywhere around the world and the backup that is stored in the Google drive can be replaced and configured to the system quickly directly from the cloud.

A list of recommended software components for the company is provided below:

- Malwarebytes
- Bitlocker
- Google drive

3.3 Cost associated with the new system

The accumulated components and their associated cost will be listed down below.

- The cost for NordVPN currently is 840 SEK annually * 28 computers. [30]
- Nedis UPS 2000va - 1 895 SEK [31]
- Malwarebytes Premium 450 SEK/annually * 28 computers[6] or Kaspersky anti-virus 330 SEK/ annually * 28 computers [9]
- Smart Brandvarnare Sikkerthjem 249 SEK * 3 [32]
- Zettle Reader 2 749 SEK * 2 [33]
- RFID-Tag 119 SEK * 20 [34]
- Trådlös bullet-kamera - 1 990,00 SEK [35]
- YUBICO YubiKey 5 NFC authentication 659 SEK * 28 [36]
- Google Drive storage business-standard 1200 SEK. [37]
- CTO 360 000 SEK/ annually

The complete cost of the system will approximately be 69 652 SEK if Malwarebytes premium is chosen or 66 292 SEK if Kaspersky Anti-virus is chosen, this will be the base price for the equipment. The CTO will cost approximately 360 000 kr per year. So the complete price for the system for a year will either be 429 652 SEK or 426 292 SEK, the former is the cost if Malwarebyte Premium is chosen and the latter is the cost if Kaspersky Anti-virus is chosen.

4. Use case scenarios

Administrator - creates an account for new employees

1. The administrator first provides logging credentials in order to authenticate themselves and log in to the systems.
2. The administrator provides log-in credentials to log in to the system.
   - 2.1. The system verifies the logging credentials provided by the administrator. if they were incorrect access is denied to the administrator and logging in to the system fails
   - 2.2. The system asks correct logging credentials to be provided
   - 2.3. The administrator retries and provides the correct username and password.
   - 2.4. Logging in to the system is successful and access is granted to the
3. After logging in successfully the administrator creates a new account and provides the new user with the access rights needed when using the system.

Reporter - writes a report

1. The reporter first provides logging credentials in order to authenticate themselves and log in to the systems.
2. The Reporter provides log-in credentials to log in to the system.
   - 2.1. The system verifies the logging credentials provided by the reporter. if they were incorrect access is denied to the reporter and logging in to the system fails.
   - 2.2. The system asks correct logging credentials to be provided
   - 2.3. The reporter retries and provides the correct username and password.
   - 2.4. Logging in to the system is successful and access is granted to the reporter.
3. Reporter is granted rights to write, edit and save a report.
4. Reporter writes a report.
5. Reporter then sends it to the editor before publishing.

5 References

[1] “Universal 2nd Factor”, [2021-01-24], url:[https://en.wikipedia.org/wiki/Universal_2nd_Factor]

[2] “Wi-FI Protected Access”, [2021-01-07],
url:[https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access]

[3]“Pretty Good Privacy”, [2021-02-23], url:[https://en.wikipedia.org/wiki/Pretty_Good_Privacy]

[4] “Remote backup service”, [2021-02-28],
url:[https://en.wikipedia.org/wiki/Backup#Remote_backup_service]

[5] “Tvåstegsverifiering”, url:[https://www.google.com/landing/2step/#tab=how-it-works]

[6] “Malwarebytes for Windows”, url:[https://www.malwarebytes.com/premium/]

[7] “Malwarebytes (software)”, [2021-02-22],
url:[https://en.wikipedia.org/wiki/Malwarebytes_(software)]

[8] “Kaspersky Lab”, [26 February 2021-02-26], url:[https://en.wikipedia.org/wiki/Kaspersky_Lab]

[9] "Kaspersky Anti-Virus 2021 | Antivirusprogram för Windows PC | Kaspersky", *Kaspersky.se*, 2021. [Online]. Available: https://www.kaspersky.se/antivirus. [Accessed: 28- Feb- 2021].

