Project Report

UNIVERSITY OF TWENTE.

Enterprise Security

Recommendations for Enhanced Security Measures at the Municipality of Wassenaar: A Case Study

Presented by:
Charumathi Palanikumar, Héloïse Garion, Lucille Aubry, Marzieh Adineh,
Medha Varsha Alur Mahesh, Ruben van Zenden, Shruthi Sajid, Sneha Ramesh

Recommendations for Enhanced Security Measures at the Municipality of Wassenaar: A Case Study

Charumathi Palanikumar
s2545160
c.palanikumar@student.utwente.nl

Héloïse Garion
s2875470
h.garion@student.utwente.nl

Lucille Aubry
s2885670
l.r.a.aubry@student.utwente.nl

Marzieh Adineh
s2548690
m.adineh@student.utwente.nl

Medha Varsha Alur Mahesh
s2505185
m.v.alurmahesh@student.utwente.nl

Ruben van Zenden
s2596628
r.vanzenden@student.utwente.nl

Shruthi Sajid
s2551993
s.sajid@student.utwente.nl

Sneha Ramesh
s2471469
s.ramesh-1@student.utwente.nl

***Abstract*— In today's world, security issues continue to shroud almost every organization, including municipalities. Even companies with the right amount of budget struggle to cope with the ongoing security and privacy demands. Mitigating cyber and security risks for municipalities can be as simple as focusing on password and email security, having a strong recovery plan, developing a set of security and focused KPIs. Furthermore, monitoring the KPIs by means of interactive dashboards and improving employee education or as involved as reshaping an organization's security posture from top-down. This paper carefully elucidates and outlines the security issues faced by the municipality of Wassenaar and attempts to provide a set of solutions (as described above) for the issues described by the teams VNG and the municipality of Wassenaar. Implementing these solutions will manifest as easy wins and can greatly make the municipality's system more resilient to cyber crime, while significantly reducing the risk of human error. Lastly, the use of Privacy-as-a-Service is proposed which can increase the organization's security, while bringing in new technology, reducing the need for man-power and justifying costs to a great extent.**

KEYWORDS- *Municipality, Security, Privacy, Cyber crime, Privacy-as-a-Service*

1. Introduction

It is no secret or surprise that a municipality has large amounts of information, and specifically the very sensitive Personal Identifiable Information (PII). This data is heavily tasked with directing vital services, managing critical infrastructure and responding to the needs of a demanding constituency [15]. That being said, municipalities, like any other organization, are vulnerable to cyber threats, that have increased with the COVID-19 pandemic. Among these cyber threats, the well-known and still escalating ransomware attacks appear to be widely used to target municipalities. Indeed, a research conducted by *Barracuda Networks* in 2020 indicated that a whopping 44% of global ransomware attacks in 2020 targeted municipalities.

A more in-depth look into such attacks against municipalities unearthed many more shocking revelations. A whitepaper by *Knowbe4* (a popular integrated security awareness training and simulated phishing platform) specifies that about 50% of states do not have a committed cybersecurity budget. Even more worrisome is the fact that 37% of states have seen a reduction in funding or no change in budget allocations at all. The lack of funding translates to municipal Information Technology (IT) systems being put at risk to increasing cyber threats because of the easiness of the attacks [20].

However, municipalities must comply to regulations such as GDPR, to protect consumers' identifiable information and foresee the consequences of such attacks. These are disastrous, as they can cause the government to bear costs worth millions of euros. In 2020, a group of hackers that attacked the servers of the Overijssel municipality of Hof van Twente and took its backups for ransom, demanded 750 thousand euros from the municipality for the backups to be released [33]. More than the monetary losses, long-term effects are often loss of reputation and a liability that can linger on for years.

Naturally, almost all municipalities recognize these security concerns and are making fastidious efforts to mitigate them. However, municipalities face a lot of revenue leakages such as maintenance of public property, reimbursements, fines due to lack of compliance to regulations etc. Due to this, it is often challenging to convince the senior management that security and privacy are indeed serious issues that need attention, even if they do not create any revenue and/ or business value [11]. This is yet another aspect that we explore as part of this project - *How do we effectively convince the management that investing in security is urgent and need of the hour?* This forms the main foundation of our research question as discussed in Section 2. This project is tackled as a specific usecase study of the municipality, as the business processes in every municipality could be different.

The remainder of this paper is organised as follows: Section 2 describes the the case, followed by the adopted Research Design and Methodology in Section 3. Following this, the potential vulnerabilities are assessed and an Attack Tree is depicted in Section 4. A step-by-step recovery plan and PaaS tools is discussed in Section 5. Section 6 discusses KPIs and relevant dashboards. In Section 7, we propose Privacy-as-a-Service solution to outsource security solutions to trusted providers. We then discuss methods to prevent human errors in Section 8, while summing up our work and elaborating on future research possibilities in Sections 9 and 10 respectively.

2. Case Description

As introduced in Section 1, this paper is very specific to the municipality of Wassenaar. The details regarding data collection, functioning, vulnerabilities were elucidated by the Chief Information Security Officer at the municipality of Wassenaar and a team of experts at *VNG* (Vereniging van Nederlandse Gemeenten or the Association of Dutch Municipalities).

A series of discussions and interviews provided us with the in-depth knowledge about the current security system at the Municipality of Wassenaar. The services offered by them is similar to the services offered by any other municipality. They are responsible for urban planning, housing traffic and transport related services, education (management of local public schools) and basic city services such as sanitation, water, electricity, food inspection, etc.

Firstly, the municipality of Wassenaar complies with 90 out of 137 measurements described in the BIO. or the Baseline Information Security framework. The BIO is a common framework of standards for information security within the entire government. Due to a common effort, it is now the sole baseline for the entire government. The BIO is based on internationally accepted standards and best practices in information security, such as ISO 27001 and ISO 27002 (ISO 27000 series) [34]. It is also important to note that compliance with the BIO is an important obligation for every municipality. The advantages of having a common baseline for security has the following advantages, according to the Dutch government:

1) Improved chain coordination between governmental and other parties will enhance information security.
2) The administrative burden for government and businesses, both on the supplying and receiving end, will decrease when unified security standards are implemented throughout the government.
3) Compliance with international regulations and standards.
4) Lesser maintenance costs.
5) Risk management and mitigation can be mapped and carried out in a structured manner.

Secondly, just like other governmental organizations of today, the municipalities make use of IT systems to improve efficiency, productivity and better decision-making. Some of these systems include ERP, performance management software systems, financial management/accounting systems, purchase order systems, citizen relationship management systems, etc. It is of prime importance to ensure these systems are secure because they contain sensitive and confidential information. As a preliminary security measure, all employees and staff are provided with work laptops and mobile phone, with Multi-Factor Authentication (MFA) for all the devices and portals.

Thirdly, the municipality of Wassenaar needs to ensure that all important data and systems are routinely backed up so that in the event of ransomware attack, server crash or other security breaches, there will be no data loss. These backups can be done in multiple ways: on-premise (using external devices such as hard drives and flash drives) or off-site using a reliable cloud provider. The municipality does indeed outsource backups to a reliable and certified third party provider.

Fourthly, routine security patches and updates on all devices, hardware and applications such as antivirus software, operating systems, etc. Municipalities should also increase awareness of performing regular security checks and updates among all employees having access to the systems. Recently, the security team at the municipality of Wassenaar was working hard to fight the Log4j [21] vulnerability that quite lately took the tech world by a storm.

Lastly, the crucial points mentioned by the team during the interviews was that:

1) While the security team has the budget to invest in latest, cutting-edge tech solutions, they are often faced with a dilemma of making investments. This is mainly due to the fact that the team feels that such investments bring with it the requirement of the right kind of human resource, equipped with the necessary technical skillset. Apart from being a security issue, this also translates into a human resource issue.
2) Security threats are rising on the agenda of upper management, but as return on investments are often invisible it does not have the priority the security team would want it to have.
3) The municipality of Wassenaar has quite a strong external security system, but a rather weak internal security system. This means that an attacker would initially find it difficult to penetrate into the IT landscape. But once this is done, the attacker can easily bring down the entire architecture, given its current strength, maturity and resilience.

