Bachelor's thesis

NTNU
Norwegian University of Science and Technology

Hubert Wozny

# Microsoft 365 customizable and resilient to ransomware

Bachelor's thesis in Digital infrastructure and cyber security
January 2022

NTNU
Norwegian University of
Science and Technology

Hubert Wozny

# Microsoft 365 customizable and resilient to ransomware

Bachelor's thesis in Digital infrastructure and cyber security
January 2022

Norwegian University of Science and Technology

NTNU
Norwegian University of
Science and Technology

# Abstract

Ransomware attack is a threat that closely follows global digitalization, as it threatens business's data, reputation, operational capabilities, and even clients. To prevent ransomware attacks from ruining businesses, security measures must be taken into consideration. Is it possible to prevent ransomware from disrupting companies and recover corrupted data?

In this thesis, I attempt to find if Microsoft 365 service gives users opportunity to protect themselves from ransomware attacks efficiently, and to what extend can it protect its users. I explore Microsoft's security features to create a custom environment and perform human-operated ransomware attacks to tests its efficiency.

The results address several features that were speculated to be most impactful in preventing ransomware attacks from ruining businesses, and compare the damage caused without them being present.

# Sammendrag

Løsepengevirusangrep er en trussel som følger etter globalt digitalisering, som den truer bedrifts data, omdømme, operasjonelle kapabiliteter, og til og med klienter. For å forhindre at løsepengevirus ødelegger virksomheten, må sikkerhetstiltak tas i betraktning. Er det mulig å forhindre at løsepengevirusangrep forstyrrer selskaper og gjenoppretter ødelagt data?

I denne oppgaven forsøker jeg å finne ut om Microsoft 365-tjenesten gir brukeren muligheten til å beskytte seg mot løsepengevirusangrep effektivt, og i hvilken grad klare den å beskytte sine brukere. Jeg utforsker Microsoft sikkerhetsfunksjoner for å lage et tilpasset miljø og utføre menneskestyrte løsepengevirusangrep for å teste effektiviteten.

Resultatene tar for seg flere funksjoner som ble spekulert til å være mest virkningsfulle for å forhindre løsepengevirusangrep fra å ødelegge virksomheter, og sammenligne skadene som er forårsaket uten at de er til stede.

# Contents

## Contents

# Figures

# Glossary

**Backup** A copy of data used primarily to recover from data loss..

**malware** It is a term used to describe malicious software, characterize by causing damage to computers, digital infrastructure, etc..

**ransomware** It's a type of malware that encrypts files, causing them to become unusable for the owner, in order to blackmail the victim to recover the file..

**virtual machine** Also known as VM, is a emulation of computer within software..

**day zero vulnerability** A vulnerability that that is either unknown or unpatched..

**outsource** means to obtain goods or services from an outside supplier

# Chapter 1
# Introduction

## 1.1 Background

For the last fifteen years, internet become more and more integrated into our lives, and businesses found opportunity to use it for their advantage. Many businesses are moving into cloud, as it makes them more productive by keeping employees more connected with each other, it further allows businesses to outsource building and maintaining infrastructure.

Covid-19 pandemic have pushed many businesses into remote work, many of those businesses needed to adapt to such work environment by investing enormous sums of money into technology and infrastructure, alternatively businesses would make use of cloud services to save initial costs and get back to business quickly.

Cloud platforms are currently competing for costumers, they are motivated to offer the best value possible for the smallest cost, this includes maintaining a secure platform, as suffering a blow to reputation could give competitors the upper hand.

One of the biggest security challenges that faces businesses today are ransomware attacks. Ransomware is highly destructive, it aims to hinder business's ability to provide services, as such they have debilitating impact on economic security and safety of a businesses, it may even cause loss of trust in the business by clients and partners all together.

## 1.2 Thesis Topic

This thesis topic is to analyse Microsoft 365 architecture/services with regards to their resistance to ransomware attacks, how easy it is to perform recovery process, and to what degree it is capable of recovering data after ransomware attack.

Focus will be on standard E5 license, since it gives access to many features such as but not limited to:

- Microsoft Defender for Cloud Apps
- Group policy support
- Microsoft 365 E5 Insider Risk Management
- Exchange archiving
- and many more.

### 1.2.1 Research Questions

**Research question 1**

To what degree does customisability of Microsoft 365 affects resilience to ransomware?

**Research question 2**

To what degree is Microsoft 365 service capable of protecting customers data?

## 1.3 Thesis outline

**Chapter 1: Introduction** The introduction chapter means to introduce you to the topic, scope of my report, and to provide the background for the project.

**Chapter 2: Theory** In this chapter, I will present all external source that provide the theoretical background needed to understand resources and services provided by Microsoft 365, as well as current ransomware threat landscape and how ransomware currently works. This chapter will also discuss some of the most relevant security best practises for the research questions.

**Chapter 3: Method** In this chapter, I will describe how experiments were performed, define test environment, and define a realistic scenario for each test. The focus of this chapter will be to define the criteria by which security configuration will prove effective, and not drasticly affect ease of use for users.

**Chapter 4: Results** In this chapter, I will present the results of my experiments.

**Chapter 5: Discussion** In this chapter, I will discuss the results from chapter 4 and answer the research questions.

**Chapter 6: Conclusion** In this chapter, I summarize the findings and define if Microsoft 365 was capable to keep up with the ever-growing threat of ransomware.

## 1.4 Scope and delimitation

The goal of this project is to assess Microsoft 365 resilience to ransomware, and how customizing the service will affect the results in question. This project is using two years old GitHub repository that shared ransomware samples to satisfy need for functional ransomware software. No modern ransomware is used during this project, that is because finding a free, modern, and functional ransomware is rather difficult.

The method used to plan the project was as follow: firstly, I decided to define the scenarios that will be used for this project, then I decided to define security features that I wish to implement into Microsoft 365 environment. When I had a general idea of what I needed to know, I began research of chosen technologies. Lastly, I created the infrastructure and tested it to generate results.

Microsoft 365 provides hundreds upon hundreds of possible features that can be customized or simply added to the test environment, due to the sheer number of features and time limitation, only few features that are deemed as having highest potential will be explored.

# Chapter 2
# Theory

## 2.0 Chapter outline

In this chapter I will present the information used as theoretical groundwork that is used in the resto of the report

## 2.1 Definitions and concepts

### 2.1.1 CIA-triad

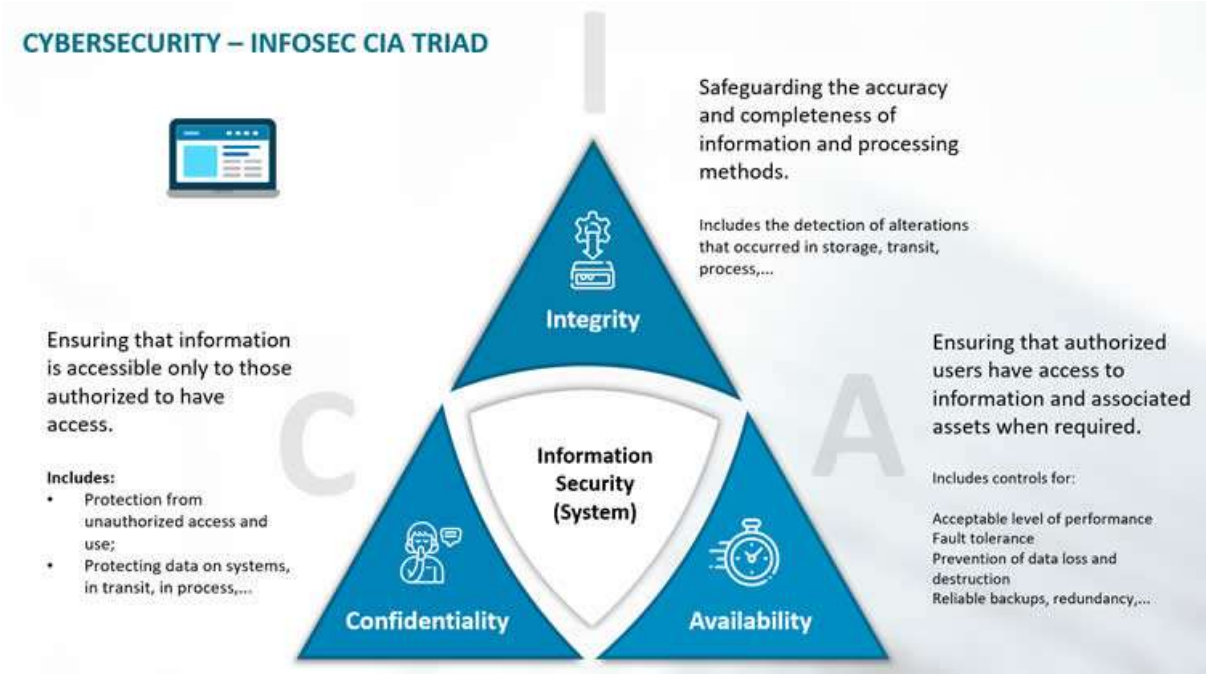



*Figure 1: Picture visually presenting and describing CIA triad*

The concept of CIA-triad is a fundamental security design. CIA stands for: Confidentiality, Integrity, and Availability. Depending on the situation and type of data business is operating with, some aspects of CIA may be more important than the others. [1]

- Confidentiality – This aspect involves data secrecy, by preventing access to data by unauthorized entity's within and outside of the company.
- Integrity – relates to data integrity, this means that data is not modified by anyone unauthorize, this makes data consistent.
- Availability – Refers to access to data by authorized personnel, it also refers to conditions under which data can be accessed by authorized personnel.

### 2.1.2 Ransomware

Ransomware is the main aspect of this project and has a dedicated chapter (2.2). Ransomware is a type of malware that renders data unusable by encrypting files, general goal of ransomware attack is to hold data ransom, and force owners to pay for decryption key that restores data to original form. Malicious actors almost always ask for payment using cryptocurrency's, bitcoin accounts for

approximately 98% of payments, making it hard to identify the actor, and making it almost impossible to recover ransom. [1]

### 2.1.3 Cryptography concepts

Cryptography is a practice of transforming information using encryption algorithm to make it unreadable, whereby only an owner of a decryption key can use decryption algorithm and transforming the data back into the original state. Cryptography in its purest form was meant to protect the data, eventually became corrupt and used to attack companies and individual as ransomware. [2]

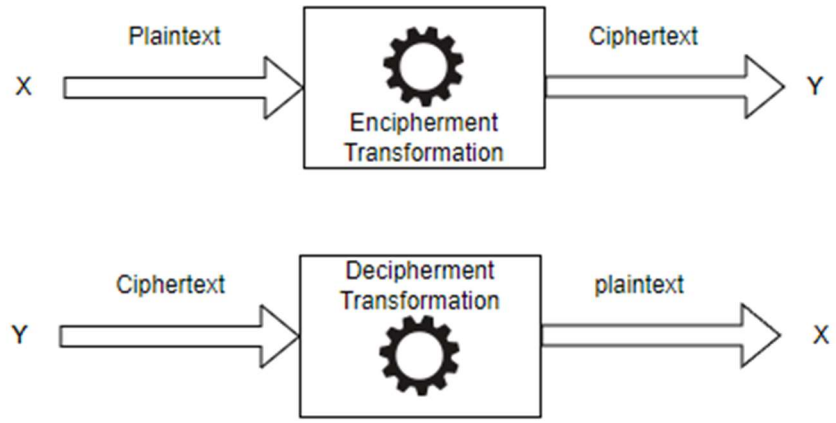



*Figure 2:This figure visualises process of cryptography*

### 2.1.4 Cloud storage

Cloud storage is storage solution for digital data, data is stored on servers hosted by third-party provider. Service-provider takes responsibility for hosting, managing, and securing data stored on servers. Service-provider has responsibility over maintaining servers and ensuring that data is always accessible via public or private internet.

Renting cloud storage is relatively inexpensive in comparison to building infrastructure, and maintaining servers at a comparable level, this paired with the fact that most service-providers allow for users to scale their data footprint depending on theirs need makes it rather popular. [3]

#### 2.1.4.1 OneDrive

OneDrive is a cloud storage solution provided by Microsoft and is a part of Microsoft 365 E5 license packet. OneDrive allows to interact with the data in cloud as if they were directly on your personal computer, it syncs all the changes with the cloud and presents itself like an additional local drive on

[1] 'Ransomware: Paying Cyber Extortion Demands in Cryptocurrency'.
[2] Konheim, *Computer Security and Cryptography*.
[3] 'What Is Cloud Storage & How Does It Work?'

windows machines. In comparison to Microsoft SharePoint, this solution focuses more on individual use rather than real-time cooperation. [4]

#### 2.1.4.2 SharePoint

SharePoint is a service integrated into Microsoft 365 that support collaboration and co-creation as a business, it allows to store, organize, share and access information from any device by many users simultaneously. SharePoint is integrated with many other Microsoft services, for eks. data stored on Microsoft Teams channels are stored in SharePoint. [5]

## 2.2 Ransomware

### 2.2.1 Definition

Ransomware is a type of malware that seeks to encrypt as much data as possible on an compromised system, afterwards it will demand that the victim pay ransom or permanently lose the data, typically the request for ransom is to be paid in cryptocurrency, to ensure anonymity of malicious actors. There are generally two types of ransomwares, first one is a crypto ransomware that encrypts data and requires ransom for a encryption key, the second is a lock ransomware, which will lock you away from your personal computer until you pay ransom. [6] Ransomware

### 2.2.2 Recovery alternatives?

There are multiple ways to recover from ransomware attack, one way is to gamble by paying the ransom and hoping that the malicious actor will fulfil his side of the deal. It is not recommended to pay for ransom as it incentivises malicious actors to perform more ransomware attacks, and provides resources needed to improve on future attacks. Many businesses may find it cheaper to pay ransom over rebuilding from scratch, but approximately 65% of ransom payers manage to recover the system successfully[8]. Recoverability of files after a ransomware attack does not seem to be a priority for malicious actors, since 46% of victims have reported that some or all data were corrupted during recover process, according to article by Cybereason [7]

One alternative is to try and break the encryption by brute-forcing random decryption keys, it can become a rather time consuming and resource demanding task, possibly costing more time and resources than recreating the data from scratch. Brute-force technic can be especially ineffective if ransomware creates different decryption key for each file.

### 2.2.3 Ransomware trends

Ransomware is a low-cost, high profit business that gained traction over the past years, what started as a random malware targeting anyone and everyone, became its own industry focusing on disrupting big businesses by maximise the damage, and in return maximising profits. One of the biggest enablers for ransomware attacks was introduction of crypto currencies, it allows for easy money laundering with use of services such as “Tornado cash” or “Mixer”.

The owner of compromised system are not the only ones affected by ransomware attacks, malicious actors can use stolen sensitive data to blackmail either clients or partners to generate more income. As an example, in October 2020 a cyber-attack on Vastaamo psychotherapy clinic took place, where

---

[4] ‘What Is OneDrive for Work or School? - Microsoft Support’.
[5] ‘What Is SharePoint? - Microsoft Support’.
[6] Meland, Bayoumy, and Sindre, ‘The Ransomware-as-a-Service Economy within the Darknet’.
[7] gmcdouga, ‘The New Ransomware Threat’.

extensive patient data were stolen and further used to blackmail businesses clients by mail individually. [8] As an ever-evolving threat, some ransomware happened to evolve into double and triple extortion schemes, and profits from such schemes should motivate all malicious actors to innovate and optimise the processes.

Despite RaaS industry constantly innovating, its growth is somewhat hindered by opportunists, and possibility of becoming prosecuted. Study done by ScienceDirect [9] elaborates that majority of tested RaaS related products were frauds. Firstly, most of analysed Raas offers on black-markets had falsified aliases and ratings, where a lot of feedback for products were artificially created at the same date with same or similar description, the exemption being negative feedback. Secondly, descriptive information about the product were usually copied from other RaaS offerings, showing lack of effort put into presenting the product. Lastly, most of renowned RaaS vendors did not earn they renown by selling RaaS products, but by selling products unrelated to RaaS. These show that a lot of opportunists on black-markets are selling fake or open-source ransomware for the premium, making it hard to participate in ransomware ecosystem. It is also rather difficult to become an affiliate in RaaS ecosystem, since there are no official channels to communicate with ransomware groups. The most likely way of being recruited is to present your skills on dark-web, afterwards hope an organised RaaS group is in need for that particular skill set and have noticed you.

According to Microsoft [7], 53.1% of ransomware attacks are targeted at Healthcare, Energy, Financial, and Media & Entertainment sectors. With the exception of Media & Entertainment, ransomware gangs target key infrastructures where unannounced failure to deliver services may have catastrophic consequences. Ransomware attacks on healthcare sector are especially sensitive, because they can affect live support systems, potentially killing numerous patients reeling on those systems.

