Cyber Readiness in Finnish Contract Fire Brigades

Antti Aitta

Master's thesis
April 2021
Technology, communication and transport
Master's Degree Programme in Information Technology
Cyber Security

jamk.fi

Description

Author(s) Aitta, Antti	Type of publication Master’s thesis	Date April 2021
		Language of publication: English
	Number of pages 188	Permission for web publication: x

Title of publication

Cyber Readiness in Finnish Contract Fire Brigades

Degree programme

Master’s Degree Programme in Information Technology, Cybersecurity

Supervisor(s)

Immonen, Jani
Kokkonen, Tero

Assigned by

Suomen Pelastusalan Keskusjärjestö SPEK / The Finnish National Rescue Association

Abstract

The Finnish contract fire brigades have a significant footprint in the fire and rescue field of Finland. They are the first, and typically only, responder of emergencies in rural areas of Finland and in cities they make the core reserve for municipal rescue services.

The history of fire brigades in Finland reach out to 19th century, and as such the methods for communications, navigation and dispatching units have evolved and digitalized significantly. As the municipal fire and rescue services have adapted to different technologies over the ages, the current technological starting point vary under different rescue departments but under different contract fire brigades as well.

The research aims to discover common attack vectors, weaknesses, and vulnerabilities that Finnish contract fire brigades might have, as well to give recommendations on how to remediate them.

The research method was chosen to be mixed: A general view could not necessarily be achieved using only qualitative method, and thorough technical research could not be conducted using only quantitative method.

As a conclusion it was confirmed, that as the resources to administrate information technology vary greatly between contract fire brigades, there is a significant attack surface for adversaries. There are little to no means to detect or respond to a security incident. However, as used technologies vary greatly, there are no singular common weakness of vulnerability, that could be easily used to attack all contract fire brigades at once.

Keywords/tags

Fire and rescue services, contract fire brigade, cyber security, command and control systems.

Miscellaneous

Appendixes 2, 3, 4, 5 and 6 defined as secret until 19 April 2046.

Kuvailulehti

Tekijä(t) Aitta, Antti	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä Huhtikuu 2021
		Julkaisun kieli: Englanti
	Sivumäärä 188	Verkkojulkaisulupa myönnetty: x

Työn nimi

Suomalaisten sopimuspalokuntien kybervalmiudet

Tutkinto-ohjelma

Master’s Degree Programme in Information Technology, Cybersecurity

Työn ohjaajat(t)

Immonen, Jani
Kokkonen, Tero

Toimeksiantaja

Suomen Pelastusalan Keskusjärjestö SPEK / The Finnish National Rescue Association

Tiivistelmä

Sopimuspalokunnilla on merkittävä rooli pelastustoimen järjestämisessä Suomessa. Harvaan asutulla seudulla sopimuspalokunta on kohteen ensimmäisenä saavuttava pelastustoimen yksikkö, usein myös ainoa. Taajama-alueella sopimuspalokunnat muodostavat merkittävän osan kunnallisen pelastustoimen reservistä.

Sopimuspalokuntien historia ulottuu 1800-luvulle ja siten myös viestivälineet, navigointikeinot sekä yksiköiden hälyttäminen on kehittynyt ja digitalisoitunut vuosien saatossa merkittävästi. Kunnalliset palo-, ja sittemmin pelastuslaitokset, ovat ottaneet erilaisia teknologioita käyttöön pitkän ajan kuluessa. Siten käytetyt teknologiat vaihtelevat suuresti pelastuslaitosten, mutta myös sopimispalokuntien välillä.

Tutkimuksen tarkoituksena on löytää yhteisiä hyökkäysvektoreita, heikkouksia ja haavoittuvuuksia, joita suomalaisilla sopimuspalokunnilla voi olla. Lisäksi tarkoituksena on antaa suosituksia näiden haavoittuvuuksien korjaamiseen.

Tutkimusmenetelmäksi valikoitui yhdistelmämenetelmä: tuloksia ei voi varmuudella yleistää käyttämällä kvalitatiivista tutkimusmenetelmää, ja perusteellista teknistä tutkimusta ei voi suorittaa vain kvantitatiivista tutkimusmenetelmää käyttäen.

Lopputuloksena tuli todennetuksi, että tietoteknisten järjestelmien ylläpitoresurssit vaihtelevat suuresti sopimuspalokuntien kesken. Tämä mahdollistaa suuren hyökkäyspinta-alan hyökkääjälle. Sopimuspalokunnilla on käytössään vähäiset keinot todentaa tietoturvapoikkeama tai tietomurto. Kuitenkin, koska sopimuspalokuntien käyttöönottamat teknologiat ja toteutukset eivät ole identtisiä, ei ollut yksittäistä yhteistä haavoittuvuutta, jolla voitaisiin vaikuttaa kaikkiin sopimuspalokuntiin.

Avainsanat

Palo- ja pelastustoimi, sopimuspalokunta, kyberturvallisuus, tietoturva, johtamisjärjestelmä.

Muut tiedot

Liitteet 2, 3, 4, 5 ja 6 määritelty salaisiksi 19.4.2046 saakka.

Contents

Figures

Tables

Acronyms

AAA	Authentication, Authorisation, Accounting
CIS	Center for Internet Security
EDR	Endpoint Detection and Response
GPS	Global Positioning System
GSM	Groupe Spécial Mobile, Global System for Mobile Communications
ISSI	Individual Short Subscriber Identity
NCSC-FI	National Cyber Security Center Finland
OSI	Open Systems Interconnection (Reference Model)
OWASP	Open Web Application Security Project
PEKE	Pelastustoimen Kenttäjohtojärjestelmä (Fire & Rescue Field Command System)
PEIP	Pelastustoimen IP-verkko (Fire & Rescue IP network)
POKE	Poliisin Kenttäjohtojärjestelmä (Police Field Command System)
PSK	Pre-shared key
RCE	Remote Code Execution
SDS	Short Data Service
SKL	Statuskoodilähetin (Status code transmitter, a product by Elektro-Arola)
SMS	Short Message Service
SQL	Structured Query Language
TETRA	Terrestial Trunked Radio
VHF	Very High Frequency
VIRVE	Viranomaisverkko (TETRA network for authorities in Finland)
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
XSS	Cross-Site Scripting
XSRF	Cross-Site Request Forgery

1 Introduction

1.1 Information and Cyber Security in General

Generally, information security is considered the technical means for protecting organisations' sensitive information. For organisations this could be financial information and intellectual property. For fire brigades the information would be mostly personnel registries and operational information, such as destination information and descriptions of a fire or other disaster. There is considerable overlap between information security and data protection, where the latter focuses on protecting personal data, such as social security numbers, medical records, and biometrics.

Cyber security on the other hand is considered being able to affect physical world over a network or computer systems. A textbook example of a cyber-attack is Stuxnet, a worm that attacked Iranian nuclear program by destroying significant number of centrifuges used to enrich uranium. (Baezner et al, 2017)

For a contract fire brigade cyber-attack could mean an attack on fire stations building management system. If a heating would be turned off in a fire station during mid-winter, it could break fire engines' water tanks or pumps. Another example would be disrupting the communications in such manner, that the dispatched alert would not reach the personnel.

A cyber kill-chain consists of seven phases: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control and Actions on Objectives (Hutchins et al). These phases are utilised in the case studies described later in this thesis.

1.2 Fire and Rescue Services in Finland

Fire and rescue services in Finland are organised under Ministry of the Interior. Regional State Administrative Agencies oversee that the municipalities organise fire and rescue services in their territory according to law.

In mainland Finland there are 22 departments of fire and rescue services, and under their command serves approximately 700 contract fire brigades (Suomen Pelastusalan Keskusjärjestö SPEK / The Finnish National Rescue Association, 2019).

There are approximately 24 000 persons working in the fire and rescue field, of which 14 500 are working on volunteer basis, 4 000 are part-time (personal contract) and 1 500 working in workplace fire brigades, such as industrial fire brigades or military fire brigades. Only 4 000 work professionally in a municipal fire and rescue department. Contract fire brigades handle majority of the daily operations on 90% of land area in Finland. On that area lives 46% of Finnish population. (Ministry of Interior, 2020)

Contract fire brigades include volunteer fire brigades, workplace fire brigades and fire brigades with personal contract. (Ministry of Interior, 2020)

As majority of personnel work on non-professional basis, there is a significant risk for information technology and cyber security being managed unprofessionally. There are also different needs between fire brigades and rescue departments, which creates significant variance in software and hardware being used.

The significance of contract fire brigade system for fire and rescue field, and evidently overall security in Finland is clear. Additionally, the emerging digitalisation of different services and tools used in fire and rescue services justifies the need of the research within this topic.

1.3 Digitalisation in Fire and Rescue Services

In Finland fire and rescue services have been adapting different electronic and later on digital methods for alerting and dispatching personnel. However, organised methods for dispatching units for operations has been introduced only recently. For example, in Espoo, neighbour city for capital Helsinki, fire alarms were received and dispatched by a bakery until 1959. The first municipal emergency response centre was established in Espoo in 1972. (Valtanen, 2009).

Nowadays alerts are received and dispatched by national emergency response centers, of which there are six serving mainland Finland (Ministry of Interior, 2020).

Alerts are received at the fire station via speech over terrestrial trunked radio (TETRA), but also as TETRA unit alerts and short data service (SDS) messages. Regional deviations occur, as for example Keski-Uusimaa Rescue Department uses SECAPP secure communications mobile application to alert contract personnel (Lehti 2017), and Länsi-Uusimaa Rescue Department uses POCSAG pager system (Markkanen, 2007).

Until 2002 command and communications were carried out over VHF radio network and after that a nationwide terrestrial trunked radio (TETRA) network, VIRVE, was taken into use (Erillisverkot, 2020). TETRA offers speech and short-data-service but lacks bandwidth intensive data transfer. Several commercial command and communication systems exists, such as Merlot Mobile and PEKE. Merlot Mobile is developed and mostly used by Helsinki Rescue Department and PEKE is widely used in other parts of Finland, sometimes also by contract fire brigades (Urpila, 2011). PEKE is based on similar command and communications software used by Finnish police, POKE. At its most basic state, a fire engine typically contains at least handheld TETRA radio, a mobile phone, and a GPS navigator. It is possible that the GPS navigator is connected to TETRA radio and receives destination coordinates over-the-air.

Finnish Emergency Services College has carried out several research on command and communication systems used in command units, and those demonstrates the complexity of interconnected systems used in fire engines and other firefighting vehicles. The research and the derived illustration in Figure 1: C&C systems in rescue vehicle describe the vast amount of modern information technology within a modern rescue vehicle.

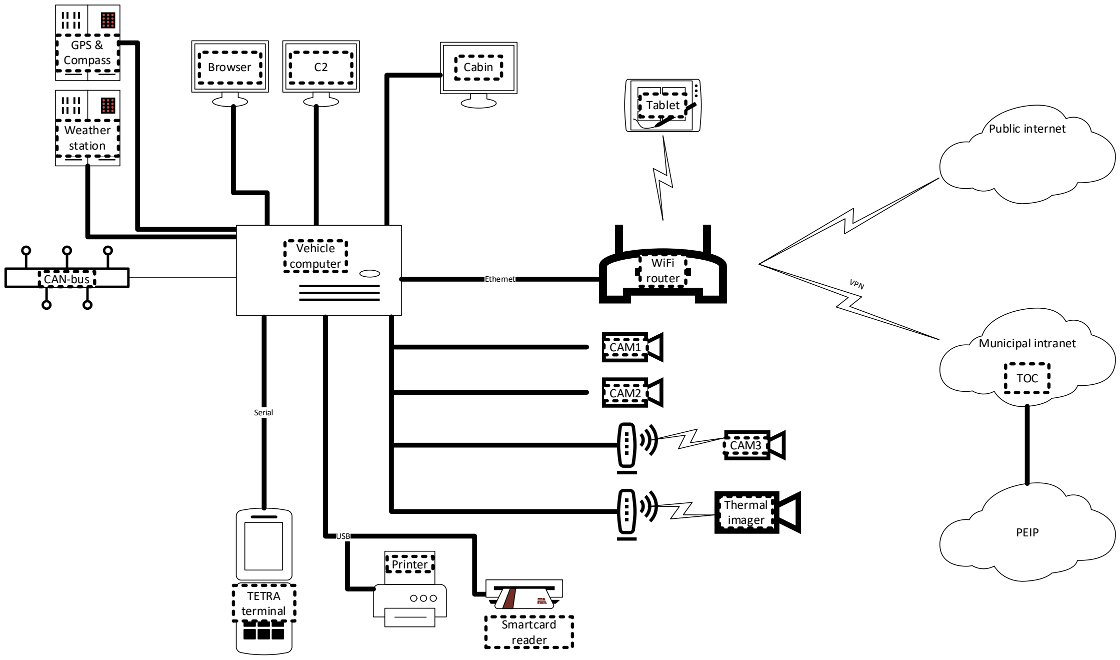

Figure 1: C&C systems in rescue vehicle

1.4 Earlier research

A nation-wide, extensive, and in-depth technical research has not been concluded. However, Marko Heikkilä has researched, as a bachelor’s thesis (fire officer, engineer), information security and data protection within contract fire brigades under Oulu Koillismaa Rescue department. This research was focused on legal basis and regulation of data privacy. As a result, Heikkilä shows, that information security is not trained and instructed sufficiently. It was noted that there is some awareness and issues around information security and data protection has been acknowledged. As the attitude was more towards a hobby than a profession, it was considered to not to be a concern for contract fire brigades. (Heikkilä, 2015)

Mikko Oinonen has conducted a research on information security risks for a single contract fire brigade, Turku volunteer fire brigade. This thesis has had a more in-depth risk and security assessment which is, however, redacted as confidential from the thesis. (Oinonen, 2014)

Tatu Urpila has researched needs for interconnected electronical devices in rescue vehicles, which gives insight for future needs for digitalisation in rescue vehicles. It did not, however, make any considerations regarding information and cyber security. (Urpila, 2011)

1.5 Previous Information Security Incidents

In Finland there appears to be two publicly disclosed cyber incident. Kymenlaakso Rescue Department had faced a breach on their website, and the server hosting it was set to distribute spam email. It was detected by their service provider, who had locked the website. The breach happened due to a vulnerability in open-source content management system. (Kouvolan Sanomat, 2013)

The second incident occurred during the research, in March 2021. The incident occurred in Päijät-Häme Rescue Department, and it was against their Microsoft Exchange server. The occurred breach used a remote code execution vulnerability in Microsoft Exchange Server (CVE-2021-27065). The said vulnerability had been disclosed on 2 March 2021, and the patch for the vulnerability had been released in parallel. The security operations centre had noted the breach, but it had been ruled out as false positive on 3 March 2021. A commercial endpoint detection and response product had raised an alert on 4 March 2021, but that had been also ruled out as false positive. However, during the weekend of 6 and 7 March 2021 the CERT-FI scanned public facing Exchange servers in Finland and the breach was verified that time. Päijät-Häme Rescue Department was notified on Monday 9 March 2021. The breach resulted in about 48 hours of downtime, during which the server was restored from a pristine backup. A third party conducted incident response, and forensics resulted, that the automatic exploit tool used had failed. Only results were the first-stage web shell ASPX-files left on the disk. As such no data leak occurred. The downtime impacted the daily work with no operational impact. (Nieminen, 2021) The time frame is crushing – it took only one day for the breach after the vulnerability had been publicly disclosed. Updating a production email server in such pace would be difficult for any business, let alone a rescue department.

Additionally, two previously non-disclosed security incidents came up during the research, of which other is described below.

In 2017, a contract fire brigade in Länsi-Uusimaa was hit by a website defacement, where links had been altered to direct to adult entertainment website. The breach occurred in an unknown vulnerability within the content management system hosted by a commercial web hotel service provider. It was discovered by an active citizen, who reported the incident to the fire brigade. For the fire brigade there were no methods on finding out the actor behind the breach. The website was built from the scratch and it took about a month to recover. The breach did not have an operational impact.

However, no incidents that have caused disruption in mission critical services are publicly disclosed.

Internationally fire brigades have encountered more cyber incidents. In 2014, North East King County Regional Public Safety Communication Agency announced that two of their fire districts had been breached. Investigation had revealed 6000 medical responses breached as well as personnel records. The personnel records included full-time and volunteer firefighters. No operational systems appear to be affected. (Databreaches.net, 2014)

In 2018, The city of Riverside's Police and Fire department got hit by a ransomware. The affected server was an archive for reports, so it did not affect operations. (HackRead, 2018)

In 2015 fire departments in Massachusetts and Salisbury got hit by a ransomware attack. The attack on Salisbury had an operational effect, as their computerised dispatch centre was forced to proceed with analogue methods. (The Hill, 2015)

In 2016 Honolulu Fire Department's computers got hit by a ransomware attack. The computers were used in administrative duties and reporting. It was separately mentioned that dispatch and command and communication systems operate on a separate network. (Government Technology, 2016)

In October 2019, Emergencyreporting.com, reported about a fire department that had had their internal servers compromised, which led them without the data needed to run operations. However, the details of the breach are unclear. (Emergencyreporting.com, 2019)

It can be summarised, that the events have been mainly affecting the day-to-day work, and operational, mission critical applications have not been affected.

2 Research

2.1 Research objectives

Objective for this research is to find out if there are significant common weaknesses in information technology systems used by contract fire brigades that could affect the daily readiness or missions. Being able to identify these issues enables the field to remediate them and eventually make fire and rescue services more resilient for cyber threats.

Disrupting public safety services, such as fire and rescue services, could enable means for hybrid warfare, where society is disrupted with non-conventional means. As such, it could prove valuable to, for example, a nation state actor.

The base assumption is, that there would be multiple ways to affect the daily operational readiness. However, mission critical systems would be more protected or not that networked and as such not that vulnerable for adversaries. The culture in fire and rescue services is safety-centric, and as such information security is not necessarily the essence. "*We've been able to extinguish fires before the Internet*" is rather common conception, even though the fire engines and command & communication systems are heavily networked in modern world.

The research tries to answer following questions:

- How wide is the attack surface of contract fire brigades' IT systems?
- Are contract fire brigades receiving enough guidance regarding IT security?
- What kind of protections there are in place at contract fire brigades' IT systems?
- What kind of capabilities does contract fire brigades have regarding incident response.
- Are there weaknesses, that can be exploited to cause disruption in day-to-day or mission-critical services.
- How common these weaknesses or vulnerabilities are?

