PART 1

1.Intel processor and AMD processor

Factors to Consider

* BASE CLOCK AND BOOST CLOCK

AWD processors range in basic clock speed from 4.5GHz in Ryzen 97950x to 4.7GHz in Ryzen 57600xx.The Core i5-13600K from Intel has a 3.5GHz (P-core), 2.6GHz (E-core), and 3GHz (P-core), 2.2GHz (E-core) processor.

boost clock: The Ryzen 9 7950X AWD processor runs at 5.7GHz, while the i9-13900k from Intel runs at up to 5.8GHz.

* BUDGET: AMD used to be less expensive than Intel in the past, and you generally got what you paid for. It's relatively near now. If you're attempting to decide between buying Intel or AMD in 2023, Intel will still generally be the better option.
* SPEED: When we narrow our focus to just typical desktop processors, Intel's 16-core Core i9-13900K, which costs a more affordable $650, takes the top spot. The fastest AMD processor is the 16-core Ryzen 9 7950X, which costs $575 and is somewhat slower than Intel's chip.
* POWER CONSUPTION AND HEAT: It is impossible to emphasize the importance of having the densest manufacturing node matched with an effective microarchitecture when comparing AMD and Intel CPU performance per watt, and TSMC's 5nm and AMD's Zen 4 are the winning combo. In terms of power usage versus performance, the most recent Ryzen processors are less powerful than Intel.
* CPU ARCHITECTURE: It is obvious that the battle between AMD and Intel CPU design is much tighter currently than it has been in recent years. The AMD Zen 4 architecture is a marvel that offers improved scalability and boasts outstanding power consumption metrics thanks to the efficiency-focused design and the TSMC 5 node.

The most potent consumer-grade processor on the market is AMD's most recent Zen-based chip. Additionally, Intel CPUs deliver the finest performance at a reasonable cost. The 13th-generation range of Intel CPUs offers the best value and is more than adequate for the majority of users, even though AMD may be the best CPU in terms of overall power.

1.2Absolute transparency

In actuality, the complete transparency of its code is the source of many other benefits associated with open-source software.

Additionally, because the code is openly accessible, customers feel more secure using it for lengthy tasks. An illustration is the adoption of Linux, an open-source operating system that benefits from regular review and prompt patches from the community.

Flexibility

Open-source software is adaptable because it gives programmers the ability to check the operation of the code and make changes as needed. The ability of this type of software to correct problematic program elements is one of its main advantages. For instance, laboratories might alter free and open-source tools for data analysis like R or Python to produce specific statistical models or techniques..

