A7011N - Internet Security

Group Assignment

Viktor Lindskog, Nico Ferrari, Anna Lind

Christer Åhlund,
Saguna Saguna,
Raihan Ul Islam

6 January 2021

1. Threats in the case

Denial of Service attacks

As the network at Video Maze lacks any protection except for the border router there is a high potential of DoS/DDoS attacks from the internet. A denial of service attack is an example of an active attack where a function or service in the network is overloaded with normal requests which cannot be responded to in time and where the function or service eventually chokes and prevents normal user access on a web server for example. “Ping of death” and SYN flooding attacks are examples of DoS or DDoS (Distributed DoS) attacks.

A denial of service attack which hinders customers to reserve and pay for Videos/DVDs would prevent business, risk losing customers and potentially also damage the reputation of Video Maze.

Malware or Ransomware attacks

Both Windows clients and Windows servers are vulnerable to virus or malware attacks and require security controls to be implemented. The case describes antivirus software to be inactive and no information was given on the server protection regarding anti malware and local firewalls. Border protection and network segregation with Firewalls with anti malware and packet and application filtering features would be recommended. Malware as viruses could stop servers and customer PCs from functioning properly and other malware as spyware could cause leakage of sensitive business information. A ransomware attack could potentially lock all Video Maze server and PCs and prevent any business at all as no Video/DVDs or any cafe items would be sold. Loss of customers and business is an obvious consequence.

Unauthorized remote access into to the system

There are no proper security controls as VPN functions in place to control remote access. Chris must be able to login remotely into the system for administrative reasons but there are no real security controls in place for securing this remote login feature. The connection is unencrypted and also lacking basic logon features as authorization, authentication and jump stations which makes it vulnerable to unauthorized remote access directly into the network and business system. The business system inside also has many vulnerabilities and in combination with remote login this exposes several critical vulnerabilities. Microsoft Access 2007 is vulnerable in many ways, it has multiple vulnerabilities with the possibility to be exploited from remote. The same goes for Windows 2003 which is an outdated and unsupported operating system which has many critical vulnerabilities. The vulnerabilities in both OS and DB affect confidentiality, integrity and availability.

Manipulation or misuse of company PCs and Servers

Customers and Clerks have high privilege accounts on physical PCs (Windows version on PCs not mentioned in the case but is assumed to be as outdated as Windows 2003 server OS.)
The user account that the personnel uses and also the account that is being used by the customers has high privileges. They all can read, write and modify files on the PC. They all could gather all the necessary tools they need to exploit the whole system without any difficulties.
Company server (Windows 2003) also have employee accounts with full read/write access which can exploit vulnerabilities in case of erroneous activities or malicious intent. This with the combination of deleted logs will cause no traceability of the user activities.
The complaint from customers on the low performance on Video Maze's system may indicate that the network and servers are used for incorrect purposes.

Network and system intrusion - Data exposure, loss or manipulation

Video Maze currently has a flat network with no separation mechanisms between the vital functions, users and customer networks which makes them vulnerable to intrusion from both external and internal perpetrators or erroneous user or administrator actions.
The transaction system and the computer bank are on the same network without any security mechanisms. Data is also processed on the same server, a server that has many vulnerabilities due to the outdated operating system and insufficient administration.
The customers and employees of Video Maze don't have any personal user account on the PCs. They all share the same account which also has a very weak password which is easy to crack.
A network and system intrusion can have different objectives. Stealing customer information as in the article Richard read in the case is one example. This could obviously lead to huge economic consequences and severe damage to Video Maze reputation. There can also be other aims like sabotage or spying on a competitor where consequences can be just as bad.

Unauthorized Database access and database manipulation

As the database is rather unprotected (users working directly against the database and no firewalls or network segregation etc.) there are several threats to be concerned about. Remote or internal access and inputting search strings directly into the database without any filtering could be used maliciously and the database is a high risk. This vulnerability with the combination of the connection of the transaction systems connected into the main server makes this risk critical to mitigate. Microsoft Access has several known vulnerabilities (listed in CVE database[1]).
The database at Video Maze also has a poor data structure where the keys in the database are making searches hard and also increasing the risk of human error. Having printouts as described in the case, to make the searches easier, can also be misused and disclosed to the wrong eyes.