[10] "WPA2-Enterprise and 802.1x Simplified", *SecureW2*, 2021. [Online]. Available: https://www.securew2.com/solutions/wpa2-enterprise-and-802-1x-simplified/. [Accessed: 28- Feb- 2021]

[11] "Security Update Guide - Microsoft Security Response Center", *Msrc.microsoft.com*, 2021. [Online]. Available: https://msrc.microsoft.com/update-guide. [Accessed: 28- Feb- 2021]

[12] "Password policy", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Password_policy. [Accessed: 28- Feb- 2021]

[13] “Power outage … or ouch! – IT Partners.” http://www.itpartnersnw.com/power-outage-or-ouch/ (accessed Feb. 28, 2021).http://www.itpartnersnw.com/power-outage-or-ouch/

[14] "Advanced Encryption Standard", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Advanced_Encryption_Standard. [Accessed: 28- Feb- 2021]

[15] Z Banach, "What Is Privilege Escalation and Why Is It Important?", *Netsparker.com*, 2021. [Online]. Available: https://www.netsparker.com/blog/web-security/privilege-escalation/. [Accessed: 28- Feb- 2021]

[16]"Pin tumbler lock", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Pin_tumbler_lock. [Accessed: 28- Feb- 2021]

[17] *Apsipa.org*, 2021. [Online]. Available: http://www.apsipa.org/proceedings_2013/papers/389_PID2943101.pdf. [Accessed: 28- Feb- 2021]

[18] "CVE -CVE", *Cve.mitre.org*, 2021. [Online]. Available: https://cve.mitre.org/. [Accessed: 28- Feb- 2021]

[19] "Patch Tuesday", *En.wikipedia.org*, 2021. [Online]. Available: https://en.wikipedia.org/wiki/Patch_Tuesday. [Accessed: 28- Feb- 2021]

[20] “Pwned Passwords”, url:[https://haveibeenpwned.com/Passwords]

[21] Cameron Summerson, “What to Do if You Lose a U2F Key”, [2018-10-03], url:[https://www.howtogeek.com/366188/what-to-do-if-you-lose-a-u2f-key/]

[22] ISO/IEC, [2013], ISO/IEC 27002.

[23] “What is 2FA”,[2017], url:[https://authy.com/what-is-2fa/]

[24] “Radio-frequency identification”, [2021-02-25], url:[https://en.wikipedia.org/wiki/Radio-frequency_identification]

[25] “Lock picking”, [2021-01-21], url:[https://en.wikipedia.org/wiki/Lock_picking]

[26] “Wi-Fi deauthentication attack”, [2021-02-08], url:[https://en.wikipedia.org/wiki/Wi-Fi_deauthentication_attack]

[27] Tatu Ylonen, “SSH(Secure Shell)”,[2020], url:[https://www.ssh.com/ssh/]

[28] Steve Symanovich, “What is a VPN?”, [2021-01-14], url:[https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html]

[29] "Malwarebytes Cybersecurity för hem och företag", *Malwarebytes*, 2021. [Online]. Available: https://www.malwarebytes.com/se/?seredirec. [Accessed: 28- Feb- 2021]

[30] *Nordvpnteams.com*, 2021. [Online]. Available: https://nordvpnteams.com/pricing/. [Accessed: 28- Feb- 2021]

[31] https://www.dustin.se/product/5011216102/ups-2000va-4-uttag

[31] “Google Workspace (Formerly G Suite): Pricing Plans", *Workspace.google.com*, 2021. [Online]. Available: https://workspace.google.com/intl/en_ie/pricing.html [Accessed: 28- Feb- 2021]

[32] ”UPS 2000va-4-uttag” , Dustin.se, 2021, [Online], https://www.dustin.se/product/5011216102/ups-2000va-4-uttag

[33] "Sikkerthjem rökalarm", *Elon.se*, 2021. [Online]. Available: https://www.elon.se/sikkerthjem-rokalarms. [Accessed: 28- Feb- 2021]

[34] "RFID-Tagg - E-safe", *E-safe*, 2021. [Online]. Available: https://esafe.se/sortiment/tillbehor/tillbehor-ovrigt/rfid-tagg/. [Accessed: 28- Feb- 2021]

[35] "Home Page - Bascom", *Bascom.se*, 2021. [Online]. Available: https://www.bascom.se/tradlos-bullet-kamera. [Accessed: 28- Feb- 2021]

[36] "YubiKey 5 NFC | Two Factor Security Key | USB-A & NFC", *Yubico*, 2021. [Online]. Available: https://www.yubico.com/product/yubikey-5-nfc/. [Accessed: 28- Feb- 2021]

[37] "Cloud Storage pricing | Google Cloud", *Google Cloud*, 2021. [Online]. Available: https://cloud.google.com/storage/pricing. [Accessed: 28- Feb- 2021]