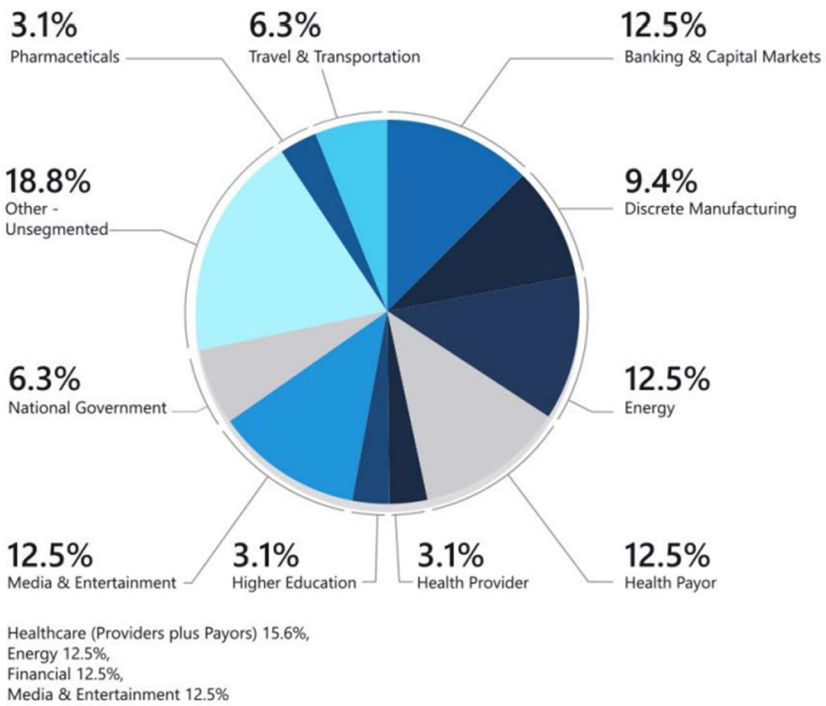



*Figure 3: Visual representation of ransomware targets by sectors*

[8] gmcdouga.
[9] Meland, Bayoumy, and Sindre, 'The Ransomware-as-a-Service Economy within the Darknet'.

### Automated ransomware

An automated ransomware such as for eks. WannaCrypt, would attempt to encrypt as many files on the system as possible, right after exploiting a vulnerability to gain access to the system [10], it would then instruct the victim on how to pay ransom, and on rare occasions, some more advanced ransomware would attempt to replicate itself and run on all devices connected to the network. Such ransomware could be distributed by email as spam, scam emails like fishing, or as disguised executable files downloadable on the internet. A rather effective countermeasure for automated ransomware was external backup, since ransomware would encrypt data accessible on system drives, ignoring data only accessible from applications, browser, or not accessible during the attack. Many companies and individuals would backup all most important documents in case of disaster, greatly reducing the threat of ransomware. This kind of attack would require very little, if any involvement of the malicious actors, making it the attack with lowest time investment required.

### Human-operated ransomware

Human-operated ransomware attack is a stark contrast to automated ransomware attack, it will mainly target highly profitable businesses that are able to pay highest ransom. Such attacks will prepare before deploying the ransomware by discreetly changing or deleting security features/systems such as backups, policies, access management, and snapshots. Attackers seek to prevent owners from recovering the encrypted data, creating a situation where paying ransomware is a more cost-effective solution in comparison to starting from scratch. Those situations pray on sunk cost fallacy [10] and basic economics to increase the likelihood of receiving the ransom.

During a successful human-operated ransomware attacks, malicious actor will have a degree of freedom within the system, allowing them to deploy malicious code that can be supplemented by creating backdoors for future use, it is an important fact because over 80% of businesses that chose to pay ransom was attacked again afterwards [11].

### Ransomware-as-a-service (RaaS)

Ransomware is currently one of the biggest security threads a business can face, mainly because in some instances it is organised like a business. Multiple hacker groups like Conti, Lockbit, or Black Basta seem to be operating on a Ransomware-as-a-service model, providing either software, customer support, or credentials to affiliates, enabling them to perform ransomware attacks on businesses. The independent research institute SINTEF proposed the following value chain for RaaS in their research article:[12]

[10] Asana, 'How Sunk Cost Fallacy Influences Our Decisions [2022] • Asana'.
[11] Admin, 'New Cybereason Ransomware Study Reveals True Cost to Business'.
[12] Meland, Bayoumy, and Sindre, 'The Ransomware-as-a-Service Economy within the Darknet'.

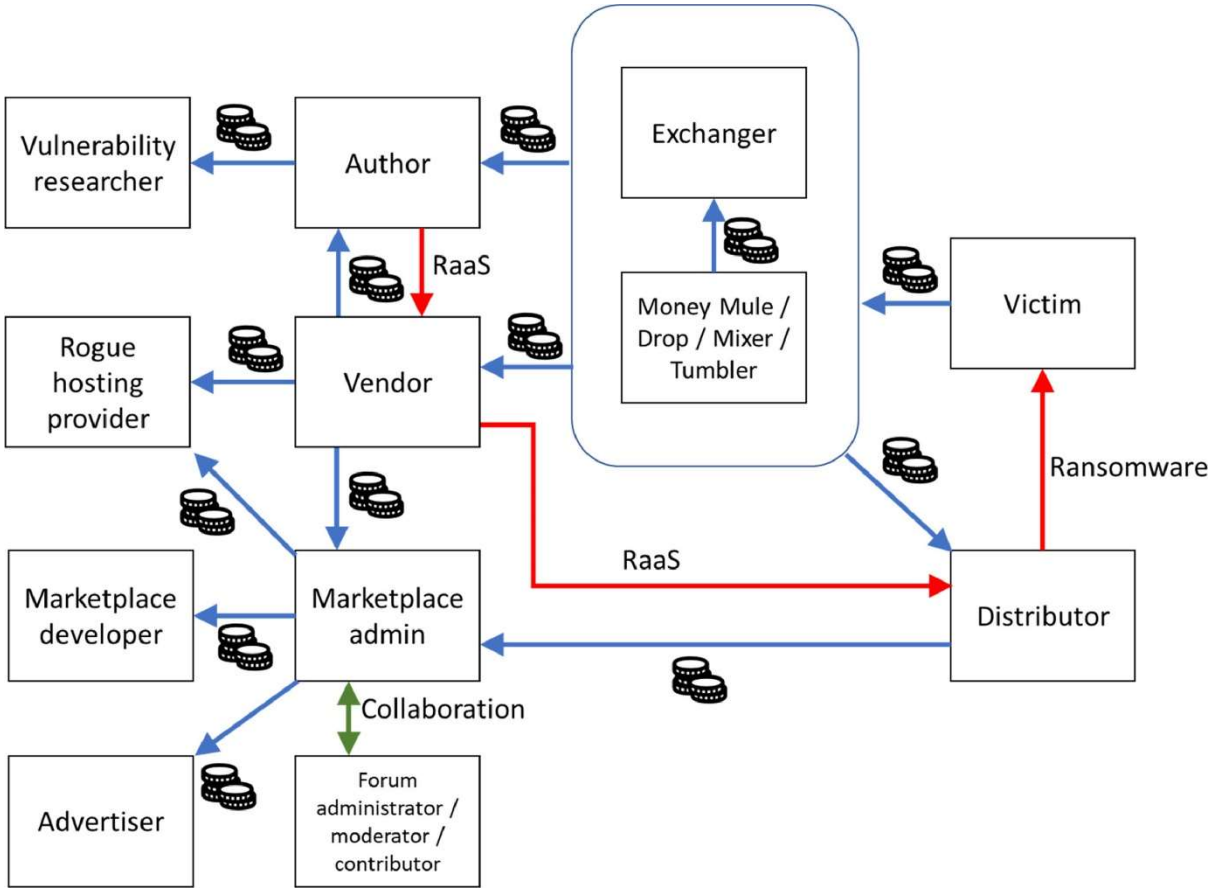



*Figure 4: Value chain for Raas model showing how money and services are distributed within Raas ecosystem*

Hacker groups that utilizing ransomware have they own methods to maximise the likelihood of victim paying ransom, one of the methods is to calculate the ransom based on data stolen during espionage, striking a balance between extorting as much money as possible, but not to discourage the victim from paying due too high ransom. Malicious actors tend to pressure decision makers of businesses, by increasing the ransom the longer business hesitates to pay up.

### 2.2.4 Costs of ransomware attack

A successful ransomware attack would disrupt the business to the point where it is partially or completely incapable of generating income, causing business to bleed savings over time on employees, licenses, loans and other expenses. Such business loses money on profits that they fail to generate, meaning that a ransom of $5 million can be considered a “peak of an iceberg” when it comes to actual recovery cost. In addition to business operation disruption and financial losses, business can suffer from loss of data access, intellectual property theft, and tarnished reputation. Intellectual property theft and tarnished reputation can have high long-term impact on the business, as stolen intellectual property can be used to find exploits.

### 2.2.5 How to prepare for ransomware attack?

Microsoft recommends three steps to prepare for ransom attacks, these steps should be run in parallel to make system security effective:

**Step 1: Incrementally remove risk**

While it is impossible to achieve 100% attack prevention, difficulty in entering the system may discourage malicious actors from attacking you, causing the attackers to move for an more vulnerable

target. One great way of protecting highly privileged accounts is to use two-factor authentication. It is important to notice that one vulnerability can lead to other vulnerability's, attackers can use compromised account to send internal emails infected with malware, bypassing spam filters and lowering victims guard down. It is recommended to follow **Zero Trust** strategy in this step.

**Step 2: Limit Scope of Damage**

Scope of damage is directly linked to resources that attackers get access to, by focusing on protecting the most privileged accounts like global admin or accounting, and utilising the principle of **Least Privilege,** we can limit what attacker get to work with. It by itself is not necessarily a solution to the problem, but rather a method to buy time for business to identify and respond to threads.

**Step 3: Prepare for recovery**

Since breaches are unavoidable, and users need to have at least some privileges, an opportunity for attackers to modify, destroy, or take some data for ransom will always exist. This does not mean that the business needs to yield to the attackers, by preparing adequate backups and forming a recovery plan, business can recover even from the worst-case scenarios.

By protecting the backups with offline storage or immutable storage, business can ensure the recoverability of the systems. Time needed to fully recover the system after a disastrous or worst-case scenario will be highly dependent on skills of IT personnel, time needed to recover from zero functionality can be shortened by performing practical exercises simulating recovery from zero scenarios.

## 2.3 The anatomy of an attack

The process of cyberattacks on cloud infrastructure, can be considered a four-phase process.

### 2.3.1 Phase 1: Reconnaissance

The initial phase revolves around gathering data on the targets, seeking a suitable target and opportunities to gain access to targets infrastructure. A suitable target is a company that generates high profits and relies on digital infrastructure or locally stored data to conduct business. As a general example, if business exposes itself on the internet to do business, it becomes susceptible to attacks.

### 2.3.2 Phase 2: Access

After locking a target and gathering enough information, malicious actors will attempt to gain access to public cloud infrastructure. Malicious actors can get access to your public cloud in multiple ways:

- **Exploiting outdated software or day 0 vulnerability**

  Since software running on infrastructure is rather complex, there always will be a vulnerability or a bug that malicious actors can take advantage of.

- **Social engineering and phishing**

  Depending on the results from reconnaissance phase, malicious actor may be able to impersonate himself as a college or co-worker to lower victim's guard, while at the same time sending them a link or email attachment containing malware.

- **Remote Desktop Protocol compromise**

  In case of weak Remote Desktop Protocol endpoints, a malicious actor can get access to user account on the network by brute-force. There are cases where users have weak passwords that

can be easily socially engineered from social media, for example combination of user's surname, last name, and date of birth.

### 2.3.3 Phase 3: Expansion

After gaining access to the system, malicious actors will travers the network, acquiring information about the resources, assets, and trying to measure the scope of access they possess. This process is called lateral movement and is usually followed by privilege escalation, where malicious actors will seek to further expand their privileges.

### 2.3.4 Phase 4: Exploitation

After elevating into high enough privileges, malicious actor can begin making changes to the system. Naturally malicious actors wish for ransom to be paid, as such they will usually remove backup and other ways of recovering the system. Backup can either be deleted or overwritten to render it useless. Malicious actors can make extra profits by selling stolen confidential data on the black market.

Since majority of victims that paid ransom are attacked again, most malicious actors must create backdoors to the system for future use, making it very easy to attack the system again after its restored. Lastly, malicious actors can deploy ransomware to encrypt data, causing loss of access to data.

## 2.4 Backup

The concept of backup is older than the internet itself, having a backup car can save you a lot of trouble if your main car breaks, but is buying a backup car worth it considering all associated costs? Fortunately for digital assets and data, backups require mainly digital storage, and it is relatively cheap! In digital landscape, any self-respecting business should consider backup as essential, it allows for effective risk mitigation. According to Microsoft azure team[7], many businesses focus solely on preventing the attack, but businesses should prioritize on reliable mitigation of the damage first, since it is currently impossible to fully neutralize the threat of a breach and provide services through the internet at the same time.

### 2.4.1 Types of backup

There are three different types of commonly used backups, these backups are full backup, incremental backup, and differential backup. Each backup type has its own advantages and disadvantages. [13]

**Full backup**

The full backup as names suggest, creates a simple clone of files, directory's, hard drives, and more. The biggest advantage of this backup type is its minimal time required to restore data, making it the best type of backup to recover from. Unfortunately, full backup has also the biggest disadvantages, since it clones all the data requested, it requires a lot of storage space due to volume of data being backed up. Amount of data being cloned, dictates the time and processing power required to perform a backup, this causes full backup to take longer than other alternatives.

[13] Wallen, 'Types of Backup'.


*Figure 5: Visual representation of full backup*

**Incremental backup**

The idea behind incremental backup, is to incrementally storage all the changes done since last backup, this also means that first backup is a full backup, since it's the incremental change of nothing to current state. The advantages and disadvantages of incremental backup are a reverse of full backup, backup speed for incremental backup is slower because it must recover data from backups in correct order, sometimes modifying same files multiple times. Incremental backup saves only files that are modified or added, greatly reducing the amount of data it will process in comparison to full backup, this greatly reduces backup time and required storage.


*Figure 6: Visual representation of incremental backup*

**Differential backup**

A differential backup can be described as a crossbreed between full backup and incremental backup. This type of backup will incrementally save changes between current point in time and the last full backup. This type of backup requires two backup components, namely the last full backup and last differential backup, making it faster and easier to recover than incremental backup but not as fast and easy as full backup. Since differential backup saves more files than incremental backup, its slower and more resource demanding to perform.


*Figure 7: Visual representation of differential backup*

## 2.5 Microsoft 365 platform

Microsoft 365 previously known as office 365 is a license-based family of tools and cloud-based services provided by Microsoft. Microsoft 365 tools are meant to greatly enhance the process of cooperation and cocreating value, by allowing customers to easily create, share and handle data.

### 2.5.1 Applications

Microsoft 365 licenses gives customers access to variety of applications and online services, following are the applications and services that were used to perform ransomware tests during the project.

**Microsoft Teams** is an app and online service used for real-time collaboration. It allows users to plan projects, share files, send messages, attend meetings, and add additional integrated apps like Forms, Azure DevOps and many more. Teams uses SharePoint as an integrated storage for projects, where with each newly created project a library is created to manage its files. One of the Teams features used a lot during the project is shortcuts, it will create a linked directory on the PC that is synchronized with project directory on SharePoint.

**Microsoft SharePoint** is a cloud storage solution, primarily designed for group collaboration.

SharePoint features version control, it allows to revers changes done to SharePoint up to 90 days prier. SharePoint incrementally saves all changes done, allowing for restoration of data to point prior to undesirable change. Version control Is based on library's, meaning that users can recover one library without affecting other libraries.

According to Microsoft vendor [14] Jerry Xu, Microsoft makes an automated backup for SharePoint every 12 hours and retains it for 14 days, this backup is meant as disaster recovery and is not directly accessible to users. In case if disaster recovery backup is needed, system administrator can contact Microsoft support engineers to recover data.

**Microsoft OneDrive** is very similar to SharePoint, it has the same interface, identical version control, and many other features. Where OneDrive differs from SharePoint is its purpose, OneDrive is suppose to be more of a individual storage, as such its not integrated into other tools like SharePoint is. OneDrive is preinstalled on every Windows 10 or newer windows operating system by default

[14] 'Back up and Restore in SharePoint Online - Microsoft Q&A'.

### 2.5.2 Role based access control (RBAC)

Role based access control is a system designed to limit what resources each user can access based on identity permissions, it prevents users with lacking clearance to access, modify or delete resources. RBAC allows system administrator to create a structure like an organization, with roles like contributors, managers, and global administrators each with unique set of privileges and permissions to access resources.

This project focuses on potential damage that compromised accounts can cause to business, lets define theirs privileges and access to resources:

**Project contributor** is an individual that contributes to the project on behalf of the company, contributors will have a specific task or part of the project to work on. Project contributor's privileges should be scoped around resources necessary to contribute to project, as each resource under users control increases attackers surface area in case of a breach.

Contributors working on an application may require privileges to run code as administrator of the virtual machine, since the same privileges are necessary to allow user to run most of ransomware executables, tests will be performed as virtual machine administrator for all users.

**Project manager** is a team leader responsible for organizing, planning, and executing the project while levitating burden of budgeting and scheduling from other team members. As person responsible for managing projects resources and leading quality assurance, project manager should have access to all the resources associated with the project.

Project manager has authority over resources, budget, and team members, this makes zero trust policy exceptionally important in case of a breach. As malicious actor may utilize authority of project manager, to gain access to resources or exploit other employees for theirs benefit.

**Global administrator** is a roll within company that has the highest digital authority, its capable of affecting almost all digital aspects of the company, this includes resources, access control, assets, services, internal communication, networking, backups and many more. As a roll with most control of business-critical systems, protecting administrative accounts can greatly limit the scope of damage an ransomware attack can cause. One great protection method for such important account is multi-factor authentication.

To comply with principles of least privilege and zero trust, employee's privileges should be regularly evaluated and adjusted based on current need. As recommended by American cyber defense agency [15], businesses should consider time-based privileges and reduce use of account with full privilege across the company to the minimum.