[1] Common vulnerabilities and Exposures, https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-328/Microsoft-Access.html

This could really affect the business in a negative way. The customers could be a victim of misuse of their account and by that terminate their membership at Video Maze.

Phishing and social engineering

The staff, including Chris, has low security awareness which can be exploited for phishing and social engineering. The IT specialist Chris has high confidence and low security awareness, this is a recipe of a bad combination. Even if the system had been in the state of the art in security, the IT system would decay drastically with Chris’s low awareness of security. This with the combination of Richard Maze's high trust and gratitude (that are shown in Chris’s high salary) makes the competence of Chris acceptable at Video Maze but is rather another sign of the low security awareness on the management level.

Also the rest of the staff and management need to be trained in IT security to at least a basic level. Everyone should be aware of the company IT security policies (equipment usage, account and password handling, GDPR basics etc) and where to turn if anything suspicious is noted.

2. OSI model security

It is fundamental to understand that all layers of the OSI model can be exploited if the vulnerabilities are left without security controls. Below some examples and suggestions on improvements for each layer.

Layer 7 - Application Layer

Threat: Vulnerabilities in applications can be exploited for DDoS attacks also on the application layer. SQL injections on the database is also a common threat, which is most likely also the case at Video Maze. This is because the users are searching directly on the database and most likely the input doesn't have any cleansing on the characters[2].
Affects: Confidentiality, Integrity, and Availability
Improvements/Countermeasures: Separate the search function from the actual database and implement a cleansing function for the input of the database. Implement Application filtering/control (normally part of modern NGFW, New Generation Firewalls, from most firewall vendors)
in the firewall to detect and prevent (IDS/IPS) any hacking attempt related to the applications run in the environment

Layer 6 - Presentation Layer

Threat: This layer defines how the data is formatted, presented, encoded, encrypted and converts the data to be used in the application level. A malformed SSL request[3] is possible to send to create a DDoS-attack.
Affects: Availability
Improvements/Countermeasures: Offload the SSL encryption as much as possible and then implement Application filtering/control in the firewall or with another ADP[4] (application delivery platform) with policies and make sure that any violation against these policies are detected and acted upon.

Layer 5 - Session Layer

Threat: Attacks on sessions, also known as session hijacking is possible to conduct to layer 5. A session hijacking could be an interception of the communication between a host and a server. It is conducted by stealing or predicting a valid session key/token. This is also called a Man-In-The-Middle attack[5] and it can be used both for listening to or delaying traffic or manipulating the messages transported.

[2] Cisco, https://tools.cisco.com/security/center/resources/sql_injection
[3] DDoS quick guide, 2020, US-CERT.cisa.gov
[4] DDoS quick guide, 2020, US-CERT.cisa.gov
[5] Stallings 2017, Network Security Essentials, page 107

Affects: Confidentiality, Integrity and Availability.
Improvements/Countermeasures: Set the least privilege for users, implement secure protocols and implement encrypted communications.

Layer 4 - Transport Layer

Threat: It is possible to eavesdrop the communication within the LAN of the IT system if TLS (Transport Layer Security) encryption is not implemented. TLS encryption in an end-to-end encryption that makes it possible to share sensitive data over the network[6]. The attack can be performed by the PC in the store with network analyzing software, from a new connected PC that belongs to the attacker or from remote by using a combination of flaws in the IT-System. Another example is TCP SYN flood attacks (Denial of service attack on the transport layer) which aims to block the network service.
Affect: Confidentiality, Availability
Improvements/Countermeasures: Set the least privilege for the users and implement TLS for the communication. Implement firewall(s) with proper configuration to filter traffic only on allowed protocols to limit the attack surfaces (also see question 3 on Firewall design).

Layer 3 - Network Layer

Threat: It is also possible to conduct attacks outside of the LAN. Attacks that can be conducted to affect the Network Layer are for example Denial of service attacks (as also mentioned above in the transport layer) like ICMP-attacks (e.g. “ping of death”)
Affects: Availability
Improvements/Countermeasures: Routers must be hardened, routing information needs to be controlled and controls of the packet filtering with a firewall should be implemented to minimize the allowed traffic and mitigate these threats. For a business like Video Maze is also possible to subscribe to services from security providers to protect from DoS/DDoS attacks from the internet (e.g. F5 Silverline DDoS protection[7])