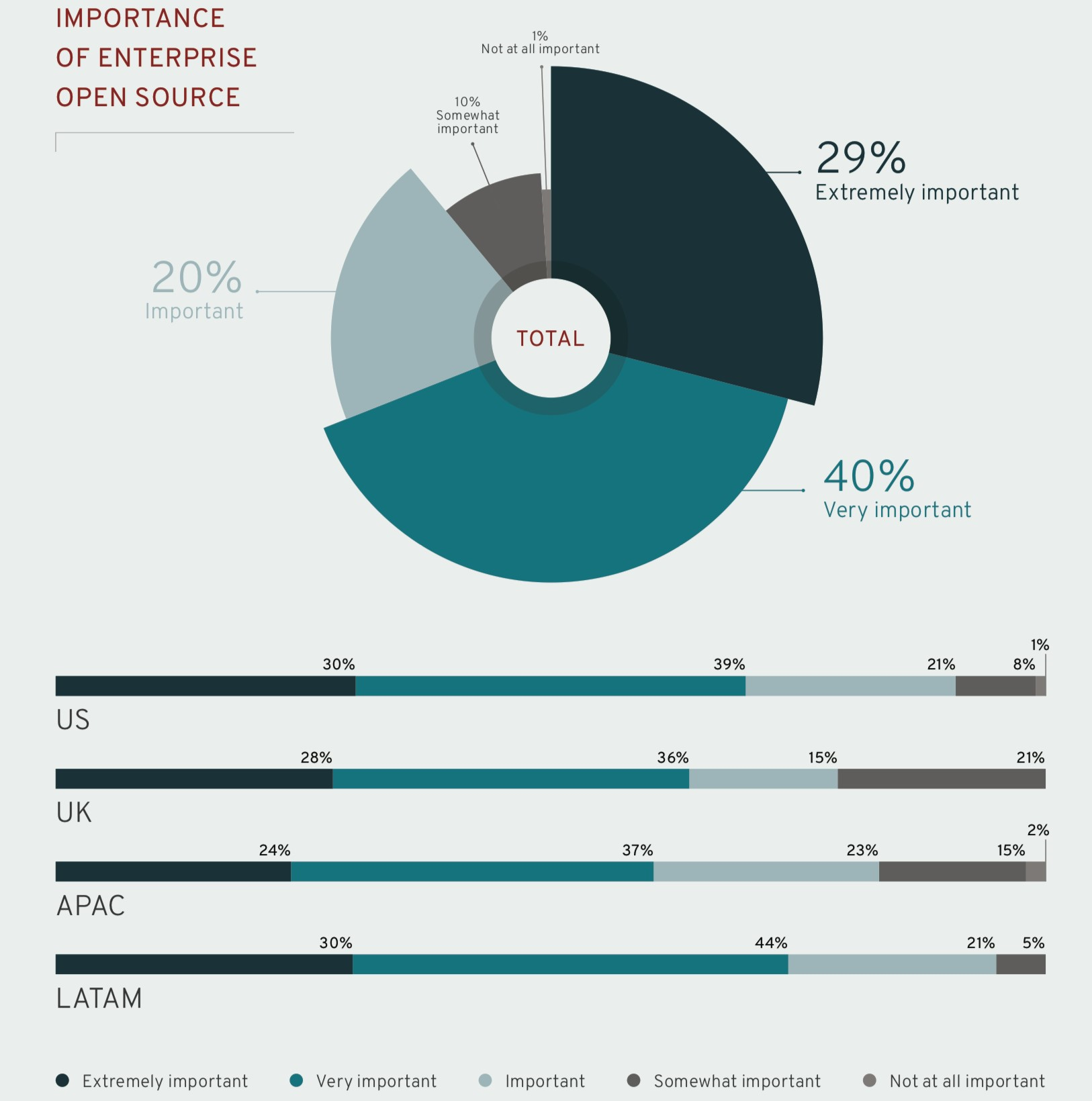
No vendor lock-in

The ability to use, modify, and distribute open-source software is one of its main benefits (more so with some licenses than others).

This independence includes the capacity to stop utilizing the software without facing serious repercussions. For example, instead of using a commercial virtualization solution, labs can select the open-source virtualization platform VirtualBox.

The power of community

The effectiveness of team cooperation is strongly supported by open-source communities and contributors. Since the source code is available to the public, developers frequently suggest improvements to it to improve functionality, security, or other factors. An excellent illustration of a project with a vibrant community that offers support, plugins, and themes is the open-source content management system WordPress.



Powering the digital transformation

This report demonstrates how companies are depending more and more on open-source software to accelerate digital transformation while improving efficiency, adaptability, and interoperability.. For instance, labs can utilize the free and open-source PostgreSQL database management system, which supports numerous operating systems and offers strong interoperability.

1.3Slightly Lower and Unreliable Data Transfer Speed

In general, wireless networks are slower than wired networks. It can be difficult to guarantee uniform and dependable signal coverage over a big campus like NOMAD Academy. Dropped connections or inconsistent network performance may occur in dead zones or weak signal locations.

Security Can Be a Concern

Compared to wired networks, wireless networks are typically a little less secure. The communication signals that are broadcast across the air and are simpler for evil actors to intercept are the main cause of this. Since educational resources and student and faculty data are kept and communicated through the network at NOMAD Academy, this can be especially problematic. To reduce these dangers, it becomes essential to implement strong security protocols such strong encryption, authentication techniques.

Connectivity May Suffer Occasionally

It is more likely that nearby wireless-enabled gadgets will cause interference or impediments. Both the performance and the quality of your connection may be affected by this. The available bandwidth may become a barrier in NOMAD Academy, because several users access the network at once for tasks like online learning, video streaming, and file sharing. As a result, internet speeds might be slower, productivity might decline, and there might be disruptions to any online classes.

1.4PHYSICAL MODEL: In the OSI reference model, the physical layer is the lowest layer. It has control over the actual physical connection between the devices. The physical layer contains information in the form of bits. It is responsible for transmitting certain bits from one node to the next.

