Linnaeus University

1DV700 - Computer Security
Assignment 2
Software design document

Group Members: <Viktor Petelin>, <Saki Dollfus Di Volckersberg>, <Sameed Alam Khan>, <Ekaterina Simakina>….

1. Introduction

Our team of consultants has analysed information which has been presented by the Company Loco News. This report focuses on improving the computer security of this company. Loco News gets a number of measures which allows it to improve the handling of sensitive and private information, keeping better track of where the information the employees use to write articles comes from etc..

1.1 Purpose of the Software Design Document (SDD)

Following the company's request, the Software Design Document sets itself a description of ways to solve problems: 1. To improve the protection of confidential, private information about users in compliance with legislative and legal regulations, 2. Protection of the database storing application and company data, 3. Assess the problems associated with application security to provide possible solutions, 4. Provide standardised and understandable documentation for the management of the company, employees, suppliers and customers for product development and implementation of innovation within a specified time frame.

1.2 Scope

Firstly, this is the standard, ISO/IEC 27002 which contains 14 security control clauses. The ISO 27002 standard is a collection of information security guidelines that are intended to help an organisation implement, maintain, and improve its information security management.

This International Standard provides guidance and guidelines for the introduction, implementation, maintenance and improvement of information security management in an organisation. The objectives set out in this national standard provide comprehensive guidance on the generally accepted objectives of information security management.

Benefits of using ISO/IEC 27002: this standard helps companies maintain the confidentiality, accuracy and availability of information to those who have access to it. Information security provides the necessary foundation for PIMS that enables companies to protect the privacy of personal information and prevent unauthorised use or disclosure of such information in accordance with regulatory, legal, and contractual requirements. ISO 27702 certification provides an internationally recognized mark of confidence for companies that they have taken all steps to meet data protection privacy requirements in addition to achieving organisation-wide information security.

Secondly, BYOD (Bring Your Own Device) security policy. Companies get the following benefits using this policy: increase workforce mobility, efficiency and productivity; cut hardware spend and software licencing costs; cut down on device management for business-owned devices

Thirdly, security mechanisms such as encipherment, access control, data integrity.

Encipherment is the security mechanism that deals with hiding and covering of data which helps data to become confidential. It is achieved by two famous techniques named Cryptography and Encipherment. Level of data encryption is dependent on the algorithm used for encipherment.

The Advanced Encryption Standard (AES) is a specification for encrypting electronic data established by the US National Institute of Standards and Technology (NIST) in 2001. AES is widely used today because it is much stronger than DES and triple DES, even though it is more complex. implement.

Access control is the mechanism which is used to stop unattended access to data which a company is sending. It can be achieved by various techniques such as applying passwords, using a firewall, or just by adding PIN to data. Access control concludes the authentication process and authorization process.

Authentication is the process of recognizing or identifying a user’s identity whether it is true, real, or not. Multi-factor authentication (MFA) improves user security.

SecurID token which has a higher level of security among other tokens.

Authorization is the process of giving people correct access to data based on their authenticated identity.

Data integrity. This security mechanism is used by appending value to data to which is created by data itself. Data integrity is important because it keeps the process going. With a constant flow of data, the integrity of the information is what allows you to maintain a database that is unimpaired and complete.

As well our team suggest to use the following security tolls:

Firewall is responsible for controlling data transmitted to and from your computer over the Internet and other networks, preventing leakage or theft of personal or confidential information, and preventing intruders from outside, so-called hackers.

VPN, when combined with additional anti-tracking tools, can increase anonymity and help hide from intruders. Using a VPN for the network not only adds an extra layer of protection, but it also makes it harder to see what a user does, since hackers will not be able to find the IP address.

Cloud security which protects data or information in the cloud from being hacked, deleted, any theft on the Internet, leaked, etc.

In addition to it, defining a programming language is an integral part of creating working software for a company. Languages must be consistent with company requests and security protocols. The language should be safe and when we call a language "safe" in some way, it formally means that there is evidence that no well-formed program in the language can do what we think is dangerous.

When developing the software, the company should keep in mind the following points:

- The different devices used could become an issue for the development
- Having both laptops and desktops means that some employees have an easier access to the software than others
- A software with sensitive information such as the one in development require particular attention. Admin privileges should be limited to those in charge of the software itself
- A single person in charge of the IT equipment management could limit the activities of the company
- The way the software is developed is influenced by the place where it is stored in

The system should follow guidelines to avoid failing or being compromised by an external individual. These guidelines include:

- Having a secured software system that uses protection methods such as anti-debugging in addition to having several layers of security
- Using a multi-factor authentication method with regular changes to the passwords and access via IP
- Storing data and control instructions separately to avoid corruption of either
- Having a central system for data verification that works on data in canonical form
- Having a cryptographic system designed by an expert on the subject
- Designing the system with an UI that allows safe navigation and lowers the risk of wanted or unwanted changes to the system
- Having a software design that allows changes from the developer side to improve the security of the system without modifying functions that do not need changes

2. System Overview

Our team has identified several guidelines that the company should follow when designing the system. We have firstly presented a general overview of the system in the context of the company. In the following section we have provided some assumptions that allow the system to work properly. Finally, constraints and risks regarding the system design have been presented in the final two paragraphs.

2.1 General Overview

The application is the focal piece of the framework and is utilised on the organisation's work area or representatives' gadgets. For the application to be usable, it should be associated with the organisation server where every one of the information is found. The association with the server is made through the neighbourhood organisation, subsequently the application is unusable to external organisation offices. A continuous reinforcement of the server is made to guarantee the accessibility of the information. Just verified and approved clients can utilise this application. We guarantee this with multifaceted verification before each application access. At last, the application can associate through the local organisation to the organisation's printers assuming we really want to print a doc.

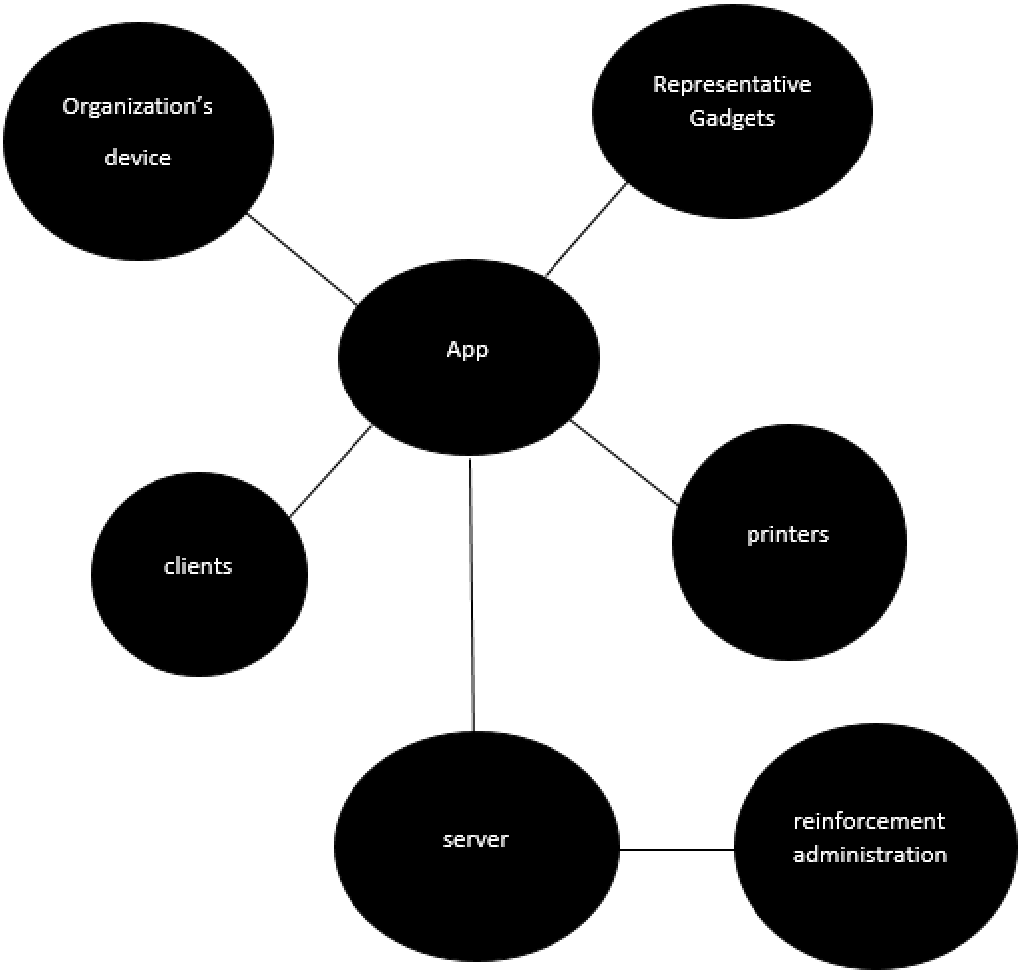
To plan the application we have chosen to utilise an item situated methodology with the plan to make the application secluded and adaptable. We ensure that each item has high attachment and low coupling to further develop the code quality and make it simple to detect defects and fix bugs. We additionally utilise the exemplification idea to give a protected API to each object.