2.2 Research Methodology

The research methodology selected for this thesis is mixed method, as there is a need to obtain results that need to be generalised, but non-quantitative data as well.

Mixed method allows combining quantitative and qualitative data. (Saunders et al, 2009; Alasuutari, 2011)

For discovering the current state of attack surface and capabilities of incident response in general level of the contract fire brigades in Finland a quantitative research method was used. Quantitative method, a survey to be specific, was used because it can be used to generalise the results. It also provides a relatively large dataset with little effort. (Laine, 2007) They survey contains multiple-choice and binary propositions, as well as open questions. The open questions are categorized in a manner that allows reviewing them as quantitative data. Survey is divided in two parts: the first aims on discovering the attack vectors and protected assets, and the latter capabilities for incident detection and response. Issues may arise on the layout and form of questions and questions may be misunderstood easily. (Valli, 2018) These issues are attempted to overcome by proper phrasing and using an IT administrator with contract fire brigade background as a test respondent. The survey had questions, that attempted to gather details regarding the potential threat actors and threat vectors. The survey was conducted as an online Webropol survey. At first the survey got 67 respondents, and later total of 110 respondents. The link for the survey was distributed by The Finnish National Rescue Association (SPEK) and local rescue associations. The survey intended on acquiring large data set that could generalised to describe the information security domain on the field of fire fighting in general. The goal was to reach at least one contract fire brigade in every single municipal fire and rescue departments in Finland. The goal was almost reached, as the participants were from 19 regions from mainland Finland, and single participant was from autonomous community of Åland. As such, this data set represents the field sufficiently.

To uncover common vulnerabilities and weaknesses contract fire brigades may incorporate into their systems, a qualitative method was used. As a qualitative method, case study was used, because vulnerabilities and weaknesses are not necessarily known by the fire brigades themselves. As such these vulnerabilities or weaknesses could not possibly be uncovered using a quantitative method. (Laine, 2007) The case studies were performed as a thorough security assessment for five chosen fire brigades around southern Finland. As the case fire brigades had multiple different systems to be assessed, an exploratory study was conducted to several systems in parallel to the case study. (Edgar et al, 2017) Because the findings are qualitative, they cannot be used as a generalisation for the whole field. As the author has long background in fire and rescue field, case study enables uncovering weaknesses, that may be common to multiple contract fire brigades, and even municipal fire and rescue services.

2.3 Research Ethics

The case studies in this research require incorporating methods considered illegal, unless operated with mutual consent. As such, a security assessment agreement was signed by both the author of this thesis and the contract fire brigades assessed.

As exploitable vulnerabilities may be uncovered during the research, it has been decided to not to disclose them in technically detailed level. Instead, a coarse description will be provided. This is due to the nature of these findings; exploiting them may result in serious consequences, such as material, monetary or human losses. Furthermore, it was decided to disclose the vulnerabilities immediately with the fire brigades in question and the NCSC-FI. The contract fire brigades which participated in the security assessment are to remain unknown to prevent them being attacked. Additionally, the respondents of the survey remain completely anonymous.

The trustworthiness and credibility of studies and material referenced in this thesis are evaluated. Where suitable, multiple references are used. In case where a literature cannot be found, a conference whitepaper of a credible security conference, such as DEFCON or BlackHat, is considered reliable. Articles published by IEEE are considered reliable.

3 Incident Detection and Response Capabilities

It is evident, that at some moment in time an incident will happen, or a breach will occur. The systems and networks should be designed and implemented in a manner, that in the event of a breach the whole system or network is not compromised.

There should always be layers of security, as there are layers on an onion. This is called defence in depth. (Bejtlich, 2013; Hathaway 2014)

In a contract fire brigade, much depends on the level of administration. If everything is outsourced and handled by a third party, there is little for a fire brigade to do, and little responsibility. However, in such case, the responsibilities should be carefully agreed on. For example, if a contract fire brigade outsources hosting of their website, and only manages the content, who is responsible for the breach and work caused by it? In that case, who is responsible for the detection?

3.1 Network Security

Network attacks are initiated over network of some kind; be it wireless, wired, local or wide area. These differ from the previous scenarios described in the section 4.1 OWASP top 10 of this thesis by the location in the OSI model. While they operate in the higher layers, on application or even presentation layer, network attacks occur in the lower layers. Even though network components may be weaponised, here networks are considered merely the way inside the network or to the target asset.

Network level access control can be achieved by proper network firewalling. The network topology should be designed in a manner that adds defence in depth. This may be achieved by proper segmentation. (Uçtu et al, 2019) Bypassing network level access control, such as firewall, is considered a network attack.

Additionally, attacks against wireless (802.11x) network are also considered as network attacks. Wireless attacks aim to either gain access to the network, or to attack the clients connected to it. Connected clients may be attacked by for example KRACK-attack or so called evil-twin rogue access point. (Vanhoef et al, 2017)

Wireless networks' using WEP security algorithm are prone to several attacks, that aim to breach the encryption key protecting the traffic. These include FMS Attack, KoreK Attack, Chopchop Attack, Fragmentation Attack and PTW Attack. (Caneill et al, 2010) As such, WEP has been considered insecure.

Some wireless attacks may be mitigated by using strong pre-shared key and WPA2 or WPA3 where appliable. It is also considered a good practice to limit the coverage of the WiFi signal by limiting transmit power or using specific directional antennas. (Vacca, 2014). Fire brigades are typically unable to implement WPA2 enterprise, as there usually are no AAA servers in place.

3.2 Endpoint Security

Information security on endpoints could be approached from multiple different angles, such as encryption, data loss et cetera. Here, for simplicity’s sake, endpoints are considered as point of origin for an attack.

Endpoint related attacks stem from either bad security practices, such as lax attitude against removeable USB memories and e-mail attachments. These attacks may be prevented by proper patch management, endpoint protection products, proper education of personnel, and aggressive network traffic inspection. (Vacca, 2017)

In addition to the endpoints controlled by the fire brigade itself, fire brigades face the risk that arises from untrusted devices brought to the network by visitors and the personnel of the fire brigade.

3.3 Monitoring and Logging

The ability to detect the security incident, be it a breach in the network or a defacement of the website relies heavily on monitoring. Furthermore, being able to investigate and perform forensic analysis on the said breach relies heavily on logging system and network events. Also, these typically are performed in tandem, as monitoring does not provide any forensic value if there is no sufficient logging in place. (Sanders et al, 2014; Vacca 2017)

As for it is not realistic for a singular contract fire brigade to set up a full-blown security operations centre, it is more important to be able to collect logs in case a breach happens. Properly set up logging enables the contract fire brigade to point out if and what data has been leaked.

4 Common Weaknesses and Vulnerabilities

Although information and cyber security may be affected through wide range of different attack vectors and vulnerabilities, it is not feasible to cover everything imaginable. These weaknesses and vulnerabilities have been chosen as these are common enough for contract fire brigades to be prone to. These are used to assess and categorise findings in the section 6.7 Summary of findings of this thesis.

4.1 OWASP top 10

The Open Web Application Security Project is a non-profit organisation providing information security guidelines for both developers and administrators. OWASP top 10 is a collection of web application security risks. For any web or mobile application OWASP top 10 proves a relevant variety for threats. (The OWASP Foundation, 2020) Additionally, some of these threats can be applied to other systems as well, such as servers or network devices.

OWASP top 10 contains following risks:

1. Injection
2. Broken Authentication
3. Sensitive Data Exposure
4. XML External Entities
5. Broken Access Control
6. Security Misconfiguration
7. Cross-Site Scripting
8. Insecure deserialization
9. Using components with Known Vulnerabilities
10. Insufficient Logging & Monitoring

Injection

Injections occur in the application if it fails to sanitise the user input of malicious content. If the user input is entered to the application without sanitation and used as is, a malicious user may execute malicious commands within the environment the application is executed. Common injection types include SQL, LDAP and OS command injections. (OWASP Top 10 – Injections, 2017; Singh et al, 2018)

SQL injection vulnerabilities occur when the adversary is able to affect the SQL query passed by the web server to the database server. If the application responds to the user with an error message it is called an error-based SQL injection. Another form is called *blind injection*, which happens when the application does not return a visible response. *Blind injection* is more difficult to exploit, as the results for the injection are not visible for the adversary. One method for verifying a blind injection is using a time-based attack. In time-based attack, the injection has a side effect, such as waiting for a period, that is longer than the server would normally take to respond (Clarke-Salt, 2012).

Injections can also occur when user input is directed as is to the underlying operating system shell. In this case, user could execute regular operating system commands from the application. The commands are executed within the context of the application. (Zhong, 2021; Singh et al, 2018)

Injections are best mitigated by implementing proper user input validation. Additionally, prepared statements are effective way to protect against injections. (Injection Prevention Cheat Sheet, 2020)

Broken Authentication

Broken authentication includes several vulnerabilities, such as session attacks, weak or default passwords and brute force attacks. (OWASP Top 10 – Broken Authentication, 2017; Singh et al, 2018)

Typical example for a session attack is session hijacking. It occurs when, for example a Cross-Site Scripting vulnerability is exploited to obtain the session identifier. With the stolen session identifier, the attacker may impersonate the user within the service. (Pauli, 2013; Singh et al, 2018; Nagpure et al, 2018)

Sensitive Data Exposure

Sensitive Data Exposure contains mostly issues with encryption implementation, or the total lack of encryption when sensitive data is transmitted. Sensitive Data Exposure may be prevented by implementing encryption where sensitive data is transmitted. In addition to the implementation, it should be properly configured to disallow weak ciphers suites. (OWASP Top 10 – Sensitive Data Exposure, 2017)

XML External Entities

XML External Entities, or XXE, occur when an attacker is able to upload or modify XML documents within the web application. XXE may be used to, for example, internal network reconnaissance or data exfiltration. It is also possible to cause a Denial-of-Service condition using XXE. XXE's stem from the improperly configured XML parsers. (OWASP Top 10 – XML External Entities (XXE), 2017; Dehalwar et al, 2017)

Broken Access Control

When an attacker is able to bypass the set access controls and, for example, can perform administrative actions without administrative role, the access control is considered broken. (OWASP Top 10 – Broken Access Control (XXE), 2017; Damanik et al, 2020)

Access Control may be bypassed in several ways. A common mistake is to hide a functionality from users on the User Interface (UI) but show it on the administrative or privileged interface. If an adversary is able to discover the specific request used to perform these actions, it is possible for the attacker to perform them as well, if the access control is not implemented properly.

Another example is login functionality, where a hidden form field declares the user role, or other values, such as an IP address, that grants more privileges within application. (Scambray et al, 2011)

Security Misconfiguration

Mistakes in security configurations can provide the attacker wider attack surface or valuable information of the target system. In some cases, it may even allow full compromise of the system. Typically, application configurations aren't hardened by default and they need additional configuring to enhance the security posture and make the application usable. Security misconfigurations may be mitigated by following the hardening guides provided by either the software or hardware vendor, or by following the CIS hardening guides. (OWASP Top 10 – Security Misconfiguration, 2017)

Cross-Site Scripting

Cross-Site Scripting (XSS) vulnerabilities target the user browser and the data within, and can be divided into three types:

- Reflected XSS
- Stored XSS
- DOM XSS

These types deviate from each other by where the malicious script resides. Reflected XSS occur within the current HTTP request. It typically requires heavy user interaction, or user opening a link containing the malicious script. (Vijayalakshmi et al, 2017; Singh et al, 2018)

Stored XSS originates from the web page itself. Stored XSS does not require any user action, because the malicious script already exists on the webpage the victim is visiting. For example, a comment section of a webpage might contain such a vulnerability, if the input has not been validated and output has not been filtered properly.

DOM XSS executes within the client-side JavaScript. This requires the JavaScript to construct elements dynamically from the user input without proper input validation and output filtering. (Portswigger – Cross-Site Scripting, 2021; Vijayalakshmi et al, 2017; Singh et al, 2018)

Cross-site scripting vulnerabilities may be mitigated by implementing user input validation and output filtering. User input should always be validated by the expected data type. Additionally, when user is allowed to enter potentially malicious content, the output should be properly filtered. Additional layer of security may be added using browser security headers, such as *X-XSS-Protection* and *Content-Security-Policy*. (OWASP Top 10 – Cross-Site Scripting, 2017; Vijayalakshmi et al, 2017; Singh et al, 2018)

Insecure Deserialization

Insecure deserialization occurs when the application uses serialized data without properly verifying the contents and ensuring their integrity. Insecure deserialization typically leads to remote code execution.

Insecure deserialization may be mitigated by implementing integrity checks on the serialized content. It is intended to prevent tampering with the serialized data. (OWASP Top 10 – Insecure Deserialization, 2017; Dehalwar et al, 2017)

Using components with Known Vulnerabilities

As modern applications typically use several languages in both server and client side. In addition, they tend to have multiple different libraries, with cross-dependencies. This means that it is more difficult to be aware of all the software, their versions and potential vulnerabilities within the application. This easily leads into situation where there are components with known vulnerabilities, and in the worst case there are publicly disclosed exploits available. This attack vector is usually caused by non-existent or badly implemented update policy.

This may be mitigated by limiting the number of different components and reviewing their dependencies before taking software into use. Furthermore, installing updates regularly help to keep up with security patches. (OWASP Top 10 – Using Components with Known Vulnerabilities, 2017; Dehalwar et al, 2017)

Insufficient Logging & Monitoring

Issues with logging and monitoring appear in systems that do not offer undeniable audit trail or that do not log events properly. Additionally, if the environment lacks a centralised logging service, the overall logging is determined insufficient. Also, if there is no monitoring or no process for actions upon alerts or detected issues, the monitoring is considered insufficient. Logging issues may be mitigated only by enhancing logging and monitoring capabilities. (OWASP Top 10 – Insufficient Logging & Monitoring, 2017; Dehalwar et al, 2017)

4.2 Security Management and Policies

Issues relating to security management and policies relate in overall bad information security practices. Security management and policies include all non-technical issues in information security. These include, but are not limited to, proper password policies, and password usage and management. Additionally, proper plans for continuity, disaster recovery and incident response are included in security management and policies. (Vacca, 2017)

4.3 Radio Frequency Replay Attack and Command Injection

As any business or organisation, fire brigades use devices that are controlled by signals on radio frequencies. These devices include remote opening system for garage doors, building management systems and IoT devices. These systems typically operate on ISM band (industrial, scientific, and medical), usually on 433MHz or 868MHz frequencies (Andersson et al, 2018).

Relevant methods for attacking aforementioned devices are replay attack and code injection. In replay attack the adversary simply records the command on the specific frequency and then replays the recording to the receiver. If the receiver is vulnerable to such attack, it will perform the actions as directed by the command. Replay attack can be mitigated by rolling-code mechanism, where a transmitter sends the 'next' sequentical code and receiver compares the received 'next' code to calculated one. (Andersson et al, 2018; Greene et al, 2020) However, in DEFCON23 (2015) Samy Kamkar presented a method to attack rolling codes (Kamkar, 2015).

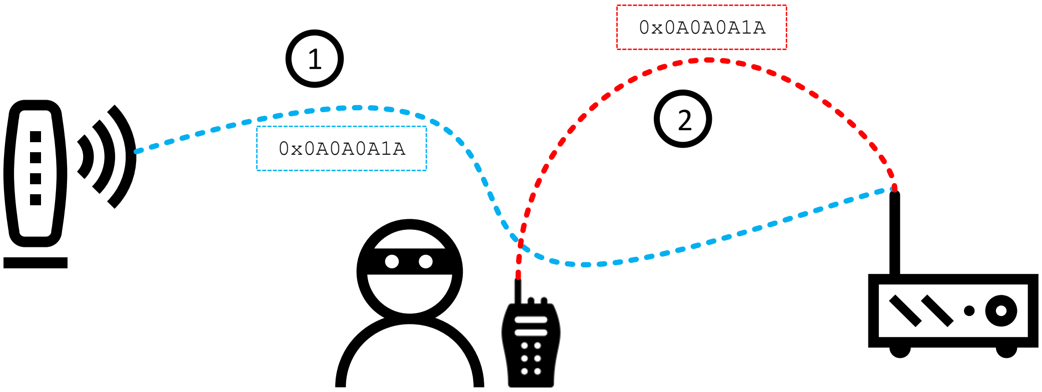

Figure 2: Replay attack

The Figure 2: Replay attack above describes the phases in replay attack. First, a RF device transmits a command over radio frequency. After that, the attacker replays the previously recorded command.

In command injection attack the command is recorded as in replay attack, but afterwards the transmitted signal is studied and used to derive other commands. These commands may be used in later phase of the attack.

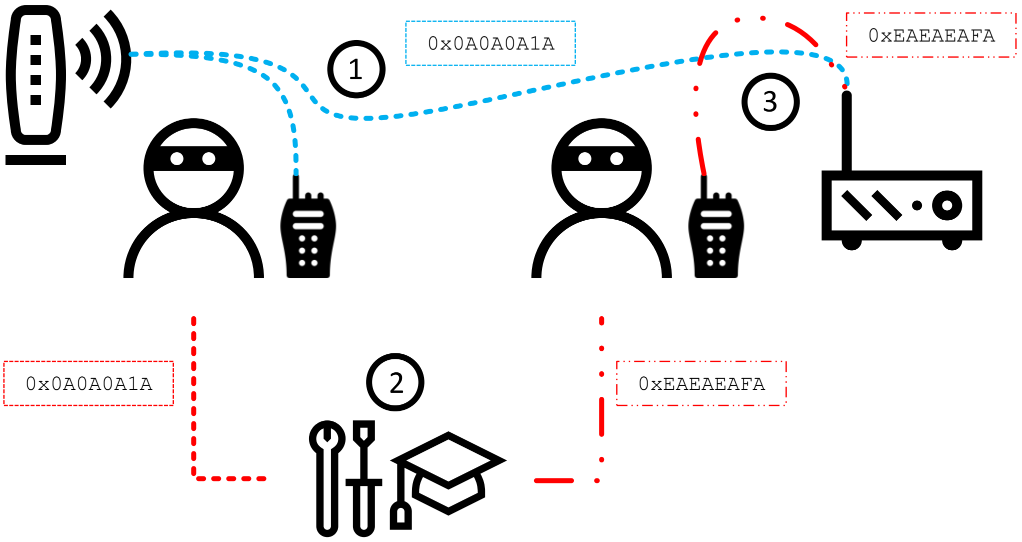

Figure 3: Command injection

The Figure 3: Command injection above illustrates the flow of code injection. First, a RF device transmits a command over radio frequency. In second phase that command is studied, and reverse engineered carefully. Finally, the attacker is able to inject own command over the radio frequency. (Andersson et al, 2018)

5 Survey

The survey was conducted as a Webropol-survey. The link for the survey was distributed by SPEK and it received 67 responses. That means about 10 percent of contract fire brigades responded for the survey. On some rescue departments, the response percentage were 0% or close to it. Due to need for getting responses from the whole country, the survey was re-opened, and the link was distributed directly to fire brigades in those rescue departments that had low response rate.