### 2.5.3 License based services

The numerous licenses that Microsoft 365 offers are catered towards groups with different needs and sizes, group sizes ranges from individuals working solo to big businesses with thousands of employees. For the purpose of this project, I will be using E5 license to test against ransomware, for

[15] 'Protecting Against Cyber Threats to Managed Service Providers and Their Customers | CISA'.

the reason of it being the most feature full and affordable packet. E5 license provides all features of Office 365 and E3 license for 38$ per month per user. During the project I was using a free trial version of Microsoft 365 E5 license that offered up to 40 users for free in 90days.

E5 license was selected for this thesis due to its variety of features and free trial option, it was possible to create and customise a Microsoft 365 solution for free with following features:

- Azure active directory plan 2
- Conditional access
- Multifactor authentication
- Retention labels
- Privileged access management
- Microsoft defender for endpoint plan 1 and 2

During this thesis a subscription for Microsoft Azure and its resources was lend to me by Norwegian institute for nature technology and science.

### 2.5.4 Azure Active Directory Premium

Azure Active directory is a solution for identity and access management, it combines directory services, advanced identity protection, and access management to protect users from attacks.

- **Multifactor authentication** – It's a feature that blocks access to resources and requires users to verify user identity with additional device or method, usually a smartphone application confirmation or confirmation send by email. This feature can be pared with conditional access to combine they strength. [16]
- **Conditional Access** – allows businesses by enforcing security polices based on conditions. Some of the most common conditions used in conditional access are IP address, device, application, and calculated risk detected according to Microsoft. Azure active directory is then able to enforce policies such as denied access, force user to multifactor authenticate, or force user to change password. As an example, we can force users that will work remotely from home, to perform multifactor authentication before gaining access to confidential data. [17]

### 2.5.5 Defender for endpoint

Microsoft Defender for endpoints is a system with many features that allow administrators to control processes, applications, and hardware to protect users against malicious attacks.

- **Attack surface reduction** – Is a set of rules that control what kind of behaviours applications are allowed, an example of attack surface mitigation rule is to disallow applications for downloading code from the internet. [18]
- **Controlled folder access** – This feature allows administrators to specify protected folders and denies untrusted apps from accessing them. Defender for endpoints adds applications to trustworthy list based on they reputation and prevalence in the system, administrators can also add own application to the whitelist. [19]

[16] Justinha, 'Azure AD Multi-Factor Authentication Versions and Consumption Plans - Microsoft Entra'.
[17] MicrosoftGuyJFlo, 'What Is Conditional Access in Azure Active Directory?'
[18] Dansimp, 'Understand and Use Attack Surface Reduction (ASR)'.
[19] Dansimp, 'Enable Controlled Folder Access'.

- **Exploit protection** – It's a feature that automatically applies exploit mitigation techniques applications and operation system processes. This feature will notify administrators of any prevented exploits in Microsoft defender for endpoint. [20]

### 2.5.6 Microsoft purview information protection

Microsoft preview is a system design with data-governance in mind, It allows administrators to curate, classify, protect, and discover data.

- **Sensitive information types** – is a feature that automatically detects data sensitivity by and categorizes data into one of three levels, High medium and low confidence level**.** This system uses primary and supporting elements to categorize confidentiality level, a primary element can be for example a 16-digit number like an account number, followed shortly after by a four-digit number like expiration date. This feature greatly supplements data classification and label policies. [21]
- **Data classification** – is a set of features that include retention labels, sensitivity labels. Let's begin with retention labels, a business can automate retention and deletion of data base on laws or agreements, some businesses have a responsibility to retain or delete data of users for a specific period, retention labels allow files to be labelled for preservation and/or automated deletion after specific time period post creation. Sensitivity labels is a feature to classify and protect data in Microsoft Word, Excel, PowerPoint and Outlook or containers such as Teams, Microsoft 365 Group, and SharePoint. Files labelled with sensitivity labels can be protected with encryption and watermarked to warn users about sensitivity of the files, and restrict what authorized people can do with the confidential files. [22]

## 2.6 Security Best Practices

### 2.6.1 Principle of least privilege

For any establishment such as factory or office isolated from the public, there are always a group of privileged individuals such as employees, owners and sometimes service providers that can enter the premises and utilize viable resources. To maintain order within organisation, boundaries must be drawn and enforced, this is especially true for cyberspace where hackers try to impersonate legitimate users and take advantage of vulnerable companies with little to no fear of repercussions.

The principle of least privilege considers assigning only minimum level of access to resources for users and processes at any given time to be the best practice. This approach reduces the surface area that malicious actors can utilize during the attack. Preferable users should have access to necessary resources only while performing duties, since after work user don't have any need for resources and access can be safely revoked until next planned work period. [23]

### 2.6.2 Zero trust

As name suggests, principle of zero trust appeals to the idea that you should trust nothing and nobody, it's a pessimistic outlook based on the fact that any account, resource or process may by under control of malicious actors at any given time without anyone knowing. According to National

[20] denisebmsft, 'Turn on Exploit Protection to Help Mitigate against Attacks'.
[21] chrfox, 'Learn about Sensitive Information Types - Microsoft Purview (Compliance)'.
[22] chrfox, 'How to Use the Microsoft Data Classification Dashboard - Microsoft Purview (Compliance)'.
[23] 'Protecting Against Cyber Threats to Managed Service Providers and Their Customers | CISA'.

Cyber Security Centre of United Kingdom, there are eight main principles to implement zero trust model into the company.

1. **Know your architecture, including users, devices, services and data.**
2. **Know your User, Service and Device identities.**
3. **Assess your user behaviour, devices and services health.**
4. **Use policies to authorise requests.**
5. **Authenticate and authorise everything.**
6. **Focus your monitoring on users, devices and services.**
7. **Don't trust any network, including your own.**
8. **Choose services designed for zero trust.**

Sense of familiarity can lead employees to drop they guard and perform actions that naturally would raise concerns, it can also be used to spot abnormalities. [24]

[24] 'Zero Trust Architecture Design Principles'; 'Introduction to Zero Trust'.

# Chapter 3
# Method

## 3.0 Chapter outline

## 3.1 Criteria for analysis

Microsoft 365 solution was evaluated based on scenarios that I will describe in chapter 3.4 and criteria described in this section. It is important to create a mental footnote that Microsoft 365 system is highly customisable, causing some systems to be more resilient than others. It's equally important to remember that features that are not being taken advantage of, don't bring benefits to users.

### 3.1.1 Resistance to ransomware attack

The topic of my thesis is to analyse how efficient Microsoft 365 solution is at mitigating damage and recovering data from ransomware attacks. To evaluate the resistance of Microsoft 365 against ransomware, few specific properties will be considered:

1. Ability to prevent files from being encrypted or deleted
2. Ease of use for tools enabling data protection
3. Baseline enabled security features
4. Ability for storage backups and versioning control to withstand deletion

### 3.1.2 Recoverability after ransomware attack

To be prepared for recovery in case where something happens is a fundamental principal for IT. Since time is of the essence for businesses, there is also a need for recovery to happen swiftly and without need for compromises in quality. To measure systems ransomware recoverability, we need to have following properties in mind:

1. Ability to recover encrypted files and data structure.
2. Ease of use for recovery systems
3. Baseline enabled recovery features

### 3.1.3 Ease of setup

Microsoft 365 provide an enormous catalogue of features and allows for integration of some external systems, some features can be harder to implement then others, which in turn can cause many clients to ignore hard-to-implement features all together.

By making setup of features easy and making features easy to discover, Microsoft can encourage administrators to utilize offered services to the higher potential. As such one of the metrics used to judge Microsoft 365 will be how easy it is to discover, enable, automate and maintain available features.

## 3.2 Configuration setup

Let's address customizability of Microsoft 365, and how difficult it is to judge its resilience based on it. Business's using Microsoft 365 come in varying sizes, with different needs, divers or lacking IT skill

sets and budgets. Those pared with breach point factors such as privileges of hacked account, will have great effect on systems resilience and recoverability. To compensate for lack of accuracy based on flexibility of Microsoft 365, I decide to perform life ransomware experiments in six test environments. Tests will be divided into two system tests, where a member of administration, management, and a contributor will be used as entry point to deploy ransomware in the system.

Let's make two scenarios to better illustrate the difference between systems, two distinct unrelated fictitious companies of different size, need for security, budget and expected IT personnel competence.

- **Default security settings –** "Rat games", small four-person company working on minimalistic video game, this company takes a loan to pay for production, it lacks any relevant security skills. Its rather easy to imagine that such company would make use of Microsoft 365 features to collaborate and completely neglect security.
  This company would need a good baseline of features to protect them by default, because no additional changes to the security will be done before eventual ransomware attack. Due to lack of security competence at the company, safe practices such as least privilege or zero trust will not be practiced.
- **Configured security setting –** "QWE Industrial", A medium size company with over fifty employees specialising in programming and digital calibration of industrial machines.
  This kind of company would most likely invest in at least one data security professional to deploy Microsoft suggested features such as security analyzer, defender for Identity, purview information protection, identity governance, identity security for teams, and automated backups.
  Company of this size should subscribe to the principles of least privilege and zero trust.

### 3.2.1 Default Microsoft 365 configuration

To measure the extension of damage a malicious actor can cause within the system, first three scenarios will be simulating an attack on business using Microsoft 365 that is not configurated. This should mark the extend of consequences in worst case scenarios, where each scenario will receive increased privileges until reaching a global administrator privilege level.

### 3.2.2 Microsoft's recommended configuration

The main goal of this thesis is to verify if Microsoft 365 can prevent data loss and how effective Microsoft365 is at recovering lost data. Measures to prevent an attack or discover a breach are not within the scope of this project. The following are the security tools recommended by Microsoft within deployment guide & assistance:

- **Conditional access** – In a realistic scenario, an attacker would attempt to use RDC from proxied IP address to gain access to the system, in such cases a requirement to multifactor authenticate each time user tries to gain access to resources form new IP would greatly enhance the security. To verify the impact that conditional access will have at preventing ransomware from encrypting files, SharePoint will require multifactor authentication to access data**.** Additionally, administrators are forced to two factor authenticate before gaining access to administrator center, this should prevent the attacker from disabling every security feature before deploying ransomware in the system. For the sake of testing, Microsoft 365 will require that users two factor authenticate hourly.
- **Attack surface reduction** – This setting was forced on all users, it blocked the following:

- executables from running unless on trusted list
- Adobe reader from creating child processes
- JavaScript and VBScript from running downloadable executable content
- All Office and Office communication applications from creating child processes or executable content
- Office applications from injecting code into other processes

Additionally, Ransomware advanced protection feature is enabled. There is a suspicion that Microsoft defender for endpoints is directly connected to Microsoft defender preinstalled on windows machines, if that's the case then all the features like attack surface reduction or exploit protection can be disabled by disabling Microsoft defender on the machine.

- **Controlled folder access** – Windows security virus & threat protection gets enabled, it is setup to protect specified files and directories from unauthorized changes, this includes directories on OneDrive, SharePoint, and directory's stored directly on the VM.
- **Data classification** – To tests multiple labels at the same time, additional directories are added to "Resources" channel on teams, each directory contain word and excel files that are labelled as either public, general, confidential, highly confidential, or a custom max security label. An additional directory is added to test retention label capabilities, retention label is configurated to prevent deletion of files for seven days after last modification.
- **Backup OneDrive** – All files saved on desktop, documents, and pictures are backed up into OneDrive backup system. E5 license in Microsoft 365 does not allow for a backup in SharePoint server.

## 3.3 Test environments

### 3.3.1 Virtual machine

To create an isolated test environment, a setup of two virtual machines on Microsoft azure is used. First virtual machine is used primarily to logging into second virtual machine using Azure AD, this is done in such a way because my main computer uses standard windows 10 version that does not permit RDC using Azure AD. Both virtual machines use Windows 10 Pro operating system.

The test virtual machines uses standard D2s v3 size with 2 virtual central processing units and 8 gigabytes of random-access memory. Virtual machine uses default settings with exception for enabling Azure AD that allows users to log into the virtual machine using Microsoft credentials.

### 3.3.2 Ransomware

Over the duration of the project, 18 ransomware samples found on github[25] were tested. Only ransomware Cerber and WannaCry were able to encrypt files while logged on as non-administrator user running executable with administrator privileges. Encryption done by Cerber was unreliable, as it was incapable of encrypting files unless executed by a global admin during testing. WannaCry shown reliable results as it was able to reliable encrypt all unprotected excel, word, pdf, and JavaScript files on Virtual machine and attached digital drives such as OneDrive and Dropbox. For those reasons WannaCry was used as ransomware of choice for the remainder of the project.

[25] kh4sh3i, 'Ransomware-Samples'.

## 3.4 Scenarios

Scenarios are a cohisent way of scoping the project and tests alike. One of throwbacks of using scenarios in a system as complex as Microsoft 365, is that one small change can drastically change the outcome of experiments. In this project there are exactly six scenarios that are tested and analyzed.

The idea behind scenarios one, two and three is to measure the severity of damage that human-based ransomware attack can cause against company unwilling or incapable to utilize Microsoft 365 security features. This may be the case for multiple reasons, company can be too small with few resources to spare on security, it can be a case of company moving to cloud before setting up security, or it can be a case of company considering security a waste of resources and just focusing on work. While first three scenarios are similar, they will make a great comparison for scenarios four, five and six.

In each scenario the system will be subjected to a human-operated ransomware attack, simulating malicious actors trying to disable any security features and delete backups or any other form of recovery assurance.

### 3.4.1 Scenario 1: Attack on project contributor account, default settings

**Description:** The first scenario is an attack on a system where no changes to security have been made and the point of entry is a project contributor. Its purpose is to verify how much unrepairable damage can attacker cause with use of contributor privileges, and how can he hinder recovery process.

**Conditions:** This scenario assumes that attacker gained access to project contributor account, gaining access to all data and privileges that impersonated employee have access to. As a result, attacker gets access to data within the confines SharePoint through Teams and Additional data on OneDrive.

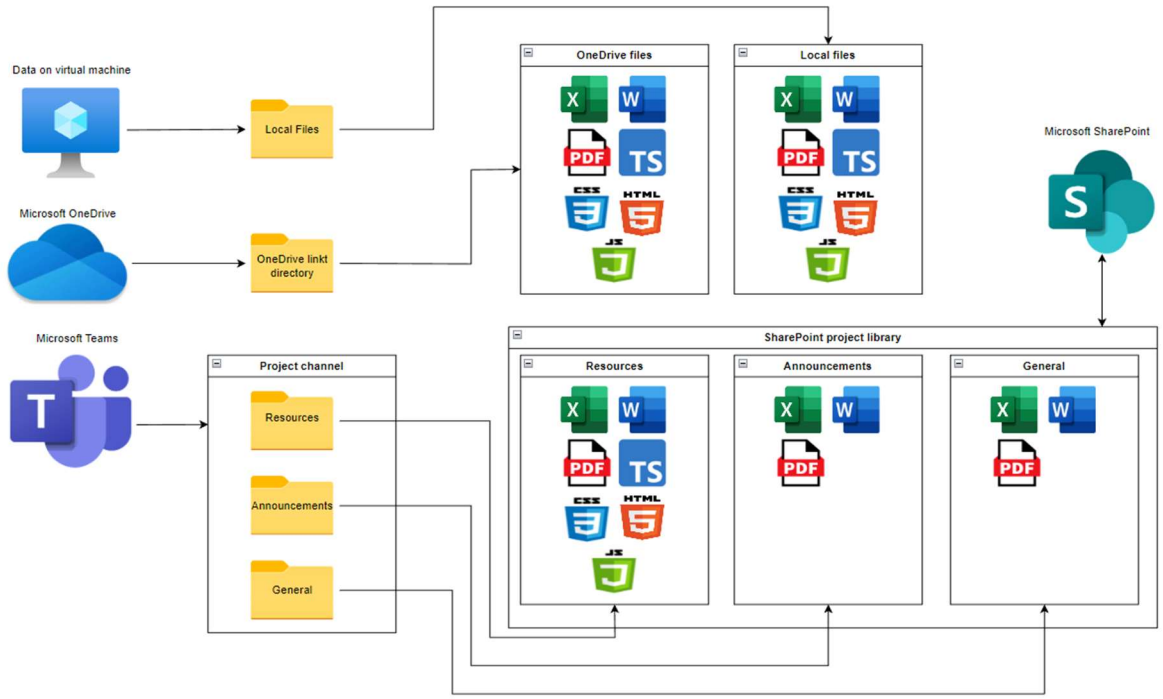


*Figure 8: Visualization of important company data accessible to the attacker on project contributor account*

**Consequences:** The worst-case consequence for this scenario is that the attacker will be able to disable file versioning before deploying ransomware into the system. Causing permanent data loss of all files that project contributor has access to. In case where data are business-critical, this could force victim organisation to pay the ransom or bear the burden of starting from scratch.

**Risk mitigation:** Microsoft 365 have some risk mitigation measures put in place by default. One of those is version control, it allows for data allocated in SharePoint and OneDrive libraries to return to previous point in time before ransomware deployment. One of the goals for the attacker will be to seek a way of disabling versioning before encrypting the files, or alternatively to override or delete version control history.

**Testing:** The assumption for this scenario is that virtual machine administrator login role is active for attacked employee. Originally purpose of administrator login was to allow contributors to test code, it will instead enable attacker to disable windows defender, link files to OneDrive, and deploy ransomware with little hindrance.