Layer 2 - Data Link Layer

Threat: Inside this LAN it is possible to perform ARP-spoofing and MAC-flooding attacks[8]. Due to the high privilege that the users have it is possible to acquire the needed tools to create these attacks. It would also be possible to connect a device for network sniffing for example if the network ports are unprotected.
Affects: Confidentiality and Availability
Improvements/Countermeasures: Set the least privilege for the users and harden the network protocols and ports so the responses to broadcasting and DHCP requests reduces. Implement

[6] Stallings 2017, Network Security Essentials, page 190
[7] Silverline DDoS protection, www.f5.com
[8] Cybersecurity News, https://cybersecuritynews.co.uk/network-vulnerabilities-and-the-osi-model/

NAC with 802.1X (link layer protocol) on network ports to force any device to authenticate and disable any unused ports (further described in question 5 in this document). Implementation of an IDS (intrusion detection system) would make it more likely to detect if there are any ARP-spoofing or MAC-flooding attacks.

Layer 1 - Physical Layer

Threat: Within the physical store there are physical PCs available for the customers to use and transaction PCs for the clerks. All of the PCs are connected with physical ethernet cables. It is possible to cut these cables[9] to the PCs and maybe even the cables between the servers and switches.

Affects: Availability

Improvements/Countermeasures: Network and server equipment should preferably be protected in locked spaces. Implement Wi-Fi as an alternative access method. For customers with their own devices a guest network would be suitable. Physical cables can be made easier to inspect to detect any sabotage quickly. Camera surveillance could also be implemented as an improvement.

[9] Cybersecurity News, https://cybersecuritynews.co.uk/network-vulnerabilities-and-the-osi-model/

3. Firewall design

The current network design lacks firewalls and any kind of network segregation. A large security risk is that Customer PCs are on the same network (subnet) as the business systems and databases as well as the employee PCs. Remote access (by Chris) is allowed in without any specific security controls.

An assumption is that because of the type of business, IT implementation and size of the company, Video Maze need to keep IT costs down, which makes the firewall solution needing to be at low cost and at the same time easy to manage. Some layering of the network is needed though.

New Generation firewalls (NGFW) can offer security controls as traffic filtering, IDS/IPS (Intrusion Detection System and Intrusion Prevention System) and malware and application filtering.

Suggested design principles

- Add DMZ for customer access from internet to protect internal systems from internet exposure
- Add Web proxy for Web server in DMZ
- Separate Customer PCs from Business systems (on external network)
- Traffic filtering in firewall on application and packets
- Remote access VPN in DMZ FW for admin purposes (and potential home access for employees)
- IDS/IPS in all existing firewalls in the solution (external as well as internal)
- Connection to/from new sites on fixed WAN connection or VPN over internet
- Protect FW logs by log shipping to a log server (the analyzing of logs is discussed further down in this document)

Suggested FW architecture

A minimum perimeter protection is a Firewall between Video Maze and the Internet but a strong recommendation is to add firewalls inside as well (see picture below). Packet filtering with a default to discard anything that is not explicitly allowed. This because Video Maze's business is quite simple and only requires allowing a very limited number of protocols like HTTPS and SMTP.

The way the customer PCs are currently used (internet access and risk of manipulation) they should be regarded as external and put behind an internal firewall and separated from business systems.

Protection from the internet is needed, therefore it is suggested to only allow HTTPS and SMTP incoming and HTTP/HTTPS and SMTP outgoing.

Application proxy[10] firewall to provide filtering for mail and web application traffic.

Implement IDS and IPS regarding Network behavior (abnormal patterns). Shop/office opening hours (VPN access excluded), DoS/DDoS detection, port scanning detection etc.

Future potential WiFi implementation should follow the same design principles and access policies.

Access policy

Incoming:

- Any to web server (HTTPS)
- ISP email relay to mail server (SMTP) (plus spam filtering)

Outgoing: Any to any HTTPS/HTTP

Inbound traffic: IPsec with TLS (certificates)