For the validation cycle ensure that it can't be circumvented and be careful with confirmation methods that rely upon presumptions about sole ownership of assets that may really be shared. The lifetime of the confirmation ought to be confined to try not to allow admittance to a client to whom it ought not. We can do as such via naturally logging out a client later at a time of dormancy. A solitary verification administration ought to be utilised so it fills in as a solitary stifle point that can't be avoided.

When the character of the client has been checked by the verification interaction, the client strategy ought to be checked prior to getting to a record, so the client doesn't approach something they shouldn't approach.

The framework ought to approve each piece of information to guarantee respectability by utilising input approval and cryptographic measures, for example, hashing. For cryptography, we utilise standard calculations to guarantee their quality and productivity.

No outsider libraries are utilised in light of the fact that it makes a reliance on an outer and normally obscure individual, which opens the product to untrusted sources and expected bugs, defects and security issues that can't be settled inside.



2.2 Assumptions

For the proposed software, we have to make several assumptions that make the process of creation possible. These assumptions would be:

- The chosen cloud services are secure and will not shut down during the time the company is using any of them
- The access to the servers will be controlled so that an unauthorised person cannot access them
- There will not be conflicts between the developed application and other applications, for example, it will not conflict with an anti-virus
- The company will follow the guidelines regarding operating system security
- The software will not have problems of compatibility with the devices used by Loco News
- Every employee who works with this application will have access to a smartphone and a PC
- The company has enough money to cover every suggestion made by our team
- The cost of development for this application will not affect negatively the company's operations or at the very least, the implementation of this application will help improving the productivity

2.3 Constraints

After checking the current situation of the company, several limits to the development of the proposed application could be identified.

The equipment operated by the company presents a challenge to the development of the application as the employees have different devices with multiple operating systems. This unevenness could slow the development of the application and could result in an increased cost, because of the coding process requiring different codes based on different systems.

The company also has both laptops and desktops. After evaluating the purpose of the application and where it will be used, we have identified that it could be convenient to change all the computers used to one type or the other before the development process, since having both laptops and desktops creates a disparity among the employees who can access the application from outside the company office and those who cannot. If the software were to be developed with laptops in mind, it could be useful to limit the access to certain information when the device is not connected to the office's wi-fi network, so that sensitive information cannot be read from another location.

The designing of such an application would require a limit on who has admin privileges inside the company, since currently every employee has them. This type of access right should be limited to those in the company who have an active role in the development and maintenance of the application because of the importance of the information that is planned to be stored inside it. Giving admin privileges to everyone means that employees could accidentally damage files that they should have not accessed or in worse cases, sensitive information could be compromised by ill-intentioned people.

It could be appropriate to assign more than one person in the IT equipment management. The company is currently in expansion and since it is developing an application to help with their work, it is safe to assume that IT is going to play an increasingly important role. A single person could limit the usage of the application, as if they are indisposed when the system has any kind of malfunctioning the application itself could possibly be unavailable and cause problems to the workflow.

The design of the software should also take into account whether it will be developed on a cloud service or on the physical servers located in the company. A cloud service could provide more security at the cost of a limit of space where data can be stored while the servers in the company would need to be relocated or better protected as they are currently unattended and exposed to external access from the neighbouring law firm.

As this software is designed for use inside the company only, with information that could potentially harm its reputation if it were revealed to the public, the application needs to be protected by a software licence of trade secret. The development process should also be supervised by an IT expert trusted by the company, to avoid leakage of information.[1]

2.4 Risks

When designing a system, the requirements are set at the beginning and the whole project is created following those guidelines. System design risks are all the risks of failure when creating the project.

For the proposed system, the project would require particular attention to who has access to the information stored in the application database, in other words to the security of the information.

The software itself is projected to be for use inside the company only but the private data could be compromised if the software were not secure enough, relying on the hope that only the employees will ever see that data. This risk can be mitigated by using binary protection methods such as obfuscation and anti-debugging, although these methods only help to delay the process of compromission or are only partially effective. The system should also rely on different levels of security for different types of information, so that not everything is revealed once a layer is breached. The system needs to be designed considering the context where it will be used and where the data will go.

To be sure that the information will only be available to those who have the rights to do so, the system needs to be designed with a secure authentication method. The ideal authentication method is multi-factor: authentication of something you know, something you have or something you are. This method gives multiple layers of security, but passwords used to access the system should be regularly reset to be considered secure. The usernames and passwords should be provided instead of created by the users themselves, to guarantee security to the account. In the case of this company, it could be useful to consider access via IP in addition to the other methods, as employees could easily access the information from outside using their laptops. Access should also be granted for a limited time and should expire after inactivity.

When designing the system, the data and the control instructions need to be stored separately to avoid corruption of the code due to the data. Untrusted data could forcefully modify the control instructions and lead to unwanted results.

The system should be designed in a way that allows to verify that the data that enters is correct and validated. This could be done by using a centralised validation mechanism that would work differently based on the nature of the application. If it were web based, the centralised mechanism would intercept all the requests and apply basic input validation to all request parameters. Parsing, syntactic validation and semantic validation should be performed on complex data formats such as word files or pictures, parser and validators should be designed to be secure enough. Before performing these validations, data should be transformed in the canonical form so that validation cannot be bypassed by encoded data. Common libraries should be used to recognise whitelisted email addresses, URLs etc. The system design should consider the implementation of validation by parsing for the input into a typed representation. Without this layer of design, there could be issues of injection vulnerabilities, the data in non-canonical form could be used to bypass the validation, flow decisions could be controlled by the harmful data etc.

When designing the system, it is vital to consider the proper use of cryptography. When designing a cryptographic system, however, there are many security issues that could arise. It is important to keep in mind the major problems. For example, these systems' operation that use exponentials can leak secret information so standard operations are preferable. Keys should also be protected correctly so that they cannot be accessed, otherwise the system could be easily compromised. Cryptography should always rely on an expert that has good knowledge on how cryptographic systems and libraries work.

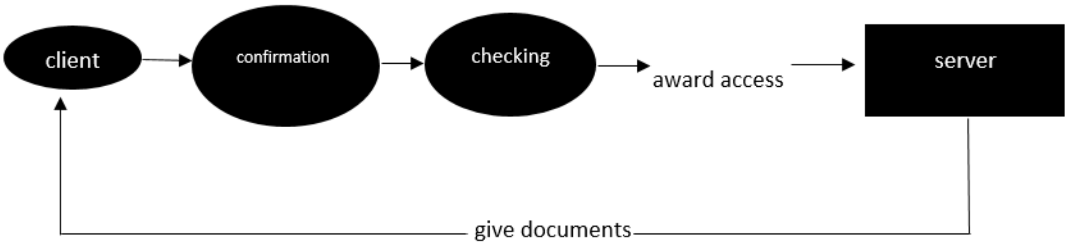
The system should also be designed with the user in mind. This is especially true if the software designed is projected to be shared with the general public, but a well-designed software can also benefit a company. Failing to properly design a user-friendly system can lead to unwanted exposure to secrets, security issues and slower work due to the difficulty of the navigation in the application.

Finally, a system needs to be designed with flexibility in mind. Threats to a system are constantly changing. In the same way, the system needs to be updated to defend itself from these threats, updates can cover loopholes that were exploited by the attackers. Updates should be regular and in small size, so that the security of each part can be better controlled. Functions that are compromised should be deactivated without affecting the whole system. It is important to do so in order to continue using the application while the issue is addressed.[2]

3. System Design

This chapter should present to the software developers the mechanisms that should be implemented.

The use of the software is to safely store (private) records required for Loco News' functional business and to give simple admittance to significant material in the information system. It depends on the plan of a web search tool that coordinates the components of the data set in a significant manner by ordering. At whatever point a representative needs to get to the information put away on the server, they should initially validate after the confirmation; admittance to the information relies upon the authorisation level of the individual client. The accompanying segments in this part give more insights regarding the framework.