Attacker will also be able to utilize services such as Microsoft Teams, SharePoint, OneDrive to connect all resources together for better ransomware coverage. According to Microsoft documentation[26], users with "Contributor" privileges are able to delete prior versions of documents , this should in theory allow the attacker to take data as hostage for ransom.

**Recovery:** Recoverability is greatly dependent on if attacker can successfully disable or delete versioning and recovery system for SharePoint and OneDrive. In case where attacker is not successful at removing versioning and the recovery system, it will become the primary method to restore system using restore function or version control. In case where attacker was able to remove versioning and recovery system, there is an option of communicating with Microsoft's engineers to perform disaster recovery, as Microsoft is obligated to perform mandatory disaster recovery backup of customers data. There is a possibility that Microsoft may refuse to restore encrypted data since those backups are for purpose of disaster recovery.

### 3.4.2 Scenario 2: Attack on project manager account, default settings

**Description:** The risk that each employee brings to the company is closely correlated to the level of privilege they have, targeting employees with higher privilege levels is a well know strategy of malicious actors whenever they prepare for attacks. As such, the second scenario is an attack on project manager within a Microsoft 365 system where no changes to security have been implemented.

**Conditions:** In this scenario I assume that the project manager is not directly responsible for transactions on behalf of the project, this means that the attacker is not able to withdraw or transfer any founts from the project to his personal account. Project manager has access to the exact same files as project contributor but with addition of "planning" directory. Project manager also has full control privilege to SharePoint, granting attacker greater chance to potentially prevent recovery of the data.

[26] 'How Versioning Works in Lists and Libraries - Microsoft Support'.

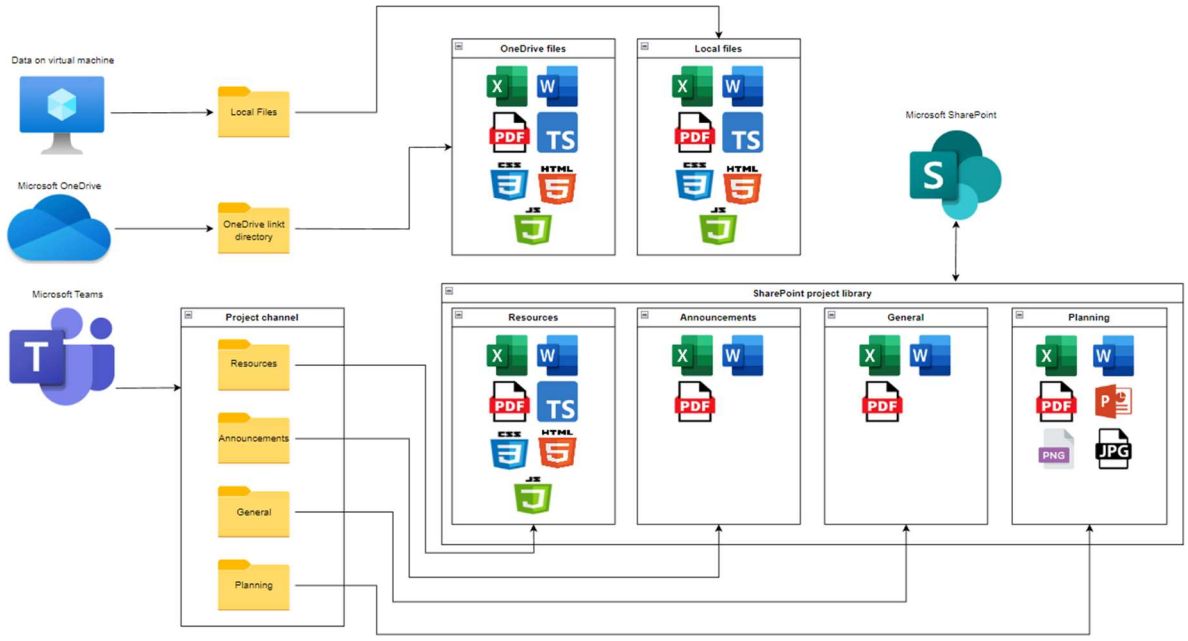



*Figure 9: Visualization of important company data accessible to the attacker on project manager account*

**Consequences:** In addition to consequences from first scenario, attacker using project manager account can also modify, delete, and add SharePoint libraries and Team group channels. There is a possibility that deleting a SharePoint library may cause clear versioning history, making it impossible to recover using restoration tool.

**Risk mitigation:** Microsoft has a retention policy in place by default, whenever a team's group channel or SharePoint library gets deleted, it automatically gets soft deleted instead, meaning that it can be restored within a period of time.

**Testing:** To test this scenario, the attackers will have to disable Windows defender, then proceed to connect all possible resources to OneDrive, follow it by encrypting files, and additionally delete Teams group channel and SharePoint libraries.

**Recovery:** Recovery for this scenario consist of two parts, firstly an administrator needs to recover deleted SharePoint library and Teams group within admin portal, secondly either an admin or project manager will have to recover encrypted data using recovery feature of SharePoint and OneDrive.

### 3.4.3 Scenario 3: Attack on global admin account, default settings

**Description** Third and last scenario on system with default settings, assumes a complete compromise of the system, where a malicious actor gains access to a global administrator account and have full control over the system.

**Conditions** The condition of this scenario is dire, since a global administrator is fully capable of disabling and deleting users, team's groups, SharePoint libraries, OneDrive libraries, messing with azure resources and much more. To limit the scope of this scenario, we will have to assume that the attacker is not interested on spend time to fiddle with company's resources, instead he will focus solely on disabling SharePoint recovery system to increase chances of ransomware being paid. Another assumption is that the attacker uses administrators account exclusively in this scenario, meaning that other accounts like project contributors and managers are not synchronized

with the cloud since the attack. Lastly, the last assumption is that project contributor has connected all resources to OneDrive within Teams.

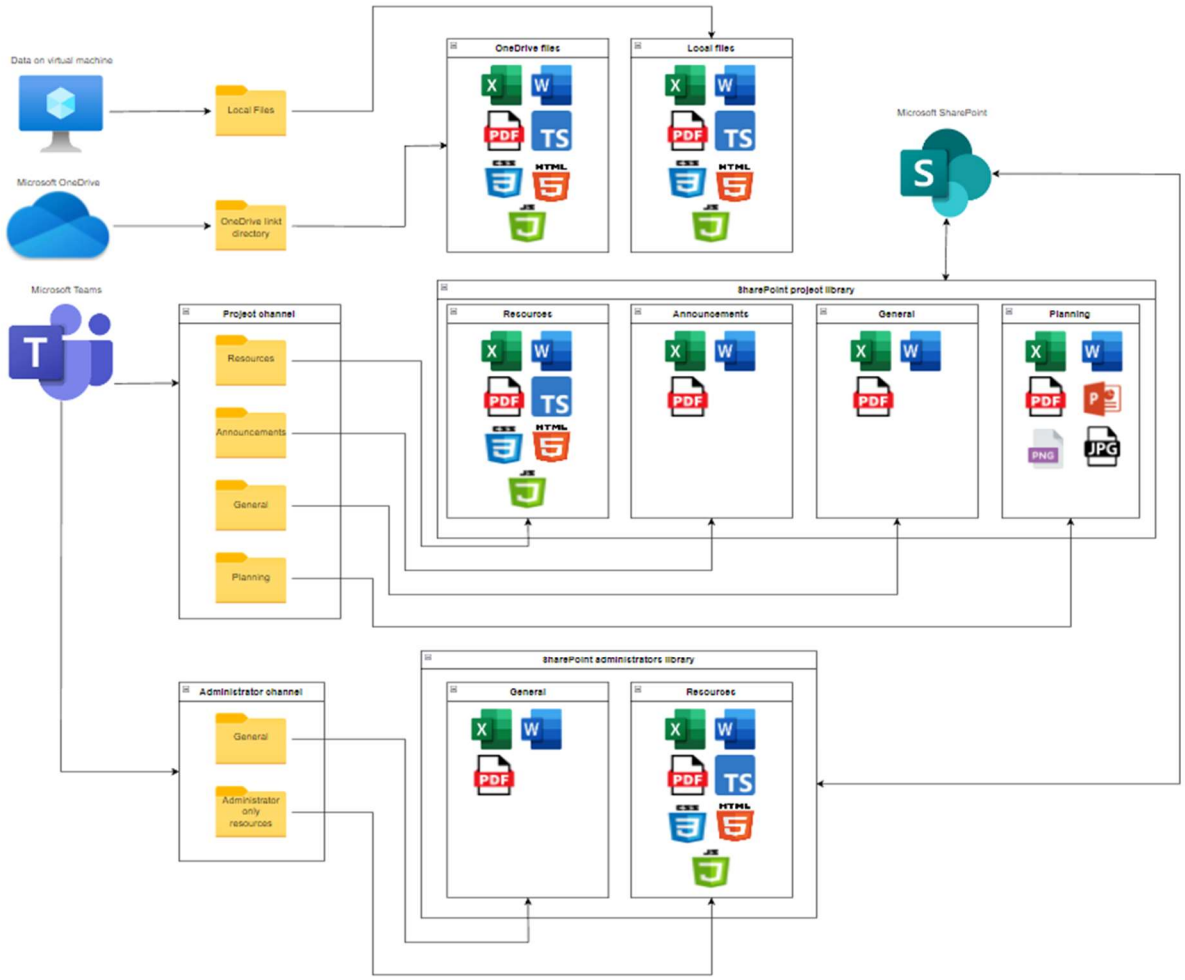



*Figure 10: Visualization of important company data accessible to the attacker on global admin account*

**Consequences** A rogue administrator or attacker with global administrator privileges can cause all kinds of trouble, not only is he able to encrypt all companies' data on Microsoft 365 platform, but he can also prevent any form of recovery systems from being used, and in some cases use azure resources to mine cryptocurrency's and for other nefarious purposes. To summarize, this kind of scenario can lead to permanent loses of all data and in some cases direct financial losses due to abuse of Microsoft azure.

**Risk mitigation** Microsoft does not offer any risk mitigation features that are enable by default to prevent a global administrator from making changes to data, policies, or changes to the system. There is a slim possibility that Microsoft support may be able to help, but proving ownership over Microsoft 365 environment may be time consuming, or indistinguishable from a malicious actor trying to exploit Microsoft support to access someone else's resources.

**Testing** As with previous tests, attacker will have to disable windows defender, then follow it by linking all resources in SharePoint within Teams to OneDrive, and lastly encrypt accessible data. We can assume that the attacker would change the global administrator account credential and prevent other users from using recovery features for SharePoint and OneDrive with policies or by revoking privileges.

**Recovery** With the assumption that recovery systems are made unviable, and data are already encrypted, one would think that there is very little that can be done to recover from such attack. In this scenario a project manager will attempt to copy project data on OneDrive that have been desynced since last login. The goal of recovery is to firstly disable auto synchronization on OneDrive, this can be done in multiple ways, like forcing user to two factors authenticate on SharePoint, creating a policy to deny access to SharePoint, or quickly disabling OneDrive synchronisation after logging into virtual machine. If the only administrator account gets compromised, then accessing policies may be impossible, but for the sake of consistence I will force two factor authentication on project manager after the attack to disable synchronisation. This should in theory give user access to "outdated" files from before encryption.

### 3.4.4 Scenario 4: Attack on project contributor account, system with multiple recommended features enabled

**Description** This scenario will simulate an attack on company that integrated few security features into Microsoft 365 ecosystem that are recommended by Microsoft. Point of entry that attacker will use is a compromised project contributor account used to gain access to company's virtual machine via RDP.

**Conditions** The condition for this scenario is that the attacker was able to remotely sign into a virtual machine using stolen employee credentials, shortly after the attacker realized that data stored on SharePoint are protected by two factor authentication.

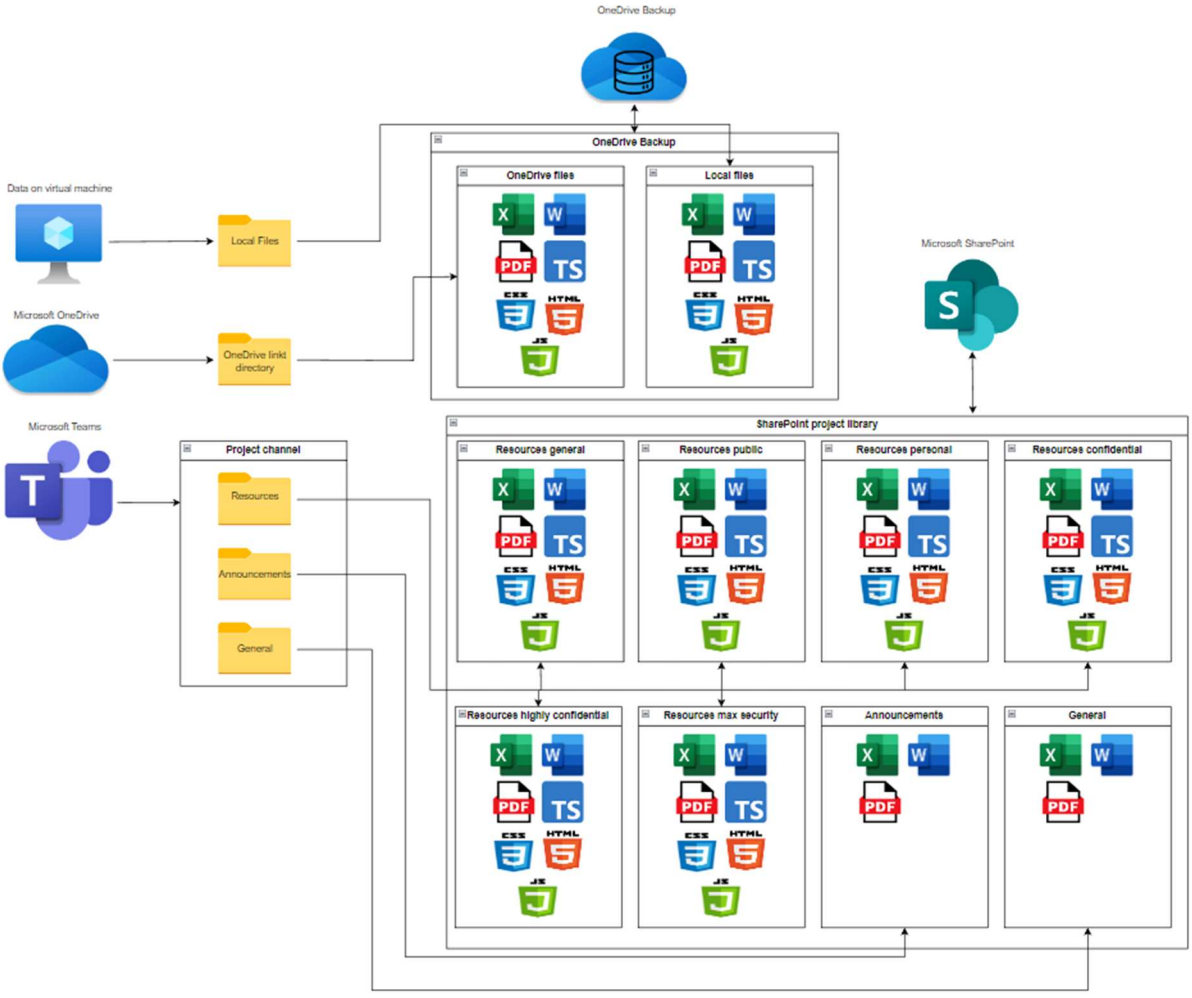


*Figure 11: Visualization of important company data accessible to the attacker on project contributor account*

**Consequences** This attack is very unlikely to cause any long-lasting damage if precaution is taken into consideration. What is fascinating about the digital world is that anything is possible if enough effort, resources, and manpower with adequate skills are put into it. As such, attackers can be creative with their approach, if given opportunity to execute code within the system, they could try to take control over virtual machine directly after employee have two factors authenticated.

**Risk mitigation** There are multiple risk mitigation factors that play a role in this scenario. Firstly, SharePoint is guarded by two factor authentication, this does not only prevent the attacker form accessing and modifying files, but also notifies employee about potential attack. Secondly, files located on Desktop, Download and in Documents directories are backed up to OneDrive, preventing attacker from permanently encrypting those files. Thirdly, attack surface reduction should in theory prevent ransomware from running rampant thanks to the advanced ransom protection. Lastly, controlled folder access received list of protected directories, it is supposed to prevent applications from modifying data in those directory's.

**Testing** I speculate that windows defender preinstalled on virtual machines is directly related to windows defender for endpoints that controls attack surface reduction and controlled folder access, if this is the case, then disabling windows defender should allow attacker to deploy ransomware or other malicious code into the system. To test this, I will disable windows defender and try to run ransomware executable.

Additionally, I will test if its possible to trick Microsoft teams into linking SharePoint data to users OneDrive, this would allow attacker to get access to data after employee two factor authenticates and synchronizes OneDrive. In theory this would give the attacker access to few hours old files, and possible even encrypt some files that are not regularly modified, by exploiting synchronization to push encryption to files that have not been modified for some time.

**Recovery** Since the expected scope of damage in this scenario is focused around local files and OneDrive synchronized linked data, recovery from backup should allow for recovery of data that were accessible through OneDrive.

### 3.4.5 Scenario 5: Attack on project manager account, system with multiple recommended features enabled

**Description** In this scenario, attacker found his way into the system by exploiting compromised project manager account, attacker will attempt to encrypt files labelled with confidentiality and retention labels.

**Conditions** This scenario is very similar to scenario four. To differentiate from it, we can assume that the employee had additionally synchronized SharePoint files to OneDrive via Teams on this virtual machine for convenience sake, as this would give the attacker access to confidential data and allow him to encrypt desynchronized data, hoping that the encrypted versions will overwrite the data on SharePoint during synchronization.