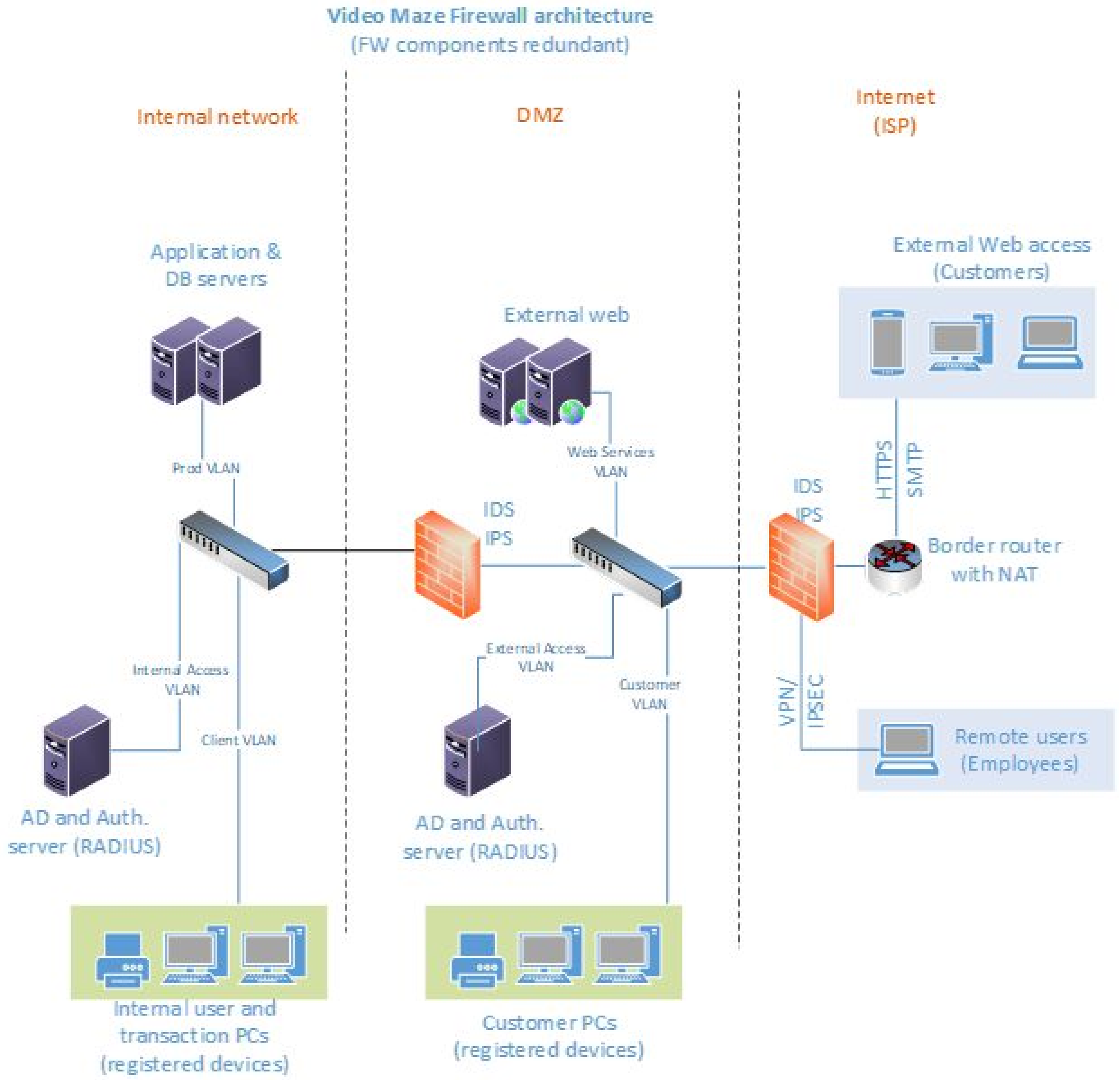
Example of firewall rules towards the internet according to above policy (table layout[11]). Traffic for VPN and RADIUS also need to be allowed but depend on the communication and device specifications.

Rule	Direction	Source addr.	Destination addr	Protocol	Dest port	Action
1	In	Any	Web server	TCP	443 (HTTPS)	Permit
2	Out	Any	Any	TCP	443 (HTTPS)	Permit
3	Out	Any	Any	TCP	80 (HTTP)	Permit
4	In	Any	Mail server	TCP	25 (SMTP)	Permit
5	Out	Mail server	Any	TCP	25 (SMTP)	Permit
6	Either	Any	Any	Any	Any	Deny

Internally the Firewalls will also be used to control other traffic like RADIUS, AD, monitoring etc.