3.1 Software Design

The software collaborates with the center of the framework, which gives all the data expected to regular work: the server. For the actual server, it is prescribed to run on a Linux appropriation as it is free and open-source programming, which is exceptionally secure against malware and digital dangers contrasted with the Windows Server OS. The OS ought to be stayed up with the latest to close any security holes that have become known. Since workers are utilizing distinctive OS (Windows, UNIX) it is smarter to foster the application for the two stages. Concerning in reverse similarity with past working frameworks it ought to be guaranteed that the application is just accessible on the latest OS. Consequently, it will compel the workers to refresh their OS and will give more devices to the engineers for the application improvement. At last, the application isn't a web application and until further notice, we just spotlight on the work area form, however on account of the adaptability brought by the measured quality of the application engineering, a versatile variant could be grown later on if necessary.

As the hardware that is utilized for the server, a Trusted Platform Module (TPM) can be utilized on which security capacities are executed that produce results when the framework is booted. By definition, this makes the framework a Trusted Computing Platform.

The actual software is planned to fill in as a web crawler and the executives framework for all archives put away in the data set. To empower simple admittance to the reports applicable to a client, significant records are expected to structure the archives in the data set. At the point when a client adds another report to the data set, a structure should be finished up mentioning specific data about the substance of the record: By giving a title to the archive, an overall subject under which it tends to be subsumed, and explicit watchwords that give more insight concerning the substance, the reports are advanced in significance and in this way made more straightforward to find. Extra meta-data can be the date of procurement of the archive just as the date of reconciliation into the data set and data about the client coordinating the record. Unveiling the wellspring of a report is likewise useful for ordering the data. In situations where certain data about an archive may not be uncovered (e.g., the source) because of lawful or jurisdictional issues, the field might be stamped "private". In addition, when the client adds a report, a checkbox ought to be ticked to guarantee that the client utilizes individual information on this archive (the source) and that the GDPR guideline is regarded. Thusly, the client is capable assuming any security issue identified with the report is raised. This equivalent cycle is rehashed when a report is adjusted to ensure that any alteration regards the GDPR.

The onboarding requests the client's accreditations, id and secret phrase, then, at that point, assuming those data are legitimate, the framework requests the client's finger impression. Then, at that point, the verification framework responds appropriately by denying access or moving to the primary screen. No "failed to remember secret word" or "make a record" buttons are accessible. A record is made by the IT group and in the event that a client loses their secret key, he needs to genuinely ask an IT colleague to make another one for him. A client recognized as an IT colleague approaches a screen to make another record or change the secret word of a client. To change a record secret phrase, the id and the record's finger impression ought to be entered.The application's interface ought to empower a client to have an outline of the multitude of archives put away and to channel them as indicated by explicit attributes, like point, date (of reconciliation or obtaining of the data), catchphrases, sources (e.g., explicit associations or people, articles, papers, TV or radio broadcasts, sites) or a Loco News representative who has coordinated a report. By giving a hunt bar, a more refined inquiry can be done considering a particular pursuit term.

The execution of the UI ought to likewise represent the client account strategy: After a client effectively verifies their character, which reports they are permitted to access, see or alter relies upon their authorization. To keep away from security holes, it ought to simply be feasible to inquiry records that fall inside the extent of a client.

Operating system

The operating system is one of the most important components of system software. The OS controls all other programs on the computer. An operating system is called protected if it provides means of protection against the main classes of threats. A protected operating system must contain means of delimiting user access to their resources, as well as means of authenticating the user who starts working with the operating system.

If security functions are not included in the operating system at the design stage of the operating system architecture and are not an integral part of it, it is required to use fragmented approaches to protecting the OS. Install an antivirus package, an encryption system, a system for registering user actions, etc.

This implies the use of different operating systems on the work devices of employees. This does not contradict the use of the presented software design components. Those operating systems for which there is no official support should be updated to new ones. An unsupported version of the operating system will no longer receive software updates, including for security systems, which entails an increase in the security and efficiency of the company.

Databases
PostgreSQL is a free and open-source relational database management system emphasizing extensibility and SQL compliance as the database. All files stored within the database are protected from reading by any account other than the Postgres superuser account.[3]

The database should not be open, there should be no way to access the database directly. You can use SQL for this. SQL is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.

Cloud Server
One of the alternatives to using physical servers is cloud servers. The company already has servers but is not physically secured properly. The recommendation would be to transfer to cloud servers. There are two private cloud options: on-premises private clouds and external private clouds.

External private clouds
Cloud resources are independent of computing systems and their geographic location. This provides significant savings by easily scaling resources according to needs and at the same time making them more fully loaded. Resources are not only protected with a firewall and perimeter encryption. Protection is also provided at the local level by introducing certain rules into virtual containers, which is especially important for the most important information. The necessary resources are allocated to create a backup and restore on demand. The task of creating backup configurations in your office is eliminated.[4]

Application software
For a successful implementation of Application software, it is necessary to define certain concepts to ensure that programmers and employees work with the company's application.

Programming language for application
1. For the server side.

The main conditions for this choice: 1. Maximum control from the programming language, strict types of languages so that the compiler or development environment catches data errors and compilation. (Javascript and Python are not suitable) 2. Compilation - checking the code before it is executed. (C is not suitable. Writing in C is time consuming and unsafe. From a resource management point of view, the programmer should work a lot with data.)

Java has a function eval that takes a string composed of that language's syntax and calls the language interpreter for that string. The data should not represent code, so this function should not be used when writing code.[2]

Program execution is memory safe until a certain list of bad things, called memory access errors, occurs: buffer overflow, dereferencing a null pointer, use after free, use of uninitialized memory, illegal release (of an already freed pointer or a pointer without errors). Java's that use garbage collection are universally considered memory safe, but also have out of memory errors.

2. For a custom application.

A web application is a piece of software that runs within any browser. In contrast to desktop applications, users don't have to download any programs to their devices because they get access to the solution right after logging into the website.

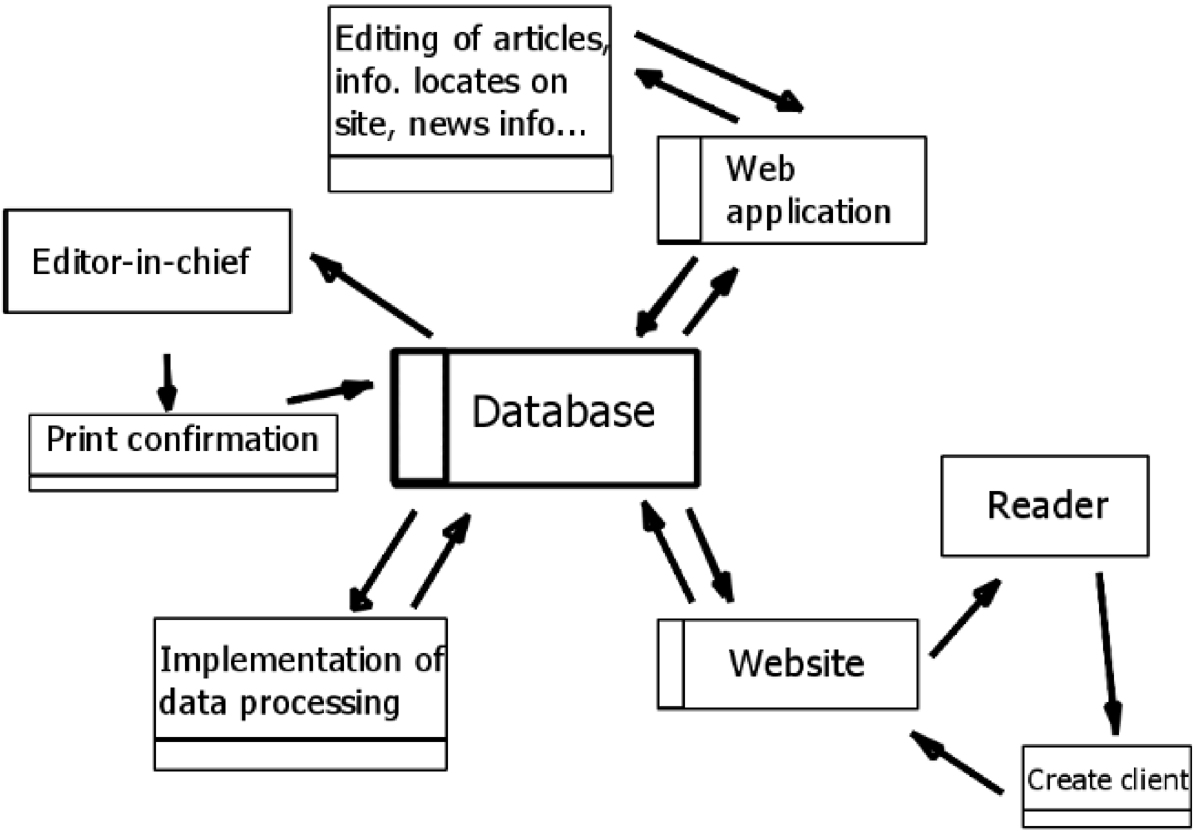
The employees of the company have different operating systems preinstalled, therefore, for the convenient implementation of this aspect, a web application using JavaScript or TypeScript is recommended.