Based on the points discussed above, we attempt to address the requests of VNG and the municipality of Wassenaar. However, our main research question is: **What are effective ways to communicate about the importance security with the upper management management?**

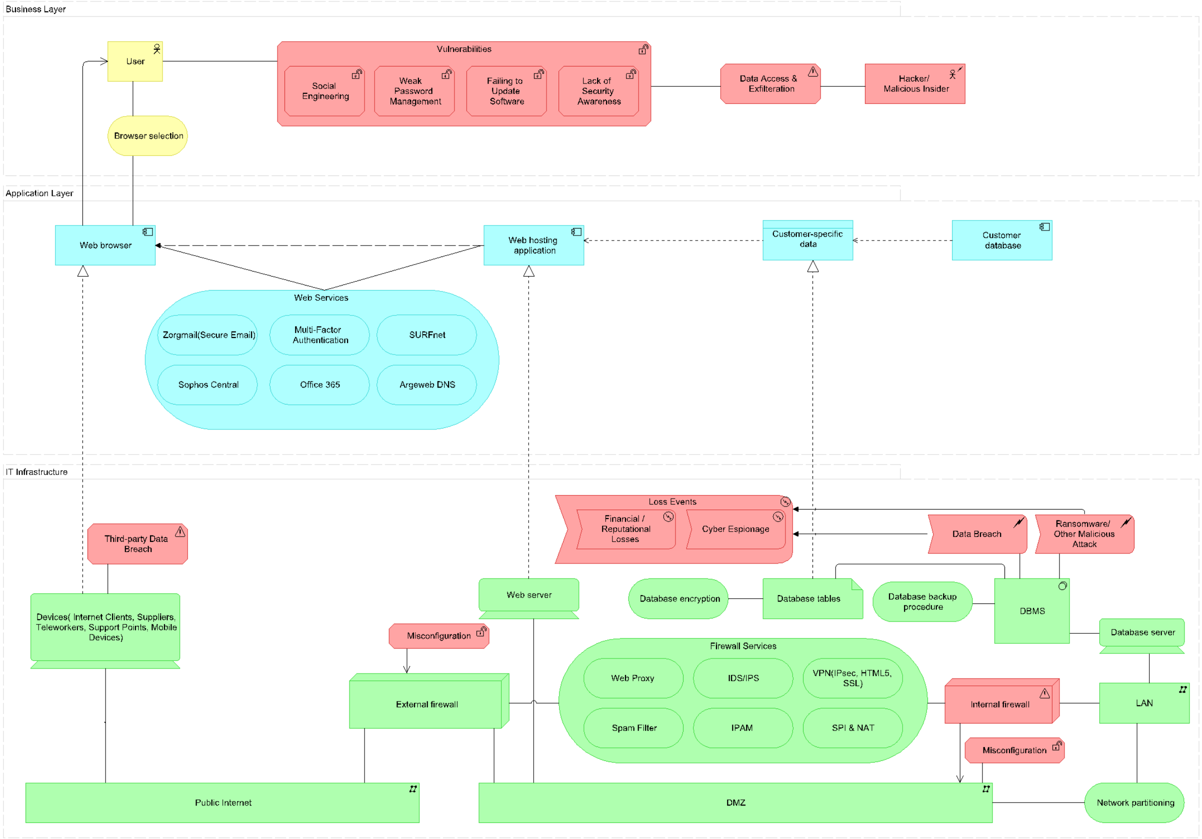


Figure 1. IT Architecture and the associated risks, vulnerabilities, threat agents and threat events

In order to tackle this research question we should address the following sub-questions:

1) What are the vulnerabilities for the Municipality of Wassenaar?
2) How can we show the management the benefits of investing in security from a business perspective?
3) What is the most efficient and effective way to develop a Disaster Recovery Plan?
4) What are the reactive and preventive strategies in case a cyber attack occurs?
5) How can human errors best be prevented?

To sum up, the case is quite complex and interesting, and requires immediate attention, as it involves large amounts of public data. The research question and the asks of the municipality of Wassenaar and VNG will be addressed in this report. Figure 6 in Appendix 1 depicts the capabilities, goals and targeted outcomes from this project. Figure 1 depicts the IT Architecture that is currently present at the municipality of Wassenaar and the associated risks, vulnerabilities and threat agents/ events (highlighted in red).

The following section discusses our research approach and the methodology that we used for achieving results for this project.

3. Research Design and Methodology

The project was carried out as a case study that was built based on semi-structured interviews with the CISO of the municipality of Wassenaar and a team of security experts at VNG.

VNG and the CISO of the municipality of Wassenaar provided us with all the necessary information and also shared formal documents such as analysis, penetration testing results, existing recovery plan etc. All this information formed the basis for our research however, references cannot be made since the documents are highly confidential. Based on all the inputs provided, we created an Attack Tree (As depicted in Section 4 using the Mitre framework [22]. KPIs/ KRIs were identified [18] and dummy data for the dashboards was created because the municipality of Wassenaar is currently not tracking the required data. The dashboards were built using Tableau Desktop [31].

The following sections discusses the vulnerabilities and details these in the form of an Attack Tree.

4. Vulnerabilities at the municipality of Wassenaar

The municipality provided us with a set of two documents (a risk analysis and a pentest) for assessing the vulnerabilities. We also had the inputs from the CISO, Theo Snellen, who provided us with an overview of the vulnerabilities. In the risk analysis document, the threats are categorised into four sections: Personnel Security, Information and Communication Technology (ICT), Physical Security, and Policy and Organization. Among these, Personnel Security and Physical Security were not highlighted by Theo Snellen and VNG, during the discussions/ interviews. Indeed, they consider ICT as a more important concern, given the current level of security. The major issue in the last section of the risk analysis document, Policy and organization, is more related to the difficulty to communicate between management and the security divisions. As mentioned in Section 2 this is one of the major problems we address as part of this paper.

Looking a little deeper into the risk analysis document, according to the ICT section, the biggest risks are:

1) Insufficient monitoring and action on vulnerabilities
2) Malware
3) Hacking
4) Unsafe behaviour of employees
5) Insufficient capacity and training for ICT

In this list, the last two vulnerabilities are based on human errors. The second one, malware, is seen as a very important risk which includes ransomware. Ransomware is the most known example of malware because of its availability to hackers: every hacker can buy ransomware as a service. It is capable of revealing data. Not only VNG and the municipality sees ransomware as a pressing risk also the mayor of The Hague, from his position of chair of the VNG, wrote a letter urging to protect against ransomware. This is why we decided to focus on it.

Moreover, if the management understands the urgency of acting against ransomware, it can be a real improvement for global security. Indeed, tackling ransomware involve reducing the number of security issues thus reducing other risks. For example, the hacking risk would lower, because there would be more surveillance for breaches. In addition, a hacker often uses malware to enter the system, thus tackling ransomware will reduce the hacking risk. The insufficient monitoring and action on vulnerabilities risk would also lower, as action would be taken to reduce the risk that a ransomware enters and develops in the current vulnerabilities of the system.

4.1. Ransomware Attacks: Principle

As said before, ransomware is a type of malware, that is, a program or software that is executed in a system to cause damage or aim at extracting information to damage a system. More specifically, once ransomware is introduced into the system, it encrypts all data, resulting in unusable files [7], [3]. Then, the hackers behind the ransomware ask for ransom in exchange for decryption. On one hand, if the ransom is not paid, hackers often threaten to sell or leak the exfiltrated data or authentication information. On the other hand, if paid, the victims have no guarantee that they will decrypt the files and not sell the data. In addition, often, the company paid an insurance to be compensated for damages in case an attack happens. But when the company pay the ransom, insurances refuse to pay for damages, therefore, they lose more money. The conclusion of this is that no victim should pay the ransom, never.

However, the consequence is disastrous: the company loses all its data. Therefore, victims must be prepared for ransomware attacks, having backups for the data (offline, done periodically) and processes to rebuild the system, from scratch if necessary, using a recovery plan. For VNG and the municipality, this recovery plan has to be updated as it does not cover the worst case scenario, that is, when the system has to be rebuilt entirely.