[10] Stallings 2017, Network Security Essentials, page 415
[11] Stallings 2017, Network Security Essentials, page 416

Overview of suggested FW structure and network segregation



4. Security design principles[12]

In order to improve the security of their system, Richard must consider first of all a **Least Privilege** security design principle. As described by Stallings (2017, p. 34), this principle limits the privileges to the minimum for its context. This is meant to limit the number of people with access to critical system security controls, certain data, services, etc. Each role in the system will have only the permissions required in order to perform its functions. In the case scenario, this principle is missing and each entity has access to restricted information and there is no categorization of users into roles or functions.

The **Layering** principle, also known as **defense in depth,** uses multiple and overlapping security layers to protect the services and information from third unauthorized entities. The risk is managed using multiple overlapping defensive strategies in order to have another layer of protection in case of a breach in one of the layers.
For example, this company is removing the DVD from their cases, probably to avoid customers stealing them but this could be not enough to protect them from internal employees. Therefore, a new security layer such as security cameras can be adopted. Another example is if anyone manages to connect a device to listen to sensitive network traffic another layer of security is encryption which will prevent the interpretation of the data being transported.

A third security design principle which must be considered in case of an improvement of the system's security is **Isolation**, meaning that the critical resources must be logically or physically isolated from public access system, the resources of each user isolated from the data of another one (if not explicitly desired) and isolation of security mechanisms.

5. Authentication and authorization

Authentication and authorization is needed for connections inside the shop/office and for connections from outside. The picture in the Firewall design question above also illustrates the accesses and authentication mechanisms.

In the store it is vital to protect the internal network and network attached equipment. Therefore it is suggested that all active physical switch ports are protected with 802.1X which forces the devices that connect to the switchport to authenticate and authorize to get an IP address (via DHCP) and being placed in the appropriate VLAN. The switch, which acts as an authenticator to the supplicants (the devices that want to connect) should have its ports configured to send an authentication request to the Authentication server (RADIUS). All internal equipment can use EAP-TLS with an installed certificate. The same method can be used also for wireless access if Video Maze should want that. The 802.1X port based security will prevent unauthorized devices from connecting to the network.

[12] Stallings 2017, Network Security Essentials, page 32-36

To allow remote access to the infrastructure for admins being able to fix problems or manage the services, a VPN connection will be required. Especially in the last year, remote access has become a necessity for many companies in order to continue their business, but this must be protected against unauthorized access. Multi factor authentication will be adopted in order to perform user authentication in an efficient and secure way, relying not only on passwords, but also on something that the user has, such a mobile phone, which can be used as a soft token. Remote access may also be required for other staff in the future. The infrastructure will be built to enable that function in the future.

The infrastructure, in order to manage the users and devices, provide authentication and manage their authorizations needs an Active Directory (AD) server. In order to communicate with Active Directory, Remote Authentication Dial-In User Service (RADIUS) such as will be used. The User will start the login phase through the VPN client on his workstation, using as credentials its username and password. The RADIUS server will authenticate these credentials with the user registered in the Active Directory using the IKEv2 protocol [13]with EAP-MSCHAPv2 authentication, which allows users to authenticate with their account- or a device-specific username and password[14]. In case of successful authentication, the AD will send an *Success* packet to the RADIUS server. The server will now prompt the user asking a soft-token as second factor authenticator, sent as SMS or email to his phone. In case of successful authentication of the second factor, by the RADIUS server, an IPsec tunnel will be established. Role based access can be established where users (and equipment) of different kinds can be given access to different assets depending on the role (customer, employees of different kinds, admins etc.)
The AD can also be used for controlling the device status and enforce policies like server hardening (e.g antivirus install[15]), patches or password policies via GPOs (Group Policy Object) upon a device joining the domain.

It is also recommended that Video Maze customers have personal accounts to use the store PCs. This to enable activity tracking to prevent Video Maze equipment to be misused. This would require the customers to register and authenticate before using the PCs for surfing. An Identity and Access Management system should be in place where the above mentioned AD plays a vital role for managing the customer accounts. To further secure customer logins the above described Multi Factor authentication with one time passwords can be added.

All customer registration and management of personal information must be handled in compliance with GDPR where customers at any time can ask to see their information or request to be deleted from the registers (“right to be forgotten”). Routines and mechanisms to fulfill these requirements also need to be implemented.