Rescue Department	Percentage
Helsinki Rescue Department	25,00 %
Tampere Region Rescue Department	23,50 %
Keski-Uusimaa Rescue Department	22,60 %
Varsinais-Suomi Rescue Department	20,80 %
Satakunta Rescue Department	20,00 %
Länsi-Uusimaa Rescue Department	19,10 %
Etelä-Savo Rescue Department	18,20 %
Etelä-Karjala Rescue Department	17,40 %
Central Finland Rescue Department	17,40 %
South Ostrobothnia Rescue Department	15,20 %
Rescue Department for Central Ostrobothnia and Pietarsaari	14,30 %
Pohjois-Savo Rescue Department	13,30 %
Kymenlaakso Rescue Department	13,20 %
Kanta-Häme Rescue Department	12,50 %
Pohjois-Karjala Rescue Department	9,50 %
Rescue Services of Lapland	9,10 %
Ostrobothnia Rescue Department	9,10 %
Päijät-Häme Rescue Services	9,10 %
Ahvenanmaa Autonomous Region	7,10 %
Eastern-Uusimaa Emergency Services Department	7,00 %
Jokilaakso Rescue Service Department	0,00 %
Kainuu Rescue Department	0,00 %
Oulu-Koillismaa Rescue Department	0,00 %

Table 1: Percentage of responded fire brigades per rescue department

The Table 1: Percentage of responded fire brigades per rescue department above shows the percentage of responded fire brigades per rescue department. Rescue departments of Jokilaakso, Kainuu and Oulu-Koillismaa received no responses at all, even though a direct request for answering the survey was sent for the fire brigades in those regions. These rescue departments have 37 contract fire brigades, which is about 5 % of all contract fire brigades.

Figure 4: Respondents by Rescue Department shows the distribution of participants by Rescue Department and the total amount of contract fire brigades by Rescue Department. The amount of contract fire brigades under a rescue department correlates partially with the number of participants per rescue department.

An assumption was, that these fire brigades could be Finnish-Swedish fire brigades, with Swedish speaking personnel, which could result in zero responses, but that does not appear to be the case. None of these contract fire brigades appear to be primarily Swedish speaking.

Total of 13,2 % of contract fire brigades in Finland responded for the survey.

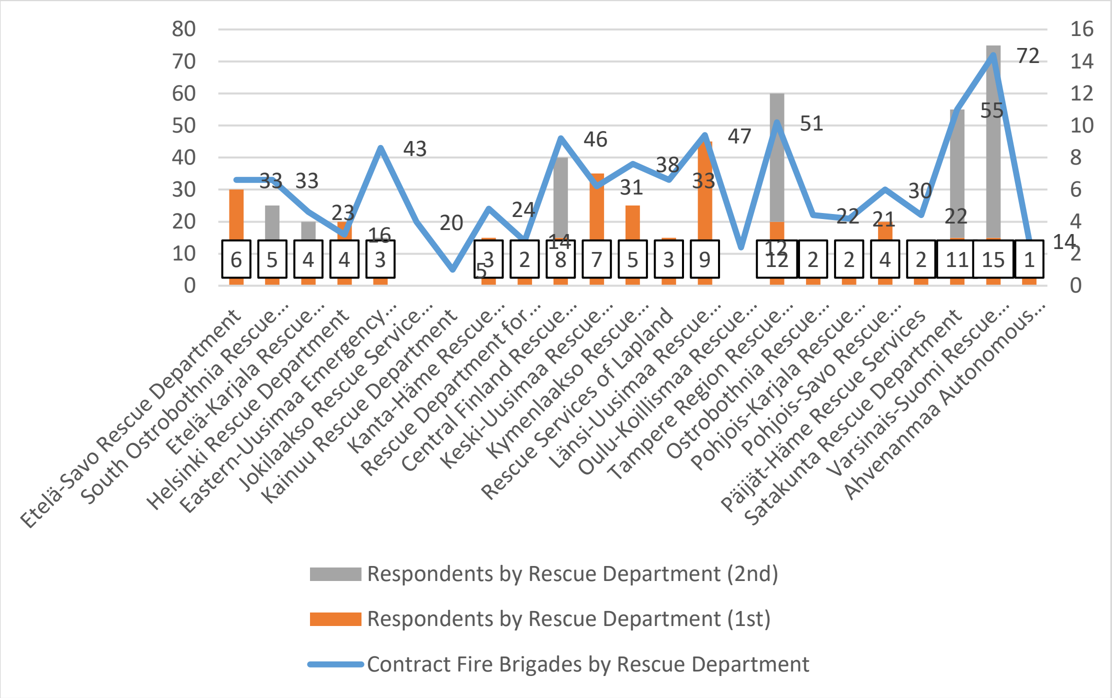

Figure 4: Respondents by Rescue Department

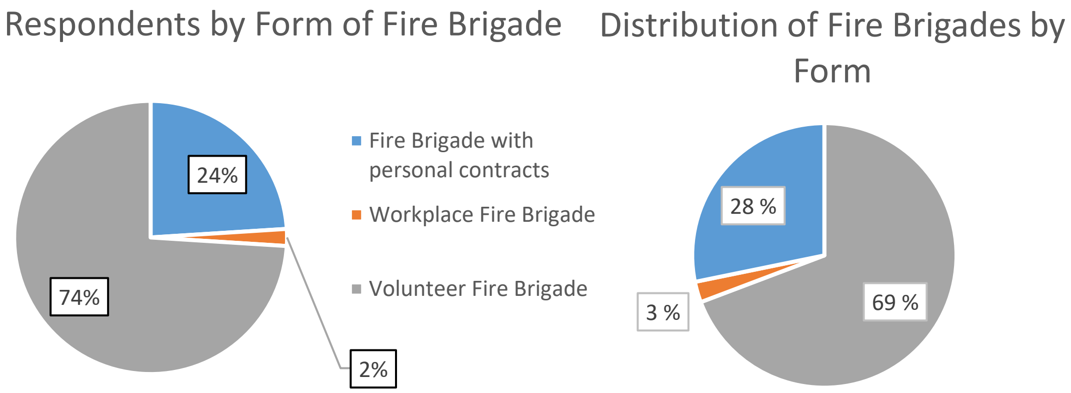

Figure 5: Distribution by the form of fire brigade

The above Figure 5: Distribution by the form of fire brigade displays the distribution by form of the fire brigade. In 2015, there were 491 volunteer fire brigades, 200 fire brigades with personal contracts and 18 workplace fire brigades (Koivunen, 2015). There were slightly more respondents from volunteer fire brigades than workplace fire brigades and fire brigades with personal contracts.

The survey had 25 arguments, where the respondents could answer by either true or false statement, or with a five-step slider with another end being Strongly agree and another Strongly disagree. Additionally, there were open question forms for describing or commenting answers.

5.1 Attack Vectors and Assets

The survey aimed on mapping attack vectors that might be common for contract fire brigades, and to find deviances between rescue departments.

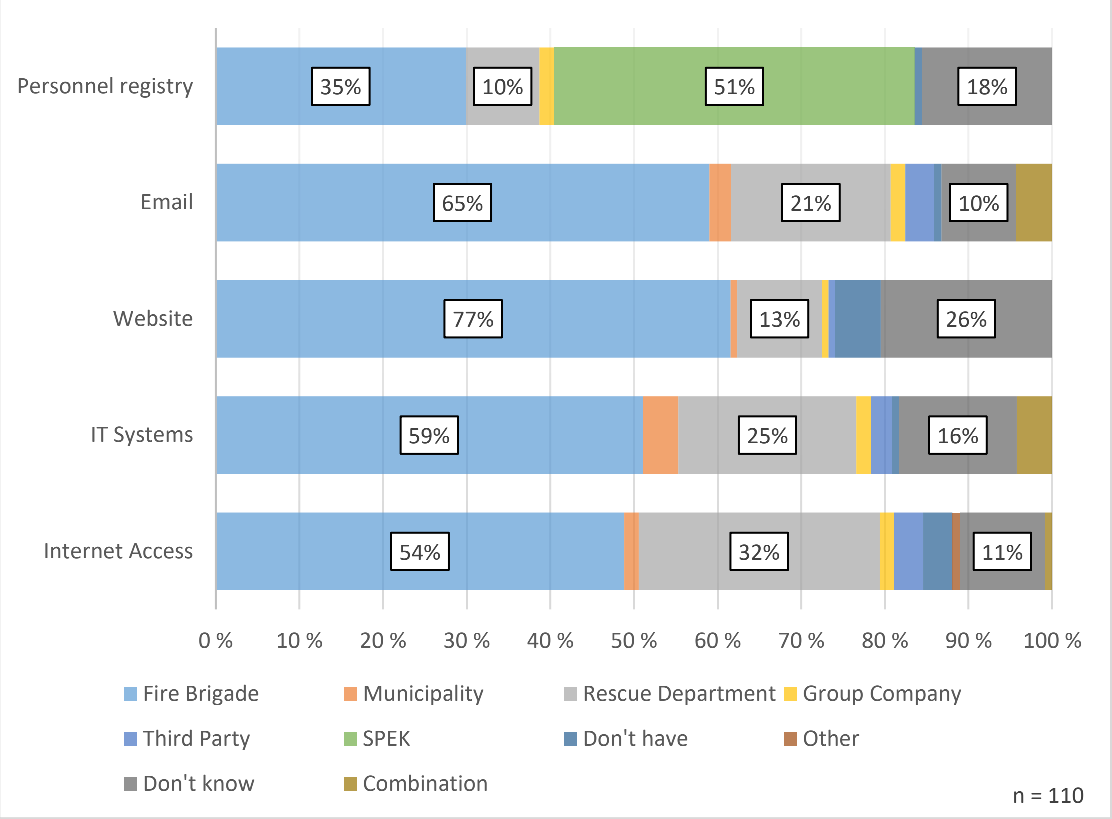

Figure 6: IT responsibilities

The above Figure 6: IT responsibilities shows how the responsibilities for different IT systems are distributed. Usually, the fire brigade itself takes care of everything, but for example the personnel registry is usually outsourced for SPEK, as most fire brigades use HAKA register.

Typically, workplace fire brigades use the resources of their group company, and do not have to administrate anything by themselves. Additionally, in some cases the local municipality offered resources for fire brigades' use and few fire brigades have been able to outsource the responsibilities to third party. Also, in some cases the responsibilities are mixed. For example, municipality or rescue department may provide some resources, such as email addresses, or internet connection to specific service, but the fire brigade itself supplements it.

A surprising finding was, that on year 2020 there are few fire brigades without any kind of internet connectivity or website.

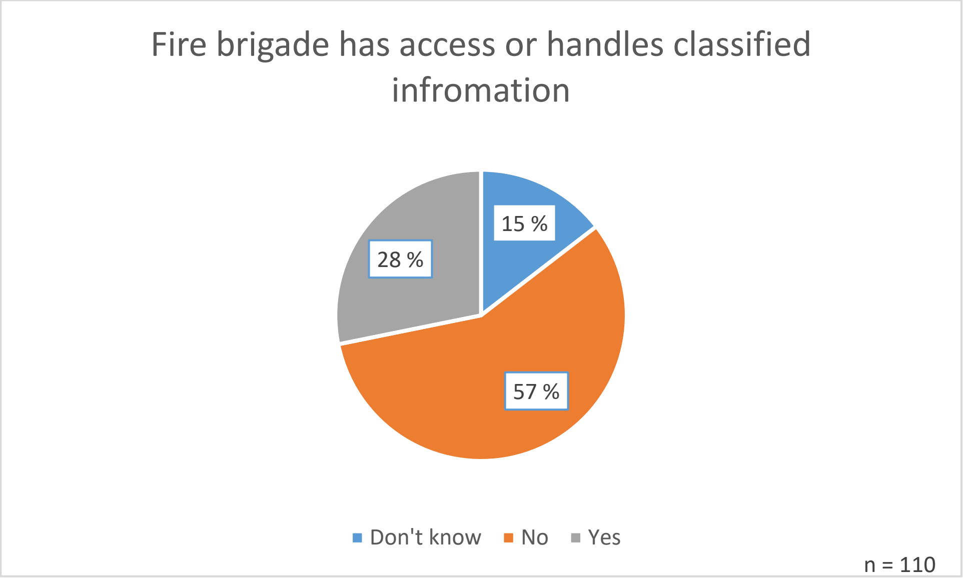

Figure 7: Handling of classified information

The Finnish law has defined classification of sensitive information. The classification system is four-tiered and is illustrated in the table below (VA 1101/2019, 2019):

Class	Label
TL IV	RESTRICTED
TL III	CONFIDENTIAL
TL II	SECRET
TL I	TOP SECRET

Table 2: Information classification in Finland

Handling, storing, and disposing classified documents are well set in the law, and concrete guides for authorities are provided by state administration. According to the Figure 7: Handling of classified information, a little less than third of the respondents consider, that their fire brigades does handle classified information.

Open responses show five respondents referring to Pronto, which is a fire and rescue resources and accident statistics tool, provided by Ministry of the Interior and maintained and developed by Finnish Emergency Services College. It is used nationwide. (Prontonet, 2020) However, no classified information is handled in Pronto. Nevertheless, the information may be otherwise sensitive and confidential. At the moment of interview, there was no knowledge if the system has been under a technical security assessment previously. Yet, the system has been audited by applying KATAKRI (Kansallinen turvallisuusauditointikriteeristö, Information security audit tool for authorities) by National Police Board. (Liukkonen, 2020)

Another one referred to Store, which is personnel and resource management solution, that is provided as SaaS solution. It is used for shift planning and payroll, for both contract and permanent staff of the rescue department. It is currently mainly in Kymenlaakso Rescue Department. (Probis, 2020)

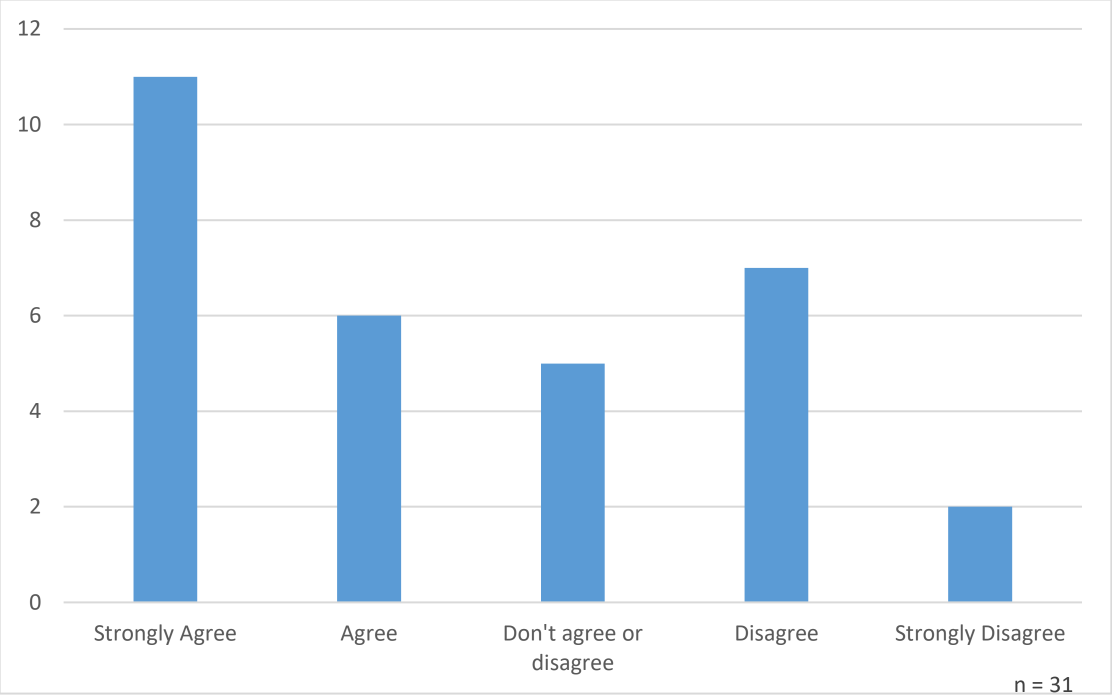

Figure 8: Rescue department has given guidance on classified information

For the respondents, who answered yes on the question if they handle or have access to classified information, additional question was shown. It was an argument "*Rescue department has given guidance on how to handle, store and dispose classified information.*" The question was a slider, where value 0 was *Strongly Disagree* and value 4 *Strongly Agree*. Responses were distributed as is shown in the Figure 8: Rescue department has given guidance on classified information. The average response is 2.55, which would indicate that majority agree with the argument. However, the Figure 8: Rescue department has given guidance on classified information shows that the responses are heavily distributed.

Respondents, who answered with either Disagree or Strongly disagree were from following rescue departments:

- Pohjois-Savo Rescue Department,
- Tampere Region Rescue Department,
- Kanta-Häme Rescue Department,
- Helsinki Rescue Department,
- Keski-Uusimaa Rescue Department,
- Päijät-Häme Rescue Department,
- Central-Finland Rescue Department
- Varsinais-Suomi Rescue Department.

If there was another respondent from the same rescue department, the response was either *Agree* or *Strongly Agree*. As the sample for this argument was relatively small and responses were conflicting, no conclusion can be made. Additionally, it is possible that the argument has misunderstood in a positive way. As fire and rescue departments are municipal authorities, they do not classify their information as described in Table 2: Information classification in Finland. Instead, they may have independent methods on labelling confidential and sensitive information.

Several Boolean, *True* or *False* statements also made.