A custom web application is based on the same concept but is tailored to your business's needs.

Communication software
Communication software is an application or program designed to transfer information from one system to another. Such software allows remote access to systems and transfers files in a variety of formats between computers.

It is recommended to use one of the protected software for the company. For example, Happeo. Happeo is unified digital workplace. An intranet, enterprise social network, and collaboration platform to engage, inform and connect your global workforce. Happeo is a complete digital workplace platform. This digital workplace provides data protection in accordance with the General Data Protection Regulation (GDPR). Happeo is hosted in Google Cloud Platform (GCP) and adheres to all implementation best practices.

Data flow diagrams
Gane-Sarson syntax is used for data flow diagramming. The diagram describes the processes - a function or sequence of actions that need to be taken in order for the data to be processed, external entities - a source of information or a recipient of any information from the system after data processing, a data warehouse - an internal data storage for processes in the system, received data before processing and the result after processing, as well as intermediate values must be stored somewhere, the data flow is displayed in the notation in the form of arrows that show what information is included and what comes from a particular block in the diagram.


Editing of articles, info. locates on site, news info...
Web application
Editor-in-chief
Database
Print confirmation
Reader
Implementation of data processing
Website
Create client

- Implementation of data processing -> (Database query in case of data editing) -> Database / Database -> (Data received on request as a result of accessing the Database) -> Implementation of data processing
- Editing of articles, news info., info. located on the site… -> (Request to editing) -> Web application -> (Request for editing data related to articles) -> Database / Database -> (Data receives on request as result of accessing database) -> Web application -> (Data receives on request as result of accessing database) -> Editing of articles, news info., info. located on the site…
- Database -> (Request for permission to post data ready for release) -> Editor-in-chief / Editor-in-chief -> (Access to placement of data from the Database on the site) -> Database -> (Data ready for release) -> Website -> Reader
- Reader -> (Data related left by the reader on their personal data) -> Create client -> (Data related left by the reader on their personal data) -> Database

3.2 Security Software Design

The Company Loco News needs to concentrate for the following security mechanism:

Access control is a security technique that governs who or what can view or use resources in a computing environment. It is a fundamental concept of security that minimises risk to an organisation.

There are two types of access control: physical and logical. Physical access control restricts access to campuses, buildings, rooms and physical IT assets. Logical access control restricts connections to computer networks, system files, and data.

According to information which we got from Loco News, the server room has no direct protection against physical access or accidents other than normal locks and a UPS for the servers. So, this company needs to protect the facility. We can suggest the following methods: use electronic access control systems that rely on user credentials, access card readers, auditing, and reporting to track employee access to restricted areas and private areas such as data centres. Some of these systems include access control panels to restrict access to rooms and buildings, and alarms and locks to prevent unauthorised access or operations [5].

Access control systems perform identification, authentication and authorization of users and objects by evaluating the required login credentials, which may include passwords, personal identification numbers (PINs), biometric scans, security tokens, or other authentication factors. Authentication is proving that asserted identity. Authentication mechanisms use any of three qualities to confirm a person's identity:

- Something a person knows. It can be passwords, PIN numbers etc.
- Something a person is. For example, biometrics characters: physical characteristic of a person, fingerprint, a face, handwriting,
- Something a person has: driver's licence, physical keys. It means that authentication has been based on tokens. There are several tokens: static token, dynamic token, active token and passive token [6].

Considering that many employees work remotely at Loco News and they often go on business trips. So, in this situation a dynamic token is suitable and useful for remote authentication. Many companies whose employees are often away from the office use the SecurID token from RSA Laboratories. This token has easy use and a higher level of security among other tokens.

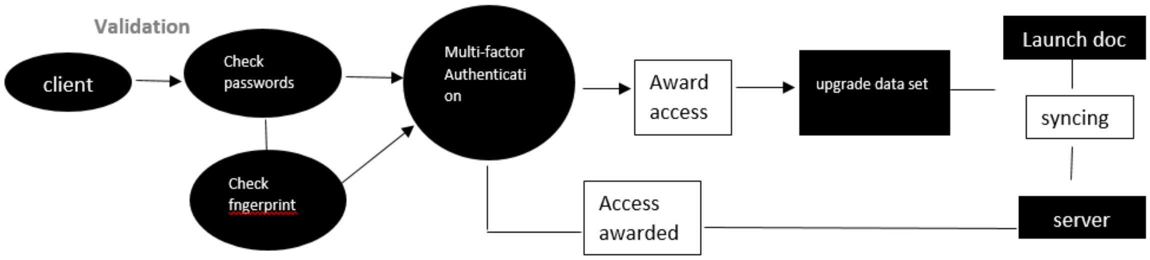
Using a SecurID token, an employee enters the current number that appears on the token when requesting an authentication application. Each token generates a random, unpredictable series of numbers that change every minute. Therefore, the authentication system understands and knows what number to expect from the employee's token. For example, two employees have SecurID tokens, but each token authenticates only its assigned owner. Entering a number from another token will not pass the authentication of the employee who sent the request. Since the token generates a new number every minute by entering the number from previous authentication also fails [6].

Take into account that the company had incidents like hardware failures, viruses and other nasty malwares therefore Multi-factor authentication (MFA) is the best way to improve security. It requires two or more authentication factors.

Multi-factor authentication (MFA) adds additional security when other security systems are unable to complete the task. User security is an area that does a lot for the overall security of a company. This should be a high priority for a company. A user should not have more access to systems and data than is required for his tasks. The company needs to establish procedures to evaluate and monitor this process to maintain overall safety.

The implementation of Multi-Factor Authentication (MFA) greatly improves user security. This must be done before accessing all business-critical applications, data and systems. The MFA includes knowledge factors and ownership factors.

Knowledge factors are usernames and passwords. A hacker can easily obtain this information using malware, as well as gain access to applications, data, and possibly other systems of the company.



However, if a company adds one or more ownership factors components, then it becomes much more difficult for an attacker to log in with stolen usernames and passwords, since then a hacker also needs to own the third component. For example, it can be a one-time code, biometric data and a token.

The best way to do the installation of MFA is to start the installation on a VPN gateway, which is designed to secure access to the data center and the applications and data that is stored there. The MFA in the VPN gateway provides protection from access to the network, not from the applications themselves [7]. We suggest to Loco News to use MFA as it will improve security.

In respect that the company has 1 WiFi router using WPA (Wi-Fi Protected Access) with PSK (Pre-Shared Key) and 4 WiFi repeaters to get better coverage, it increases the likelihood of sensitive information which can be compromised. On an unsecured public Wi-Fi network, hackers can easily intercept everything that a company sends and receives. Without a VPN, an Internet Service Provider (ISP) has access to everything that a user does on the network. Note that internet traffic may include sensitive information such as a bank account information, credit card numbers or login credentials. Attackers use wide networks, so accessing the Internet without a username, password, and VPN poses a higher risk.

To mitigate this risk, the company should use a VPN and set a password to use the Internet on its premises. The main purpose of using a VPN is to hide online activity, create enhanced privacy and internet security for a PC or any other device.

VPN helps to protect a company, a user from hackers and surveillance on public networks. VPN is also useful for hiding IP address, browsing activity, and identity on any Wi-Fi network. It helps a user to browse the web safely and securely by encrypting the connection and hiding the location, username and password to log in.

VPN, when combined with additional anti-tracking tools, can increase anonymity and help hide from intruders. Using a VPN for the network not only adds an extra layer of protection, but it also makes it harder to see what a user does, since hackers will not be able to find the IP address [8].

Access control includes authorization which is the process of giving people correct access to data based on their authenticated identity. Many companies face the following problem: an employee quit, but still has access to the assets of that company. This can create security holes because the asset that the person uses to work, such as a smartphone that has the company's software installed, is still connected to the company's internal infrastructure, but is no longer tracked because the person no longer works for the company.

If the moment is not taken into account and the appropriate settings are not made, then it can cause problems for an organisation. Hackers can hack into a former employee's device and gain access to confidential company data, since the device is no longer displayed to the company, but is still connected to the company's infrastructure. A hacker can view confidential information, change passwords [6].

One solution to this problem is to rigorously monitor and report who has access to protected resources so that when a change occurs, they can be immediately identified, and access control lists (ACLs) and permissions can be updated to reflect the change.

If a particular access control technology is difficult to use, it can be misused or bypassed by an employee, creating security and compliance gaps. That is the reporting or monitoring application is difficult to use, then the reports themselves can be compromised due to human error, which could lead to a security breach because no important permission change or security vulnerability was reported.