That is why, in this project, we also make a proposal for the recovery plan, in addition to mitigating the initial risk by proposing solutions like Privacy as a Service (PaaS) and solutions to prevent human errors.

4.2. Ransomware Attacks: Consequences

As mentioned in Section 4.1, if there are no backups, the company loses its data. Furthermore, if they are leaked to the public, its reputation is also affected. They may also have to pay a fine for non-compliance with regulations such as GDPR. A good way to understand to what extent ransomware can affect organizations is to present two examples of ransomware: WannaCry (2017) and Conti (2019). These are described in detail in the following paragraphs.

WannaCry is a ransomware containing worm-like features which allow it to spread across the IT system of the network. The $300 ransom had to be paid in bitcoin. If not paid after three days, it became $600. It affected more than 150 countries and 230 000 computers. The estimated amount of money earned is around $4 billion [19].

Conti is a Ransomware-As-A-Service which targets big companies in the retail, manufacturing and construction sectors, and governments from North America and Europe. The data stolen are published on their website [10]. According to [12] between July 2021 and November 2021 it made at least 130 victims and earned around 7$ million in bitcoin.

4.3. Ransomware Attacks: the Attack Tree, or Origin of the Attack

In order to explain how a ransomware attack can occur in the municipality, an attack tree is created see Figure 2. An attack tree is a conceptual diagram used to explain how an asset or target (e.g. a person or enterprise) might be attacked. The root of the tree in Figure 2 is the encryption of data in order to ask for money. According to SocRadar [30], Barker

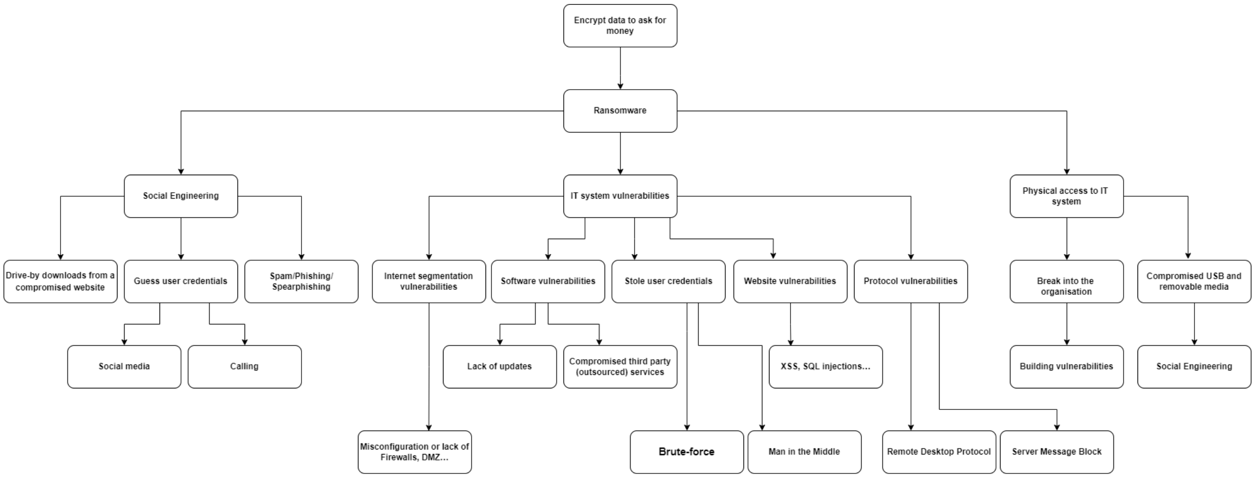

Encrypt data to ask for money
Ransomware
Social Engineering
IT system vulnerabilities
Physical access to IT system
Drive-by downloads from a compromised website
Guess user credentials
Spam/Phishing/ Spearphishing
Internet segmentation vulnerabilities
Software vulnerabilities
Stole user credentials
Website vulnerabilities
Protocol vulnerabilities
Break into the organisation
Compromised USB and removable media
Social media
Calling
Lack of updates
Compromised third party (outsourced) services
XSS, SQL injections...
Building vulnerabilities
Social Engineering
Misconfiguration or lack of Firewalls, DMZ...
Brute-force
Man in the Middle
Remote Desktop Protocol
Server Message Block

Figure 2. Attack Tree

[4], Mitre [23], and Challita [6], there are three ways for this kind of attack to be successful:

Social Engineering: downloading of malicious files from compromised websites, spam, phishing, spear phishing or guessing of a user's password (e.g. via social media or a call).

Vulnerabilities in the IT system: it can come from a vulnerability in the network architecture such as a bad Internet segmentation, for example, caused by a configuration, a lack of firewalls or demilitarized zone (DMZ). They can also be software vulnerabilities due to lack of updates, or a compromised third party (when the company outsources its services). The company's website can also have vulnerabilities, making attacks such as, SQL injection or XSS breach possible. Vulnerabilities in the configuration and use of the Remote Desktop Protocol (RDP) and Server Message Block (MB) protocols can also be a problem. Finally, brute force and Man-In-The-Middle attacks can allow an attacker to steal an employee's credentials that allows him to install what is needed for a ransomware attack.

Physical access to the IT system: an attacker can break into the organization's building if there is not enough physical security. Furthermore, unaware employees can use a compromised USB and removable media that a malicious person gave them.

These points are summarised by the attack tree shown in Figure 4.

4.4. Ransomware Attacks: Detection

The best way to detect a ransomware attack on your infrastructure is by monitoring all activity information from the devices. Especially, the execution of command lines or scripts that suspiciously modifies, destroys, or exfiltrates data can be detected in log files from devices. Also, what can help is analysing what is downloaded on devices and trying to protect your system from spam (modules exist for email software).

4.5. Ransomware Attacks: Mitigation

As already mentioned before, the only solution to soften a ransomware attack is to have data backups and a recovery plan. To mitigate the risk, before an attack happens, solutions involve preventing human error, blocking execution of files that appear to be ransomware or using a solution such as Privacy-As-A-Service which will be covered in section 7.

5. Recovery Plan

The municipality of Wassenaar has an outdated IT disaster recovery plan (ITDRP). Therefore research is done on how to establish such a plan, which steps should be followed, and what are important issues to be addressed. First of all, let us dive into the question "what is an IT disaster?". An IT disaster can be explained in many ways but in general terms it means, the unplanned interruption of normal business processes resulting from an interruption in IT infrastructure components used to support them. A disaster recovery plan's primary objective is to provide business continuity after a disruption (due to man-made or natural causes) has taken place. "A disaster recovery plan should ensure that all of your systems and data can be restored to normal operation quickly in the event of a natural or a technical disaster." [24]

5.1. Step-by-step approach

The first step [17] in creating an ITDRP is identifying the systems and resources that are most critical to the business operations. This can be done by first doing a business impact analysis and second a risk assessment analysis. By performing a business impact analysis, one identifies the most essential resources for keeping the organization running. Adding a risk assessment analysis on top of that enhances the prioritization for risk mitigation.

The second step is identifying possible vulnerabilities which have been done by third parties in the form of a pentest, vulnerability scans for network and server infrastructure, court of auditors investigation information security, a gap analysis, and risk analysis information security. However, the municipality of Wassenaar could also decide to identify possible vulnerabilities themselves. Therefore a vulnerability management process should be designed.

Identifying vulnerabilities is by itself not enough. It can be further improved by monitoring the vulnerabilities and in doing so preventing problems from occurring. Monitoring vulnerabilities can be done by the use of both Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) which will be further touched upon in section 6.