- Members of the fire brigade use personal accounts in fire brigade related matters.
- Fire brigade has a wireless network.
- Fire brigade has internet connected devices in their vehicles.
- Fire brigade has internet connected devices.
- Fire brigade has an electronical automation system for building systems.
- Fire brigade has an electronic access control system.
- Fire brigade has a system for informing personnel if one can respond for an emergency.

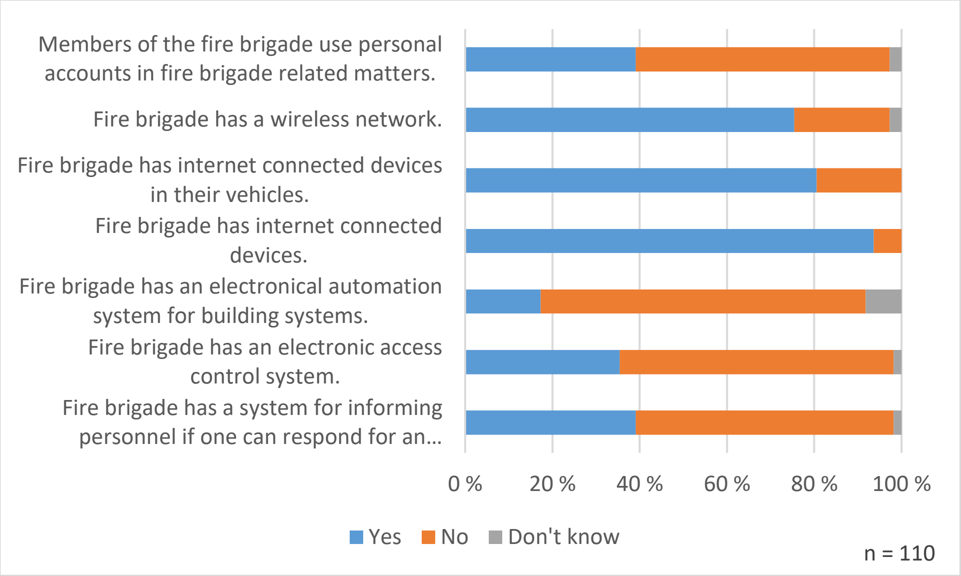

Figure 9: True and false statements

Figure 9: True and false statements shows the distribution of responses to true or false statements. A significant risk arises, as majority of fire brigades do not use personal accounts for fire brigade related matters. This is considered bad practise. There are several issues with using shared account. For example, as multiple people have access to a single account, it is more difficult to provide an audit trail, and as such it is significantly harder to monitor usage. If an information security incident happens, such as data leak, it will be more difficult to investigate and gather forensic evidence. Additionally, shared user accounts make password changes difficult, especially if no password management software is used. Shared passwords tend to be weak, such as *Summer2020*. Also, when personnel change, the password for shared account is usually not changed, resulting multiple people knowing the password. (Johnson 2020)

Open comments reveal that it is very common, that fire brigades have a common computer, which has a single shared account. This is typical solution around Finnish fire brigades, and it is possible to harden these workstations so, that the shared account is relatively safe to use. It was also mentioned that the contract personnel do not have access to the network of the rescue department (South-Ostrobothnia Rescue Department). Another respondent commented that there are no personal accounts for any IT systems provided by the rescue department (Varsinais-Suomi Rescue Department).

Few fire brigades have building automation system. This may provide an attack vector for disrupting both day-to-day functions and operational readiness. NSCC-FI has scanned and researched Finnish internet connected devices and discovered hundreds of insecure building automation devices (NCSC-FI 2019).

Less than half of the respondents acknowledged, that the fire brigade has electronical access control or a system for informing personnel if one is able to respond for an emergency. Attacking these two would provide methods for disrupting both day-to-day functions and operational readiness. Electronic access control systems are typically based on RFID-tags. RFID has weaknesses for both *sniffing* and *spoofing*, which allows cloning of the access control tag. (Vacca, 2014) RFID tags can be cloned easily with relatively cheap and easy-to-use equipment, such as Proxmark (Proxmark, 2020). There are few commercial software used for informing personnel if one is able to respond on emergency, such as Secapp and Elektro-Arola Salsa. It would disrupt the operational readiness if the availability or the integrity of data of such systems could be influenced.

80 % of the fire brigades have internet connected devices, such as command & communication and navigations systems, in their vehicles. Influencing the availability of these, or the integrity of the data they provide would significantly disrupt the operational readiness.

In addition to the true or false arguments it was asked what greatest concern about information security of the fire brigade is. The answers were classified with one or more classes. The classes intend to describe the concern in unified way. Classifying varying comments proved to be difficult. Using CIA-triad or STRIDE for classifying these comments allowed classifying only a quarter of comments, which would not give sufficient sample. Instead, a multi-dimensional threats classification model was used. This classification model was introduced in The 5th International Conference on Ambient Systems, Networks and Technologies (ANT 2014). The model is created by Mouna Jouiniam, Latifa Ben Arfa Rabaia and Anis Ben Aissab. It aims on combining threat techniques and impacts, as well as threat actors and attack vectors. The model is further described in the Figure 10: The multi-dimension threats classification model (Jouiniam et al, 2014) below.

This hybrid model classifies threats with a five-tier method:

1. Threat source
2. Threat agent
3. Threat motivation
4. Threat intent
5. Threat impact

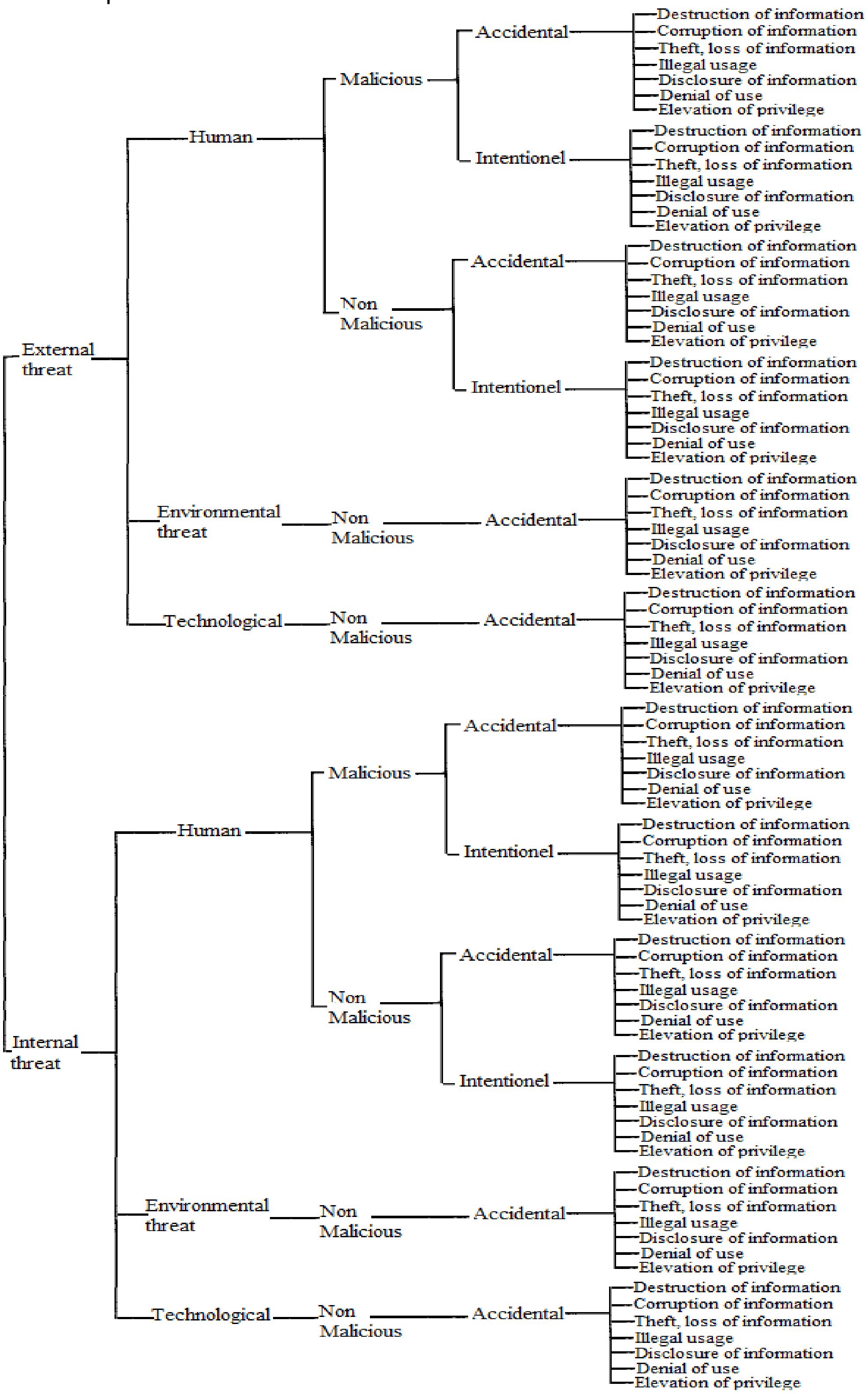
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Malicious
Human
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Non Malicious
External threat
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Environmental threat
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Technological
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Malicious
Human
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Non Malicious
Internal threat
Intentionel
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Environmental threat
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege
Technological
Non Malicious
Accidental
Destruction of information
Corruption of information
Theft, loss of information
Illegal usage
Disclosure of information
Denial of use
Elevation of privilege

Figure 10: The multi-dimension threats classification model (Jouiniam et al, 2014)

Most responses allowed classifying until the threat impact, as usually it was not included in the response. Additionally, many responses contained several different threats and allowed multiple classes. As such 50 entries were classified. In slightly over half of the responses, 52%, the threats were classified as external, and rest were classified as internal. Out of all entries, 64% were classified as human threat, 26% as technological threat and 10% as environmental threat. In 72% of cases the intent was classified as non-malicious and rest as malicious threats. It is also worth noting, that every malicious threat was considered as an external threat.

The impact was classifiable in 13 cases out of 50, and 38% were classified is disclosure of information, 23% with denial of service. Rest were *Destruction of information* (15%), *Illegal usage* (15%) and *Theft, loss of information* (8%).

Common denominator is user. Internal human error, with non-malicious intent by accident was classified 19 times. If it was possible to define impact, it was disclosure of information in all the cases. Many of the respondents were concerned about loss of data in form of user accounts and passwords, or even privacy related data gathered and cumulated from the emergency site.

5.2 Capabilities for Incident Detection and Response

In addition to the attack vectors, incident detection and response capabilities were surveyed. Figure 11: Incident response capabilities displays personnel, hardware, and software capabilities for incident response in fire brigades.

In roughly half of the cases (52%) the fire brigade has a person responsible of IT infrastructure. In many cases, fire brigade has an IT administrator, who is in that role either by profession or chance. Typically, there is only one person, not a complete team with varying technological know-how. As mentioned before, some have background in IT field, but many are in the role with a consumer knowledge of IT.

Slightly less than half of the respondents (44%) said to have a person responsible for information security matters. The percentage seems high, and there is possibility that respondents have mixed up data protection and privacy with information security. Nonetheless the IT administration and IT security tend to be connected.

11 % of the respondents said that their fire brigade had encountered an information security incident, such as a breach or website defacement. Out of those responses, up to 83% had investigated the incident. This percentage also seems high in the light of the previous responses.

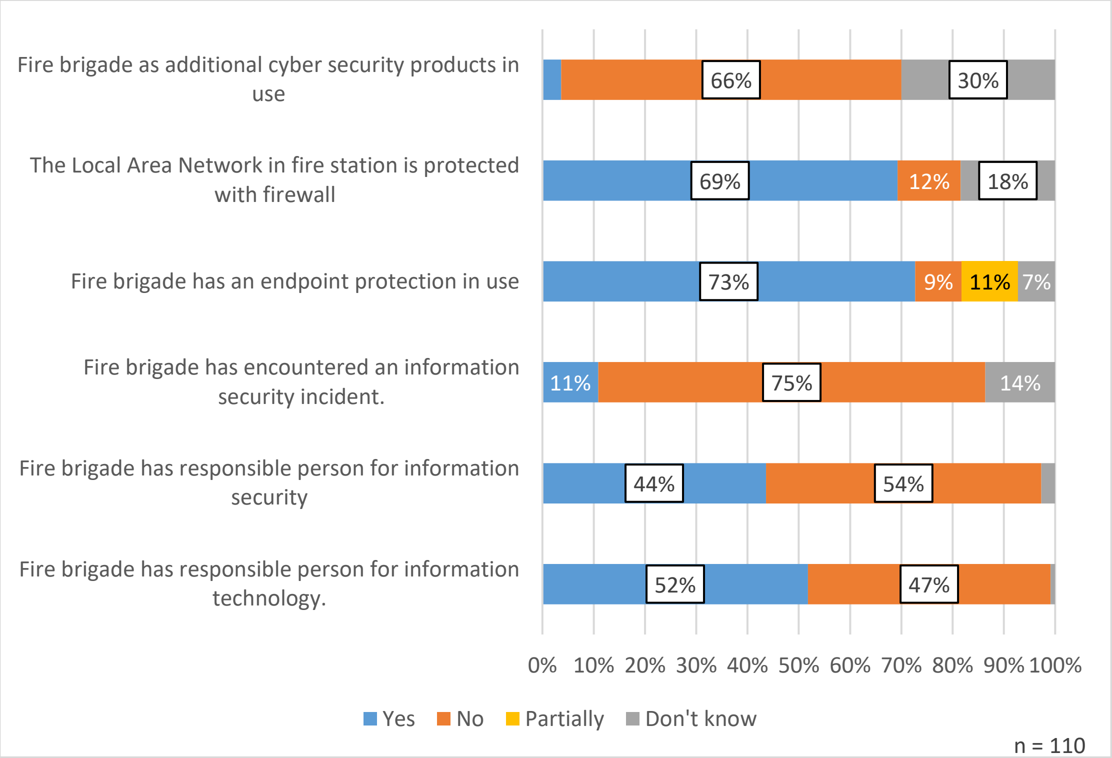

Figure 11: Incident response capabilities

73% percent of the respondents have endpoint protection installed in the devices they use. 11% responded as partially, and open comments described that typically Microsoft Windows PCs have anti-virus and firewall of some kind installed, but tablet devices and smartphones do not have. Additional comment was that their Linux server do not have endpoint protection.

69% percent of the respondents said that the local area network (LAN) of the fire brigade is protected with a network firewall. Given that about half of the respondents said their fire brigade have an IT administrator, this number also seems relatively high. It is more likely, that the fire brigade has a consumer grade modem or router capable of network address translation (NAT) that does prevent the public internet accessing the internal network.

Four percent of the respondents told to have additional cyber security products in use. Open comments mentioned protected connections to remotely piloted aircraft system (RPAS) and virtual private networks (VPN).

In the incident detection and response category there were two five-tier arguments, which are illustrated in Figure 12: Incident response and guidance below.

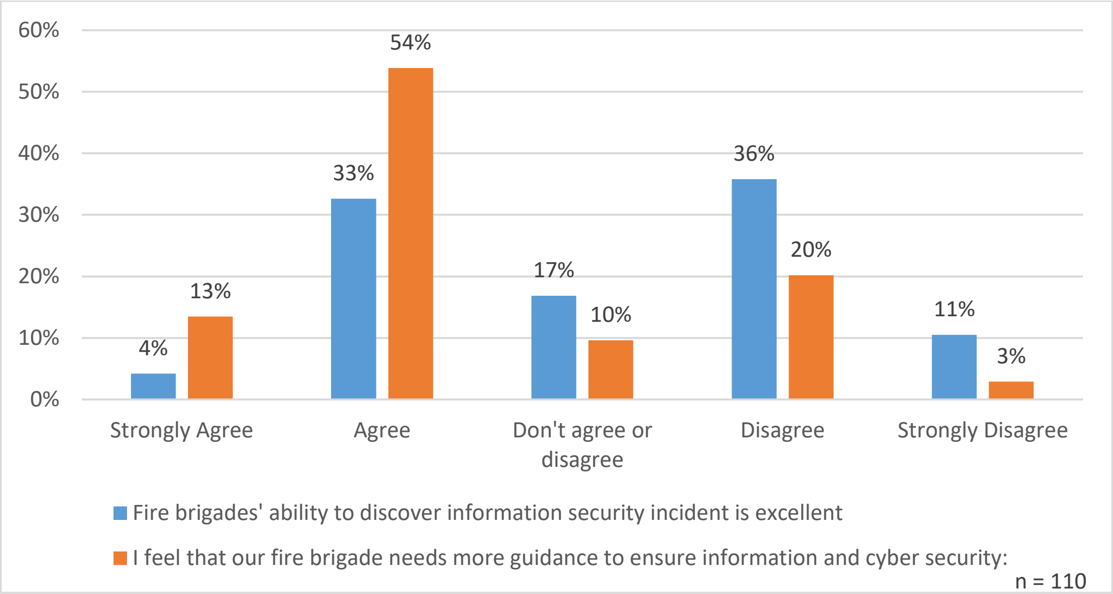

Figure 12: Incident response and guidance

The argument "*Fire brigades' ability to discover information security incident is excellent*" had an average of 1.84, which would round up to "*Don't agree or disagree*". The argument "*I feel that our fire brigade needs more guidance to ensure information and cyber security*" had an average of 2.61, which would round up to "*Agree*".

The distribution, however, for the argument "*Fire brigades' ability to discover information security incident is excellent*" is mixed, with slight lean-to disagreement. Mostly respondents do agree on the argument "*I feel that our fire brigade needs more guidance to ensure information and cyber security*".

In addition, open comments were classified with forementioned multi-dimensional hybrid classification model. 39 comments were classified.