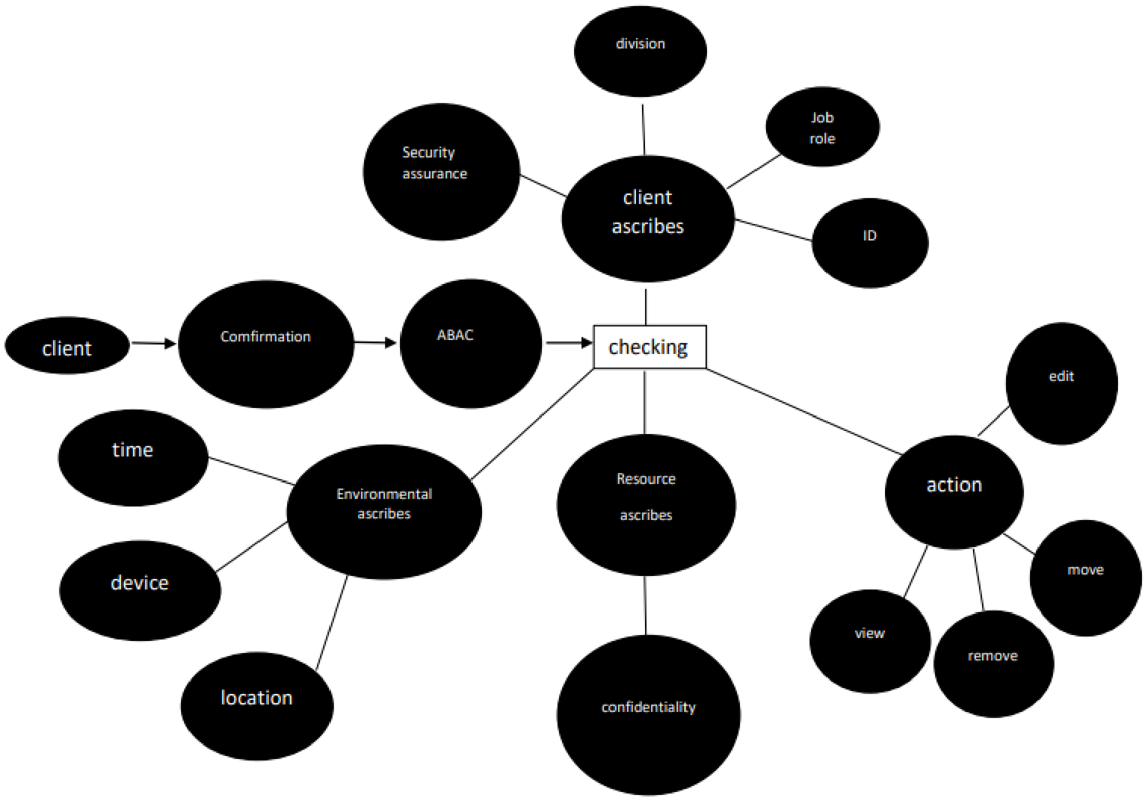
To solve this problem that company needs to use Microsoft Active Directory (AD) software which includes several components to support access control, reporting, and monitoring: password management tools, provisioning tools, identity repositories, security policy enforcement tools [9].

There are different models of access control. Considering all information which we got from Loco News we can suggest the following model which is suitable for this company:

1. Role Based Access Control (RBAC). It is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with specific business functions - for example, executive level, engineering level 1, etc. - rather than based on the identity of individual users. The role-based security model builds on a complex structure of role assignments, role authorization, and role permissions, designed using role-based engineering to regulate employee access to systems. RBAC systems can be used to enforce MAC and DAC structures.

2. Access control based on rules. This is a security model in which the system administrator defines the rules governing access to resource objects. Often these rules are based on conditions such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.

3.ABAC (Attribute Based Access Control): When the client is signed into the framework, access choices as indicated by the Attribute-Based Access Control (ABAC) model must be assessed, which rely upon specific qualities of the client, the assets to be gotten to, the planned activity and ecological variables. As described in the figure, client credits allude to the individual attempting to get entrance. Models incorporate username, ID, age, work title and job, office and exceptional status. Asset credits portray the asset that is being gotten to and can, for instance, identify with its privacy. The activity is how the client will manage the asset, for instance, seeing, altering, moving or erasing. Natural credits depict the setting of the entrance endeavor. Models incorporate time, area or the gadget being utilized. While it is more confounded to execute contrasted with Role-Based Access Control (RBAC), ABAC is not difficult to scale and takes into consideration an exceptionally designated way to deal with information security ABAC is completely described in the figure below:



Access control implementation. For implementing access control the company has to include an identity and access management system. These systems provide access control software, a user database, and policy management tools for access control, auditing, and enforcement.

When a user is added to an access control system, system administrators use an automated provisioning system to configure permissions based on access control structures, job responsibilities, and workflows. Best practice for least privilege restricts access to only the resources that employees need to perform their direct job functions.

When using this security method, the following difficulties can arise:it is difficult to keep track of constantly evolving assets as they are distributed both physically and logically. However, this issue can be solved by authentication and authorization which are described above [10].

The next security mechanism is data integrity which is having correct and accurate data in a database. When a user stores data in the database he or she doesn’t want to have repeating values, incorrect values or broken relationships between tables. Data Integrity can be maintained using constraints. These constraints define the rules according to which the operations like updating, deletion, insertions etc. It has to be performed to maintain the data integrity. There are mainly four types of Data Integrity:

- Entity Integrity. It ensures that the data is not specified more than once and that no field in the database is empty. The integrity of an entity depends on the generation of primary keys - unique values that identify pieces of data.
- Referential Integrity is a set of procedures to ensure consistent storage and use of data. Only appropriate changes, additions or deletions of data are made. Rules that are contained in the database structure are used as foreign keys. Rules can include restrictions that prevent redundant data entry, ensure correct data entry, and prohibit entry of data that does not apply.

- Domain Integrity
- User-Defined Integrity

Maintaining data integrity is important for several reasons.

- First, data integrity ensures recoverability and retrieval, traceability (to source), and connectivity.
- Second, protecting the integrity and accuracy of data also increases stability and performance, improving reusability and maintainability.
- On top of that, Data increasingly influences decision making in the enterprise, but it must undergo various changes and processes in order to move from a raw form to more practical formats to define relationships and facilitate informed decision making.

Therefore, data integrity is a top priority for today's businesses.

Data integrity can be compromised in a variety of ways, making data integrity techniques an essential component of effective enterprise security protocols. Data integrity can be compromised due to:

- Human error, malicious or unintentional
- Transmission errors, including inadvertent changes or data compromise during transmission from one device to another.
- Bugs, viruses / malware, hacking and other cyber threats
- Hijacked hardware such as device or disk failure
- Physical threat to devices

A number of measures can help prevent these problems: data backup and duplication, input validation to prevent invalid data entry, error detection / data validation to detect errors in data transmission, as well as security measures such as data loss prevention, access control, encryption data [11].

Considering that the organisation wants to improve the security of its organisation and several incidents like Hardware failures, Viruses and other nasty malwares: Denial of Service, Trojan. We strongly recommend using Advanced Encryption Standard.

The Advanced Encryption Standard (AES) is a specification for encrypting electronic data established by the US National Institute of Standards and Technology (NIST) in 2001. AES is widely used today because it is much stronger than DES and triple DES, even though it is more complex. implement.

- AES is a block cipher.
- Key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

This means it accepts 128 bits in input and outputs 128 bits of cipher ciphertext on output. AES relies on the principle of network-for-damage-reshuffle.

The AES algorithm is popular with companies because it cannot be broken even with modern technology. To date, the only vulnerability remains in the implementation of the algorithm [12].

Loco News should use encryption across the board as this company has 3 big newspaper printers/presses connected via network and 22 desktop printers connected via USB to each employee workspace. Using encryption across the board, not only a large amount of data will be processed, but also a wide variety of data. To protect data, companies need to use encryption for computers, data at rest, data in transit, and data in the cloud. USB devices and phones must also use encryption if they handle sensitive data. Not all data needs to be encrypted, but intellectual property and confidential information requires encryption. Many Loco News employees work remotely and often travel so encryption serves as a security measure for teleworking and travelling employees. With greater availability and flexibility when it comes to where a person works, encryption helps protect devices and maintain data integrity no matter what network the device is on [13].

In addition to all of the above Loco News should use cloud security tools which help to handle sensitive information.