Authentication and authorization in expansion sites

For future expansion a similar network layout as for the main site is suggested. Authentication and authorization of user equipment and users will be made on the main site. The sites will be interconnected with a VPN connection over the internet (can be made redundant and also exchanged for WAN

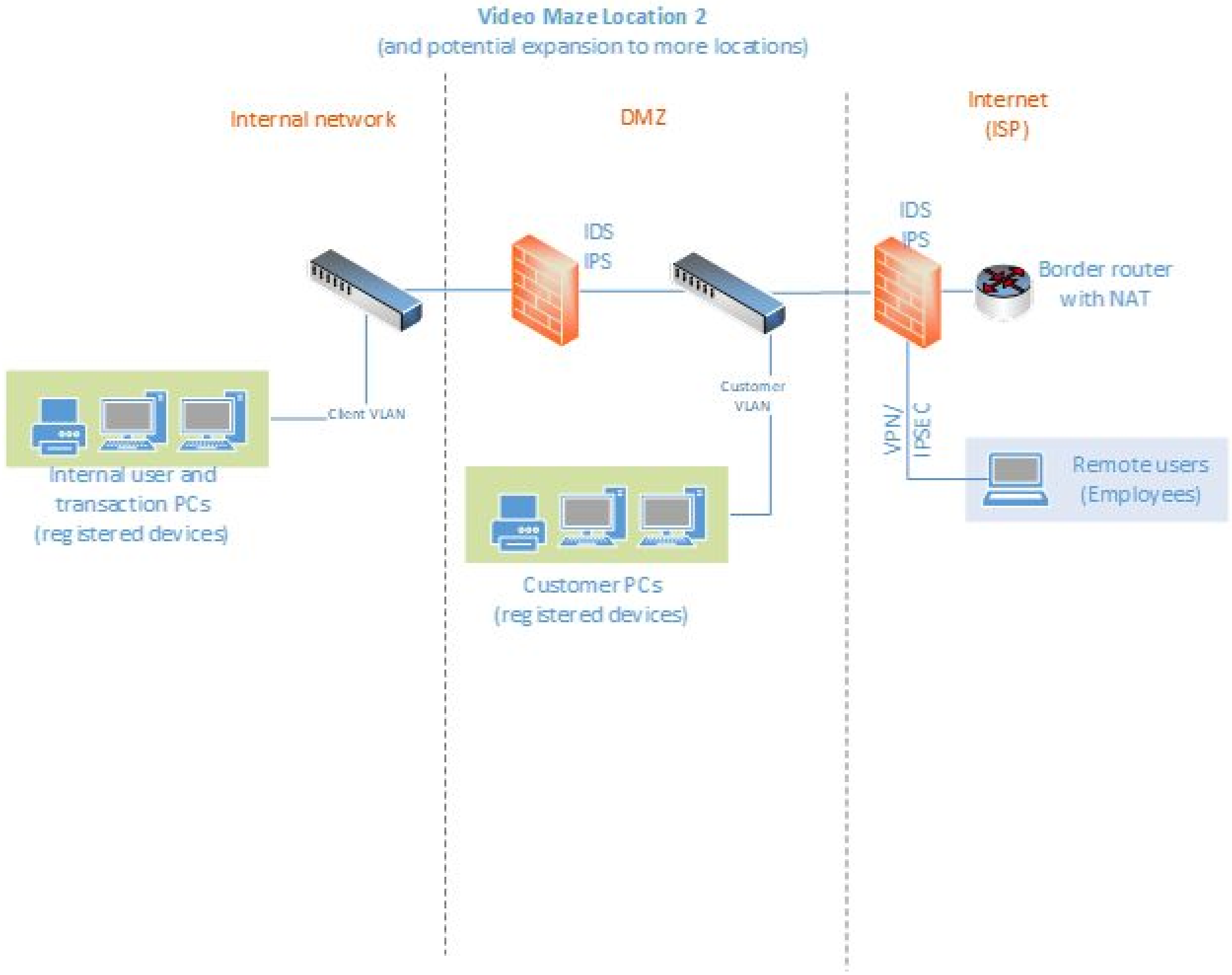
[13] Internet Key Exchange Protocol Version 2 (IKEv2), Internet Engineering Task Force (IETF)
[14] Guide to IPSec VPNs., NIST Special Publication 900-77
[15] Use group policy to install software, 2020, docs.microsoft.com

connections if required. The main applications and databases are also suggested to be kept in the main site and made accessible only after authentication and authorization.