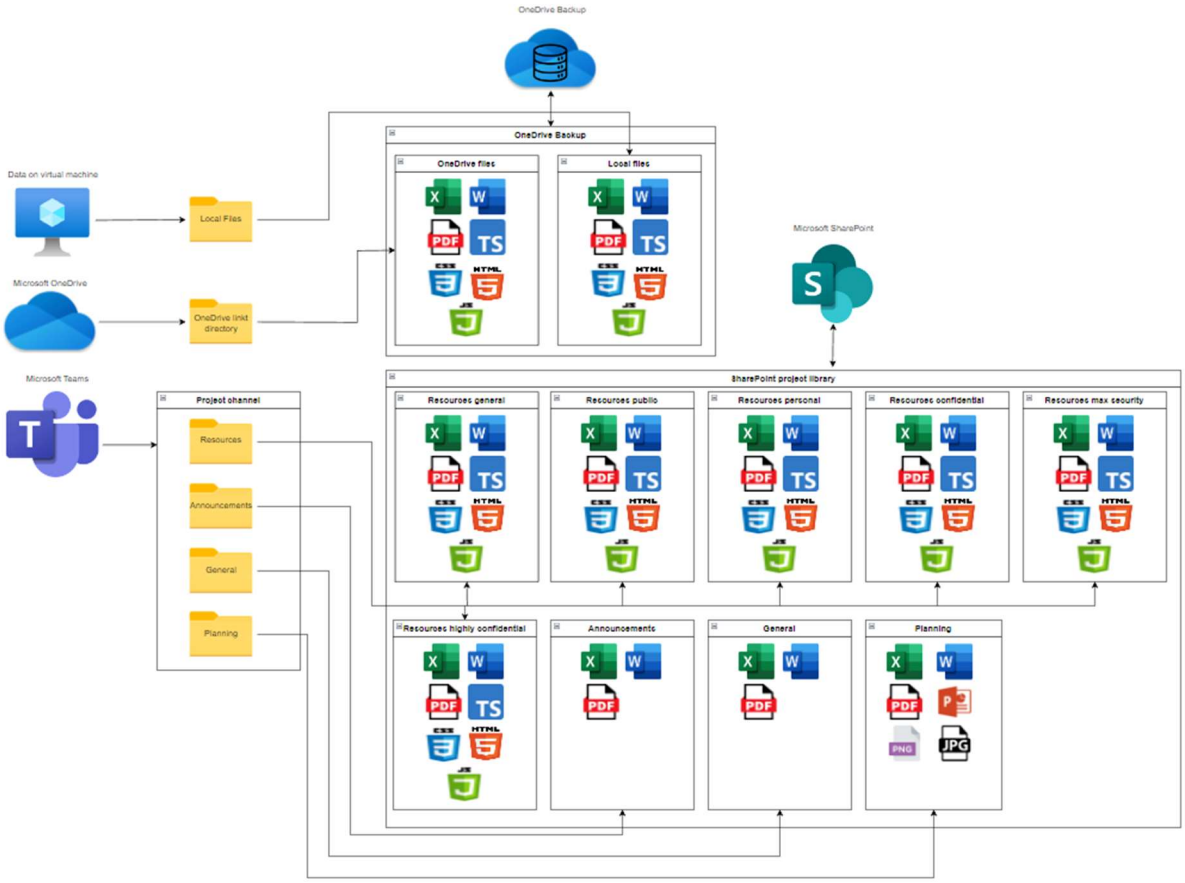



*Figure 12: Visualization of important company data accessible to the attacker on project manager account*

**Consequences** If the malicious actor manages to encrypt desynchronised files on OneDrive without detection, next time employee passes two factor authentication can cause all the files to synchronize with the cloud, and subsequently encrypt data in cloud as a result. This attack is unlikely to be devastating on its own, as restore functions on OneDrive and SharePoint should be able to reverse the changes.

**Risk mitigation** SharePoint and OneDrive recovery systems should allow an administrator to recover majority of the data, additionally a backup of documents, desktop and download directories into OneDrive**.** By disabling synchronization, and reverse encryption with file versioning, it should be possible to mitigate majority of the risk. This scenario uses the same risk mitigation techniques as scenario four.

**Testing** In this scenario I tested if any classification types would prevent ransomware from encrypting files, to test this, multiple directories were added, each containing excel and word files with one of five default confidentiality labels. Additionally, one directory will contain files labelled with retention label, this is supposed to prevent deletion of the file for seven days after last modification.

**Recovery** Recovering with SharePoint and OneDrive recovery to point in time, together with OneDrive backup for local files should make it possible to recover all important files in this scenario.

### 3.4.6 Scenario 6: Attack on global admin account, system with multiple recommended features enabled

**Description** This is the last scenario, where an attacker will find a way to exploit compromised global administrator account to perform ransomware attack on companies' virtual machine.

**Conditions** Condition for this scenario is the same as in scenario five, to diversify from last scenario, I will assume that the attacker have managed to exploit a window of opportunity, by running a executable ransomware after administrator have successfully two factor authenticated.

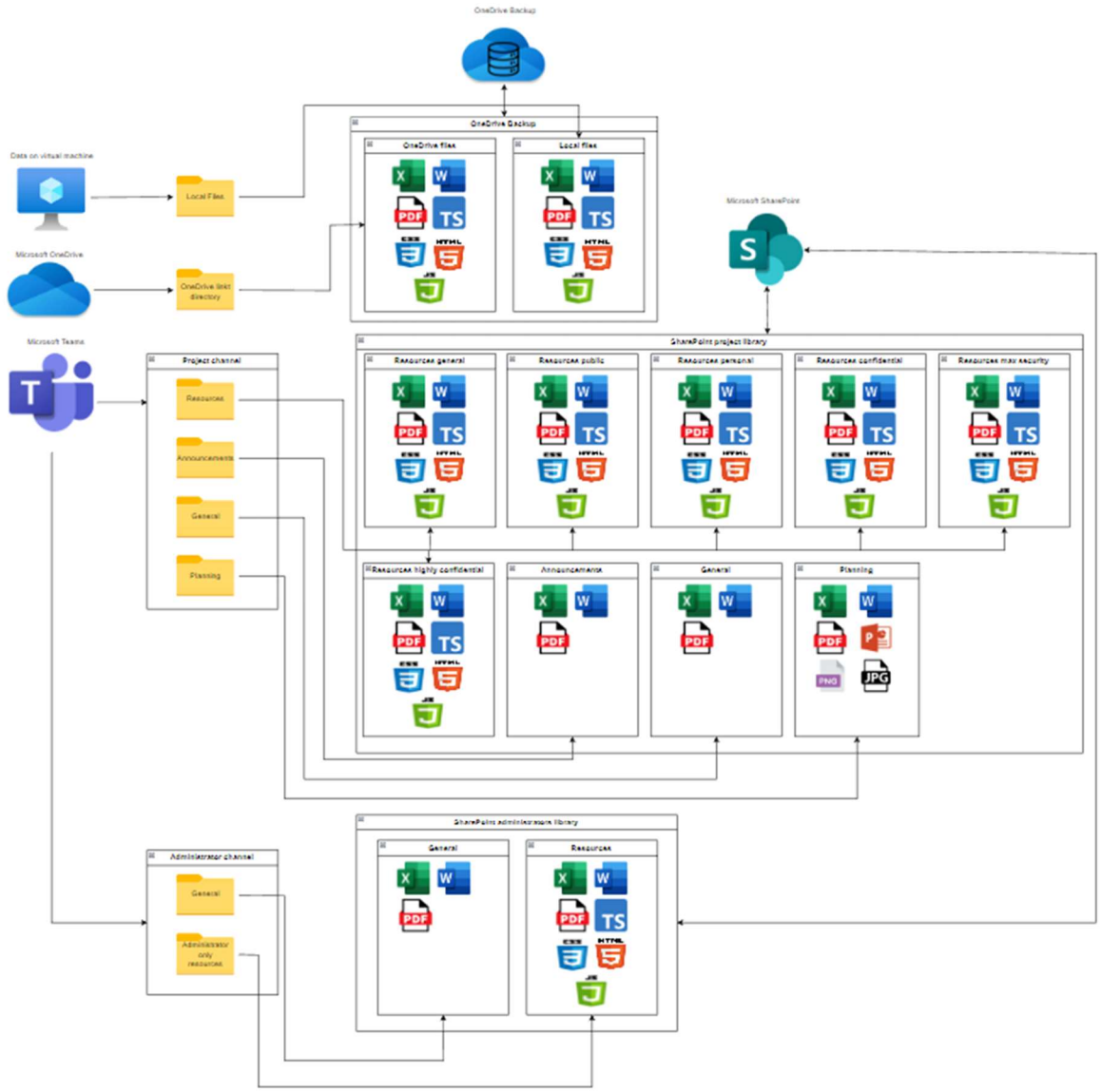


*Figure 13: Visualization of important company data accessible to the attacker on global admin account*

**Consequences** With the assumption that the attacker did not gain access to administration portal on Microsoft 365, due to requirement of additional two factor authentication, we can assume that there is a very low probability that this attack will have any long-lasting consequences on the business. Files that may become unrecoverable are local files stored somewhere beside download, documents and desktops, as those are covered by OneDrive backup.

**Risk mitigation** This scenario uses the same risk mitigation techniques as scenario four.

**Testing** For this scenario I wanted to test if retention policy, sensitivity labels, and surface attack reduction would affect ransomware software differently if affected files were synchronized to cloud, as its possible that some features may protect files in real time only if synchronized.

**Recovery** Majority of data that can be encrypted, should also be possible to restore using OneDrive backup together with SharePoint and OneDrive restore functions.

# Chapter 4
# Results

## 4.1 Results

In this chapter, I will present the result of the analysis based on the data acquired in chapter 3. This chapter is separated by each scenario, starting with analysis of the ransomware software.

### 4.1.1 Testing ransomware

A total of 18 different ransomware samples have been tested at the beginning of the project. Each of these samples were immediately recognised by Windows defender as potential threat promptly deleted. First batch of tests done on these samples was done as user without virtual machine administrator privileges, as a result each executable required administrator privileges to run. During these initial tests, two samples yielded any results. Namely “Cerber” and “WannaCry”.

Sample “Cerber” was able to change background picture to a ransom message but was unable to encrypt any data on the machine. My hypothesis is that “Cerber” creates child processes that also require elevated privileges to function, this is supported by the fact that running “Cerber” executable as user with virtual machine administrator privilege leads to files being encrypted in addition to changing background picture.

In stark contrast, sample “WannaCry” was fully functional and capable of encrypting files even when users virtual machine rights were not elevated to administrator status. During test “WannaCry” would travers each drive accessible, this includes local drives, files shared onto OneDrive, and cloud storage like Dropbox. The way “WannaCry” performed encryption was peculiar, rather than perform bit shift on a file to scramble data into unreadable mess, it would create a copy of the files that was encrypted and delete the original afterwards. This means that “WannaCry” would create encrypted copy of a file if it was allowed to read the file and create new files in the directory, but could delete the file only if it had writing privileges for this set of data. During initial testing I was able to confirm that this “WannaCry” sample was able to create encrypted copies of following file types: Word, Excel, JavaScript, PNG. Jpag, and PowerPoint. “WannaCry” sample was not able to work with HTML, CSS, or TypeScript.

Because “WannaCry” makes it easier to verify if encryption failed due to missing read or write privileges, it was chosen as ransomware used in further testing.

This knowledge opens multiple research questions that were not explored during this project, for example if it’s possible to recover deleted data from memory? [27] Files deleted on a Windows 10 system are not necessarily permanently lost, as deleting files only frees the space where memory was located and allows system to over-write this memory, in theory it’s possible to recover deleted files using “Windows File Recovery”, unfortunately its use is limited to local storage devices and does not support cloud storage and network files.

[27] ‘Recover Lost Files on Windows 10 - Microsoft Support’.


*Figure 14: Contents of github repository providing ransomware samples*

### 4.1.2 Testing scenario 1

(See 3.4.1 for method)

The users impersonator was able to disable windows defender live protection feature from windows security panel, this action would disable windows defender for all users on this virtual machine, that includes project manager and global administrator accounts if they chose to use the same virtual machine. It would be recommended to have separate virtual machines for each user, as this would prevent users from disabling windows defender features for other.

To link data on SharePoint into OneDrive, I used an integrated function “Add shortcut to OneDrive” found in Microsoft Teams, that allowed for directories to be treated as local drives and subsequently allowed ransomware to encrypt data on SharePoint. Files that were not packaged into a directory could not be linked to OneDrive, to increase the coverage for ransomware, all files and directories would be moved into a directory for each teams channel before linking to OneDrive. It is possible to link files to OneDrive directly from SharePoint, but teams method was more familiar for me personally.

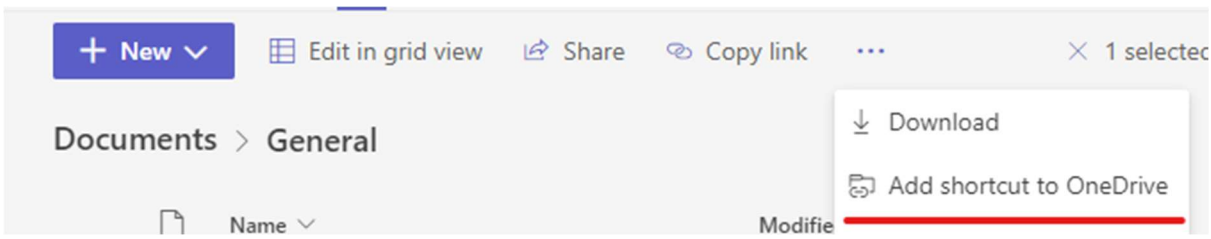



Figure 16: *Instruction on adding shortcuts to OneDrive within Microsoft Teams*

To prevent recovery, I tried to disable version control from SharePoint and OneDrive libraries, this turned out to not be possible since 2018 when Microsoft enforced mandatory version control [28], where SharePoint and OneDrive are forced to store at least one hundred of latest primary versions. Precious versions can be manually deleted, but this has not effect on recovery system of SharePoint or OneDrive. Additionally, since "WannaCry" sample would delete the original file, it had no effect on version control since the only change done to each file was its soft deletion. Files deleted by "WannaCry" sample were send into trash been, where they could be manually deleted or restored.

Afterword's first encryption test was performed, since windows defender was disabled, ransomware was able to encrypt numerous files, both local and cloud stored files were replaced by encrypted WannaCry type files with corresponding names. Figure below visually represents the data that ransomware was able to access, and which were replaced with encrypted versions.

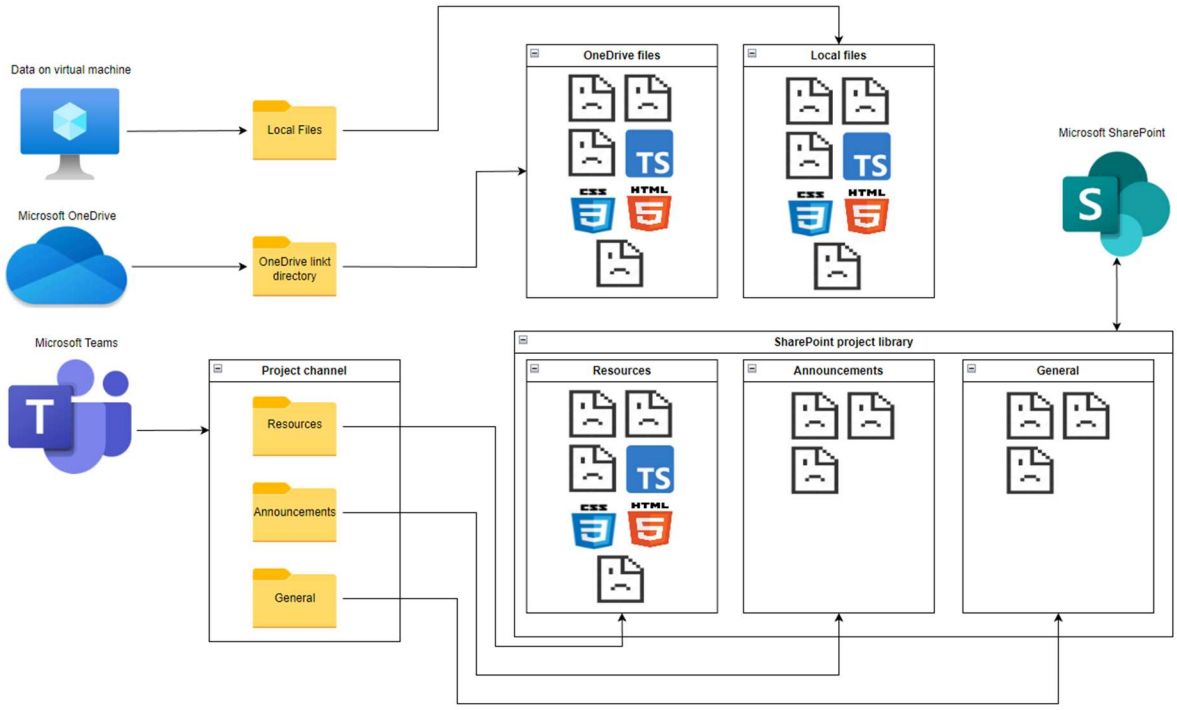



*Figure 15: State of file accessible by project contributor after ransomware attack.*

During testing I was hoping that SharePoint or OneDrive would prevent data from being encrypted, by either recognizing that singular user modifies, creates, or deletes too many files in short period of time, and require user to log into the account with credentials to proceed. Unfortunately, during the testing, ransomware was able to encrypt data without resistance. Notable, few minutes after ransomware encrypted files, OneDrive was able to notice that the user was most probably a victim of ransomware attack and notified him, notification had a button that led to recovery system for OneDrive.