The third step is developing a plan of action. This plan of action can be developed by conducting a brainstorming session with the management and corporate employees. Each department could develop its own recovery plan providing directives on how to quickly resolve a crisis including phone numbers of people who must be notified immediately. Involving the management and corporate employees enhances their understanding of the importance of security which is one of the bottlenecks of the municipality of Wassenaar (Section 2). In case of a geophysical, hydrological, or meteorological disaster traveling to an alternate site may be required but be sure to assess it based on the essential resources and associated risk. Possible recovery strategies:

- **Vendor maintenance agreement** Incorporate an agreement within your hardware vendor contract that they are responsible for equipment recovery, repair, and replacement including damage by external factors such as a fire or flood.
- **Hot sites**: A fully equipped facility that the organization can shift to in case of an emergency. The hot site can also be used to practice the ITDRP to make sure that the management and employees are prepared for any disasters that could occur in the future.
- **Cold sites**: An empty building that is wired and computer-ready. However, in case of a disaster, all equipment needs to be installed which can easily take hours.
- **Mirrored site**: A fully equipped mirrored facility means all nightly backup tapes are mirrored so that recovery will only involve the current day's transactions. The startup time is usually the same day.

Another important part of the plan of action is selecting the right backup strategy. The municipality of Wassenaar outsourced its backups which is the reason why no recommendations are provided on that matter.

The fourth step is conducting a verbal walk-through with the employees that are involved in the recovery plan. This verbal walk-through is also used to discuss the what-if scenarios and outline individual tasks and responsibilities. This makes sure that the employees are actively involved in the process and have the opportunity to come up with novel ideas. By doing so, the likelihood of a smooth implementation of the recovery plan will be increased. Lastly, the municipality of Wassenaar should continuously update and test the recovery plan.

5.2. Benefits of IT disaster recovery plan (DRP):

Undeniably, an ITDRP details structures for reducing interruptions and resumes operations rapidly in the aftermath of any disaster. It is important to keep the business running even after the attack and therefore an ITDRP should be planned to prevent data loss and enable sufficient IT recovery

Having an ITDRP would help the municipality in several ways:

1) **Cost Efficiency:** ITDRP requires several components that improve cost efficiency. The main ones include prevention, detection, and correction. Prevention reduces the risk of man-made disasters. Detections, quickly identify the problem when occurred, and correction restores lost data and enables resumption of operations. Achieving cost efficiency goals demands the system to have regular maintenance in optimal conditions, high-level analysis of potential threats, and implementation of innovative cybersecurity issues. Adopting a trusted cloud-based data management as a part of ITDRP could reduce the cost of backups and maintenance. The below are a few areas to explore cost-effective disaster recovery.
   - **Understand recovery needs:** Just by understanding what needs to be recovered in time of a total disaster outage, the cost of recovering from a disaster can be reduced. This can be done by establishing a RPO and RTO. This way, maintenance cost of the idle data can be avoided saving us a couple of pennies.
   - **Accurately size the Disaster Recovery (DR) storage system:** Since users only need immediate access to the document they were working with most recently, typically a two week time frame, the capacity of the storage system at the disaster recovery (DR) sites can be dramatically reduced which results in 100 TB of storage system in the data center can be reduced to 10TB at the DR site.
   - **Disaster Recovery (DR) site should be virtualized:** Even if the primary system is not 100 percent virtualized, the DR site has to be virtualized. Virtualization keeps server costs at a minimum and can further reduce the capacity requirements by allowing DR storage systems to support duplication and compression.

   By incorporating these plans the municipality could reduce up to 5 percent of the amount used for maintenance and storage.
2) **Increased productivity:**Allocating specific roles and responsibilities along with accountability demands increases effectiveness and productivity in the team. The designated worker/employee will be held responsible as a result each person owning the task will be obligated to handle their accountabilities which would reflect the quality of work.

3) **Citizens' Trust:** Customers do not easily forgive when they get to know that their personal information is out there in the public or when it is in hands of the unknown. An ITDRP would help the municipality meet and maintain a higher quality of service towards the public in any situation by reducing the risk of data loss and downtime, and ensuring they receive better service from the government.
4) **Scalability:** Planning disaster recovery would allow the municipality to come up with innovative solutions to reduce the cost of maintenance, backups, and recovery. Cloud-based storage and related technologies would simplify the process and make the process add flexibility and scalability as there is tons of data that is getting fed into the system on an everyday basis [32].

5.3. Possible Strategies that Could be Adapted by Municipality for Disaster Recovery Plan (DRP):

The right set of strategies and tools will help the municipality implement an ITDRP. The most effective strategies for the Municipality has been listed down below:

1) In-house backup systems : The It teams should develop backup servers strategically at different locations inside the premises. Using in-house hardware could eliminate the dependence of vendors which could save up the municipality the expenses of leasing equipment. It is also important that the backup tapes are offline. If back-up servers are kept on-premise, there is always a risk of these servers also being targeted in an attack. When they're offline, this risk is already smaller. However, when there is a natural disaster, on-premise back-ups can still be damaged. Therefore, back-up servers should be housed at a different geographical location too.
2) Data and restoration: We know that the municipality or any business in that matter cannot tolerate downtime. Data Mirroring, actual parallel computing, or multiple data synchronizations will be a great solution yet expensive.
3) Cloud-Based disaster recovery strategies: If the municipality would look into backing up data on the cloud, Many Cloud-based vendors offer Disaster recovery as a Service(DRaaS). This will be a good option as the vendor manages and maintains the data for the client. They can host and manage applications, data security services enabling access to information via a web browser. These vendors can enhance cybersecurity as they monitor everything on a regular basis and also offer data filtering and malware threats. If they detect an outage at the client site, they hold all the client data automatically until the systems are restored. The cloud is essential to security planning and disaster recovery. However, make sure that the vendor signs a non-disclosure agreement since you are dealing with data of civilians.

Few advantages of DRaaS which might save resources for the municipality would be as mentioned:

1) DraaS will allow organizations to place their backup servers at different geographic locations than their primary area. Geographic distributions make them more resilient to disasters that have affected a large area.
2) Ease of use: DraaS providers manage everything on behalf of their customers, They take the responsibility of finding an appropriate place and hardware and other components, locating an appropriate data center that is suitable to the client's situation. This can save some time for the employees to concentrate on other work.
3) Expert Guidance: Reputable service providers will typically have deeper knowledge and experience in DRP and managing data security than the in-house team while the In- house IT team will still hold access and will still be able to manage data storage, run reports and recover lost data on their own.
4) Security: DraaS solutions are more secure than the traditional methods. If the municipality's data is corrupted or attacked, DRaaS will be able to provide the most recent backup to the organization. Since the data is stored in the cloud, information retrieval will be much easier. DRaaS has various security technologies resulting in strict data protection.[32]

Few Challenges involved in adapting to DRaaS is mentioned as below:

1) The municipality must trust the service provider to implement the plan in the event of a disaster and meet the RTO and RPO.
2) The municipality will have to rely on a service provider's security when fail-overs occur [27].

6. Key Performance Indicators & Dashboard

As mentioned in section 5.1 monitoring vulnerabilities is crucial to prevent problems from occurring. The KPIs and KRIs that we found most important for the municipality of Wassenaar can be found in Tables 1 and 2 respectively. The indicators are shown on the security dashboard which can be found in section 6.1 and are filterable on a time frame. Furthermore, the Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are valuable to define and measure. RPO is the amount of data the company is willing to lose after a disaster occurs and answers the question "How much data could be lost without significantly impacting the business?" An example of a RPO could be: after a ransomware attack occurs 4 hours of data may be lost. This also means that the backup strategy should be changed accordingly. RTO is the acceptable downtime of the systems after a disaster occurs and answers the question "How much time should it take to recover from a business process disruption?". RTO is important to define thoughtfully since the recovery plan should be designed in such a way that the RTO will be achieved under all circumstances.