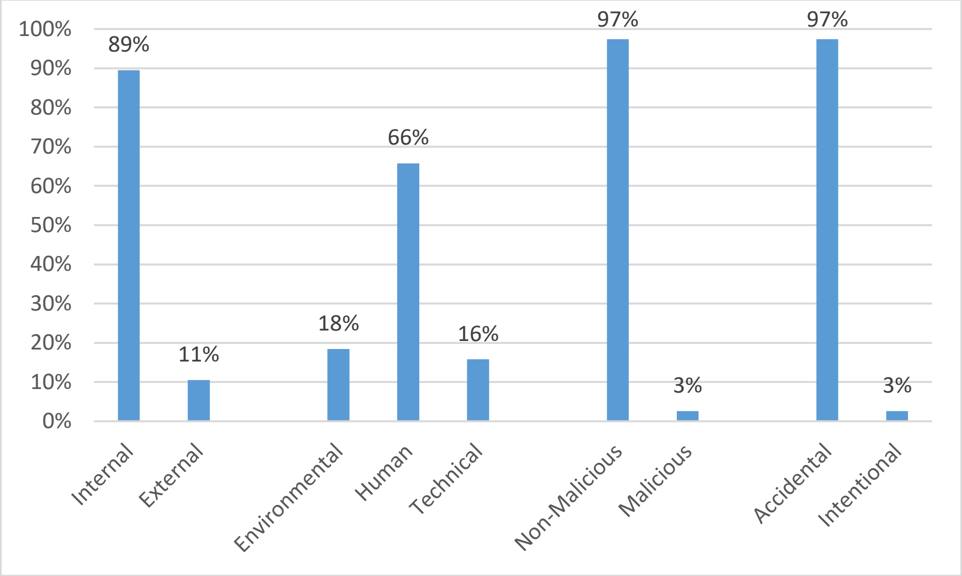

Figure 13: Incident response classifications

Figure 13: Incident response classifications above illustrates the classifications of open comments on concerns regarding incident response capabilities. The most common concern was human; lack of exercise, knowledge and education. The userbase is vast and IT experience is varied. It was also noted that fire brigades do not have technical means to monitor and detect incidents. Many feels, that they are totally dependent on Internet Service Providers or the municipal rescue department.

6 Case Studies

In addition to the survey, several case studies were conducted. The participants were gathered from the participants of the survey. All participants are from Southern Finland region, although only few are from the capitol area.

Prior to the case study, a scoping meeting was held with the representative from the fire brigade. These persons were responsible for administrating the information technology infrastructure in those fire brigades. The extent of the security assessment was agreed upon in the said scoping meeting. In several cases, this was a wake-up call regarding the responsibilities on the IT infrastructure. Amount of documentation were close to none and thus it required vast amounts of investigation and research to find out which systems are in use, what for and where they are hosted.

Parts of cyber kill-chain described in *1.1 Information and Cyber Security in General* of this thesis were conducted. For resources, that were under the administration of certain fire brigade, a reconnaissance was conducted. Shared environments and software-as-a-service platforms were ruled out of the reconnaissance phase, as it could have disrupted service of other clients using the same service. After reconnaissance, if there were any vulnerabilities discovered, they were weaponised and afterwards delivered and exploited. During these assessments, Installation, Command & Control and Actions on Objectives were not performed.

For remote servers and web services, reconnaissance was performed using Nmap, Nikto and dirb. On server hosts, a cis-cat collector was executed.

6.1 Case 1

Fire brigade in case 1 operates under Keski-Uusimaa rescue department, and is typical, yet active fire brigade in the area, with around 100 missions on yearly basis. They have a rescue unit, tanker unit and personnel carrier. Information Technology is managed by a member in fire brigade who is an IT administrator by profession. However, there is not much of dedicated IT security in place.

Publicly Available Services

The fire brigade has their e-mail set up on Office 365 and their website hosted in Azure. In addition to their Internet site, they hosted an in-house developed, mission critical web application that was used to support fire water logistics. The application is supposed to be used with internet browser on mobile device that supports location services.

Other Services

In addition to publicly accessible services, the fire brigade had a monitoring server set up. The server user Paessler PRTG as monitoring software. It was intended mostly on monitoring availability of services and validity of certificates used on publicly available services.

Local Area Network

The local area network was simple flat network. They had a local server in the network, but that was ruled out-of-scope, as they were in process of ditching the server.

Wireless Network

Wireless networks were set up with the consumer-grade wireless routers, that had same SSIDs and they granted access to the same local area network.

Network Topologies

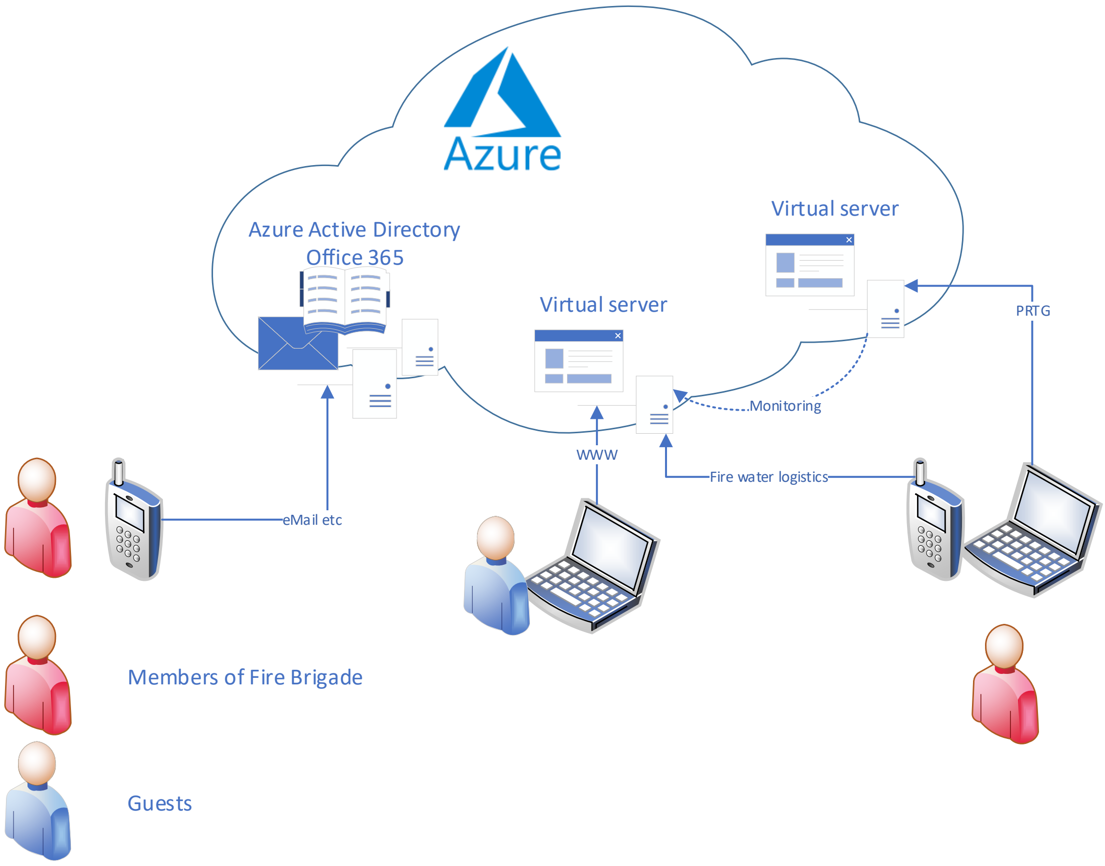

Figure 14: Publicly available services

The Figure 14: Publicly available services above illustrates the services and related topology in Azure. The one virtual server running Centos Linux serves both the website of fire brigade and an application used for fire water logistics. The Figure 15: Local services shows the topology of local services on the fire station. It shows, that even though there is a relatively large local network, it does not have valuable assets for the attacker.

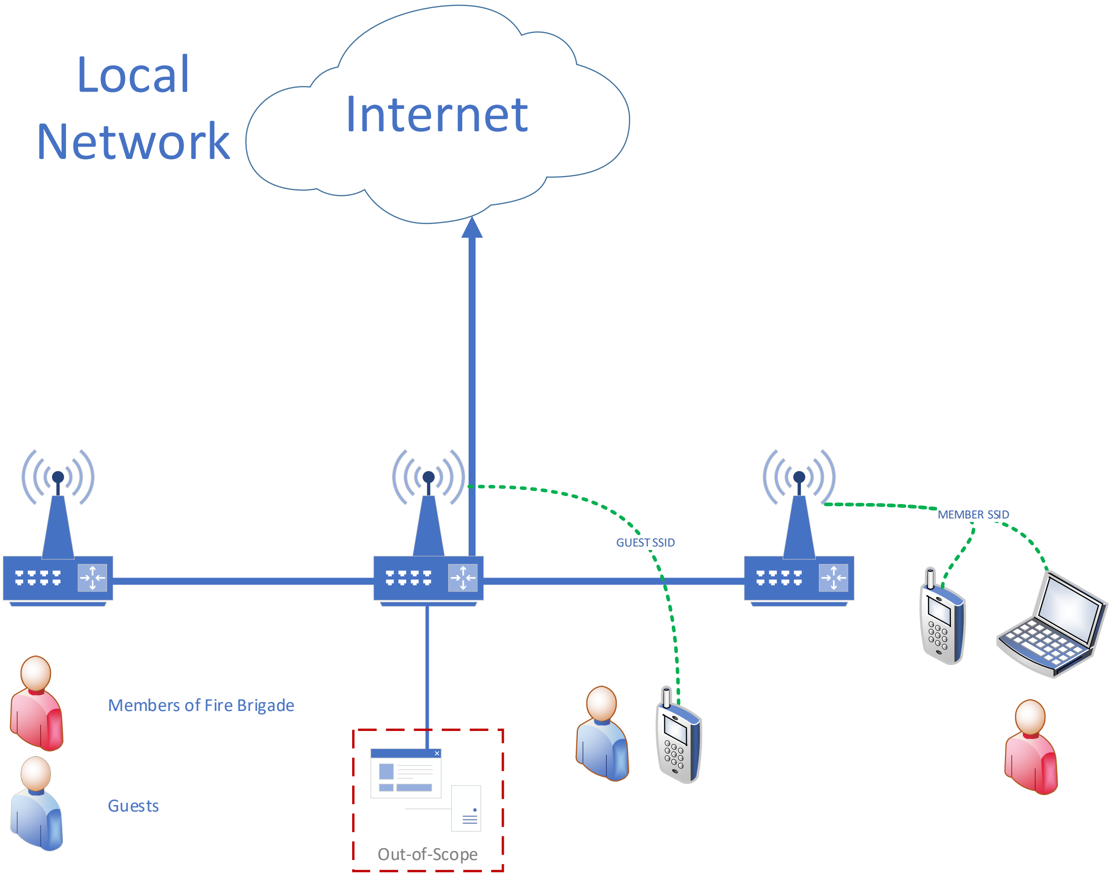

Figure 15: Local services

The network described in Figure 15: Local services is of flat topology. In the local area network, there were not much of mission critical applications or information.

Summary of Findings in Azure

There were few weaknesses in the configuration of Azure environment. Although these could not be leveraged and used to take down or disrupt mission critical services, remediating them will enhance the security posture. Most important finding in the Azure was lax firewall settings, which allowed management traffic from wide network area, which appeared to belong to Telia. Furthermore, the operating system disks were not encrypted.

Summary of Findings in Publicly Available Services

The most important findings in publicly available services are described in section *6.6 Major Findings* of this thesis.

Several other findings also exist. The web application had a backup file, let it be *backup.zip*, in the root of the public web server. This was easily found and acquired using Nikto Web Vulnerability scanner during the reconnaissance phase of the assessment. Nikto Web Vulnerability Scanner is used to detect the web server and configuration issues. Additionally, Nikto does detect files and and directories that should not be publicly accessible. (Nikto Developers, 2020) The said backup file contained the full source code for the application and database credentials. This allowed performing a source code review that was not originally in scope, and it made it rather easy to spot an SQL injection in the application.

There were also issues with implementing preventive measures for Cross-Site Request Forgery (XSRF) attack.

Furthermore, the Joomla version used were found outdated, although there were no security issues fixed in the more recent versions.

Summary of Findings in Local and Wireless Network

The network had a flat topology, with three consumer-grade wireless access points. In addition, there were no servers or other high-value targets. Wireless network was configured with WPA2 and PSK, and two access points out of three were configured with WPS. It was possible to capture the WPA2 handshake over-the-air. However, the PSK was strong enough, that it was not possible to crack it during the assessment.

6.2 Case 2

The fire brigade in case 2 operates under Länsi-Uusimaa rescue department and is a typical city-area contract fire brigade. They have around 30 operations yearly and have a rescue unit and a personnel carrier. The IT infrastructure is managed by a member of fire brigade who is IT administrator by profession.

Publicly Available Services

The fire brigade has a WordPress site hosted at Nebula’s web hotel. Additionally, their email is set up on Microsoft Office 365.

Local Area and Wireless Network

The fire brigade has a flat network topology with several consumer-grade wireless access points. There are plans, however, to replace existing network infrastructure in the near future.

The local network has an office workstation used by the members of the fire brigade.

Other Networked or Connected Hardware

There is electronical access control system that uses Bewator Entro with COTAG access control tags. Additionally, there is an automation system for lights inside and outside the fire station, that are turned on when an alert is received from the emergency response centre.

Network Topologies

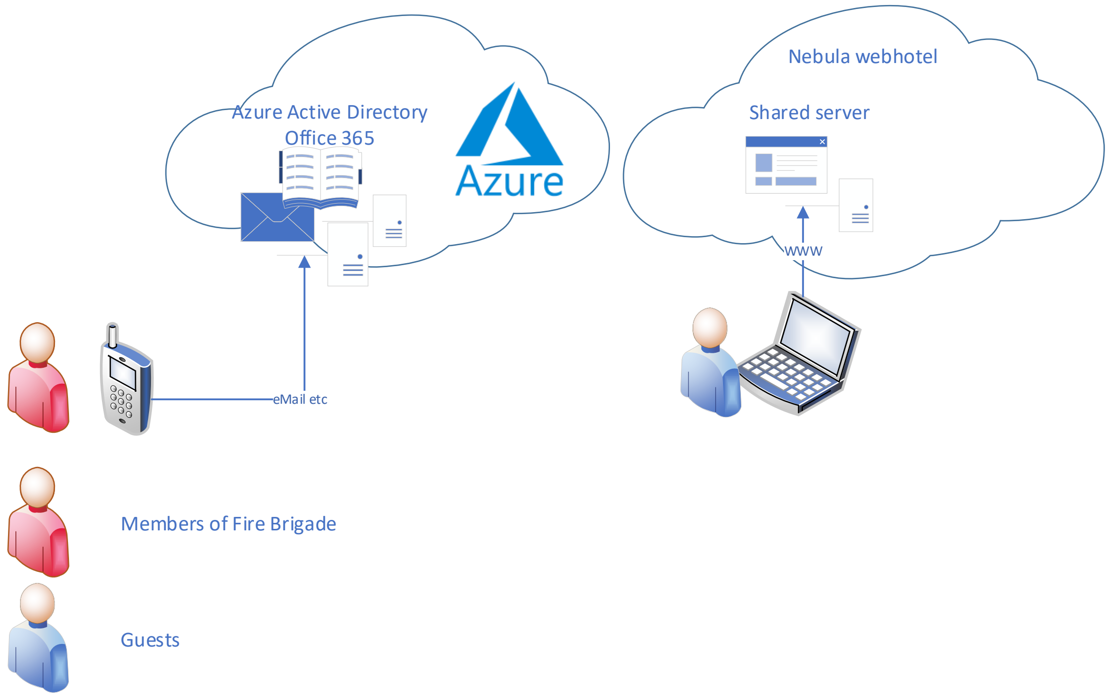

Figure 16 Publicly available services

The Figure 16 Publicly available services illustrates the division between services used by members of the fire brigade, and outside guests.

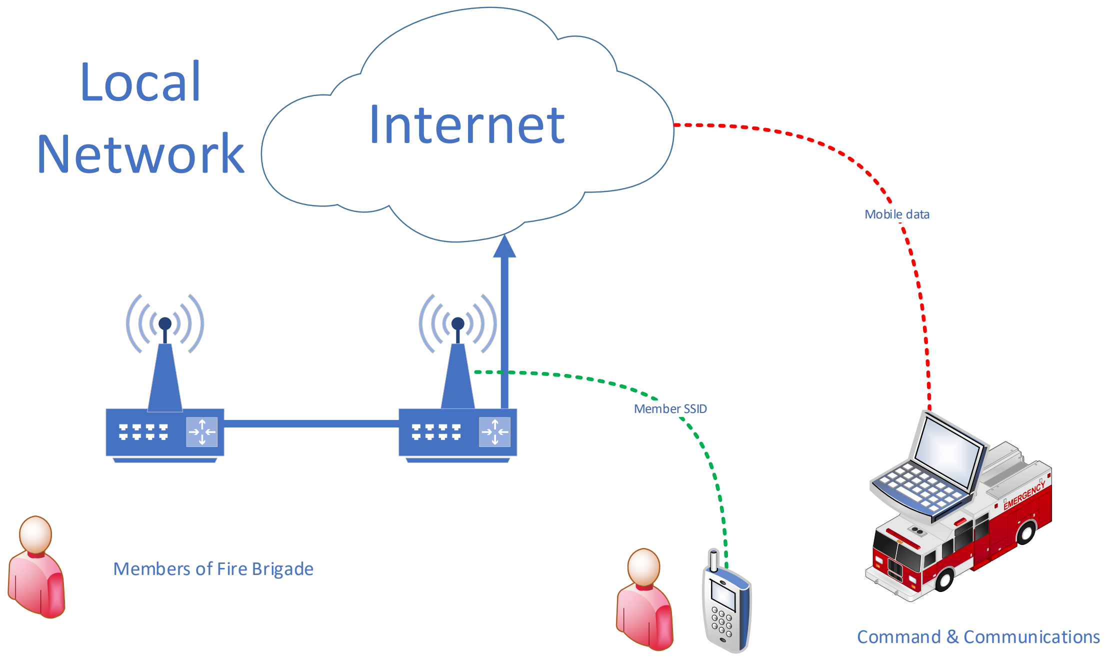

Figure 17 Local network

The Figure 17 Local network illustrates the users and topology of local network. In addition to local network, the fire-engine mounted command & communications laptop is directly connected to the internet via a 3G modem.

Summary of Findings in Azure

As the Azure was only used as a directory service for users using the Microsoft Office 365 suite, there were no deviations to CIS benchmark. However, a notable improvement for security would be implementing MFA, at least for the administrative users.

Summary of Findings in Publicly Available Services

The most important findings in publicly available services are described in section *6.6 Major Findings* of this thesis.