THE DATALINK LAYER: Through the data connection layer, the message is transmitted from one node to another. The main duty of this layer is to ensure error-free data transmission over the physical layer from one node to another. When a DLL joins a network, it is required to send a packet to the host using its MAC address.

NETWORK LAYER: Data transport between hosts that are a part of different networks is made easier by the network layer. Additionally, it manages packet routing, which is the selection of the quickest path from among several possibilities for transmitting the packet. The IP addresses of the sender and receiver are inserted into the header by the network layer.

TRANSPORT LAYER: From the network layer to the application layer, services are transferred via the transport layer. The data in the transport layer is referred to as segments. It is responsible for making sure that the complete message is conveyed. The transport layer also provides confirmation of successful data transmission and retransmits the data in the event that an error is found.

SESSION LAYER: This layer is in charge of connection establishment, session maintenance, authentication, and security in addition to assuring security.

PRESENTATION LAYER: The Presentation layer is also known as the Translation layer. In this step, the application layer's data is obtained and formatted for network transmission.

APPLICATON LAYER: The topmost layer in the OSI Reference Model's stack of levels is the Application layer, which is implemented by network applications. These programs must use the network to communicate the data they produce. Additionally, this layer serves as a gateway for application services to connect to the network and display to the user the data they have received.

PART-2

2.Authentication and two factor authentication

When you attempt to access sensitive network locations, businesses could additionally request multi-factor authentication. By requiring at least one additional step, such as entering a temporary code given to your smartphone, to log in, this offers an extra degree of security.

Early in the new millennium, programmers created stronger authentication mechanisms with multiple layers of security.

Before getting access, users had to submit two forms of verification using multi-factor authentication. Additionally, single sign-on (SSO) simplified the authentication procedure by requiring users to provide their credentials at only one access point, which was independently verified.

Install security software updates and back up your files

Maintaining the most recent versions of your operating system, web browsers, and security software is essential for adhering to IT security best practices. Protections against malware and viruses are continuously updated to target and counteract fresh cyberthreats.

Install any security updates as soon as the organization gives out instructions for their installation. The use of personal gadgets at work is likewise covered by this. Quickly installing updates enables defense against the most recent cyberthreats.

Your data is frequently the target of cyberthreats. To prevent a data breach or malware attack, it is standard practice to safeguard and back up files.

Embrace education and training

All staff members at NOMAD Academy should participate in regular, in-depth security awareness training sessions. Some technical knowledge is also beneficial. It's beneficial to understand the procedure for granting IT access to your devices as well as some fundamental phrases related to computer hardware. When you contact support and they require quick access to information to fix a problem, having that knowledge can help you save time.

Consult your IT department for a list of approved cloud providers if you wish to backup data to the cloud. This might be a part of an organization's AEU policy. A violation of the policy could result in termination.

2.2.Physical network security

This safeguard stops unauthorized people from physically accessing equipment like routers or storage areas for cables. Locks, biometric authentication, and a variety of additional tools are used to accomplish this. Intruders are kept out of the protected area using deterrence physical security methods. Tall perimeter walls, barbed wire, obvious evidence that the location has active security, commercial video cameras, and access controls are typical defenses. All of them are intended to send the message loud and clear to thieves that trespassing is not only challenging but also extremely likely to result in their capture.

Technical network security

In firms that use computers or almost any form of technology, technical security is a particularly popular type of security. It deals with developing sufficient ways to handle the danger of technical failure or hacking and identifying security system flaws. With the migration of data to cloud drives and portable devices, it is challenging to guarantee a safe session and transfer of information because the majority of data lives in a non-physical form. Untrusted networks and devices, as well as interactions with unauthorized systems, lack security protections. These are some of the primary factors contributing to a growing demand for technological security on networks and between devices.

Administrative security network

Network security administrators oversee, evaluate, and manage security across computer networks, playing a vital role in the security of businesses. They set up firewalls and anti-virus software to protect data and maintain IT systems. In order to prevent unauthorized users from gaining access to company networks, they frequently design and execute efficient network security policies and guidelines across the networks. They assess the network for operational issues, troubleshoot the problems, and report them. They have advanced knowledge of mitigation techniques and defensive tactics, making them masters at spotting network operations, security concerns, and security lapses in an organization's network.

There are numerous different encryption techniques, each created with specific security requirements in mind. Asymmetric encryption and symmetric encryption are the two primary methods of data encryption.