Ultimately, ransomware was able to encrypt 18 out of 27 files, of which 9 were not supported by the ransomware sample.

[28] https://techcommunity.microsoft.com/t5/user/viewprofilepage/user-id/33926, 'New Updates to OneDrive and SharePoint Team Site Versioning'.

### 4.1.3 Recovery scenario 1

Recovery of data on SharePoint and OneDrive very simple, both OneDrive and SharePoint have recover library function, it registers every major change done to each file in storage and saves it as a history of changes for 30 days. User can select a point and revers every change done until this point.

All the files that were stored either on SharePoint or OneDrive made full recovery, out of 14 encrypted files in digital storage, all 14 were successfully recovered with none becoming corrupted.

Encrypted files that were stored locally on the virtual machine, were not recoverable by any default Microsoft 365 service.

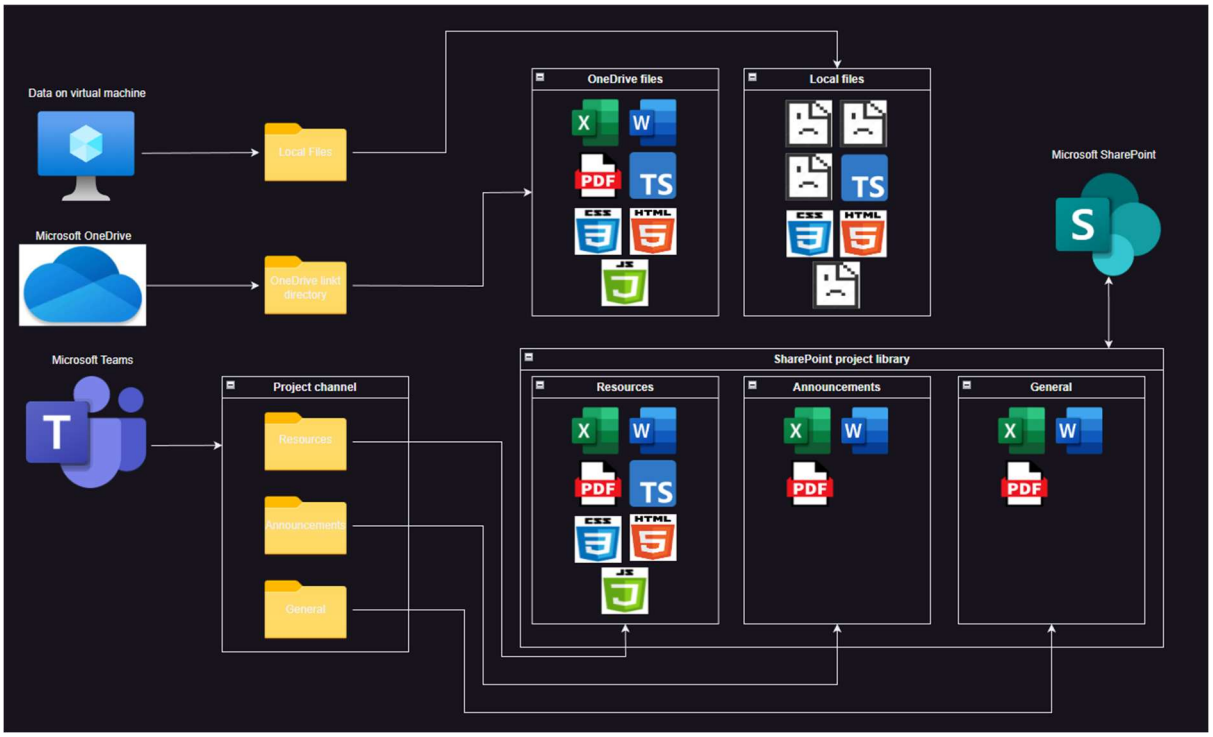



*Figure 16: State of project contributor files after recovery from ransomware attack.*

### 4.1.4 Testing scenario 2

(See 3.4.2 for method)

Majority of the setup and results were consistent with results from first scenario. One of the key differences I was looking forward to, was verifying if giving user more privileges would make Microsoft 365 system more sensitive to abnormalities. Unfortunately, just like in the first scenario, attacker was able to encrypt files without any notable resistance.

**Test 1: Delete group using Teams**

After performing all the actions from first scenario, the entirety of the project on Microsoft Teams was deleted, SharePoint site can be deleted using SharePoint admin center.

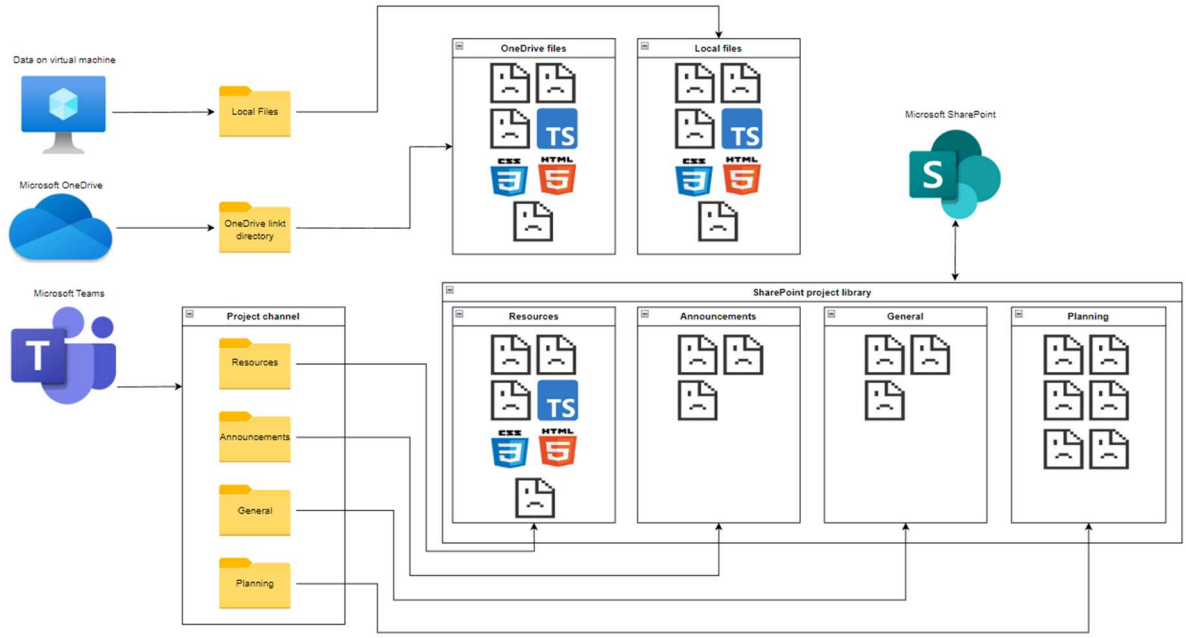



*Figure 17: State of file accessible by project manager after ransomware attack.*

**Test 2: Delete group using PowerShell**

After performing all the actions from first scenario, attacker would first delete Teams group using Microsoft teams, afterwards attacker used PowerShell to find the id of soft deleted teams group with following command *Get-AzureADMSDeletedGroup* and proceed to hard delete the Teams group with the following command *Remove-AzureADMSDeletedDirectoryObject -Id <objectId>.* The same process can be repeated if SharePoint is deleted from SharePoint admin center.

```
PS C:\Windows\system32> Get-AzureADMSDeletedGroup

Id                                   DisplayName                    Description
--                                   -----------                    -----------
fd8b52f9-86fa-407e-84a9-551e066262a2 Project 2 Ransomware test [copy] Project 2 Ransomware test [copy]


PS C:\Windows\system32> Remove-AzureADMSDeletedDirectoryObject -Id fd8b52f9-86fa-407e-84a9-551e066262a2
PS C:\Windows\system32> Get-AzureADMSDeletedGroup
PS C:\Windows\system32>
```

*Figure 18: Presenting how to hard delete a group in PowerShell.*

In this scenario, ransomware was able to encrypt 24 out of 33 files, of which 9 were not supported by the ransomware sample. Additional file types that have been added for these tests were PNG, JPEG, and Microsoft PowerPoint.

### 4.1.5 Recovery scenario 2

**Recovery from test 1:**

Teams group and SharePoint libraries are soft deleted by default, they can be restored from within admin center in 30-day period. Soft deleted Teams and SharePoint groups can be restored from Exchange admin center, just as shown I figure below.

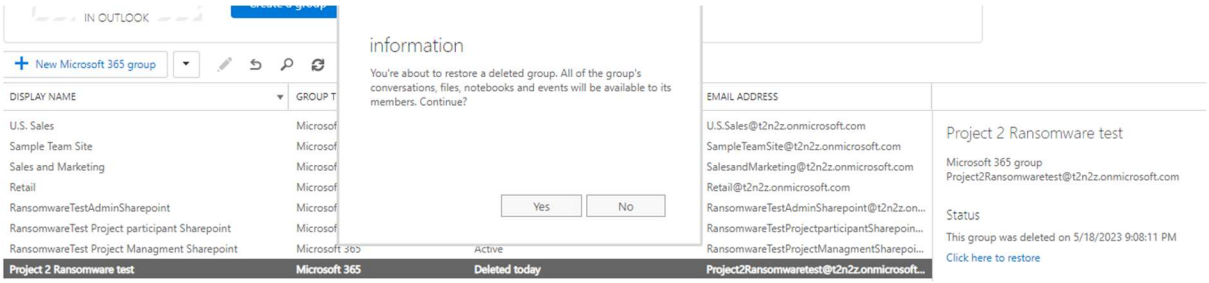



*Figure 19: Illustration for how to restore soft deleted teams channel.*

Afterward steps from first scenario recovery can be repeated were repeated to restore data on SharePoint and OneDrive. Restoring SharePoint from deletion had no effect on recovery system. As a result, all the encrypted data with the exception of local files were restored, meaning that 20 out of 24 encrypted files were successfully restored.

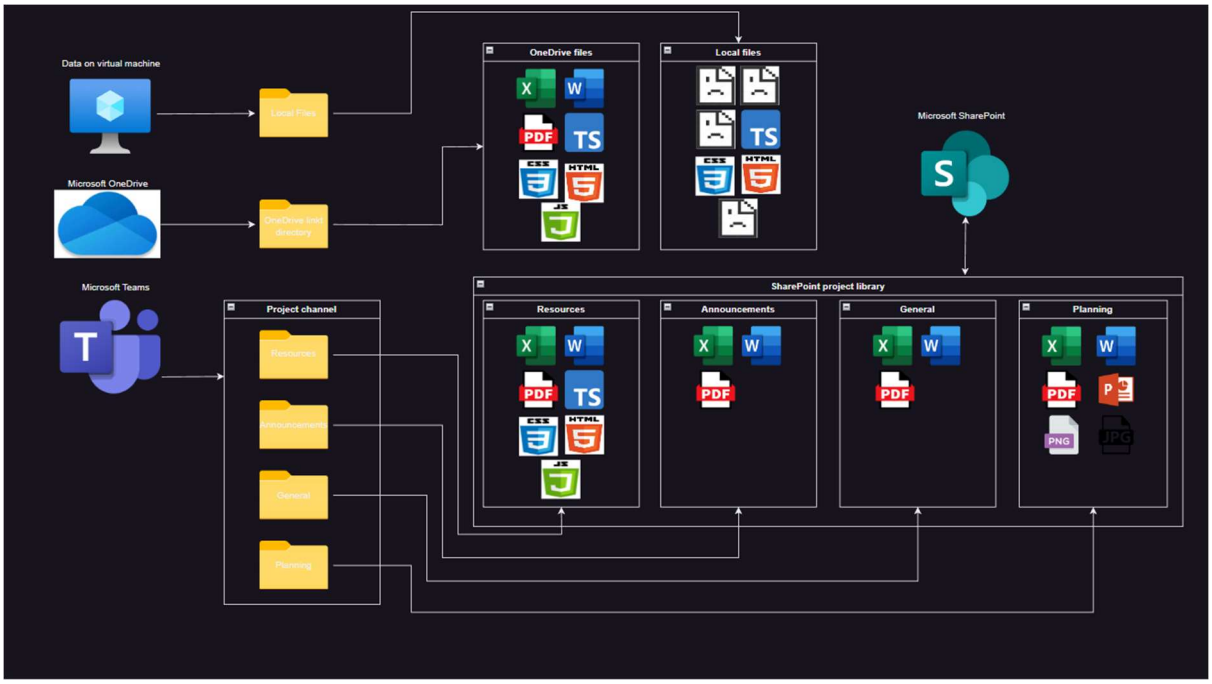



*Figure 20: State of project manager files after recovery from ransomware attack on soft deleted SharePoint site.*

**Recovery from test 2:**

Recovery from hard deletion of Teams group and SharePoint library is technically impossible, data have been permanently deleted and are unrecoverable. In such situation, its very likely that the attacker would propose to provide a copy of the files in exchange for ransom.

This test ultimately leaves the user with following data. With grant total of 10 out of 33 files usable in the end. This shows that preventing the attacker from disabling features such as soft delete is crucial.

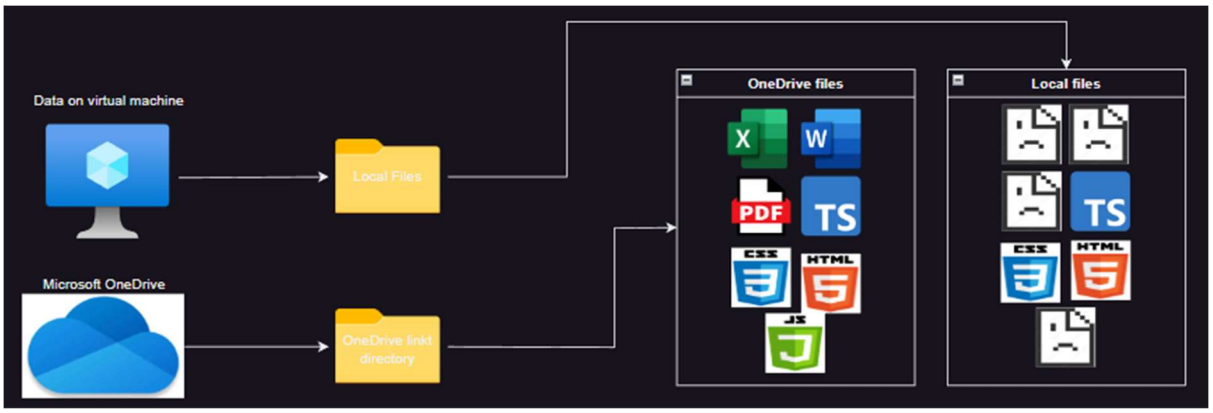



*Figure 21: State of project manager files after recovery from ransomware attack on hard deleted SharePoint site.*

### 4.1.6 Testing scenario 3

(See 3.4.3 for method)

Testing of this scenario required the same initial steps as first scenario. Since global administrator account had all possible privileges, it should be possible to finally verify if Microsoft 365 services can prevent ransomware from encrypting data in cloud, as users with highest privilege level should make the system most sensitive to abnormal behaviour indicating account compromise. Unfortunately, from results it seems that Microsoft 365 does not analyse user behaviour by default, failing to prevent an attacker from performing ransomware attack. At least that is the case for a system with small number of files like the one tested during this thesis, it is possible that if ransomware would continually make changes to cloud stored files, it would eventually trigger a response. This hypothesis is based on the fact that OneDrive seem to be able to recognize that user have most likely been a victim of ransomware recently, and it takes several minutes for OneDrive to notice.

Figure X: State of file accessible by global administrator after ransomware attack.

In this scenario, ransomware was able to encrypt 31 out of 43 files, of which 12 were not supported by the ransomware sample.

### 4.1.7 Recovery scenario 3

In this scenario it is impossible to regain data that were taken for ransom, instead I was trying to use desynchronised data from OneDrive as a form of backup, unfortunately during testing I concluded that files linked to OneDrive are in fact just a link to the data, not a literal copy of the file that would register and synchronize changes with the cloud version. As such, it is impossible to recover any data using OneDrive links. This concludes that base Microsoft 365 system does not provide any mean of recovery in scenarios where point of entry is a global administrator account. Securing accounts with high privileges should be the highest priority for a small company, as results from initial encryptions were identical for all three scenarios, results of recovery are highly diverse and seem to become progressively wors with higher privileges of compromised account.

### 4.1.8 Testing scenario 4

(See 3.4.4 for method)

Despite enabling attack surface reduction in windows defender for endpoints, it has no effect after disabling windows defender real-time protection, ransomware was till able to access files even in directories specified to deny access for applications. This means that giving user virtual machine administrator privileges can negate effectiveness of windows defender, to counter this a policy should be added to prevent users from disabling real-time protection in windows defender.

Teams and SharePoint require two factor authentication to link data with OneDrive, this means that option of linking data into OneDrive cannot be exploited to steal information. However, requirement to reauthenticate does not desynchronise or log of user from OneDrive, this means that if original user have authenticated and the authentication expired, then malicious actor will still be able to read and copy data linked to OneDrive.

Two factor authentication was able to prevent the attacker from accessing and encrypting any files except for files stored locally on the virtual machine.