Several other vulnerabilities were uncovered as well. The management interface for the WordPress instance were not restricted and additionally there were no brute-force protection. On top of that, the login was performed in plain text without TLS encryption in place. Even though these do not directly and immediately pose threat to the system, they significantly endanger the system.

Summary of Findings in Other Networked Devices

The most important findings in other networked devices are described in section *6.6 Major Findings* of this thesis.

In addition, the command and communications laptop used in the fire engine of fire brigade in Case 2 was connected to the internet using 3G modem. This was considered an issue, as the 3G modem had bridged its connection directly to the laptop and the laptop had a Windows XP installed. The operating system has been considered end-of-life in 2009.

6.3 Case 3

The fire brigade in case operates under Helsinki rescue department and is a typical city-area contract fire brigade. They have a rescue unit and a personnel carrier. The IT infrastructure is managed by a member of fire brigade who does not have an IT background.

Publicly Available Services

The fire brigade does not currently have a website, and their email is set up on Microsoft Office 365.

Other Services

The fire brigade has a local Microsoft Windows Server 2019 in place used as VPN endpoint and the CCTV recording server.

Local Area Network

The local area network is segmented very well. The segmentation has a guest network, an office network for fire brigade’s members and a secure network which has security devices, such as burglar alarm system and closed-circuit television system.

Wireless Network

There are two different wireless networks. One is maintained by the fire brigade itself and it has two SSID's configured: one for guests and one for fire brigade's members. The other wireless network is administrated by the rescue department and it is used to configure and administrate the Merlot Mobile command and communication workstation.

Other Networked or Connected Hardware

The garage has an automatic lifting-doors with a remote controller using radio frequency. They have Merlot Mobile set up in their fire engine. The Merlot Mobile workstation connects to a separate wireless network maintained by the rescue department.

Network Topoplogies

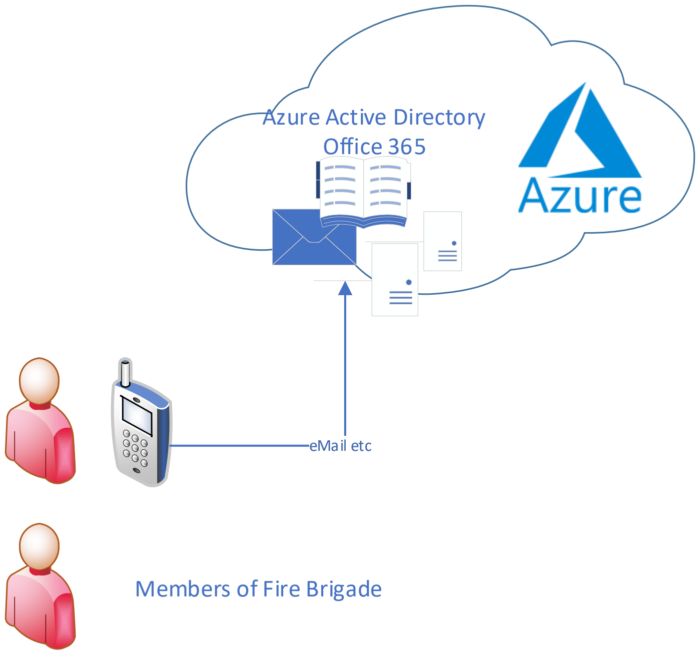

Figure 18 Publicly available services

The Figure 18 Publicly available services above illustrates the public services used by the fire brigade. It is worth noting, that there are no public services for guest users. The Figure 19 Local services below illustrates the local services. The Merlot Mobile is connected to a network beyond the administration of the fire brigade, and as such it was ruled out of scope.

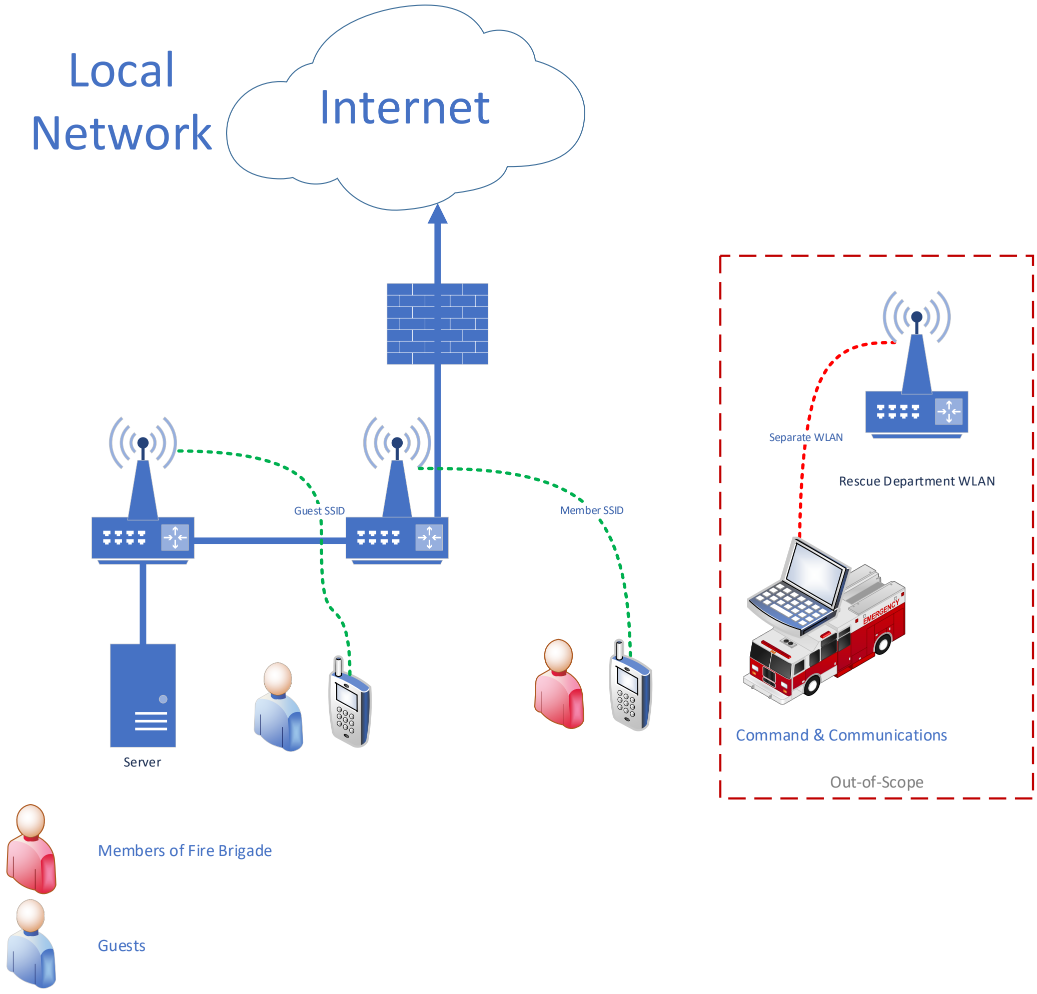

Figure 19 Local services

The fire brigade in case 3 deviates from other fire brigades, in positive way, and it does have segmentation implemented in their network. The segmentation is better visualised in Figure 20 Logical Network Topology. It is also noteworthy, that the server used as VPN server and CCTV recorder has interfaces in both the secure network and member network.

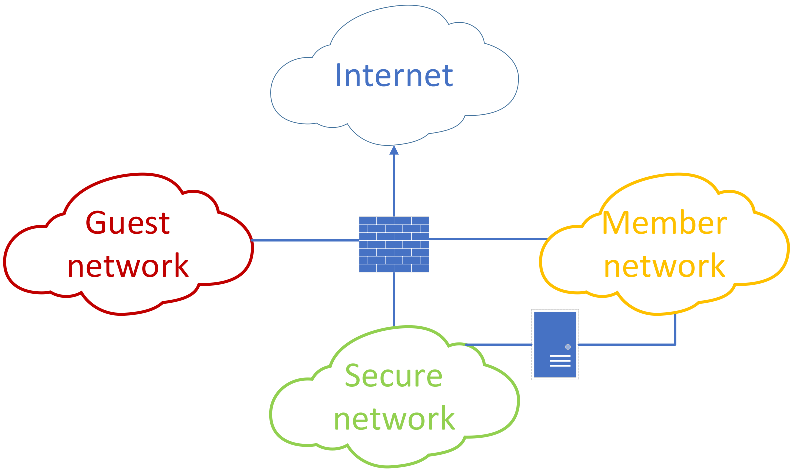

Figure 20 Logical Network Topology

Summary of Findings in Azure

On Azure, several deviations from CIS hardening recommendations were discovered. These include disabled Network Watcher and Access Keys not being rotated properly.

Summary of Findings in Other Networked Devices

The most important findings in other networked devices are described in section *6.6 Major Findings* of this thesis.

Summary of Findings in Local Network

The office PC used for regular paperwork and internet browsing appeared to be missing proper endpoint protection.

Generic malware was brought to the PC using USB RubberDucky, which downloaded an Empire payload over the internet. USB RubberDucky is essentially a programmable keyboard, which types everything that it has been programmed to type. As such, it can easily open a PowerShell command prompt and download malicious data. It can be used as a dropper for other malware. Empire, previously known as PowerShell Empire, is a post exploitation framework using PowerShell. This should have been noticed on the PC, as the command-and-control server had already been burnt, and the author of this thesis had been contacted by Finnish authorities regarding the server. Nevertheless, the payload did connect to the command-and-control server, without endpoint protection intercepting and preventing the traffic.

The firewall on the network edge operated as DNS server. As such, it was possible to enumerate domains that were in the firewalls cache, meaning the domains that had been visited by someone in the network. This could enable gathering intel of other services used by the fire brigade in case the attacker would try a supply chain attack. Supply chain attack is an indirect attack, where instead of the actual target, a trusted third party is breached instead. This third party is then used as a bridgehead to the actual target.

In addition, a login prompt on the firewall was discovered to be open to the internet. However, it was unclear if this was an administrative interface or interface for VPN access.

6.4 Case 4

The fire brigade in case operates under Kanta-Häme rescue department and is a typical rural area contract fire brigade. They have a rescue unit, tanker unit and a personnel carrier. The IT infrastructure is managed by a member of fire brigade who has an IT background but does not do IT administration professionally.

Publicly Available Services

The fire brigade has a custom in-house created website with static content. It is hosted on a shared virtual server by Louhi Networks Oy. Additionally, their email is set up on Microsoft Office 365.

Local Area and Wireless Network

The local area network and wireless connectivity is provided by third party, who refused to participate in the assessment. Thus, it was ruled out-of-scope.

Other Networked or Connected Hardware

The fire brigade has a gate, that is opened by a call to specific number. The gate restricts access to the fire station perimeter.

Their garage has an automatic lifting-door with a remote controller using radio frequency.

Additionally, they have a storage room within the fire station. The entry is granted by PIN-code entered to built-in keypad lock on the doorknob.

In the fire engine they have a PEKE command and communication workstation and in the tanker vehicle they have an Actis navigator, that is connected to VIRVE and receives destination coordinate messages.

Network Topologies

The Figure 21 Publicly available services illustrates the division between services used by members of the fire brigade, and outside guests.

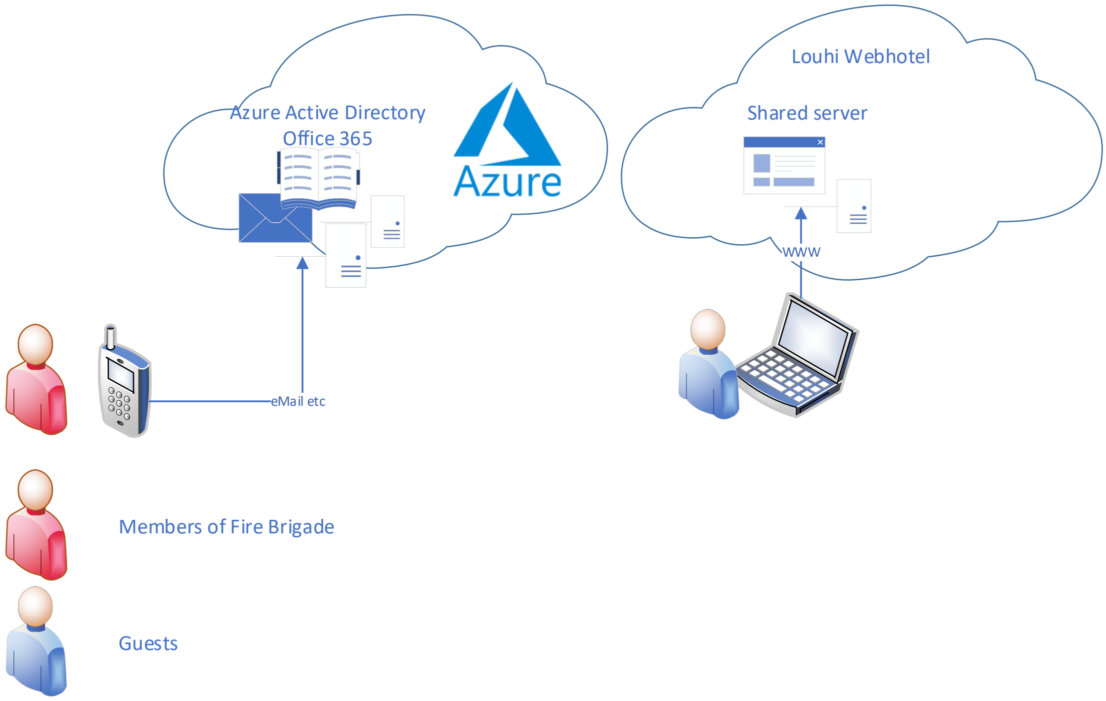

Figure 21 Publicly available services

Summary of Findings

As Azure was used as a directory for handful of users, there were no issues with the configuration on Azure. The public website only had static content, thus no findings.

The more important findings in other networked devices are described in section *6.6 Major Findings* of this thesis.

6.5 Case 5

The fire brigade in case operates under Kanta-Häme rescue department and is a typical rural area contract fire brigade. They have a rescue unit, tanker unit and a demountable truck. The IT infrastructure is managed by a member of fire brigade without IT background.

Publicly Available Services

The fire brigade has a WordPress site hosted by WordPress. Additionally, their email is set up on Microsoft Office 365.

Local Area and Wireless Network

They have a flat network topology with no services provided. As such the local area network and wireless network were ruled out of scope.

Network Topologies

The Figure 22 Publicly available services illustrates the division between services used by members of the fire brigade, and outside guests.

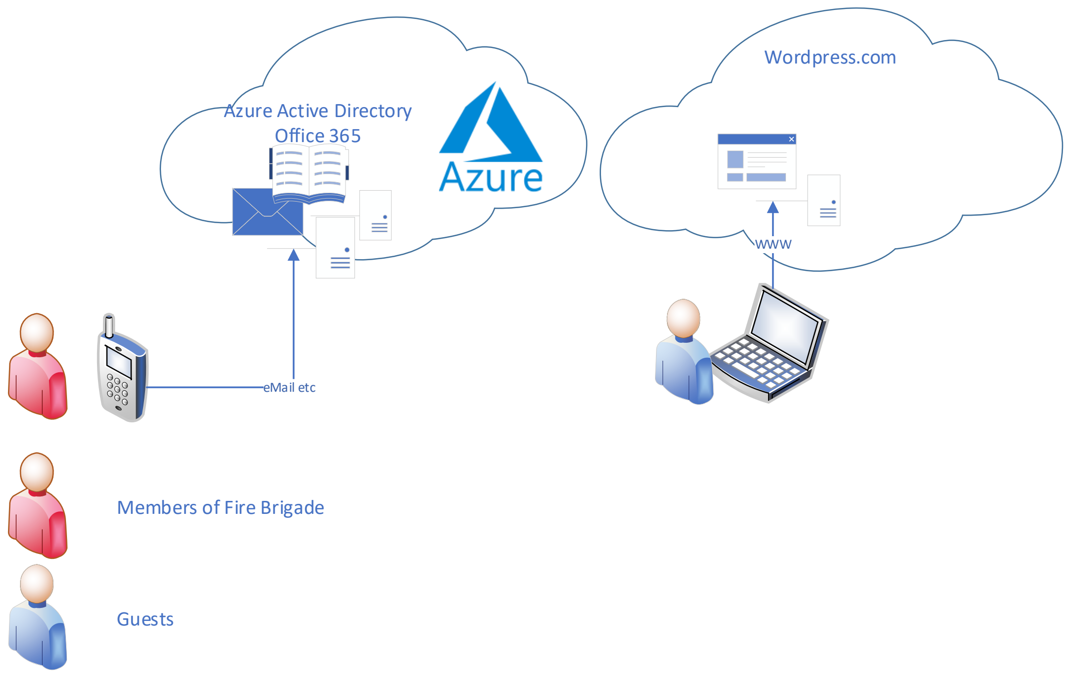

Figure 22 Publicly available services

Summary of Findings

As Azure was used as a directory for handful of users, there were no issues with the configuration on Azure. The public website was hosted on WordPress.com, but there were few low priority security hardenings to be done.

6.6 Major Findings

It is evident, that as many fire brigades have enrolled into the Microsoft's non-profit program, Office 365 and Azure Active Directory provides a significant attack vector to contract fire brigades. It also seems, that there are no security hardenings in place. For example, Multi Factor Authentication (MFA) was used by only one fire brigade.

Additionally, fire brigades tend to have easy-to-use and common content management systems (CMS) in use, such as WordPress. It is a double-edged sword, as they are well maintained and vulnerabilities are patched relatively fast, but they are also targeted by attackers.

Networks wise the networks are typically flat and uses consumer grade network devices, but there are deviations. However, typically these networks do not have high-value targets within, so the flat topology does not pose imminent security risk.

As there were additional in-house software development, it does provide additional attack vector for an adversary. Hence the software developed in-house by fire brigades should be done with security in mind.

An SQL Injection and Cross-Site Scripting Vulnerabilities

Fire brigade in Case 1 had a web application used to help in fire water logistics when on mission. As such, the application could be considered mission critical, as stable supply of water used in extinguishing fires is crucial. Here the SQL injection lies in a location parameter that is provided by the users' browser. Even though that is not something the user directly insert and then send, but instead provided by JavaScript, it can still be intercepted by a proxy tool, Burp Suite, in this case. The location parameter was, however, restricted by its length and as such that could not be exploited, even though it did show the parameter being vulnerable. When an injection, such as ”*1′ OR ′1′ = ′1*“ was provided as the location value, the database server responded with an error that was presented to the user. The application had another parameter, which was not restricted in any way, but caused the server respond with a value of *1* every time regardless of the content provided by the user. As such it was possible to attempt a blind SQL injection.