KPI Identifier	KPI Description
KPI 1	The number of vulnerabilities per type of importance
KPI 2	The number of scanned URLs
KPI 3	The number of scanned IP addresses/ networks
KPI 4	The number of internal and external servers and applications
KPI 5	The number of assets, for example, windows, servers, applications, etc.
KPI 6	The number of internet-facing assets and applications
KPI 7	The cost of resolving vulnerabilities
KPI 8	The cost associated with incidents caused by vulnerabilities
KPI 9	Recovery Point Actual: the actual amount of data that was lost during the disaster
KPI 10	Recovery Time Actual: the actual time needed to recover after a business process disruption
KPI 11	The amount of time taken to resolve or remediate a vulnerability

Table 1. VULNERABILITY KEY PERFORMANCE INDICATORS (KPIS)

KRI Identifier	KRI Description
KRI 1	Total number of open (not yet analyzed or have work in progress) vulnerabilities
KRI 2	The number of open vulnerabilities per business application
KRI 3	The number of open vulnerabilities per server or system including middleware and software
KRI 4	Percentage of open vulnerabilities in relation to closed issues in a month
KRI 5	The status of the remediation progress and number of vulnerabilities per asset
KRI 6	The number of internet-facing assets and applications
KRI 7	An overview of the remediation solution type

Table 2. VULNERABILITY KEY RISK INDICATORS (KRIS)

The dashboards in section 6.1 could be further extended by additional visualizations listed below:

- An overview (e.g. a bar chart) of the amount of time passed by between the detection and remediation per vulnerability. You could even define a KPI as an additional steering measure such as "the average time passed by between the detection and remediation of vulnerabilities"
- An overview (preferably a line graph) of the number of deployments within and outside of the scheduled maintenance windows.

To help the security team convincing the management board financial KPIs are defined that can be added to dashboards shown in section 6.1. we were not able to include the financial KPIs due to the lack of data provided by the municipality of Wassenaar. The KPIs are listed down below:

1) **Digital Assets**
   - Number of digital assets
   - Number of internet-facing assets, applications
   - Number of internal and external servers, applications
2) **Data**
   - % of data will be used for unrelated purposes
   - % of data shared with third parties
   - % of data that will not be deleted or anonymized
3) **Financial**
   - Ratio of Privacy Benefits to Investment
   - Return on Security Investments
   - Number of trainings provided to employees per Year

6.1. Dashboards

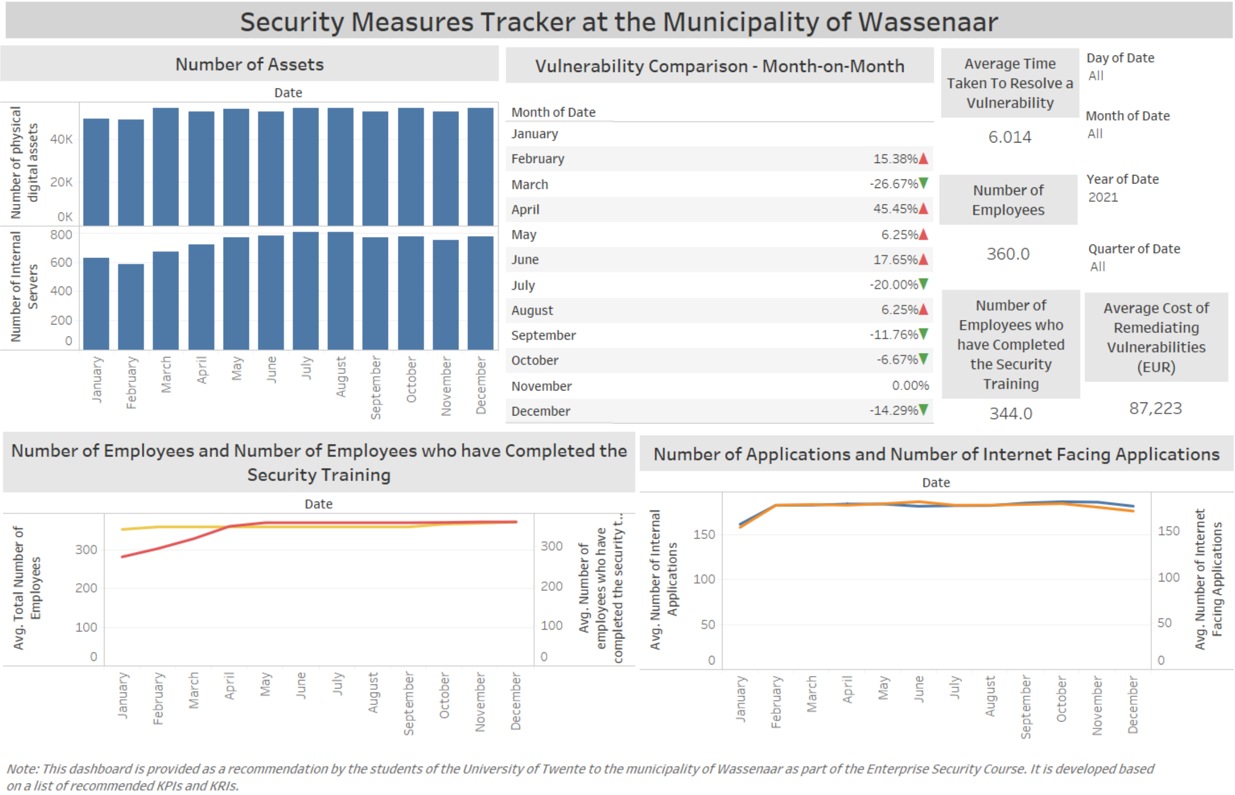
Two dashboards (Figures 3 and 4) were developed using *Tableau*, which show a number of KPIs that are mentioned in the previous section. The dashboards were developed to showcase the security team of the municipality of Wassenaar the valuable insights that data can bring. The dashboards can be used for monitoring their vulnerabilities and are also useful when the management supported the idea of investing more into security. The management can see how the control measures are changing over time while investing more into security. As being said in the previous section, an additional dashboard can be realized showing the proposed financial KPIs that can help the security team convincing the management board.

7. Privacy-as-a-Service Solutions

As mentioned in the Case Description (Section 2) one of the main problems faced by the municipality of Wassenaar is related to budget utilization. The security team currently has the budget to invest in security solutions, but is often faced with a dilemma of making investments. This is mainly due to the fact that the team feels that such investments bring with it the requirement of the right kind of human resource, equipped with the necessary technical skillset. Apart from being a security issue, this also translates into a human resource issue. Thus most of our research was targeted towards resilient and affordable solutions to be adopted by the municipality of Wassenaar. One of the most sustainable options that stemmed out was using Privacy-as-a-Service (PaaS) or Data Privacy-as-Service (DPaaS) tools.

PaaS or DPaaS solutions allow users to comply to regulations such as GDPR, while protecting data at the very root, i.e., data stored on the cloud, on premise, or in a hybrid fashion and data flowing through APIs. These tools also address the need for deploying skilled man power if an investment is made. This means that when the data privacy requirements are outsourced to a trusted provider, the requirements are gathered by the experts at the provider's end. Depending on the payload sizes that have to be protected, a fee is charged from the customers (the municipality of Wassenaar, in this case).

Contrary to the municipality's current notion that a dedicated team of security professionals will be required to be hired if an



Security Measures Tracker at the Municipality of Wassenaar

Vulnerability Comparison - Month-on-Month

Month of Date	
January	
February	15.38%▲
March	-26.67%▼
April	45.45%▲
May	6.25%▲
June	17.65%▲
July	-20.00%▼
August	6.25%▲
September	-11.76%▼
October	-6.67%▼
November	0.00%
December	-14.29%▼

Average Time Taken To Resolve a Vulnerability	6.014
Number of Employees	360.0
Number of Employees who have Completed the Security Training	344.0
Average Cost of Remediating Vulnerabilities (EUR)	87,223