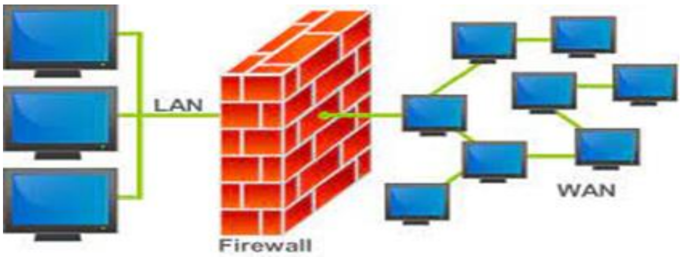
Cloud security means protecting data or information in the cloud from being hacked, deleted, any theft on the Internet, leaked, etc. It is accomplished through a group of applications, firewalls, policies, VPN controls, technologies, small software tools, and more. This security is part of network or computer security that is provided by specific cloud service providers who perform a number of functions to avoid cloud security issues. However, they don’t have control over how a company uses the service, what data the company adds to it and who has access. In this way, companies can weaken cybersecurity in the cloud through their configuration, sensitive data, and access policies as data in the public cloud is stored by a third party and it is accessible over the Internet. There are a number of challenges in maintaining a secure cloud. The company should follow a series of processes to keep the system from crashing.

- The company needs direct access to the cloud service. It means an application programming interface (API) needs to be connected to the cloud service. When connecting to the API, the company can view the following processes: what data is stored in the cloud; who uses the cloud data; roles of users with access to cloud data; with whom cloud users share data; where is the cloud data; where is the access to cloud data and where it is downloaded from, including from what device.
- Using cloud data encryption prevents unauthorised access to data.
- Implementing system and application access controls ensure that only authorised users can access cloud data and applications.
- Implementation Access Block. It means that when a person with an unauthorised device tries to access cloud data, he or she will be blocked.

4. Performing file scanning and analysis of network traffic. These processes allow a company to prevent the entry of malicious programs [14].

Firewall is responsible for controlling data transmitted to and from company’s computers over the Internet and other networks, preventing leakage or theft of personal or confidential information, and preventing intruders from outside, so-called hackers.

A big advantage of using a hardware firewall is if your network has more than one computer. All machines in the network will be connected to one router, which will immediately act as a firewall for the machines. Look at Graph 2.



Graph 2

Firewall prevents computers from outside intruders. It blocks data transmission from your computer other than those that are permitted.

However, firewall has several drawbacks:

- Does not protect against user-downloaded programs.
- Does not block messages from mail programs.
- Unable to prevent the user from creating erroneous exceptions that could put the computer at risk.

To solve these problems is to configure your firewall to block everything. This may sound a little odd, but this is only the first step. If the company blocks everything, then it is obvious that nothing will work. After it the company consistently allows only what they need to work on the computers, thereby not missing or forgetting to block some third-party program.

There are several types of Firewall. We suggest to Loco News to use *threat-focused Firewalls*. These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused Firewall the company can know which assets are most at risk, quickly react to attacks with intelligent security automation, detect evasive or suspicious activity with network and endpoint event correlation, decrease the time from detection to clean up with retrospective security that continuously monitors for suspicious activity and behaviour even after initial inspection, reduce complexity with unified policies that protect across the entire attack continuum [15].

As well the company can use antivirus such as Kaspersky, Nod 32.

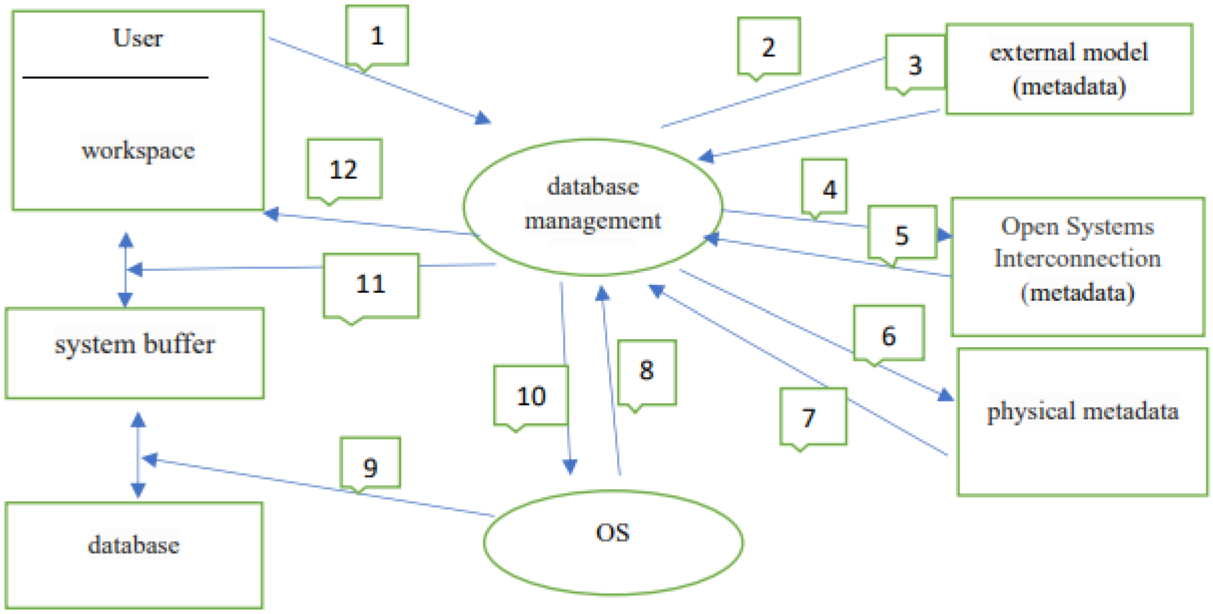
The work with the website and web application of the company should be carried out through HTTPS connection. HTTPS - only encrypted HTTP connection, must use TLS (an algorithm for ensuring communication encryption) of the protocol not lower than version 1.2 and not use SSL.

Data leakage - the programmer's computer is not as secure as the server. On a personal computer, a programmer should not store data from a database, but only work with servers or applications that are on servers.

4. Use Case Scenarios

During the working day, a number of functions are performed every day, which are repeated. For example, a user makes a request to get data. See graph 3.

The process of passing a user request.



Graph 3. Scheme of the passage of a request to the database.

1. The user sends a request to the database management system to receive data from the database.
2. An analysis of the user's rights and the external data model corresponding to a given user confirms or denies this user's access to the requested data.
3. If access to data is denied, the database management system informs the user about it (number 12) and stops further data processing, otherwise the database management system determines the part of the conceptual model that is affected by the user's request.
4. The database management system receives information about the requested part of the conceptual model.
5. The database management system requests information about the location of data at the physical level (files or physical addresses).
6. The information about the location of the data in terms of the operating system returns to the database management system.
7. The database management system asks the operating system to provide the necessary data using the operating system tools.
8. The operating system downloads information from storage devices and sends it to the system buffer.
9. The operating system notifies the database management system about the end of the transfer.
10. The database management system selects from the delivered information in the system buffer only what the user needs and sends this data to the user's workspace.

For example, a user can again send a new request to database management system, then the external model and access rights will no longer be checked for him or her, and if further analysis of the request shows that the data can be in the system buffer, then the database management system will only take 11 and 12 steps in processing request.

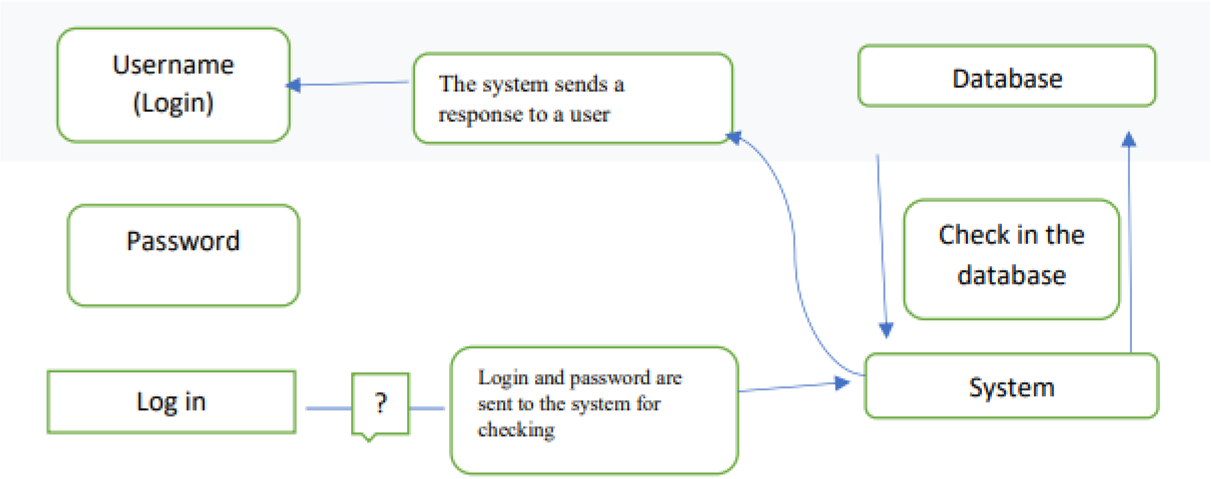
Sometimes a user is unable to connect to the database management system. Instead, he or she receives a 4062 error message or a 4064 error message that is similar to the following. Error message when a user connects to an instance of SQL Server: "Cannot open user default database". It happens as the database can be in suspicious mode, no longer exists; the user has been suspended; a user is offline or the database can be set to emergency mode [16].