An open-source tool, SQLMap, was used to discover the correct injection. SQLMap is an automated tool for SQL injections and database takeover, which is able to dump database, enumerate users and tables and even create a TCP connection between the database server and the adversary. (SQLMap, 2020) A transfer of a reverse shell backdoor was tried, but it appears that the database user was not able to write into the webserver data location. As such, it was not possible to completely take over the server and gain a shell access to it. However, data exfiltration was possible, and it could have provided additional intel required for takeover, but as time was significant constraint during the assessment, this was not advanced further.

Additionally, the parameter that was SQL injectable without restrictions, was vulnerable with a Cross-Site Scripting vulnerability. However, as there were no authentication and no session cookies in place, exploiting the Cross-Site Scripting vulnerability was pointless.

Remote Code Execution

The fire brigade in Case 2 has a WordPress instance running on Nebula’s web hotel service. They have not been applying security controls nor performed any hardening for the service. As Well, the WordPress admin-panel was publicly available and the access to it was not restricted in any way.

For assessing the service administrative privileges were obtained. Using these credentials, it was possible to modify the *404.php* file in the WordPress itself, and effectively it enables executing any PHP code. The 404.php was modified to contain a PHP reverse shell, and afterwards a non-existent page was visited. This caused the web hotel server to call back and open a reverse shell connection.

As the representative of the fire brigade informed, that they do not have shell access normally, this was reported to the NCSC-FI on 27 August 2020, and they responded on 2 September 2020. The NCSC-FI had investigated the matter and contacted Nebula, who had then confirmed that their web hotel clients do have shell access via SSH to the server.

Nevertheless, it would have been possible to acquire database credentials, and WordPress credentials with their hashed passwords, with the reverse shell access. Defacing the website would have also been possible, but that would have been possible with just the administrative access to the WordPress. Obtaining the administrative access to the WordPress would have required either brute-force or phishing, as the administrative access was not restricted.

The root cause were that dangerous PHP functions, such as system(), was not disabled on the server, but as the server is not maintained by the fire brigade, they have no influence on the issue. What could be done, is to set following configuration for WordPress:

```
define('DISALLOW_FILE_EDIT', true);
```

This effectively prevents creating the malicious PHP file.

POCSAG Used in Building Management System

The fire brigade in Case 2 uses ELIT IHC to control lights inside the fire station and on the outside perimeter. The system uses its own proprietary cabling, and it is not connected to the Internet nor any TCP/IP network inside the fire station. However, they do have a system set up, that when an alarm is received, lights are turned on on the fire station’s outside perimeter as well in the garage. This system uses Post Office Code Standardization Advisory Group (POCSAG) system for receiving the alerts as pages. The POCSAG system used within Länsi-Uusimaa Rescue Department is well documented in master’s thesis of Kimmo Markkanen. From the forementioned master’s thesis it was possible to find out correct radio identity code (RIC) for the fire brigade in this case. By monitoring the correct frequency for several weeks, it was possible to figure correct parameters, such as 1200 bps transmit rate and correct message format. Using Raspberry Pi and a software called *rpitx* it was possible to transmit the POCSAG message initiating the alarm within the fire station.

It was recommended to move for an authenticated solution for receiving the alerts. Additionally, it was recommended to not to connect any critical components, such as access control, to the current system in place.

Radio Controlled Garage Door Susceptible for Replay Attack

The fire brigade in Case 3 has a radio-controlled door for their garage, where the fire engine is held. The radio controller uses 868MHz frequency, which is commonly used by different consumer and business grade remote controlled devices, such as remote-controlled lights, garage doors, gates et cetera. This is susceptible for a replay attack. This was exploited by recording the command used to open the garage door, and the then it was replayed back using HackRF One and Universal Radio Hacker. Few remediations exists. It was recommended, that members of the fire brigade use a mechanical latch, that prevents opening the door, to prevent opening the door if it is not intended. Also, one could restrict the access to the premises to prevent recording and replaying the signal, but that is challenging as directional antennas and amplifiers may still boost the signal from far away. As a future consideration, it was advised, that when selecting the manufacturer of the remote-controlled door, security should be kept in mind.

Navigation System Controllable by a Third Party

Fire brigades in Case 2 and Case 4 uses navigators that receive a destination coordinates for the accident site over VIRVE network. Fire brigade in Case 2 uses a laptop with Elektro-Arola SNP software and an additional Garmin navigator which has a Elektro-Arola status code transmitter (SKL, statuskoodilähetin) connected. Fire brigade in Case 4 uses Actis navigator with Elektro-Arola SNP software.

As it is possible to send SMS from a public GSM network to VIRVE via a gateway, that is publicly announced in the communications guide for VIRVE network (Ministry of the Interior, 2011). Additional information needed is the ISSI number of TETRA terminal connected to the navigator. Also, even though the destination message format is not public information, it is only slightly obfuscated and trivial. A well-resourced attacker is able to obtain both of these pieces of information. In addition to conventional espionage, it is possible to listen and decode ISSI numbers registering for a base station on the radio frequency TETRA uses.

It is then possible for an adversary to, for example, cause a sabotage for critical infrastructure, and afterwards direct the responding rescue units to another location. This would effectively delay the start of the rescue operation, thus maximising the damage. Only reasonable attacker would be a state actor with hybrid-warfare intent.

For the fire brigades in the cases described, it was recommended to educate the drivers to detect anomalies in navigation and to prepare vehicles with an additional navigation method. The issue appears wide, as this kind of navigation systems are in use in many rescue departments in Finland. Due to the previous, this was reported to NCSC-FI and Elektro-Arola. NCSC-FI responded on 18 November 2020 that the issue has been directed to a risk-management process for different parties.

6.7 Summary of findings

In the technical assessments there were total of 50 findings. Many of these findings are not necessarily specific to fire brigades, but common information security issues. As such, reviewing them thoroughly does not add value to this thesis.

These findings have been categorised by the different attack vectors described in sections *3 Incident Detection and Response Capabilities* and *4 Common Weaknesses and Vulnerabilities* of this thesis.

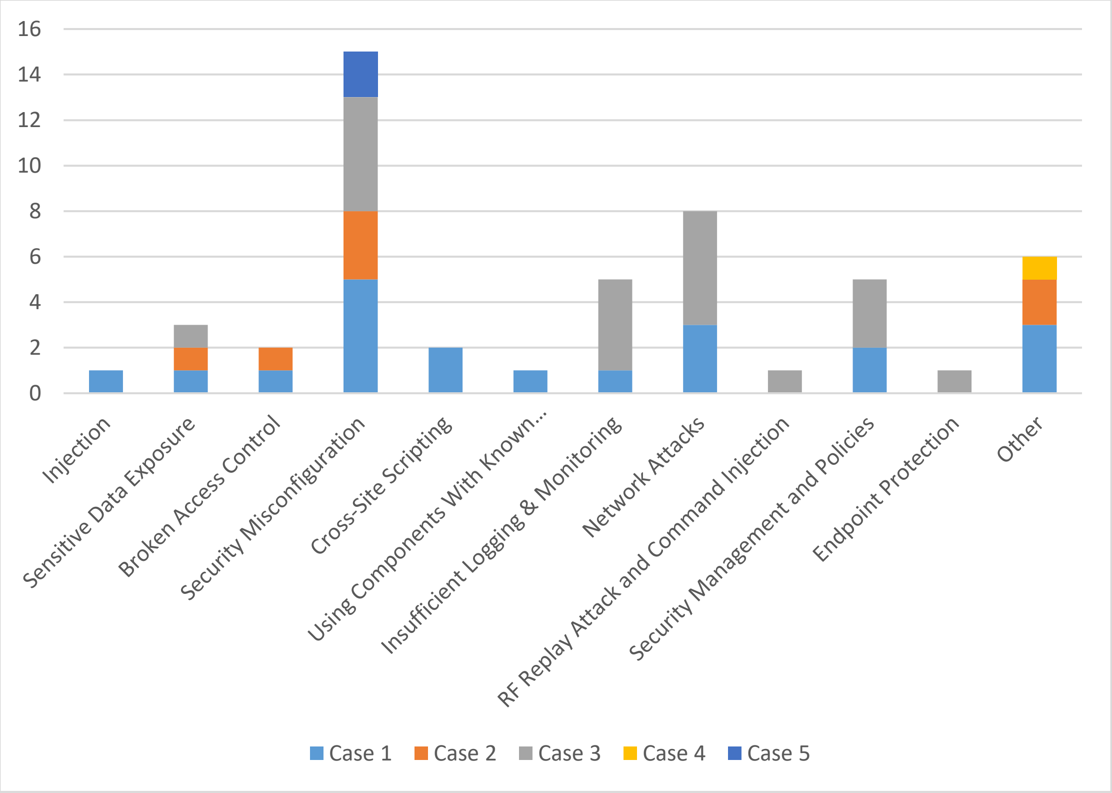

Figure 23 Distribution of findings by attack vector

The Figure 23 Distribution of findings by attack vector above illustrates the categorised findings distributed between case fire brigades. It is noteworthy, that fire brigades in Case 4 and Case 5 both have significantly small number of findings compared to other fire brigades.

It is also notable, that the larger the IT infrastructure is, the easier it is to uncover security issues. Larger IT infrastructure highlights issues in security hardenings, logging and monitoring and security management and policies. Larger IT infrastructure tends to result in larger networks, which also adds up in attack surface.

Most case fire brigades had security misconfigurations in place. These issues are easily mitigated by hardening guidelines and following best practices. Implementing secure configurations enhance the security posture significantly.

The issues in other category are partially described in the section *6.6 Major Findings* of this thesis. In addition to those, fire brigades in Case 1, 2 and 4 had issues, which could not be categorised. These include following issues:

- A CSRF vulnerability.
- State changing requests made with HTTP GET.

- a potential indicator of compromise within server platform.

7 Results

The survey indicates that the attack surface of fire brigades appears to be vast. This is due to both lack of expertise in implementing technology, and the simultaneous need for nearly enterprise grade information technology infrastructure. Personnel in fire brigades are aware of the risks the digitalised environments pose. Thus, fire brigades are in grave need of easy-to-comprehend and easy-to-implement security guidance. Fire brigades do typically have a consumer grade endpoint protection on local computers, which appear to be adequate. However, there is rarely any network level protection, even though there are valuable assets within network. Networks are typically unsegmented, and there is no monitoring in place. This makes it difficult to detect and respond in case of a breach or other incident. The reliability of the survey is supported by the over 10% rate of responses of the amount of contract fire brigades in Finland. Moreover, the respondents background profile matches the distribution of different forms of contract fire brigades.

Critically thinking, some questions on the survey could have been designed better. It seems, that few arguments were misunderstood. For example, for a individual with little information security knowledge, it is easy to confuse information security and data protection. The awareness on the latter has been significantly elevated ever since the General Data Protection Regulation were put into effect. Overall, the survey should have been translated into Swedish, as there are multiple Swedish-speaking contract fire brigades in Finland. Also, the survey should have been marketed and advertised better, and if it were distributed using additional parties, such as Finnish Contract Fire Brigades’ Union (Suomen Sopimuspalokuntien Liitto SSPL), there could have been more respondents. It is also possible, that the respondents were from the fire brigades, where there is at least some knowledge on information technology. Contract fire brigades with no awareness would not probably have even responded.

Even though several vulnerabilities and weaknesses were uncovered during the case studies, they are not as common, that they would provide means to take down or significantly degrade the operational readiness of majority of fire brigades. However, vulnerabilities described in *Radio Controlled Garage Door Susceptible for Replay Attack* and *Navigation System Controllable by a* may be used to disrupt readiness of numerous fire brigades.

The results in the survey confirms the finding made by Marko Heikkilä. His bachelor's thesis pointed out, that data protection and information security training was not on adequate level at contract fire brigades under Oulu Koillismaa Rescue Department. (Heikkilä, 2015) This finding was made, even though there were no respondents from contract fire brigades under Oulu Koillismaa Rescue Department, and it indicates that the issue is wider and applies to more rescue departments.

8 Conclusions

During the research it became clear that the fire and rescue field in Finland is rather resilient, since even though mission critical services could fail, there are usually ways to overcome these issues. The nature of the field is to adapt in dynamically changing situations, and a cyber incident would not necessarily reduce operational readiness of single fire brigade. However, a major cyber incident disrupting the command & communications system backend could affect the overall operation readiness. It is obvious, that as old field as fire and rescue services are, they have great variance in the digitalised and technologized services used. This is especially due to municipal rescue departments and different contract fire brigades have independently adapted to various technologies. As the field has been historically severely fragmented, there is no unified IT infrastructure in use. Hence, it is more resilient to cyber incidents. However, there has not always been a commercial or otherwise ready solution that suits the specific needs for a fire brigade and as such highly customised or self-developed solutions exist. Software or systems development cannot, by any means, be seen as a core functionality of a fire brigade, and information security even less. This greatly increases a risk for cyber incident within the fire brigades.

The selected research methodologies suited this kind of research very well. The quantitative survey gave good amount of data for analysing and it enabled making generalised conclusions. The qualitative case study combined with explorative study allowed to discover common weaknesses. It is unlikely, that the results could have been gathered using different methodology.

8.1 Recommendations

Fire brigades are recommended to harden their public facing applications and networks.

Fire brigades that are taking Microsoft's generous non-profit program in use should consider hardening their services. While several hardening guides exist, and for example CIS hardening guide is extensive, NCSC-FI has their own security guidelines for Office 365 users, in Finnish language. If the fire brigade uses service from Azure, more technical hardening measures are needed to ensure security. As emails are primary vector for different phishing schemes and malware distribution, securing the Office 365 greatly enhances the security posture of any organisation.

Many fire brigades have automatic garage doors in use. If these use RF controllers, they should be considered vulnerable if there is no explicit proof from the manufacturer that they would not be susceptible to RF recording and replaying. In these cases, the fire brigade should always use the mechanical latch to prevent the garage door from being opened without permit. Preventing the access to the fire station premises enhances the overall security posture. Typically fire stations have valuable tools and vehicles, that are worth protecting. If one would steal a fire-engine, it would most likely disrupt the fire brigades' ability to respond emergencies.

When a fire brigade considers taking any building management or access control systems in use, they should consider the information security aspects as well. Especially, when these devices are connected to internet.

When adapting new technologies to support operations, these technologies should be protected, and their security posture should be assessed. Furthermore, there should always be a backup method for mission critical applications.

In case fire brigade uses obsolete software, such as end-of-life operating systems, they should be upgraded immediately. These pose severe risk for the whole network.

In addition to the risks described above, typically contract fire brigades face a significant key-person risk. There is usually only one administration, who has all the knowledge. As there is very little documentation and IT knowledge in general, if this one keyperson simply decides to quit, there might be no one to take place.

8.2 Future research and development

There is no immediate need for more research in this topic, at least in technical level. However, it could be beneficial to research the incident detection and response capabilities as a case study, as these were ruled out of this research. This could be executed as a *purple teaming* exercise. In *purple teaming* exercise the attacks the exercise adversary, *red team*, performs are coordinated together with the defender, *blue team*. This kind of approach would give more technical insight on the incident detection and response capabilities.

Furthermore, in the future when digitalisation takes more steps in the field, this should be reconsidered. It would be beneficial for SPEK to continue following this topic. SPEK could also encourage IT-administrators and developers in contract fire brigades to attend for an open-source project, which could be used for contract fire brigades to share, collaborate, and audit the software developed by themselves. This project could be hosted in, for example GitHub. It could help spread best practices and general information security know-how.

As majority of survey respondents agreed that they need more guidance on information security matters, this could also be a place for SPEK to act. Gathering and providing easy-to-implement guides for securing environments that fire brigades commonly use, would be a low-hanging fruit to pick. This could also be worked in collaboration with municipal rescue departments. In fact, there is a co-operative action to gather information security personnel in municipal rescue departments to share knowledge and create guidance and documentation.

References

Alander J, 2017. *The Radio Paging Networks Used by the Rescue Services in Finland* (Final project, engineering). Savonia University of Applied Sciences. Available at: https://www.theseus.fi/bitstream/handle/10024/73947/Alander_Juha.pdf

Alasuutari P, 2011. *Laadullinen tutkimus 2.0*. Vastapaino.

Alcorn W., Frichot C., Orru M., 2014. *The Browser Hacker's Handbook*. John Wiley & Sons, Incorporated.

Andersson J. Balduzzi M. Hilt S. Lin P. Maggi F. Urano A. and Vosseler R. 2018. *A Security Analysis of Radio Remote Controllers for Industrial Applications*. Trend Micro. Accessed on 5 February 2021. Available at: https://documents.trendmicro.com/assets/white_papers/wp-a-security-analysis-of-radio-remote-controllers.pdf

Barnett R.C., Grossman J., 2012. *Web Application Defender's Cookbook: Battling Hackers and Protecting Users*. John Wiley & Sons, Incorporated

Baezner M. Robin P., 2017. *Hotspot Analysis:Stuxnet*. ETH Zürich. Accessed on 6 February 2021. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-04.pdf

Bejtlich R, 2013. *Practice of Network Security Monitoring: Understanding Incident Detection and Response*. No Starch Press, Incorporated.

Caneill M, Gilis J-L., 2010. *Attacks against the WiFi protocols WEP and WPA*. Accessed on 14 February 2021. Available at: https://matthieu.io/dl/papers/wifi-attacks-wep-wpa.pdf

Clarke-Salt J, 2012. *SQL Injection Attacks and Defense*. 2nd ed. Elsevier Science & Technology Books.

Damanik V.N.N., Sunaringtyas S.U., 2020. *Secure Code Recommendation Based on Code Review Result Using OWASP Code Review Guide*. Institute of Electrical and Electronics Engineers.