Day of Date: All

Month of Date: All

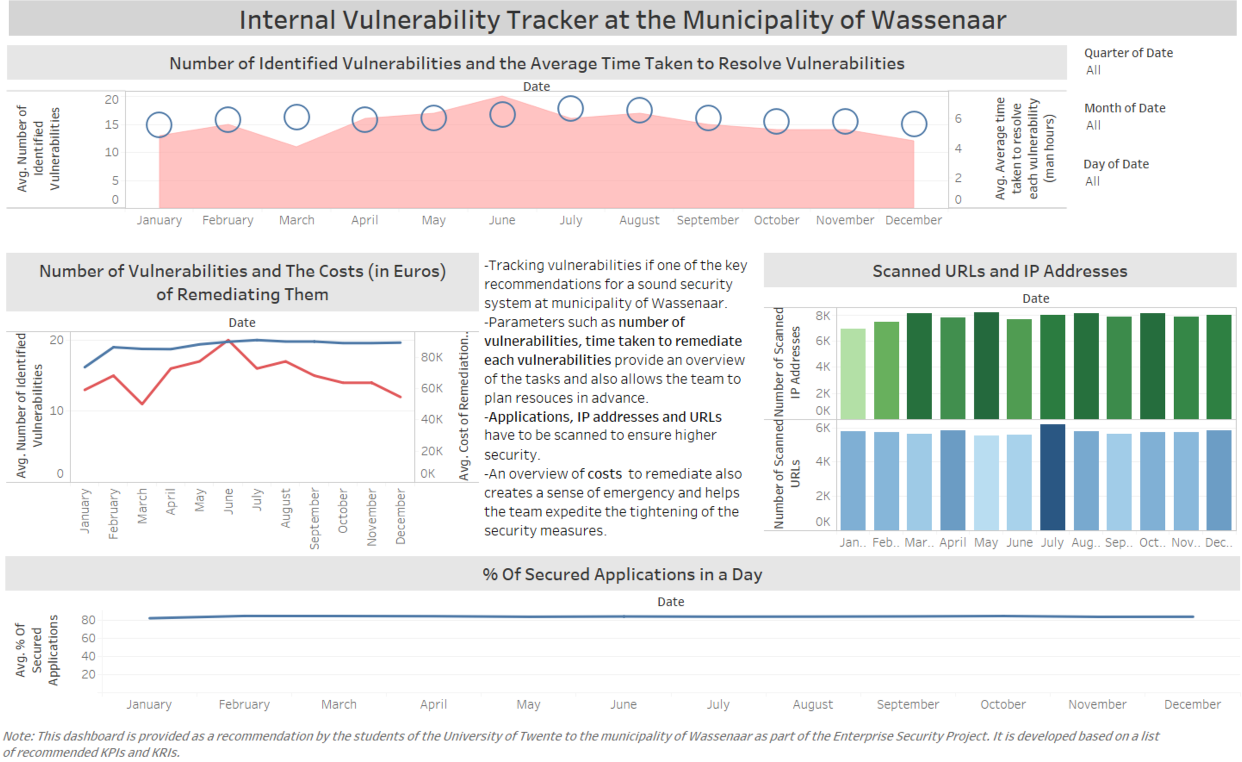
Year of Date: 2021

Quarter of Date: All

Note: This dashboard is provided as a recommendation by the students of the University of Twente to the municipality of Wassenaar as part of the Enterprise Security Course. It is developed based on a list of recommended KPIs and KRIs.

Number of Assets
Date
Number of physical digital assets
40K
20K
0K
Number of Internal Servers
800
600
400
200
0
January
February
March
April
May
June
July
August
September
October
November
December
Number of Employees and Number of Employees who have Completed the Security Training
Avg. Total Number of Employees
300
200
100
0
Avg. Number of employees who have completed the security t..
Number of Applications and Number of Internet Facing Applications
Avg. Number of Internal Applications
150
100
50
Avg. Number of Internet Facing Applications

Figure 3. Security Measures Tracker at the Municipality of Wassenaar



Internal Vulnerability Tracker at the Municipality of Wassenaar

Quarter of Date: All

Month of Date: All

Day of Date: All

-Tracking vulnerabilities if one of the key recommendations for a sound security system at municipality of Wassenaar.
-Parameters such as **number of vulnerabilities, time taken to remediate each vulnerabilities** provide an overview of the tasks and also allows the team to plan resouces in advance.
-**Applications, IP addresses and URLs** have to be scanned to ensure higher security.
-An overview of **costs** to remediate also creates a sense of emergency and helps the team expedite the tightening of the security measures.

Note: This dashboard is provided as a recommendation by the students of the University of Twente to the municipality of Wassenaar as part of the Enterprise Security Project. It is developed based on a list of recommended KPIs and KRIs.

Number of Identified Vulnerabilities and the Average Time Taken to Resolve Vulnerabilities
Date
Avg. Number of Identified Vulnerabilities
20
15
10
5
0
Avg. Average time taken to resolve each vulnerability (man hours)
6
4
2
0
January
February
March
April
May
June
July
August
September
October
November
December
Number of Vulnerabilities and The Costs (in Euros) of Remediating Them
Avg. Number of Identified Vulnerabilities
Avg. Cost of Remediation..
80K
60K
40K
20K
0K
Scanned URLs and IP Addresses
Number of Scanned IP Addresses
8K
6K
4K
2K
0K
Number of Scanned URLs
Jan..
Feb..
Mar..
April
May
June
July
Aug..
Sep..
Oct..
Nov..
Dec..
% Of Secured Applications in a Day
Avg. % Of Secured Applications
80
60
40
20

Figure 4. Internal Vulnerability at the Municipality of Wassenaar

investment is made, PaaS platforms simplify this conundrum to a very large extent. The PaaS platform, if chosen correctly will be able to create a bridge between the three 'lands' that are usually kept separate: technical tools, regulations and skillset. They would be bound together by moulding a special 'toolbox' to solve present and future issues. Instead of spending money on human resource, the municipality can choose to invest in a good platform that meets their requirements. A discussion with the Chief Executive Officer of a UK based Data Privacy company, *eXate*, opened up many such interesting and promising opportunities for investment. Their tools *APIgator* [13] and *DATAgator* [14] work to protect data right at the endpoints and storage hubs. With clients across the globe, including a large Dutch bank, they offer promising solutions to a wide range of industries. There are many more solutions by companies such as *Privitar* [25], *SecuPi* [28], and *Very Good Security* [29] that offer these services.

Additionally, the amount of money that should be invested in such solutions can be estimated with the help of the Gordon-Loeb Model [16], which suggests that a company should invest less than, or at most equal to, roughly 37% of their estimated losses from their security breaches.

Therefore, to sum up, looking at investment options tending towards outsourcing data protection will prove beneficial for the municipality of Wassenaar.

8. Preventing Human Errors

As discussed in Section 1 municipalities are at the crossroads between housing sensitive citizen data and managing poorly secure networks. This makes them vulnerable to a plethora of security attacks and threats. In cybersecurity, one of the most common threats, among others, is human errors and far too often, these are overlooked. Human errors can be thought of as lack of action by employees or users while engaging in software systems thereby causing security breaches. These breaches can be as simple as failing to use a strong and encrypted password to something as damaging as downloading a malware-infected attachment to the software systems. Data breaches at Municipalities can be crippling in terms of the costs that are incurred there-after, restructuring the intellectual property and realigning regulatory requirements. The most common human errors that are threatening to the data at any organization are discussed in section 8.1, 8.2, and 8.3 [8].

8.1. Ineffective means of handling sensitive data

Human errors often stem from slips and lapses that occur while doing routine tasks and activities. More often than not, these errors occur when the users handle large amounts of sensitive data that lead to data compromises and leaks out of carelessness. Some of the most common careless mistakes made by users include sending sensitive data via email to the wrong recipient, accidentally deleting important files, sharing confidential data to peers and colleagues via insecure applications, forgetting to backup critical data, etc.

Negligence among users can also lead to delaying software updates, disabling security features and using unauthorized systems. It is but natural for users who have no prior knowledge on the importance of following security protocols at workplaces to unintentionally compromise sensitive information.

- Dismissing software updates can lead to ransomware attacks that affect systems running older versions of certain operating systems or applications.
- Unintentionally disabling security features at work could also put the organization's data at risk. This could be something along the lines of pressing pause on the antivirus feature update or browser security.
- Users can also download software applications that are unauthorized or don't conform to the software requirements of the organization giving leeway to malicious and ransomware attacks.

8.2. Not having enough knowledge on security standards

Employees and users lacking the basic knowledge on the importance of security protocols and cybersecurity measures can disclose sensitive information unintentionally. This gives way to bigger threats at the workplace like phishing emails and ransomware attacks on software systems. Phishing emails are convincing enough to make users on the other side of the screen give up their credentials and click on links that redirect them to some malicious content.