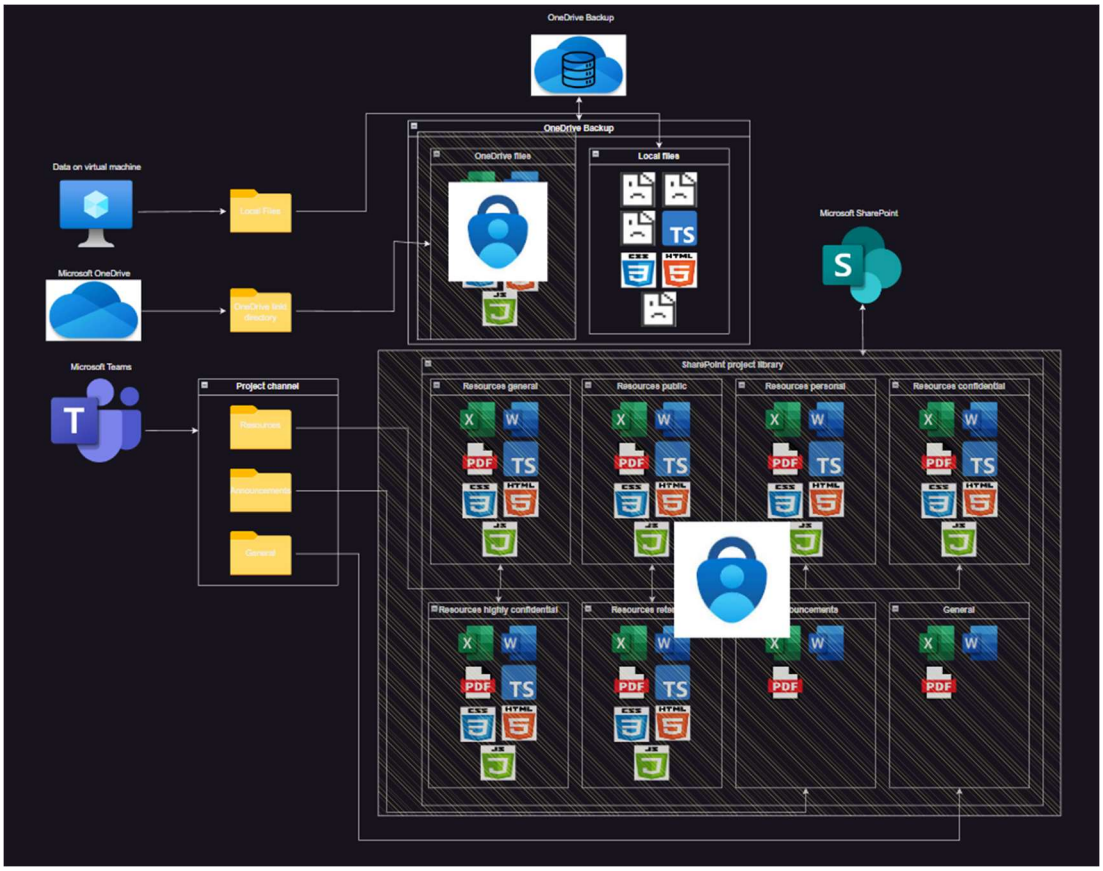



*Figure 22: State of file accessible by project contributor after ransomware attack.*

### 4.1.9 Recovery scenario 4

One additional function of OneDrive that was not explored in three first scenarios it that it allows users to create a backup of files located on Desktop, in Documents directory and Download directory. By storing local files directly on desktop, I was able to recover all encrypted local files.

### 4.1.10 Testing scenario 5

(See 3.4.5 for method)

To verify if data classification can prevent files from being encrypted, six directories were created to verify if either private, public, genera, confidential, or highly confidential labels would be able to prevent ransomware from encrypting the data. Confidential and highly confidential labelled files were returning error whenever opened by users after they were downloaded from cloud, despite that, ransomware sample was able to create a encrypted copy of the files and delete the original. After inspecting the encrypted versions of the files, file labelled confidential and file labelled highly confidential seemed to have almost nothing in common after encryption, despite having identical contents. This leads me to believe that confidential labelled files are encrypted whenever taken out of cloud storage, this does not prevent the attacker from taking away your access to the data, but it prevents attacker from accessing and selling the data on the black market.

Last label to be tested was a retention label. In this scenario, retention label was supposed to retain file for seven days after it was last modified, it functioned as intended since ransomware sample was able to create an encrypted copy of the file but was not able to delete the file afterwards.

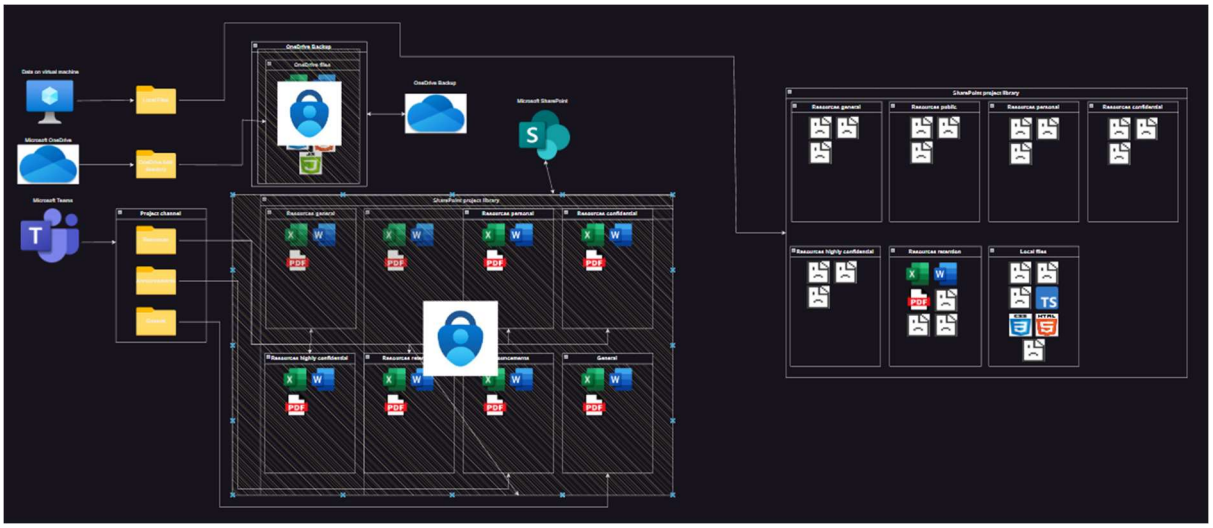


*Figure 23: State of file accessible by project manager after ransomware attack.*

### 4.1.11 Testing scenario 6

(See 3.4.6 for method)

As a final test, I decided to verify if labelling will bring different result for data in cloud, this test assumes that the attacker found a way to bypass two factor authentication on SharePoint. The assumption is also that the attacker is not able to authorize into admin center without two factor authentication. Results shown that labelling does not work differently in cloud and locally, results are identical.

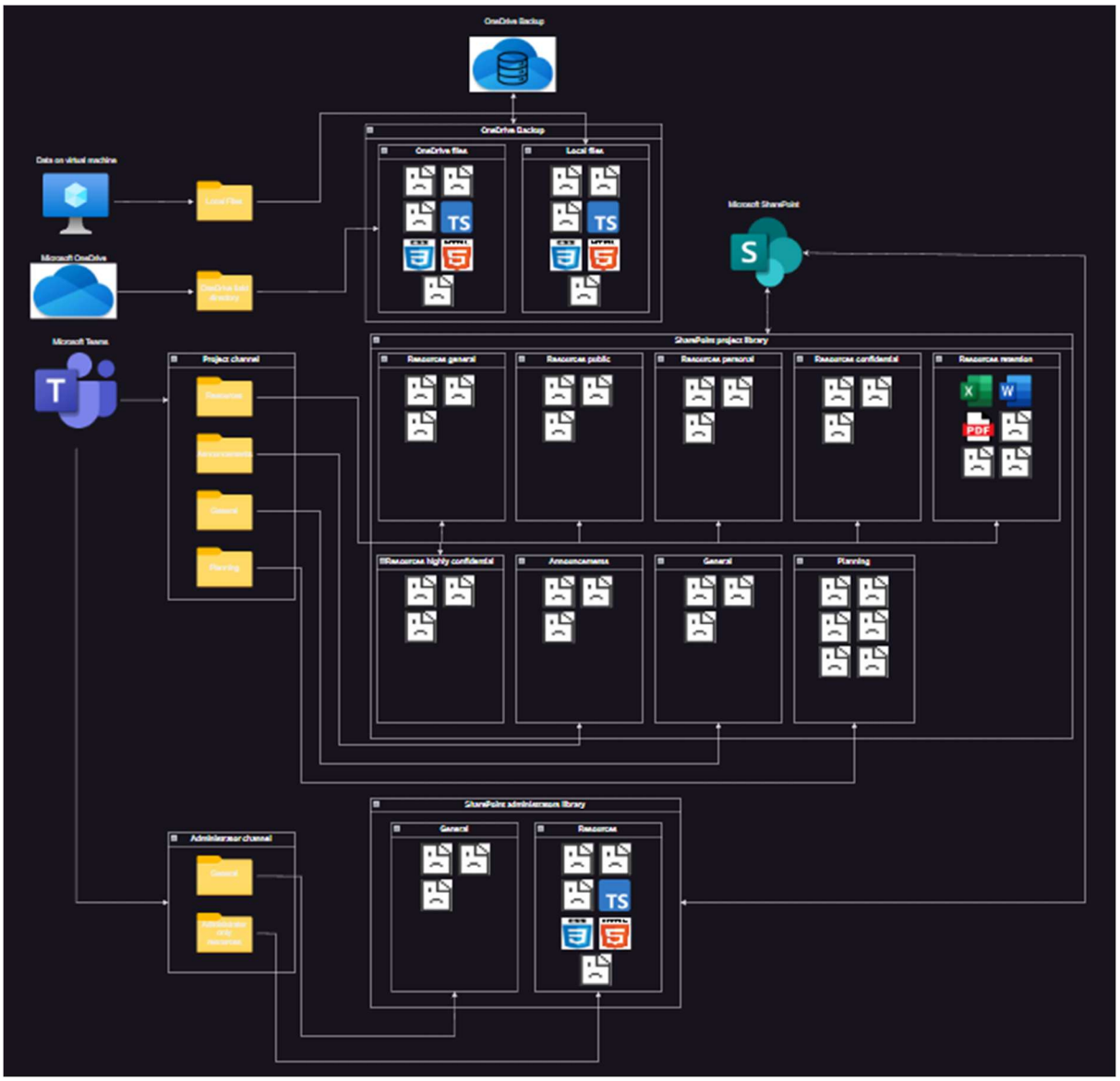


*Figure 24: State of file accessible by global admin after ransomware attack.*

### 4.1.12 Recovery scenario 6

By using recovery features from OneDrive and SharePoint paired with OneDrive backup, I was able to recover all the files to its original state.

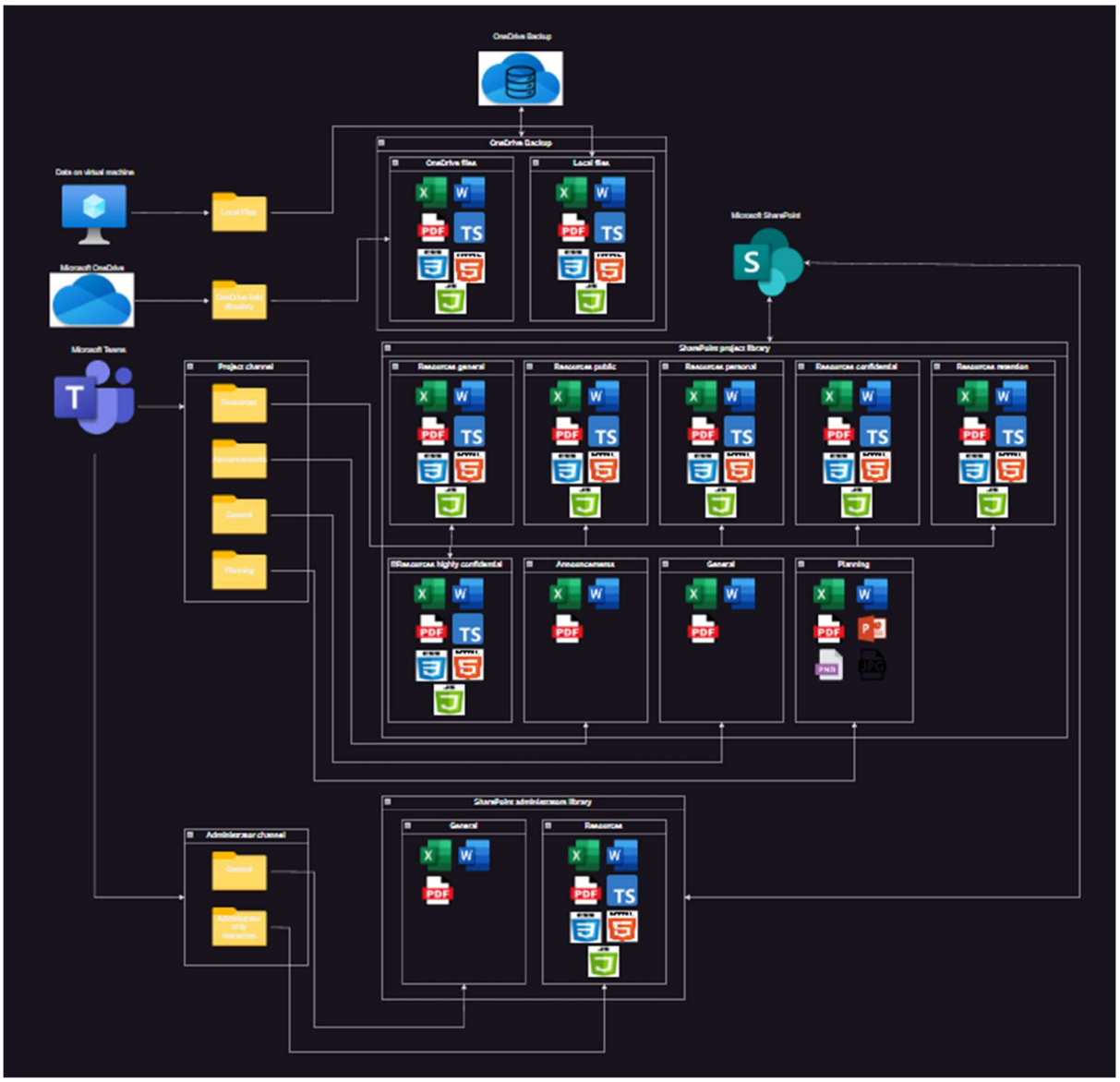



*Figure 25: State of global administrator files after recovery from ransomware attack*

# Chapter 5
# Discussion

The topic of this thesis is to analyze cloud service Microsoft 365 with regards to its resistance to ransomware, recoverability after incidents, and effort required to customise the service for company's needs. In this chapter I will discuss the results of testing and answer the research questions presented in 1.2.1.

**Research question 1**

To what degree does customisability of Microsoft 365 affects resilience to ransomware?

**Research question 2**

To what degree is Microsoft 365 service capable of protecting customers data?

Based on my findings in chapter four, I will discuss effectiveness of the two systems that were tested. I will use this discussion to identify the most relevant findings to best answer research questions.

## 5.1 Discussion on default Microsoft 365 services

Let's begin by seeing that Microsoft 365 at its core is a package of interconnected tools, and tools tend to perform better in hands of experienced users, they are also more likely to break in hands of an amateur.

With that being said, based on the findings from chapter four, the biggest contributing factor that causes an increase in unrecoverable damage were the privileges that compromised account was assigned at the time of the attack. Microsoft 365 in its default state is unable to prevent ransomware from encrypting any data, as it seems to greatly rely on Windows Defender for protection against malware and viruses.

One feature that is not a part of default Microsoft 365 and could greatly counteract effects of ransomware within the cloud, is a pattern recognition-based isolation. The general logic behind pattern recognition system is that we as humans do things way differently and work less efficiently than machines. Likelihood of a legitimate user making changes to over one hundred different files within a single minute is very low, this paired with one or several patterns such as:

- Changes done to every file name uses identical string, for example changing "taxes" into "taxes_wancy"
- Each affected file has its name exclusively elongated
- Changing every file type into identical type, for example from "taxes.txt" into "taxes.txt.wanncry"
- Affected files have their size exclusively increased

This feature would at the very least slow the attacker, thus giving administrators time to counteract, or in the best-case scenario would prevent the attacker from encrypting data in cloud, by temporarily revoking privileges of the compromised account.

On a positive note, the default Microsoft 365 seems to be great at preventing data loss when the compromised account has little privileges. Recovery systems of SharePoint and OneDrive seem to work exceptionally well, since recovery for small system like the one being tested during this project, takes less than five minutes, and lets users return to the precisive point in time. Changes done within OneDrive and SharePoint seems to be recorded like a differential backup, this may complicate the recovery if anyone makes significant changes during the ransomware attack, as reversing changes to a point before ransomware attack will also reverse all other changes to that point. Lastly, SharePoint and OneDrive retain the change log for its recovery system for over 30 days, it is rather unlikely that a victim of ransomware attack would not notice what happened in time, especially since OneDrive is able to notice and notify user about the attack.

To summarize, base Microsoft 365 offers little resilience if we exclude Windows defender, but dissent recoverability for services like OneDrive and SharePoint.