Damele B., Stampar M. *SQLMap*. Accessed on 8 August 2020. Available at: http://sqlmap.org/

Databreaches.net, 2014. *WA: Fire department medical response records and personnel information hacked*. Accessed on 9 February 2021. Available at: https://www.databreaches.net/wa-fire-department-medical-response-records-and-personnel-information-hacked/

Dehalwar V., Kalam A., Kolhe M.A., Zayegh A., 2017. *Review of web-based information security threats in smart grid*. Institute of Electrical and Electronics Engineers.

Edgar T.W., Manz D.O., 2017. *Research Methods for Cyber Security*. Elsevier Science & Technology Books.

Emergencyreporting.com, 2019. *Combatting Cyber Attackers: The Basics of Cyber Security for Fire Departments*. Accessed on 9 February 2021. Available at: https://emergencyreporting.com/blog/combatting-cyber-attackers-the-basics-of-cyber-security-for-fire-departments/

Government Technology, 2016. *Ransomware Virus Infects Honolulu Fire Department Computers*. Accessed on 9 February 2021. Available at: https://www.govtech.com/dc/Ransomware-Virus-Infects-Honolulu-Fire-Department-Computers.html

Greene K., Rodgers D., Dykhuizen H., McNeil K., Niyaz Q., Al Shamaileh K., 2020. *Timestamp-based Defense Mechanism AgainstReplay Attack in Remote Keyless Entry Systems*. Institute of Electrical and Electronics Engineers.

HackRead, 2018. *Ransomware Attack Wipes Out Police and Fire Department Data*. Accessed on 9 February 2021. Available at: https://www.hackread.com/ransomware-attack-wipes-out-police-fire-department-data/

Hathaway M.E., 2014. *Best Practices in Computer Network Defense: Incident Detection and Response.* IOS Press, Incorporated.

Heikkilä M, 2015. *Information Security and Data Protection of the Contract Fire Brigades in Oulu -Koillismaa Rescue Department*. Accessed on 2 October 2020.

Available at: https://www.theseus.fi/bitstream/handle/10024/99888/Heikkila_Marko.pdf

The Hill, 2015. *Local fire department battling hackers*. Accessed on 9 February 2021. Available at: https://thehill.com/policy/cybersecurity/238969-local-fire-department-battling-hackers

Hutchins E.M. Cloppert M.J. Rohan M. Amin. *Intelligence-Driven Defense*. Lockheed Martin Corporation. Available at: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Jokinen P., Bamberg J., Laine M, 2007. *Tapaustutkimuksen taito*. Gaudeamus.

Johnson D, 2020. *The Use and Administration of Shared Accounts*. SANS Institute. Accesssed on 20 October 2020. Available at: https://www.sans.org/reading-room/whitepapers/basics/administration-shared-accounts-1271

Jouinia M. Rabaia L.B.A. Aissa A.B., 2014. *Classification of security threats in information systems*. Available at: https://www.sciencedirect.com/science/article/pii/S1877050914006528/pdf?md5=e2c1a62a477f1251106e844735049415&pid=1-s2.0-S1877050914006528-main.pdf

Kamkar S., 2015. *DRIVE IT LIKE YOU HACKED IT – DEFCON23*. Accessed on 5 February 2021. Available at: https://samy.pl/defcon2015/2015-defcon.pdf

Koivunen P. 2015. *Pelastustoimi ja sopimuspalokunnat Suomessa*. Suomen Sopimuspalokuntien Liitto. Available at: https://sspl.fi/images/OPASPANKKI/2015/Pelastustoimi_ja_sopimuspalokunnat_Suomessa_2painos/1_OPAS_Sidosryhmaesite.pdf

Kouvolan Sanomat, 2013. *Hakkeri iski Kympen sivuille*.

Lappeteläinen J, Sadinmaa K, 2015. *VIRVE – a tool for paramedic. Virve-training material Oulu University of Applied Sciences of Emergency Nursing program* (Bachelor's Thesis). Oulu University of Applied Sciences, Degree programme in Emergency nursing, Degree programme in Nursing and health care, Option of nursing. Available at: https://www.theseus.fi/bitstream/handle/10024/98973/Lappetelainen_Juha.pdf

Lehti J., 2017. *The use of Secure Communication App in Central-Uusimaa fire department* (Bachelor's thesis). XAMK South-Eastern Finland University of Applied Sciences. Available at: http://urn.fi/URN:NBN:fi:amk-2017122022250

Liukkonen H., 2020. Planner, Finnish Emergency Services College. Interview on 3 November 2020.

Markkanen K, 2007. *Selecting Technologies for the Control System of Public Warning Sirens and Fire Brigade Alarms* (Master's Thesis). Helsinki University of Technology, Department of Electrical and Communications Engineering. Available at: http://lib.tkk.fi/Dipl/2007/urn010030.pdf

Ministry of the Interior, 2011. *Pelastustoimen VIRVE-viestiohje.* Accessed on 6 June 2020. Available at: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79327/smjulkaisu_242011.pdf

Ministry of Interior, 2020. *Emergency Response Centres*. Accessed on 29 September 2020. Available at: https://intermin.fi/en/emergency-response/emergency-response-centres

Ministry of Interior, Rescue Services 2020. *Pelastuslaitokset – Pelastustoimi*. Accessed on 7 July 2020. Available at: https://www.pelastustoimi.fi/pelastustoimi/pelastuslaitokset

Ministry of Interior, Rescue Services 2020. *Sopimuspalokunnat – Pelastustoimi*. Informational website on volunteering in fire and rescue services. Accessed on 7 July 2020. https://www.pelastustoimi.fi/pelastustoimi/sopimuspalokunnat

Nagpure S., Kurkure S., 2017. *Vulnerability Assessment and Penetration Testing of Web Application*. Institute of Electrical and Electronics Engineers.

NCSC-FI. *Kuka sammutti valot? Puutteellinen rakennusautomaatiolaitteiden suojaus verkossa altistaa kyberuhille*. Accessed on 21 October 2020. Available at:

https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kuka-sammutti-valot-puutteellinen-rakennusautomaatiolaitteiden-suojaus-verkossa

Nieminen M., 2021. ICT Specialist. Päijät-Häme Rescue Department. Interview on 11 March 2021.

Nikto developers, 2020. *An introduction to Nikto Web Vulnerability Scanner.* Accessed on 6 August 2020. Available at: https://cirt.net/nikto2-docs/introduction.html

Oinonen M., 2013. *SECURITY RISK ASSESSMENT FOR A VOLUNTEER FIRE BRIGADE ASSOCIATION* (Bachelor's Thesis). Turku University of Applied Sciences, Business Data Communications and Information Security. Accessed on 2 October 2020. Available at: https://www.theseus.fi/bitstream/handle/10024/76763/Oinonen_Mikko.pdf

The OWASP Foundation, 2017. *OWASP Top 10.* Accessed on 6 January 2021. https://owasp.org/www-project-top-ten

The OWASP Foundation, 2017. *Injection*. Accessed on 6 January 2021. https://owasp.org/www-project-top-ten/2017/A1_2017-Injection

The OWASP Foundation, 2017. *Broken Authentication*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication.

The OWASP Foundation, 2017. *Sensitive Data Exposure*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A3_2017-Sensitive_Data_Exposure.

The OWASP Foundation, 2017. *XML External Entities (XXE)*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A4_2017-XML_External_Entities_(XXE).

The OWASP Foundation, 2017. *Broken Access Control*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A5_2017-Broken_Access_Control.

The OWASP Foundation, 2017. *Security Misconfiguration*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A6_2017-Security_Misconfiguration

The OWASP Foundation, 2017. *Cross-Site Scripting (XSS)*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A7_2017-Cross-Site_Scripting_(XSS).

The OWASP Foundation, 2017. *Insecure Deserialization*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A8_2017-Insecure_Deserialization.

The OWASP Foundation, 2017. *Using Components with Known Vulnerabilities*. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A9_2017-Using_Components_with_Known_Vulnerabilities.

The OWASP Foundation, 2017. Insufficient Logging & Monitoring. Accessed on 20 January 2021. Available at: https://owasp.org/www-project-top-ten/2017/A10_2017-Insufficient_Logging%2526Monitoring.

The OWASP Foundation 2020. *Injection Prevention Cheat Sheet*. Accessed on 6 February 2021. Available at: https://cheatsheetseries.owasp.org/cheatsheets/Injection_Prevention_Cheat_Sheet.html#defense-option-1-prepared-statements-with-parameterized-queries

Pauli J, 2013. *The Basics of Web Hacking: Tools and Techniques to Attack the Web*. Elsevier Science & Technology Books

Portswigger, 2021. Cross-Site Scripting. Accessed on 3 February 2021. Available at: https://portswigger.net/web-security/cross-site-scripting.

Probis. *Store*. Accessed on 19 October. Available at: https://www.probis.fi/store/

Prontonet. *Pelastustoimen resurssi- ja onnettomuustilasto PRONTO*. Accessed on October 16 2020. Available at: https://prontonet.fi/

Proxmark, 2020. Accessed on 21 October 2020. Available at: https://proxmark.com/.

Valli R., Aarnos E., 2018. *Ikkunoita tutkimusmetodeihin 1*. PS-kustannus.

Sanders C., Smith J., Randall L., 2014. *Applied Network Security Monitoring: Collection, Detection and Analysis*. Elsevier Science & Technology Books.

Saunders M., Lewis P., Thornhill A., 2009. *Research Methods for Business Students, 5th edition*. Pearson Education Limited.

Singh H., Dua M., 2018. *Website Attacks: Challenges And Preventive Methodologies*. Institute of Electrical and Electronics Engineers.

Suomen Erillisverkot, 2020. *Erillisverkkojen kehitys*. Accessed on 30 September 2020. Available at: https://www.erillisverkot.fi/erillisverkot

Suomen Pelastusalan Keskusjärjestö SPEK / The Finnish National Rescue Association, 2019. *Palokuntatoiminta*. Accessed on July 7 2020. Available at: https://www.spek.fi/vaikuttaminen/palokuntatoiminta/

Uçtu G., Alkan M., Doğru İ., A., Dörterler M., 2019. *Perimeter Network Security Solutions: A Survey*. Institute of Electrical and Electronics Engineers.

Urpila T., 2011. *Electrical device and information technology in firefighting vehicles of volunteer fire departments* (Bachelor’s Thesis). Laurea University of Applied Sciences, Degree Programme in Security Management. Accessed on 2 October 2020. Available at: https://www.theseus.fi/bitstream/handle/10024/40251/Urpila_Tatu.pdf

VA 1101/2019. *Valtioneuvoston asetus asiakirjojen turvallisuusluokittelusta valtionhallinnossa*. Accessed on 16 October 2020. Available at: https://www.finlex.fi/fi/laki/alkup/2019/20191101

Vacca, 2014. *Network and System Security*. Elsevier.

Vacca, 2017. *Computer and Infromation Security Handbook*. Elsevier.

Valtanen J, 2009. *Savua ja tulta – Espoon pelastustoimi 1956-2004*. Länsi-Uusimaa Rescue Department.

Vanhoef M, Piessens F, 2017. *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. Accessed on 14 February 2021. Available at: https://papers.mathyvanhoef.com/ccs2017.pdf

Vijayalakshmi K., Leema A.A., 2017. *Extenuating Web Vulnerability with a Detection and Protection Mechanism for a Secure Web Access*. Institute of Electrical and Electronics Engineers.

Zhong W., 2021. *Command Injection*. The OWASP Foundation. Accessed on 3 February 2021. Available at https://owasp.org/www-community/attacks/Command_Injection

Appendices

Sopimuspalokuntien kybervalmiudet

Tervetuloa vastaamaan suomalaisten sopimuspalokuntien kybervalmiuksia tutkivaan kyselyyn. Kysely on täysin anonyymi, eikä vastauksista voida päätellä vastaajaa tai kyseessä olevaa sopimuspalokuntaa.Taustatietoina kerätään palokuntamuoto sekä pelastuslaitos, jonka alueella palokunta toimii.

Lisätietoja tutkimuksesta saat: Antti Aitta / antti.aitta@leppavaaranvpk.fi

Taustatiedot

1.

Pelastuslaitos, jonka alueella palokunta toimii: *

Valitse listalta pelastuslaitos, jonka kanssa palokunnalla on palokuntasopimus, tai jonka kanssa on muodostettu henkilökohtaiset sopimukset.

○ Helsingin pelastuslaitos

○ Länsi-Uudenmaan pelastuslaitos

○ Keski-Uudenmaan pelastuslaitos

○ Itä-Uudenmaan pelastuslaitos

○ Varsinais-Suomen pelastuslaitos

○ Kanta-Hämeen pelastuslaitos

○ Päijät-Hämeen pelastuslaitos

○ Kymenlaakson pelastuslaitos

○ Etelä-Karjalan pelastuslaitos

○ Etelä-Savon pelastuslaitos

○ Keski-Suomen pelastuslaitos

○ Pirkanmaan pelastuslaitos

○ Satakunnan pelastuslaitos

○ Etelä-Pohjanmaan pelastuslaitos

○ Pohjanmaan pelastuslaitos

○ Keski-Pohjanmaan ja Pietarsaaren alueen pelastuslaitos

○ Pohjois-Savon pelastuslaitos

○ Pohjois-Karjalan pelastuslaitos

○ Jokilaaksojen pelastuslaitos

○ Kainuun pelastuslaitos

○ Oulu-Koillismaan pelastuslaitos

○ Lapin pelastuslaitos

○ Ahvenanmaan alue

2. Palokuntamuoto: *

○ Vapaaehtoinen palokunta

○ Henkilökohtaisen sopimuksen palokunta

○ Laitos-/tehdaspalokunta

○ Sotilaspalokunta

○ Muu ________________

Hyökkäyspinta-ala

3. Palokunnan internetyhteyttä hallinnoi: *

○ Palokunta

○ Pelastuslaitos

○ Muu ________________

○ En tiedä

4. Palokunnan IT-järjestelmiä hallinnoi: *

○ Palokunta

○ Pelastuslaitos

○ Muu ________________

○ En tiedä

5. Palokunnan internetsivuja hallinnoi: *

○ Palokunta

○ Pelastuslaitos

○ Muu

○ En tiedä

6. Palokunnan sähköpostijärjestelmiä hallinnoi: *

○ Palokunta

○ Pelastuslaitos

○ Muu

○ En tiedä

7. Palokunnan jäsenrekisterin (Esim. HAKA) teknisestä ylläpidosta (taustajärjestelmän ja infrastruktuurin ylläpito) vastaa: *

Palokuntayhdistys ylläpitää oman jäsenrekisterinsä tietosisältöä, eli tietoja jäsenistään, mutta kuka vastaa henkilörekisterin teknisestä ylläpidosta?

○ Palokunta

○ Pelastuslaitos

○ SPEK

○ Muu

○ En tiedä

8. Palokunnalla on käytössään tai muutoin pääsy viranomaisen turvaluokiteltuun aineistoon. *

○ Kyllä

○ Ei

○ En tiedä

10. Avoimet kommentit tämän sivun kysymyksiin:

Hyökkäyspinta-ala

11. Palokunta käyttää hälytyksiin ilmoittautumisjärjestelmää: *

Esimerkiksi SALSA tai Vaahtotykki.

○ Kyllä

○ Ei

○ En tiedä

12. Palokunnalla on käytössään sähköinen kulunvalvontajärjestelmä: *

○ Kyllä

○ Ei

○ En tiedä

13. Palokunnalla on käytössään sähköinen taloautomaatiojärjestelmä: *

○ Kyllä

○ Ei

○ En tiedä

14. Palokunnalla on käytössään internetiin kytkettyjä laitteita: *

Esimerkiksi työpöytätietokone, kannettava tietokone, matkapuhelin, tablet-tietokone.

○ Kyllä

○ Ei

○ En tiedä

16. Palokunnalla on paloasemakiinteistössään käytössä langaton lähiverkko: *

○ Kyllä

○ Ei

○ En tiedä

17. Palokunnan jäsenet käyttävät palokuntatoimintaan liittyvissä laitteissa ja palveluissa henkilökohtaista tunnusta: *

○ Kyllä

○ Ei

○ En tiedä

18. Mikä aiheuttaa suurimman huolen palokunnan käyttämien laitteiden, palveluiden tai tuotteiden tietoturvassa?

19. Avoimet kommentit tämän sivun kysymyksiin:

Havainnointikyky

20. Palokunnalla on IT-vastaava. *

○ Kyllä

○ Ei

○ En tiedä

21. Palokunnalla on tietoturvavastaava. *

○ Kyllä

○ Ei

○ En tiedä

22.
Palokunta on kohdannut tietoturvapoikkeaman edellisen viiden vuoden aikana:
*****

Esimerkiksi virushavainto tai tietomurto.

○ Kyllä

○ Ei

○ En tiedä

25.
Palokunnan kyvykkyys havaita tietoturvapoikkeamia on erinomainen. *

Täysin eri mieltä Täysin samaa mieltä □ En tiedä

26.
Koen palokunnan tarvitsevan enemmän ohjeistusta tieto- ja kyberturvallisuuden varmistamiseksi:
*

Täysin eri mieltä — Täysin samaa mieltä □ En tiedä

27. Palokunnan käyttämissä päätelaitteissa on päätelaitteen suojaus (virustorjunta tai vastaava).
*

Päätelaitteella tarkoitetaan esimerkiksi kannettavaa tietokonetta tai tablet-laitetta.

○ Kyllä

○ Ei

○ Osittain

○ En tiedä

28. Paloasemakiinteistön internetin sisäverkko on suojattu palomuurilla. *

○ Kyllä

○ Ei

○ En tiedä

29.
Palokunnalla on muita tietoturvatuotteita käytössään. *

Muita tietoturvatuotteita voisi olla esimerkiksi SIEM tai IDS/IPS-järjestelmät.

○ Kyllä

○ Ei

○ En tiedä

32. Mikä aiheuttaa suurimman huolen palokunnan kyvykkyydessä havaita tietoturvapoikkeamia?

33. Avoimet kommentit tämän sivun kysymyksiin:

Kiitos kyselyyn vastaamisesta! Muista napsauttaa Lähetä-painiketta lähettääksesi vastauksesi!

Appendix 2. Security Assessment Report – Case 1 (Defined as secret)

Appendix 3. Security Assessment Report – Case 2 (Defined as secret)

Appendix 4. Security Assessment Report – Case 3 (Defined as secret)

Appendix 5. Security Assessment Report – Case 4 (Defined as secret)

Appendix 6. Security Assessment Report – Case 5 (Defined as secret)