To resolve this error, a company should specify a valid accessible database in the connection string. To prevent the error when the default user database is not available, log in as a user who can modify logins. Then change the default user database to the database that is currently connectable [13] .

Authentication processes.

Every day a user enters a password, login, that is, confirms his or her identity.

The graph 4 shows the mechanism of matching the login and password.

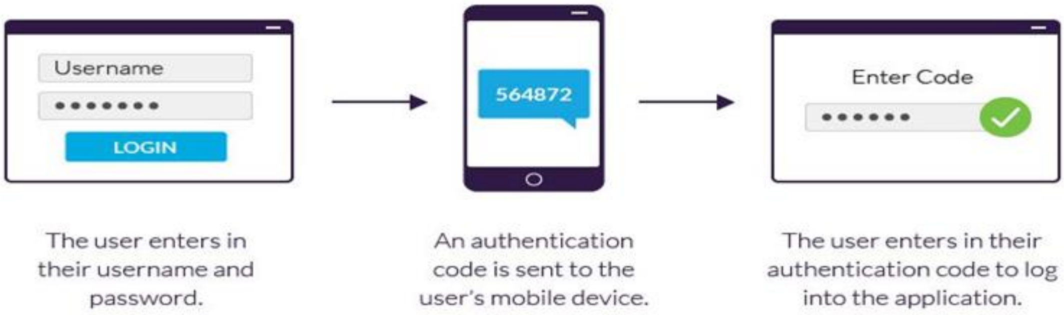

Username (Login)
The system sends a response to a user
Database
Password
Check in the database
Log in
?
Login and password are sent to the system for checking
System

Graph 4. The process of checking the compliance of the login also takes place in several stages.

1. User Enters login
2. User Enters password
3. User Submits data for verification
4. The system receives the data entered by the user, searches for the user in its database, checks the correspondence of the username and password.
5. The system sends the result of the check to the user.
6. We get the result of the check.

The verification process is the same for all authentication methods.

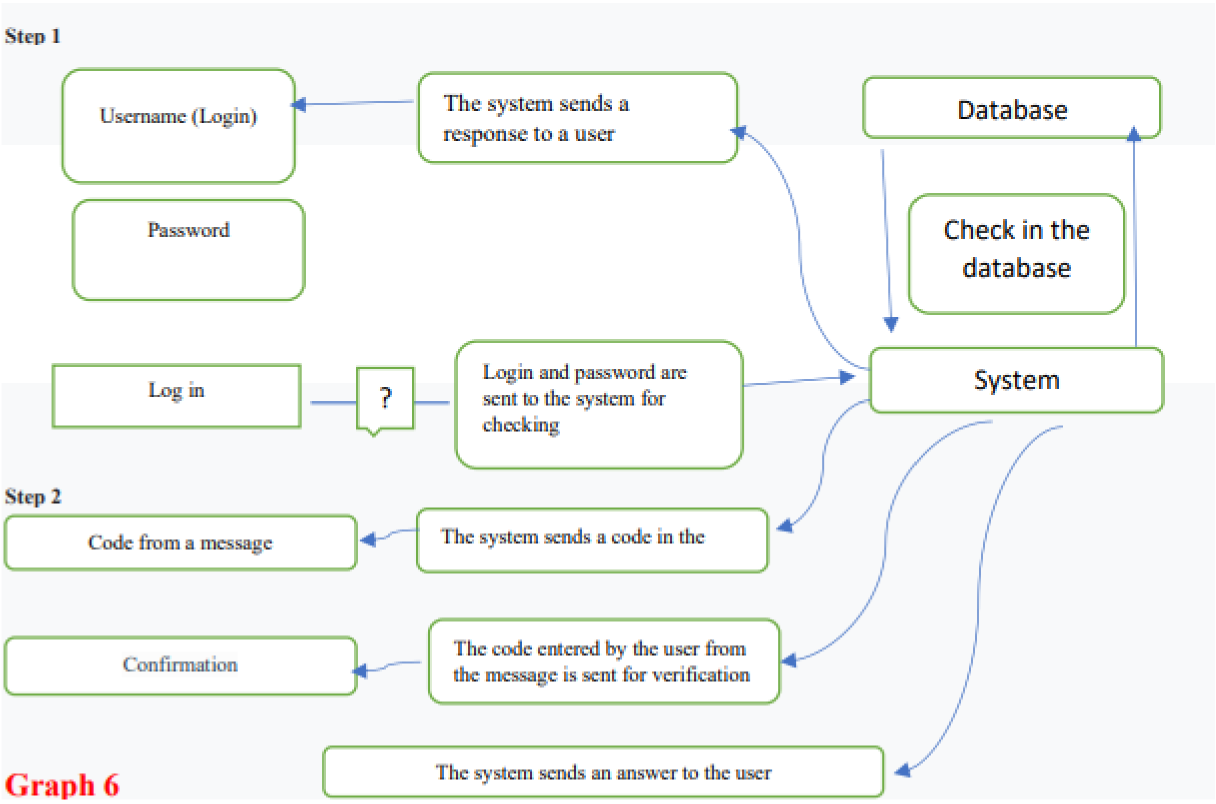
Two-factor authentication. Look at Graph 5.


Username
LOGIN
564872
Enter Code
The user enters in their username and password.
An authentication code is sent to the user's mobile device.
The user enters in their authentication code to log into the application.

Graph 5

In some cases, an additional measure of protecting the user's credentials may be required, and this is why a two-factor authentication mechanism is introduced - this is when the user needs to authenticate his identity in two different ways. An example is - entering Email + Password, and then the phone number and SMS code.

Simplified Two Factor Authentication Scheme. Look at the graph 6.


Step 1
Username (Login)
The system sends a response to a user
Database
Password
Check in the database
Log in
?
Login and password are sent to the system for checking
System
Step 2
Code from a message
The system sends a code in the
Confirmation
The code entered by the user from the message is sent for verification
The system sends an answer to the user

Graph 6

At the first stage, a user enters a username and password. After it the user sends them to the system for verification - just like in regular authentication. The system verifies the username and password, and sends a response (verification result) to the user. The answer can be either positive or negative. If the answer is positive, then the user proceeds to the second stage. At this time, he or she should receive a message with a confirmation code in the form of symbols or a link. After entering the confirmation code, the user again sends the data to the system for verification. If the answer is positive, then the user gets access to this data. If the answer is negative, then the user gets the opportunity to try again, or the authentication process starts over.

During the process of checking the login and password, it can be that authentication is not passed and a user has not gained access to his or her personal data. This can happen for the following reasons:

1. Login entered incorrectly.
2. The password was entered incorrectly.
3. No connection to the server.
4. Error checking data by the server.
5. The limit of erroneous authentication attempts has been exceeded.
6. The user account is blocked by the administrator.

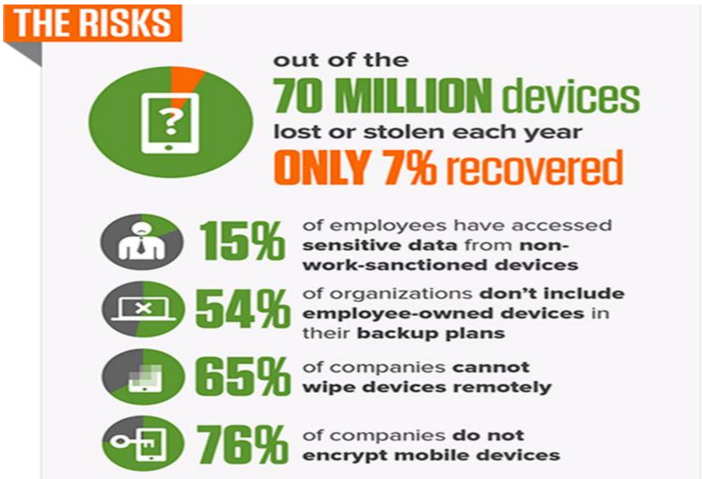
Limits for erroneous authentication attempts are introduced to enhance the security of users' personal data. After exceeding the limit, the password is usually restored. In a system with an increased level of control over the user's security, measures are taken to block the account the moment the user's identity is confirmed [14].