## 5.2 Discussion on Microsoft 365 customizability

If Microsoft 365 would have to be described in one word, this word would be “customizable”. This service is in fact so customizable, that describing each option could make for a bachelor project by itself. With that being said, the difference of resilience in a default and custom Microsoft 365 environment is noticeable even with very few changes being done.

Let’s discuss the most impactful security feature that was added to my custom Microsoft 365 environment first, that is conditional access or more precisely two factor authentication. Microsoft’s two factor authentication is very reliable, that is because you cannot accidentally approve it. Many two factor authentication apps will simply ask you if you approve or deny the authentication, giving you opportunity to accidently approve the attacker, while Microsoft will ask you for a number that’s shown only to the person authenticating. Additionally, two factor authentication will notify user about the potential threat, exposing attacker and providing evidence of account compromise to the user. Enforcing two factor authentication exclusively onto SharePoint also prevented attacker from using OneDrive and accessing files through Teams, reducing attack surface area to local files only.

Otherwise attack surface reduction and controlled folder access ended up as the greatest disappointment during testing. Just to clarify, I do not mean that these are useless or meaningless, but since both are directly tied to Windows defender, they ended up disabled by the attacker each time. If it is possible to enforce two factor authentication before disabling windows defender, then attack surface reduction would probably become the second most impactful feature in my custom Microsoft 365 environment.

My opinion on labels is mixed, retention label was useful in my experiments but that is the case because the ransomware sample would replace files rather then encrypt them. Sensitivity labels were also unable to prevent ransomware from either reading or deleting the files. After encryption, I inspected the encrypted files and found that two identical files with different labels had different contents. I have two different theories for why it’s the case, first theory is that this ransomware sample would print meta data into the file, second theory is that ransomware was unable to read the contents and only written encrypted metadata into the new file. The difference between those two theories is significant because one claims that the attacker can access confidential data despite the

label, rendering labels useless against ransomware attacks, while the other theory claims the opposite.

The only feature affecting recoverability that I implemented into my custom Microsoft 365 environment was OneDrive backup, as it can backup files that are stored in either Documents directory, Downloads directory and on Desktop. As someone who have previously made 3d models as a hobby, I cannot stress enough how important the Documents directory is on Windows systems, it is a default storage location for many applications, losing it can cost hundreds of man-hours. Overall, improved resilience caused recoverability to be less significant during testing of custom Microsoft 365 system, but backup for OneDrive managed to cover for whenever system failed to prevent encryption.

It is rather hard to define if Microsoft 365 is hard or easy to customize, since this is dependant on the changes that you wish to make. As an example, with a little google search and around ten minutes of my time, I was able to enforce two factor authentication on SharePoint for selected users. As a counter example, I was unable to enforce two factor authentication for users whenever they make changes to Windows defender. Fortunately, Microsoft offers alternatives, such as multi factor authentication for remote desktop services that can become a substitute. With that being said, there are many features that can be enabled with few mouse clicks, and there are some features that require a custom XML file to function, in general I would say that features impactful for this project were not hard to implement. The number of features that can be added or customized in Microsoft 365 is overwhelming, this can discourage newcomers from experimenting and perfecting theirs Microsoft 365 environment, to prevent that focus on the needs of the company first and making small and gradual changes.

The end result is that with very few changes, this Microsoft 365 environment became fairly resilient to ransomware and its recoverability expanded in coverage.

## 5.3 Research questions

The purpose of this project was to answer the research questions from chapter 1.2.1, by using my experience with Microsoft 365 and its customization.

### 5.3.1 Research question 1

**To what degree does customisability of Microsoft 365 affects resilience to ransomware?**

There are many ways to protect your environment from threats, and Microsoft makes it simple to make first steps towards improving data security, since if done correctly, resilience of Microsoft 365 environment will drastically improve just like shown in this thesis. Not every custom Microsoft 365 environment will be equally resilient, and more importantly attacks will most likely be very distinct, as ransomware groups put a lot of time, money, and effort into development of more efficient and more likely to succeed techniques of attack.

Just like malicious actors, so should businesses invest money, time, and effort into creating more reliable and resilient systems, applications, and workspaces. A small change like adding two factor authentication can have enormous effect on environments resilience in some scenarios, but it brings no benefits if user runs malicious code after two factor authenticating. In contrary to results of this thesis, if scenarios would focus on malicious code executed by legitimate user, then windows Defender and attack surface reduction would in theory have the greatest impact on environments resilience and two factor authentication would have no impact whatsoever.

In summary the aspect of customisability that Microsoft 365 provides, greatly affects resilience against threats like ransomware. It can be compared to building a wall that protect companies digital assets, I should protect from all sides and will always be as strong as its weakest point.

### 5.3.2 Research question 2

**To what degree is Microsoft 365 service capable of protecting customers data?**

The threat of ransomware is constantly evolving, there is always a possibility that a new vulnerability, software or undefined factor will enable malicious actors to wreak havoc and profit from it. Which is why, those responsible for data security need to constantly improve unless they want to be taken advantage of.

There are multiple variables that can impact the results of an attack, for example an attacker could use more capable ransomware, one that could exploit a new vulnerability to spread and run itself on every company's machine, a hypothetical day zero vulnerability like this would be impossible to protect against, unless system is customized to be very strict and highly sensitive for such exact situation. Microsoft in a literal sense let you dictate rules on your Microsoft 365 environment, and by this definition an administrator can prevent any attack if properly prepared for it, the only limiting factors are time, money, personnel skill level, and how big reduction in availability company is willing to tolerate.

To protect the business from attacks, there are three fundamental steps that each company should make, first one is to incrementally remove the risk by focusing on attack surface reduction, secondarily to limit the scope of damage by mitigating lateral traversal and implementing end to end session security, then lastly to prepare for recovery by creating secure backups and prepare for highly disruptive recover from zero scenarios.

Microsoft is a highly reliable company with good reputation, and its service Microsoft 365 is as capable of protecting customers data as users will allow it to be. Meaning that Microsoft 365 can protect customers data, given that its security features are implemented correctly. Very few features are universally effective, and administrators should prepare for all types of attack equally since digital security is like a chain, and a chain is as strong as its weakest link.

## 5.4 Future work or Limitations

This thesis explored several customization options that I considered to be the most impactful for Microsoft 365 environment, due to time constrains scope of the thesis was limited to the selected few. I decided to add a list of some features and threats I chose not to explore due to time limitation.

**Use of "Cerber" ransomware sample:** Some tests like for example sensitivity labels have given me unclear results, performing tests using multiple ransomware samples could present different results and more data to analyze.

**Life monitoring and protection:** Microsoft has an impressive catalogue of monitoring tools, they could greatly help in recognizing ransomware attack attempts and would shorten preparation time for a attack.

**Use of more advanced Ransomware:** This thesis would greatly benefit from a modernised version of ransomware, as old samples were easily recognized by Microsoft defender and promptly quarantined. By using a ransomware never reported to Microsoft, I could test the life-protection feature of Microsoft defender and more thoroughly test attack surface reduction.

# Chapter 6: Conclusion

## 6.1 Summary

In my thesis answered two research questions. To what degree does customisability of Microsoft 365 affects resilience to ransomware, to what degree is Microsoft 365 service capable of protecting customers data?

I have described and presented the threat that ransomware poses, and some ways to customize Microsoft 365 environment to increase resilience, limit scope of damage, and expand recoverability. Based on this, I performed six different attacks within six different scenarios to present how Microsoft 365 performs. These attacks provided me with insight into which features have the greatest impact on human-operated ransomware attacks.

The key feature during testing was two factor authentication, as it functioned like secondary layer of role-base access control and eliminated the single point of failure with was credential based authentication. My findings show that customizability of Microsoft 365 can increase security as evident when comparing results from scenarios, as results from first three scenarios varied considerably in comparison to last three scenarios.

## 6.2 Future developments

There is a steep competition between malicious actors and developers of security features, as malicious actors are always exploring new ways to wreak havoc by exploiting vulnerabilities and attempting to make profits out of it. As developers implement new features and patch vulnerabilities in the system, so does ransomware evolve to seek new vulnerabilities to exploit.

We cannot predict the future, systems are constantly growing in number, size, and complexity, while malware explores vulnerabilities that are made in the process. We cannot prevent all attacks, sooner or later a malware or a virus will manage to breach the security, and the only think we can really do is prepare for it.

## 6.3 Greater context

This thesis only scratches the surface of what Microsoft 365 is capable of, there are numerous features that can become a deal breaker when it comes to preventing ransomware. There are many factors that can contribute to security systems failure, some of these are out of companies control, like human factors. We cannot control other humans, we can only encourage and educate them by maintaining security focused mindset to prevent human error.

Due to shir size, configuring Microsoft 365 environment can seem overwhelming, but by making constant improvements over a long period of time, even a small team can greatly improve security over time. Digital systems must be secured to the best of the ability, since the system must be able to prevent every attack, and malicious actors may only need to breach the system once.

# Bibliography


Admin, Cyber. ‘New Cybereason Ransomware Study Reveals True Cost to Business’. Accessed 19 May 2023. https://www.cybereason.com/press/new-cybereason-ransomware-study-reveals-true-cost-to-business.

Asana. ‘How Sunk Cost Fallacy Influences Our Decisions [2022] • Asana’. Asana. Accessed 19 May 2023. https://asana.com/resources/sunk-cost-fallacy.

‘Back up and Restore in SharePoint Online - Microsoft Q&A’. Accessed 19 May 2023. https://learn.microsoft.com/en-us/answers/questions/348043/back-up-and-restore-in-sharepoint-online.

chrfox. ‘How to Use the Microsoft Data Classification Dashboard - Microsoft Purview (Compliance)’, 17 February 2023. https://learn.microsoft.com/en-us/microsoft-365/compliance/data-classification-overview.

———. ‘Learn about Sensitive Information Types - Microsoft Purview (Compliance)’, 25 April 2023. https://learn.microsoft.com/en-us/microsoft-365/compliance/sensitive-information-type-learn-about.

Dansimp. ‘Enable Controlled Folder Access’, 17 May 2023. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-controlled-folders.

———. ‘Understand and Use Attack Surface Reduction (ASR)’, 8 March 2023. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/overview-attack-surface-reduction.

denisebmsft. ‘Turn on Exploit Protection to Help Mitigate against Attacks’, 3 May 2023. https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/enable-exploit-protection.

gmcdouga. ‘The New Ransomware Threat: Triple Extortion’. Check Point Blog, 12 May 2021. https://blog.checkpoint.com/security/the-new-ransomware-threat-triple-extortion/.

Google Cloud. ‘What Is Cloud Storage & How Does It Work?’ Accessed 19 May 2023. https://cloud.google.com/learn/what-is-cloud-storage.

‘How Versioning Works in Lists and Libraries - Microsoft Support’. Accessed 22 May 2023. https://support.microsoft.com/en-us/office/how-versioning-works-in-lists-and-libraries-0f6cd105-974f-44a4-aadb-43ac5bdfd247.

https://techcommunity.microsoft.com/t5/user/viewprofilepage/user-id/33926. ‘New Updates to OneDrive and SharePoint Team Site Versioning’. TECHCOMMUNITY.MICROSOFT.COM, 14 June 2018. https://techcommunity.microsoft.com/t5/Microsoft-OneDrive-Blog/New-Updates-to-OneDrive-Versioning/ba-p/204390.

‘Introduction to Zero Trust’. Accessed 19 May 2023. https://www.ncsc.gov.uk/collection/zero-trust-architecture/introduction-to-zero-trust.

Justinha. ‘Azure AD Multi-Factor Authentication Versions and Consumption Plans - Microsoft Entra’, 30 January 2023. https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-licensing.

kh4sh3i. ‘Ransomware-Samples’, 8 May 2023. https://github.com/kh4sh3i/Ransomware-Samples.

Konheim, Alan G. *Computer Security and Cryptography*. John Wiley & Sons, 2007.

Meland, Per Håkon, Yara Fareed Fahmy Bayoumy, and Guttorm Sindre. 'The Ransomware-as-a-Service Economy within the Darknet'. *Computers & Security* 92 (1 May 2020): 101762. https://doi.org/10.1016/j.cose.2020.101762.

MicrosoftGuyJFlo. 'What Is Conditional Access in Azure Active Directory? - Microsoft Entra', 28 February 2023. https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview.

'Protecting Against Cyber Threats to Managed Service Providers and Their Customers | CISA', 11 May 2022. https://www.cisa.gov/news-events/alerts/2022/05/11/protecting-against-cyber-threats-managed-service-providers-and-their.

'Ransomware: Paying Cyber Extortion Demands in Cryptocurrency'. Accessed 19 May 2023. https://www.marsh.com/us/services/cyber-risk/insights/ransomware-paying-cyber-extortion-demands-in-cryptocurrency.html.

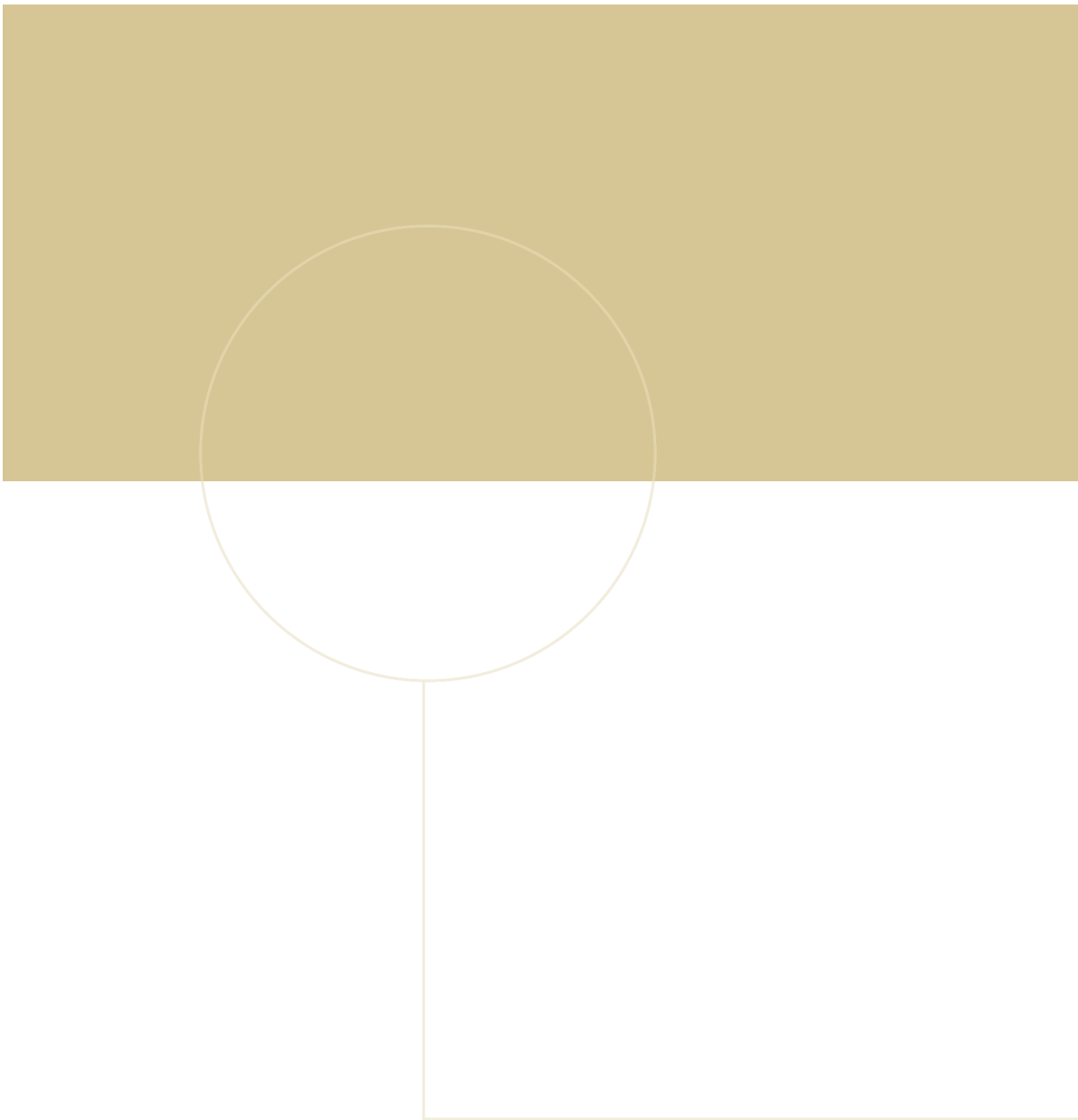
'Recover Lost Files on Windows 10 - Microsoft Support'. Accessed 19 May 2023. https://support.microsoft.com/en-us/windows/recover-lost-files-on-windows-10-61f5b28a-f5b8-3cc2-0f8e-a63cb4e1d4c4.

Wallen, Dave. 'Types of Backup: Full, Differential, and Incremental'. Spanning, 31 March 2020. https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/.

'What Is OneDrive for Work or School? - Microsoft Support'. Accessed 19 May 2023. https://support.microsoft.com/en-us/office/what-is-onedrive-for-work-or-school-187f90af-056f-47c0-9656-cc0ddca7fdc2.

'What Is SharePoint? - Microsoft Support'. Accessed 19 May 2023. https://support.microsoft.com/en-us/office/what-is-sharepoint-97b915e6-651b-43b2-827d-fb25777f446f.

'Zero Trust Architecture Design Principles'. Accessed 19 May 2023. https://www.ncsc.gov.uk/collection/zero-trust-architecture.



NTNU

Norwegian University of
Science and Technology