8.3. Weak password policy and credentials

When employees and users fail to follow a password management policy for access to sensitive data, they give leeway to hackers and malicious users to access accounts by performing brute-force attacks. These human errors can be as simple as storing passwords in plain text, using the same passwords for multiple accounts, and using unsafe password managers that have weak encryption protocols.

8.4. Measures that can be taken to prevent human errors at the Municipality

The management at the Municipality should take it upon themselves to educate employees on the criticality of security protocols at workplaces to avoid human errors. This should stem from the management level where investing in good security practices should not be seen as an IT problem but an organization problem that is resolved cross-functionally across all departments. There needs to be a plan in place that can handhold employees and users to adhere to good security practices that can prevent human errors from happening. More often than not, users and employees are in the dark about taking the right course of action when handling sensitive information.

Formal Security Awareness and Training Program: Introducing an educational approach to train employees at the workplace is imperative to make everyone understand the importance of following well-structured IT policies and best practices. Awareness can be included in the process of onboarding employees and as a mandatory training for the existing employees. Security courses on basic anti-social engineering, email security, internet security, information exchange procedures are available on the market for free or at low cost. This will also help the non-technical employees to identify the possible threats caused by the most obvious but simple cyber security crimes such as email phishing, voice phishing social engineering, etc. In case of any security violation or suspicions, employees should be aware on what actions to take. There are no infallible ways to protect the organization from cyber security attacks, but educating the employees with best security practices and potential threats can assist in reducing the likelihood of occurrence of such events caused by human errors. By doing this, municipalities and organizations can protect their reputation, reduce unnecessary incur of costs as part of cybersecurity issues and secure their IT infrastructure and data.

Stronger Password Management Policy: Establishing and incorporating a secure password manager [1] application allows employees and users using the software systems to create and save passwords without having to remember them every time or run the risk of writing them down on sticky notes and leaving them unattended on the desks. If Municipalities currently have a Two-Factor Authentication in place, they can go the extra mile and mandate the usage of a Dynamic Password Controller to strengthen secure access to accounts and confidential information. This is a viable solution to combat a weak password policy at the municipality as it acts as a centralized vault to store all passwords in fully encrypted forms. It also provides visibility of the users and employees who access the systems thereby enabling authorized access to software systems and applications.

Privilege control and access management: By exerting control over the access and permissions granted to users, the management can ensure that employees only have access to data that is required for them to perform their daily functions [5]. One way to do this is by establishing separate account access for administrative and other user accounts. This limits the exposure of information on a high-level and reduces the risk of attacks caused due to human errors and negligence.

9. Conclusion

This report examines the security issues at the municipality of Wassenaar and provides recommendations based on careful understanding and analysis.

The municipality is tasked with protecting large amounts of public information, most of which is PII. These data points play a key role in almost all the business process in the municipality. In order to prevent any major cyber attack, Security-by-Design is a suggested method of approaching any security strategy. A detailed vulnerability assessment followed by the design of Attack Trees can help the teams understand the possible events that can serve as entry points for malware, such as ransomware. A detailed assessment such as this will serve as an effective preventive strategy.

For all plans and strategies to materialize into reality, it is important that we convince the management about the urgency in security investments. Since the management likes to see numbers and facts rather than theoretical barrage, we developed a set of KPIs and KRIs to track, monitor and analyse. For an added level of preparedness, it is not just sufficient to prevent, but it is important to have a strong recovery plan in case of an attack. The report also addresses the step-wise process that can be adopted for updating the municipality's current recovery plan. A strong recovery plan serves are a reactive strategy and can help the municipality be resilient even if an attack occurs.

Furthermore, the human element in any organization can also provide a lot of room for errors resulting in catastrophic consequences, for which we provide some suggestions. to reduce human errors in business processes, in terms of security. Lastly, we recommend Privacy-as-a-Service solutions, so that the municipality can choose the best solution according to their needs, while not investing in manpower and ensuring the proper utilization of security budget. The amount of money to be invested in such security can be backed-up using a quantification using the Gordon-Loeb model.

With that, this report covers the research questions described at the beginning of this report. While every municipality has similar business processes, the internal architecture and strategies can vary. Hence, our recommendations will be tailored according to the specific needs of the stakeholder. It is important to note that security recommendations are not a *one-size-fits-all* solution.

The scope of the project can indeed be expanded, given the time and resources. The following section discusses possible future work related to the same (and other similar) usecase(s).

10. Future Scope

The solutions discussed in this report have been provided based on extensive research and discussion with the teams at the municipality of Wassenaar and VNG. Further to our current work, points for further research include the following.

Most security trainings teach employees what not to do, but employees almost always end up breaking these rules. A strategy to circumvent these issues would also serve as valuable inputs for any organization.

Most importantly, it is important to balance privacy and utility while developing a security strategy. When one increases, the other definitely decreases and vice versa. This also involves multiple organizational costs that need to be accounted for. Finding the right balance between privacy and utility, while leveraging costs is probably the hardest problem that is yet to be solved.

Acknowledgements

The team would like to convey their sincere gratitude towards the stakeholders from the municipality of Wassenaar and VNG for their valuable inputs and unconditional support. We would also like to convey our gratitude to Professors Abhishta and Florian, for their constant support throughout the project.

References

[1] Ahola, Micke. *The Role of Human Error in Successful Cyber Security Breaches*. Ed. by usecure. URL: https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches.

[2] Associates, Belbin. *The Nine Belbin Team Roles*. Ed. by Belbin Associates. 2022. URL: https://www.belbin.com/about/belbin-team-roles.

[3] ATT&CK, Mitre. *Data Encrypted for Impact*. 2015. URL: https://attack.mitre.org/techniques/T1486/.

[4] Barker, William C. et al. *Cybersecurity Framework Profile for Ransomware Risk Management*. Tech. rep. Sept. 2021. DOI: 10.6028/nist.ir.8374-draft.

[5] BeyondTrust. *Privileged Access Management (PAM)*. URL: https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam.

[6] Challita, Antonio. *The four most popular methods hackers use to spread ransomware*. Aug. 9, 2018. URL: https://www.itproportal.com/features/the-four-most-popular-methods-hackers-use-to-spread-ransomware/.

[7] CISA. *RANSOMWARE 101*. URL: https://www.cisa.gov/stopransomware/ransomware-101.

[8] Coffey, John W. *Ameliorating Sources of Human Error in CyberSecurity: Technological andHuman-Centered Approaches*. 2017. URL: https://www.iiis.org/CDs2017/CD2017Spring/papers/ZA253LY.pdf.

[9] Coker, James. *Local Government Organizations Most Frequently Targeted by Ransomware*. Aug. 27, 2020. URL: https://www.infosecurity-magazine.com/news/local-government-targeted/.

[10] Continews, ed. URL: https://continews.click/.

[11] Disk, Jungle. *Three Ways to Convince Your Superiors to Invest in Cybersecurity*. Aug. 26, 2019. URL: https://www.jungledisk.com/blog/2019/08/26/3-ways-to-convince-your-superiors-to-invest-in-cybersecurity/.

[12] Elliptic. *Conti Ransomware Nets at Least $25.5 Million in Four Months*. Nov. 18, 2021. URL: https://www.elliptic.co/blog/conti-ransomware-nets-at-least-25.5-million-in-four-months.

[13] eXate. *About APIgator*. 2020. URL: https://www.exate.com/apigator.

[14] eXate. *DATAgator*. 2020. URL: https://www.exate.com/datagator.

[15] Eytan, Oren. *Municipal Cyberattacks: A New Threat Or Persistent Risk?* Ed. by Forbes. July 22, 2021. URL: https://www.forbes.com/sites/forbestechcouncil/2021/06/22/municipal-cyberattacks-a-new-threat-or-persistent-risk/.

[16] Gordon, Lawrence A., Loeb, Martin P., and Zhou, Lei. "Investing in Cybersecurity: Insights from the Gordon-Loeb Model". In: *Journal of Information Security* 07.02 (2016), pp. 49–59. DOI: 10.4236/jis.2016.72004.