In order to perform a secure communication between the two sites, a VPN with architecture *Gateway-to-Gateway* will be used. Every device connected to the network will need a certificate managed in the Certificate Authority server in the main site. In order to create a VPN between the two sites IPSec will be used with IKEv2 protocol using EAP-TLS authentication. EAP-TLS provides certificate-based authentication.

Suggested secondary site layout (and potential future expansions):

(Customer web access only to the main site)



Discussion

To conclude this assignment the answers and reasoning in the above questions are not aspiring to be solving all security needs of Video Maze. A number of weaknesses were mentioned in the text and, although not required for the assignment, some examples of important issues to be handled worth mentioning are:

Policies and guidelines

It is strongly suggested that Video Maze establishes clear policies and guidelines for IT security and use of company equipment. The policies and guidelines should be easy to understand and act as support for the staff and customers to act correctly. The customer policy and guidelines will of course differ from the staff policy and guidelines but they both aim to protect both assets and people from IT security risks. The policies should cover things such as network and equipment use, requirements to access the network, account and password management, and also what obligations you have (and possible consequences if non compliant), The guidelines should act as help for how to act to be compliant with the policies.

Saving log entries and analyzing logs

An important tool for tracking of activities is log handling. Logs at Video Maze are currently just deleted and not analyzed. Log entries from firewalls and servers should be protected from manipulation by shipping to a separate log server. The logs should also be analysed for detection of malicious behavior or intrusion attempts (and for traceability of suspicious user activities). This can be done in real time or for forensic purposes after a suspected intrusion or data/system manipulation. The cost of these kinds of tools (part of SIEM, Security and Information Event Management systems) can be quite high so a balance between the value of the business and the cost of security must be considered. Cloud services may be considered for this (Security as a service, SecaaS, is offered by several CSPs)

Backup of data and configurations

The existence of an online mirror server would not protect against logical errors or a ransomware attack where the mirrored system will be affected as well. The best and cheapest way to recover from one of these events is to restore the systems from a recent and fresh backup. The tolerance of lost data will help decide upon the backup frequency. Backing up configurations will also provide the means of a quick restore or re-creation of servers and network equipment. Backups should be kept separated from the original data in case of physical incidents as fire or flooding. Also backup can be consumed as cloud services.

Training

The clerks of Confectionery and Video/DVD should annually perform a basic security awareness training with adaptations to the business of Video Maze. This training will turn the regular clerks from a potential security threat (with their lack of security knowledge) to a security asset that will help to identify threats and vulnerabilities and maintain the defined way of working.

The rest of the personnel of Video Maze should annually perform an extended security training. The extended security training is acquired to gain the right security knowledge for this kind of business and to get the knowledge about the recent threats and how to mitigate them with the best practise of today's techniques. If necessary the IT specialist(s) can put through even deeper knowledge in IT security and training to get the best suitable security expertise. The IT specialist can also be one of the trainers to train the rest of the staff of Video Maze and to make sure that necessary level of security awareness is accomplished for Video Maze.

References

Common vulnerabilities and Exposures, Accessed January 3, 2021 from https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-328/Microsoft-Access.html

DDoS quick guide, 2020, Accessed January 4, 2021 from https://us-cert.cisa.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

William Stallings, Network Security Essentials, sixth edition, Great Britain 2017, Pearson

Silverline DDoS protection, Accessed January 2, 2021 from https://www.f5.com/products/security/silverline

Barker, Elaine, et al. , Guide to IPSec VPNs., NIST Special Publication 900-77, https://doi.org/10.6028/NIST.SP.800-77r1

Cisco, Accessed December 28, 2020 from https://tools.cisco.com/security/center/resources/sql_injection

Cybersecurity News, Accessed December 28, 2020 from https://cybersecuritynews.co.uk/network-vulnerabilities-and-the-osi-model/

New Horizons Learning Group, Accessed December 28, 2020 from https://training.nhlearninggroup.com/blog/7-layers-of-cybersecurity-threats-in-the-iso-osi-model

Use group policy to install software, Accessed January 5, 2020 from https://docs.microsoft.com/en-us/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software

Internet Key Exchange Protocol Version 2 (IKEv2)
https://tools.ietf.org/html/rfc5996