Data is encrypted and decrypted using two unique cryptographic asymmetric keys utilizing asymmetric encryption, sometimes referred to as public-key cryptography. A "public key" and a "private key" are the names of these two keys.

Typical asymmetric encryption techniques

RSA: For secure data transfer, RSA is a well-known method that encrypts data with a public key and decrypts it with a private key.

PKI: Public key infrastructure PKI uses digital certificates to provide and maintain encryption keys as a means of key management.

Symmetric encryption methods:

Symmetric encryption is a type of encryption where only one secret symmetric key is used to encrypt the plaintext and decrypt the ciphertext.

Common symmetric encryption methods:

* Data Encryption Standards (DES): DES is a low-level encryption block cipher algorithm that converts plain text in blocks of 64 bits and converts them to ciphertext using keys of 48 bits.
* Triple DES: Triple DES runs DES encryption three different times by encrypting, decrypting, and then encrypting data again.

Data backups

The main goal is to restore lost data from an unforeseen event, such as an accidental deletion or file corruption, which is frequently brought on by a virus. An illustration of this is ransomware, which encrypts all of your data when it infects your computer and allows you to roll back the data at any time you choose. This scenario frequently occurs in businesses that have databases and applications and want to test those programs using a particular set of data. Ensure that critical data is periodically backed up to safe and dependable offsite or cloud storage locations by implementing a strong data backup strategy.

2.3.PROTECTION AGAINST CYBER SECUIRITY

The bulk of network attacks originate on the internet. In this industry, there are experts, and then there are ransomware attacks. If they are careless, they might interfere with several data networks. These exploits can't impact machines thanks to network security.

ACCESS LEVELS

The security software is accessible to different users at different levels. The authorization strategy is used after the authentication procedure to decide if the customer is allowed access to particular resources.

You may have noticed that, for security purposes, some collaborative papers are password-restricted. Who has access to which resources is understood by the software with clarity.

To ensure that only authorized users can remotely access critical resources, network security devices can implement access controls such as virtual private networks (VPNs) or authentication techniques.

DOS PROTECTION

Technology from Akamai for DoS and DDoS protection increases resilience and offers a comprehensive defense against the biggest and most difficult attacks. By fine-tuning mitigation for your online and internet-facing services wherever they are hosted, our purpose-built solutions minimize single points of failure and decrease risk across IT systems.

Protection from DoS and DDoS for websites, applications, and APIs

The comprehensive protections offered by Akamai App & API Protector are meant to safeguard entire web and API estates. App & API Protector is a user-friendly solution that integrates market-leading technologies in web application firewall, API security, bot mitigation, and DDoS and DoS protection. It was created with a customer-focused automation and simplicity.

KEEP YOUR DATA SAFE

As was already mentioned, network security stops unauthorized access. A network holds a lot of sensitive data, including private client information. Anybody who gains access to the network could endanger this private information. Network security needs to be able to safeguard them as a result.

CENTRALLY MANAGED

Network anti-malware is controlled by a single person known as the network administrator, unlike PC encryption software. The latter can thwart hackers before they can do any damage, but the former is susceptible to malware and virus attacks. This is because the program was set up on a computer without an internet connection.

When network security devices are combined with a centralized security event management system, security events can be thoroughly tracked, correlated, and analyzed.

PART 3

3.CONFIDENTIALITY

This idea emphasizes the need to guard against unwanted access to private or delicate data. Financial data, business plans, personally identifiable data (PID), such as a Social Security Number (SSN) or date of birth, password-protected records, email records, payment data (including credit/debit cards), and protected health information may all fall under this category, but they are not the only ones..

NOMAD Academy uses appropriate backup and recovery procedures and routinely backs up important data. NOMAD Academy uses appropriate backup and recovery procedures and routinely backs up important data.

INTEGRITY

This component of the CIA trinity ensures the information is reliable, true, and accurate. In other words, it ensures that the information is reliable and unaltered. Whether the data is kept on a laptop, on a storage device, a data center, or in the cloud, it needs to be protected while it's being used, traveling, and being stored.

Data integrity can be preserved by using encryption, hashing, digital signatures, digital certificates, intrusion detection systems, audits, version control, authentication, and access controls..

The academy uses encryption to protect private information while it is in transit and at rest. For instance, to prevent unauthorized access in the event of a breach in physical security, NOMAD Academy may encrypt data kept in databases or on portable storage devices.