[17] Hawkins, Steve M., Yen, David C., and Chou, David C. "Disaster recovery planning: a strategy for data security". In: *Information Management & Computer Security* 8.5 (Dec. 2000), pp. 222–230. DOI: 10.1108/09685220010353150.

[18] Kaplan, Robert S. and Norton, David P. *The Balanced Scorecard—Measures that Drive Performance*. URL: https://hbr.org/1992/01/the-balanced-scorecard-measures-that-drive-performance-2.

[19] Kaspersky. *What is WannaCry ransomware?* URL: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

[20] Knowbe4. *The Economic Impact of CyberAttacks on Municipalities (Whitepaper)*. 2020. URL: https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf.

[21] Logging, Apache. *Apache Log4j Security Vulnerabilities*. URL: https://logging.apache.org/log4j/2.x/security.html.

[22] MITRE. *Mitre Att&CK*. 2015. URL: https://attack.mitre.org/.

[23] Mitre. *Input Capture: Web Portal Capture*. 2015. URL: https://attack.mitre.org/techniques/T1056/003/.

[24] Mohamed, Hossam Abdel Rahman. "A Proposed Model for IT Disaster Recovery Plan". In: *International Journal of Modern Education and Computer Science* 6.4 (Apr. 2014), pp. 57–67. DOI: 10.5815/ijmecs.2014.04.08.

[25] Privitar. *Privitar*. 2022. URL: https://www.privitar.com/.

[26] Ramesh, Sneha. *The Third Party Problem: When Data Breach is Out of Your Reach*. Aug. 2, 2021. URL: https://www.exate.com/post/third-party-data-breaches.

[27] Rock, Tracy. *23 Disaster Recovery Statistics You Should Know*. July 1, 2020. URL: https://invenioit.com/continuity/disaster-recovery-statistics/.

[28] SecuPi. *SecuPi*. 2022. URL: https://www.secupi.com/.

[29] Security, Very Good. *Payment Data Security & Compliance Infrastructure for Modern Organiza-*

tions. 2022. URL: https://www.verygoodsecurity.com/.

[30] SOCRadar. *Top Five Causes of Ransomware Attacks*. Ed. by SOCRadar. Oct. 7, 2021. URL: https://socradar.io/top-five-causes-of-ransomware-attacks/.

[31] Tableau. *Tableau*. 2003. URL: https://www.tableau.com/.

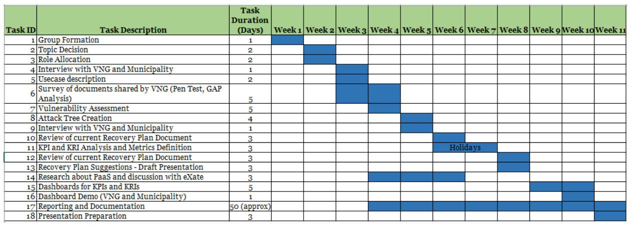
[32] TechTarget. *Lower disaster recovery costs in five steps*. URL: https://searchdisasterrecovery.techtarget.com/tip/Lower-disaster-recovery-costs-in-five-steps.

[33] Times, NL. *Hackers demanded €750,000 from Dutch municipality in ransomware attack: report*. Dec. 7, 2020. URL: https://nltimes.nl/2020/12/07/hackers-demanded-eu750000-dutch-municipality-ransomware-attack-report.

[34] VNG. *Informatie Beveiligings Dienst*. Jan. 1, 2020. URL: https://www.informatiebeveiligingsdienst.nl/project/baseline-informatiebeveiliging-overheid/.

Appendix 1

Internally, a set of roles were divided among the team of eight, based on the scores obtained in the Belbin Roles [2] test. The final team comprised a Shaper, Coordinator, Resource Investigator, Implementer, Completer Finisher and Team Workers. Tasks were split and responsibilities were allocated according to the assigned roles. The project was executed based on carefully curated plans and semi-structured interviews. An overview of the planning is depicted in the Gantt Chart Shown in Figure 5.



Task ID	Task Description	Task Duration (Days)	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11
1	Group Formation	1	■										
2	Topic Decision	2		■									
3	Role Allocation	2		■									
4	Interview with VNG and Municipality	1			■								
5	Usecase description	2			■								
6	Survey of documents shared by VNG (Pen Test, GAP Analysis)	5			■	■							
7	Vulnerability Assessment	5				■							
8	Attack Tree Creation	4					■						
9	Interview with VNG and Municipality	1					■						
10	Review of current Recovery Plan Document	3						■					
11	KPI and KRI Analysis and Metrics Definition	3						■ Holidays	■				
12	Review of current Recovery Plan Document	3								■			
13	Recovery Plan Suggestions - Draft Presentation	3								■			
14	Research about PaaS and discussion with eXate	3				■	■	■					
15	Dashboards for KPIs and KRIs	5									■	■	
16	Dashboard Demo (VNG and Municipality)	1										■	
17	Reporting and Documentation	50 (approx)				■	■	■	■	■	■	■	■
18	Presentation Preparation	3											■

Figure 5. Planning of Activities for the Project

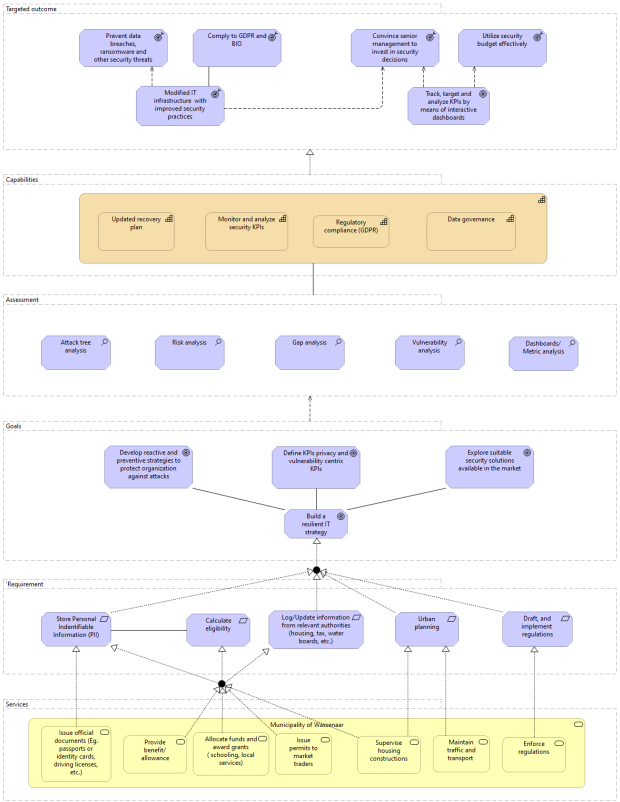

Targeted outcome
Prevent data breaches, ransomware and other security threats
Comply to GDPR and BIO
Convince senior management to invest in security decisions
Utilize security budget effectively
Modified IT infrastructure with improved security practices
Track, target and analyze KPIs by means of interactive dashboards
Capabilities
Updated recovery plan
Monitor and analyze security KPIs
Regulatory compliance (GDPR)
Data governance
Assessment
Attack tree analysis
Risk analysis
Gap analysis
Vulnerability analysis
Dashboards/ Metric analysis
Goals
Develop reactive and preventive strategies to protect organization against attacks
Define KPIs privacy and vulnerability centric KPIs
Explore suitable security solutions available in the market
Build a resilient IT strategy
'Requirement
Store Personal Indentifiable Information (PII)
Calculate eligibility
Log/Update information from relevant authorities (housing, tax, water boards, etc.)
Urban planning
Draft, and implement regulations
Services
Municipality of Wassenaar
Issue official documents (Eg. passports or identity cards, driving licenses, etc.)
Provide benefit/ allowance
Allocate funds and award grants (schooling, local services)
Issue permits to market traders
Supervise housing constructions
Maintain traffic and transport
Enforce regulations

Figure 6. Motivation Model for the Project - Project Goals, Capabilities and Targeted Outcomes

Appendix 2

Figure 6 depicts the motivation for the projects and also describes the associated goals and principles.