5. Use other security tools

Take into account that the company, Loco News, allows its employees to use their own devices like smartphones and tablets, so our group of the consultants recommend using a BYOD (Bring Your Own Device) security policy. By following the right approach to identifying risk and designing an effective BYOD policy, the company can get a number of benefits and improve security.

BYOD security is often a concern for companies, as an organisation has to (in one form or another) control smartphones, tablets and laptops that do not belong to the company, but these devices are personal assets of employees.

The research was conducted among organisations that did not use BYOD policies and identified the risks to which they were exposed. Look at the graph 7.



THE RISKS

out of the 70 MILLION devices lost or stolen each year ONLY 7% recovered

15% of employees have accessed sensitive data from non-work-sanctioned devices

54% of organizations don't include employee-owned devices in their backup plans

65% of companies cannot wipe devices remotely

76% of companies do not encrypt mobile devices

Graph 7.

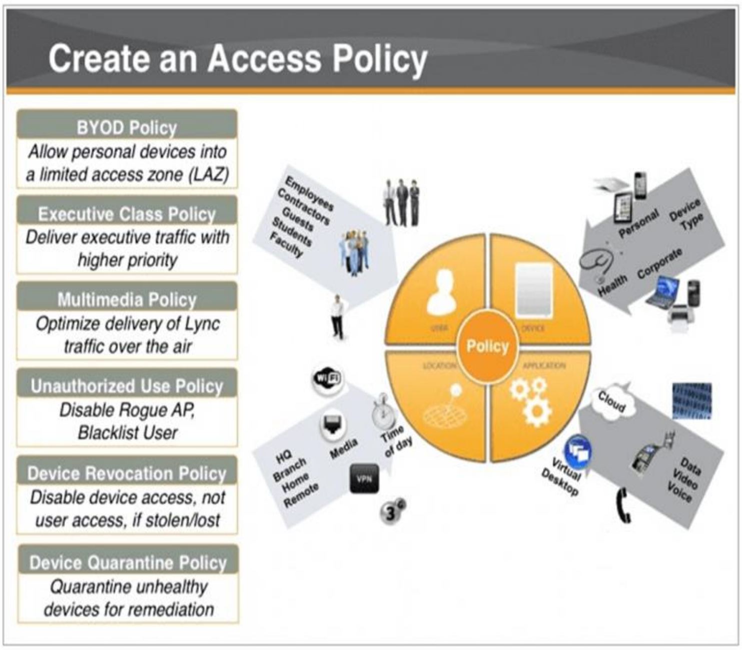
Creating a BYOD policy Loco News should consider the following points:

1. Interviewing employees. It's an efficient way to get information about the devices of employees which they currently use.
2. A list of applications and information assets to which employees are allowed to have access from their personal devices.
3. A list of applications and information assets to which employees are prohibited to have access from their personal devices.
4. Minimum necessary Security measures for devices. For example, SSL certificates for device authentication.
5. Two-factor authentication for any applications and programs that are accessed from employee-owned devices.
6. When an employee quits a job it is also an important factor in outlining a company's BYOD policy. The definition of clear policies that explain the procedures to be followed when an employee leaves the company, such as how the IT department cleans up an employee's device, should be explained in detail in written policies.
7. It is necessary to point out the responsibility of employees for the leakage of confidential

company data caused by negligence or disregard of the rules.

8. Data must be encrypted, password protected, and only transferred in applications approved by the company.

An effective BYOD security solution must consider several elements. See graph 8 [17] .



Create an Access Policy

BYOD Policy
Allow personal devices into a limited access zone (LAZ)

Executive Class Policy
Deliver executive traffic with higher priority

Multimedia Policy
Optimize delivery of Lync traffic over the air

Unauthorized Use Policy
Disable Rogue AP, Blacklist User

Device Revocation Policy
Disable device access, not user access, if stolen/lost

Device Quarantine Policy
Quarantine unhealthy devices for remediation

Graph 8.

In addition to it the company should use the international standard ISO / IEC 27002, which focuses on best practises for information security management. This is now fundamental to the consolidation of an information security management system to ensure the continuity and maintenance of security processes in line with the strategic objectives of the organisation.

The main purpose of ISO 27002 is to establish guidelines and general principles for starting, implementing, maintaining and improving information security management in an organisation. It also includes the selection, implementation and management of controls, taking into account the risks of the company.

Benefits provided by using ISO 27002:

- Better understanding of information security;
- Stricter control over confidential assets and information;
- Faster approach to implementation of control policies;
- Ability to identify and correct weaknesses;
- Promotes cost reduction by preventing information security incidents.
- Compliance with laws and other regulations [18].

References

[1] WIPO, “Trade Secrets” [Online]. Available: https://www.wipo.int/tradesecrets/en/ [Accessed: December 18, 2021]

[2] Avoiding the Top 10 Security Design Flaws, https://ieeecs-media.computer.org/media/technical-activities/CYBSI/docs/Top-10-Flaws.pdf”

[3] POSTGRESQL, chapter 28. SECURITY. SQL Standard. 2021. [Online]. Available: https://www.postgresql.org/docs/7.0/security.htm [Accessed: December 12, 2021]

[4] Jaydip Sen, “Security and Security and Privacy Issues in Cloud Computing Computing”, Microsoft Word. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1303/1303.4814.pdf

[5] A. Tunggal, “What is Role-Based Access Control (RBAC)? Examples, Benefits, and More”, in *UpGuard*, October 2021, [Online]. Available: https://www.upguard.com/blog/rbac

[6] C.P. Pfleeger, S.L.Pfleeger, J. Marglies, Toolbox: Authentication, Access Control, and Cryptography, in ”Security in computing”, 15 edition, Pearson Education Inc., 2015 [Online]. Available: Security in computing by Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies (z-lib.org).epub.pdf

[7] Microsoft,” How it works: Azure AD Multi-Factor Authentication”, in *Microsoft 2021*, June 2021, [Online]. Available: https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks [Accessed: December 12, 2021]

[8] E. P. Sidell, “Why Do I Need to Use a VPN?”, in *Avast Academy*, March 2021, [Online]. Available: https://www.avast.com/c-do-i-need-a-vpn [Accessed: December 12, 2021]

[9] Enterprise management (EM360), “Top 10 Active Directory Management Tools”, in *Enterprise management* [Online].October 2020, Available: https://em360tech.com/top-10/top-10-active-directory-management-tools [Accessed: December 12, 2021]

[10] S. Gentry, “Access control: Models and methods”, in *InfoSec Institute*, March 2021, [Online]. Available: https://resources.infosecinstitute.com/certification/access-control-models-and-methods/ [Accessed: December 12, 2021]

[11] C. Brook, “What is Data Integrity? Definition, Best, Practices & More”, in *Digital Guardia*n, December 2020, [Online]. Available: https://digitalguardian.com/blog/what-data-integrity-data-protection-101 [Accessed: December 12, 2021]

[12] Geeks for geeks, “Advanced Encryption Standard (AES)”, in *Geeks for geeks*, December 2021.[Online]. Available: https://www.geeksforgeeks.org/advanced-encryption-standard-aes/ [Accessed: December 12, 2021]

[13] Endpoint Protector, “5 Ways Big Companies Protect their Data”, in Endpoint Protector, December 2018, [Online]. Available: https://www.endpointprotector.com/blog/5-ways-big-companies-protect-their-data/ [Accessed: December 12, 2021]

[14] E. Katz, “Top 12 Cloud Security Tools for 2021”, in *Spectral*. [Online]. Available: https://spectralops.io/blog/top-12-cloud-security-tools/ [Accessed: December 12, 2021]

[15] Geeks for geeks, “Introduction of Firewall in Computer Network”, in *Geeks for geeks*, November 2019, [Online]. Available: https://www.geeksforgeeks.org/introduction-of-firewall-in-computer-network/ [Accessed: December 12, 2021]

[16] A. Alam,”SQL Database Error 4062/4064 – Cannot Open User Default Database”, in *Nucleustechnologies*.[Online]. Available: https://www.nucleustechnologies.com/blog/sql-database-error-cannot-open-user-default-database/ [Accessed: December 12, 2021]

[17] C. Brook, “The Ultimate Guide to BYOD Security: Overcoming Challenges, Creating Effective Policies, and Mitigating Risks to Maximize Benefits”, in *Digital*

Guardian, November 2020. [Online]. Available:https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating [Accessed: December 12, 2021]

[18] Ostec "ISO 27002: Best Practises for Information Security Management", in *Ostec*, 2021. [Online]. Available: https://ostec.blog/en/general/iso-27002-best-practices-ism/ [Accessed: December 12, 2021]