AVAILABILITY

Following this strategy ensures that systems, applications, and data are always accessible to and accessed by authorized users. Networks, systems, and applications need to be continually available to ensure that critical business processes go on as usual.Your data systems' accessibility may be impacted by human error, hardware, software, network, power, natural disasters, and cyberattacks. NOMAD Academy develops comprehensive disaster recovery plans to overcome unforeseen disruptions and ensure the availability of critical systems and data..

3.2 PHISHING ATTACK

Phishing attacks are false emails, texts, calls, or websites that are intended to trick users into downloading malware, disclosing sensitive information (such as Social Security and credit card numbers, bank account numbers, login credentials), or taking other actions that expose them or their organizations to cybercrime.

Identity theft, credit card fraud, ransomware attacks, data breaches, and other serious financial losses for people and businesses are frequently caused by successful phishing attempts.

The most prevalent form of social engineering, or the technique of misleading, bullying, or coercing people into giving information or assets to the incorrect persons, is phishing. Attacks using social engineering rely on pressure and human mistake to succeed.

RANSONWARE ATTACK

Ransomware is a type of malware designed to bar a user or company from accessing files on a computer. By encrypting these files and demanding a ransom payment for the decryption key, cyberattackers put organizations in a scenario where paying the ransom is the quickest and least expensive alternative to regain access to their files. Several variations of ransomware have added extra features, like data stealing, to improve the incentive for victims to pay the ransom.

Ransomware is currently the most obvious and prominent type of malware. Recent ransomware attacks have severely harmed a number of businesses, shut down local services, and impacted hospitals' ability to provide vital services.

SOCIAL ENGINEERING

A broad variety of malicious actions carried out through interactions with other people are referred to as "social engineering" in this context. Users are psychologically manipulated into disclosing important information or making security mistakes. Social engineering attacks can take one or more steps. A perpetrator first researches the target to obtain background information such as likely points of entry and lax security measures in order to get ready for an assault. The attacker next tries to gain the victim's trust by promising rewards in exchange for later security-breaking actions like releasing private information or granting access to essential resources.

PASSWORD ATTACK

The majority of people prefer to use passwords as their access verification mechanism, so it might be appealing to a hacker to figure out a target's password. There are numerous ways to do this. People frequently save copies of their passwords on pieces of paper or sticky notes that they leave about the house or on their desks. In order to get the password, an attacker has two options: either they can do it themselves or they can hire an insider.

An attacker may also try to intercept network transmissions in order to gain credentials that the network has not encrypted. They can also employ social engineering, which involves convincing the target to enter their password to fix a purportedly "important" problem. Sometimes the assailant can simply guess the

3.3. Strong WEP/WAP Encryption on Access Points

Strong encryption methods on wireless access points prevent unwanted users from connecting to your network even when they're close. If the encryption method is unreliable, an attacker could be able to brute force his way into a network and launch man-in-the-middle attacks. The used encryption is more powerful the safer it is. According to NOMAD Academy, sensitive data, such as login passwords or personal information, should only be exchanged across encrypted networks. This can be done by using protocols like SSL/TLS for website communication.

Public Key Pair Based Authentication

Attacks using the man-in-the-middle usually involve spoofing. At various points along the stack, RSA-based public key pair authentication can be used to confirm that the parties you are talking with are the parties you intend them to be.

Force HTTPS

HTTPS can be used to securely communicate over HTTP by utilizing public-private key exchange. By doing this, any data that an attacker might be sniffing is stopped from being used. Websites should only use HTTPS and not provide HTTP alternatives. Browser plugins can be added by users to force HTTPS for all queries.

Virtual Private Network

VPNs can be used to create a secure environment for sensitive data within a local area network. They use key-based encryption to provide a secure subnet for communication. In this way, a hacker won't be able to decrypt the communication in the VPN even if he has access to a shared network.

3.4. SPAM FILLERS

find unauthorized email and stop it from reaching a user's mailbox. Spam filters evaluate emails according to rules or patterns created by a company or a vendor. More advanced filters employ a heuristic method that looks for spam by suspicious word patterns or word frequency.

Within NOMAD Academy staff and students can save time and effort by effectively screening out spam emails instead of manually going through and removing irrelevant emails. By enabling users to prioritize critical emails and concentrate on their primary duties and obligations, this increases productivity.

WEB FILTERS

solutions that stop users' browsers from loading specific pages from specific websites. Different web filters are available for household, business, institutional, and private use.

Allowed listing: The purpose of allow lists is to specify the websites that a user, machine, or program is allowed to access.

Block list: The complete opposite of allow lists are block lists. Instead of listing the websites that a user may access, they list the websites that they advise against visiting. All traffic is examined when using a blocklist, and any traffic going to a destination on the list is discarded.

Content filtering: The complete opposite of allow lists are block lists. Instead of listing the websites that a user may access, they list the websites that they advise against visiting. All traffic is examined when using a blocklist, and any traffic going to a destination on the list is discarded. This helps maintain a safe and secure browsing experience for staff and students.

AUTHENTICATION

The act of verifying a user's identification is called authentication. It is ensured that only users with legitimate credentials can access secure systems thanks to this. To authenticate themselves when seeking to access data on a network, a user must submit secret credentials.

Single sign-on and multi-factor authentication

Early in the new millennium, programmers created stronger authentication mechanisms with multiple layers of security.

Before getting access, users had to submit two forms of verification using multi-factor authentication. Additionally, single sign-on (SSO) simplified the authentication procedure by requiring users to provide their credentials at only one access point, which was independently verified. NOMAD academy can use this methord to limit the unneccary permitions

DATA ENCRYPTION

Data encryption is one of the many methods that corporations may protect their data. Plaintext (readable data) is converted through encryption into ciphertext (random data), which can only be deciphered with a unique cryptographic key. In other words, data is scrambled using encryption as a security measure so that only authorized employees may decipher it. Encryption should be used by NOMAD Academy for both stationary and moving data.

NETWORK ACCESS CONTROL(NAC)

involves restricting access to network resources to endpoint devices that comply with your security policy. Some NAC solutions have the ability to automatically secure non-compliant nodes before granting access. NAC is most useful when the user environment is essentially static and can be strictly controlled. In situations with a wide range of users and rapidly changing technologies, such those found in the education and healthcare sectors, it may be less beneficial. In order to authenticate devices before granting them access to the network, NOMAD Academy can employ NAC. This ensures that the network will only allow authorized devices to connect.

3.5.RISK MANAGEMENT

The ability to detect threats to information and subsequently safeguard it without compromising access or productivity makes risk management an essential part of infosec. A corporation can install measures to limit this risk after determining the level of risk it is willing to take with the aid of risk management. NOMAD Academy must regularly examine the risks to its information assets, such as student data, intellectual property, and administrative systems, to find any potential vulnerabilities and threats.

DATA CLASSIFICATION

In case information is ever compromised or stolen, data categorization classifies data according to category, sensitivity, and impact. To enhance access control and establish how long it should be kept on file, data can be categorised.

Organizations may assess the value of their data, determine whether it is at danger, and put the right information security policies and security measures in place to reduce that risk by using data categorization. Additionally, classification makes it easier to comply with pertinent industry or regulatory regulations like GDPR, HIPAA, or PCI-DSS.

CHANGE MANAGEMENT

Another essential infosec element is the use of a formal change management approach. Inadequate management of data and system changes can result in outages that limit availability, restrict authorized users' access to the data they require, or compromise data security.

ASSET MANAGEMENT

Asset management was formerly straightforward, but with today's complicated IT environment, it has grown increasingly challenging. There is an increasing need to purchase new management and security solutions as the number and variety of devices we use expands. The operation of NOMAD Academy depends on effective information asset management. This entails identifying and categorizing information assets, determining ownership and responsibility, and putting in place suitable security measures.

BUSINESS CONTINUITY(BC) AND DISASTER RECOVERY(DR)

Disaster recovery and business continuity are also crucial infosec security concepts. Business-critical operations can be maintained during and after an interruption (such a cyberattack or natural disaster) with the help of effective business continuity planning.

A disaster recovery strategy ensures that the business can quickly regain access to its vital information systems and IT infrastructure in the event of a calamity. It guarantees that data is available, unaltered, and lowers the likelihood of data loss. In infosec, redundant systems and data backups are both common BC/DR techniques.

REFERENCES

<https://www.digitalcitizen.life/amd-vs-intel/>

<https://www.strongdm.com/authentication>

<https://reciprocity.com/blog/what-are-the-principles-of-information-security/>

<https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>

<https://www.imperva.com/learn/application-security/social-engineering-attack/>