TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Deniss Solovjov 001585IASB

COMPUTER NETWORK SECURITY IN THE CONTEXT OF A LARGE COMPANY

Bachelor's thesis

Supervisor: Eduard Petlenkov
PhD

Tallinn 2019

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Deniss Solovjov 001585IASB

SISEVÕRGU TURVALISUS SUURE ETTEVÕTTE NÄITEL

Bakalaureseöö

Juhendaja: Eduard Petlenkov
PhD

Tallinn 2019

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Deniss Solovjov

18.11.2019

Abstract

The purpose of this work is to create applications that protect corporate intranets and corporate data.

1. Reconstruction of IT infrastructure at headquarters in Tallinn (number of computers about 60, number of servers 5, number of network drives (NAS))
2. Reconstruction of IT infrastructure in German and French branches.
3. Connection to VPN and DC at Headquarters and Affiliates
4. Configuration of a centralized security system (prohibiting the use of personal memory sticks, hard drives, and other devices that can damage computer devices, data, and corporate intranets)

Finally, check that the planned work has been carried out as planned and that the company's intranet is secure.

This thesis is written in English and is 36 pages long, including 5 chapters, 18 figures and 4 tables.

Annotatsioon

Sisevõrgu turvalisus suure ettevõtte näitel

Töö eesmärgiks on luua rakendus mis kaitseb sisevõrku ja korporatiivseid andmeid suures ettevõttes. Töö koosneb järgmistest etappidest:

1. IT infrastruktuuri ümberehitus peakontoris Tallinnas (arvutite arv umbes 60 tk, serverite arv 5 tk, võrguketaste (NAS) arv on 3tk)
2. IT infrastruktuuri ümberehitus Saksamaa ja Prantsusmaa filiaalides.
3. Peakontori ja filiaalide ühendamine VPN'ga ja DC'ga
4. Tsentraliseeritud turvasüsteemi seadistamine (isiklike mälupulkade, kõvaketaste ja muude seadmete kasutamise keelamine, mis võivad kahjustada arvutiseadmeid, andmeid ja ettevõtte sisevõrku)

Lõpuks kontrollida, et töö on teostatud plaanijärgselt ja ettevõtte sisevõrk on kaitstud.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 36 leheküljel, 5 peatükki, 18 joonist, 4 tabelit.

List of abbreviations and terms

IT	Information Technology
NAS	Network Access Storage (network drive)
VPN	Virtual private network
DC	Domain Controller
SWITCH	Network commutator
WIFI	Wireless internet
MALLWARE	Malicious software that may harm your computer
BITCOIN	Cryptocurrency
BACKUP	A copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event
AP	Access Point
POE	Power Over Ethernet
LAN	Local Area Network (intranet)
VLAN	Virtual Local Area Network
CENTOS 7	Linux version
AD	Active Directory
MU - MIMO	Multi - User, Multiple Input, Multiple Output
IP	Internet Protocol
BOTNET	The computer network, which consists of a number of machines running the robots - a separate software
GPO	Group Policy Object (group policy configuration)
USB	Universal Serial Bus
NAT	Network Address Translation

Table of contents

List of figures

List of tables

1 Introduction

Nowadays, the Internet impinges on almost every area of our lives. Every day, more and more new technologies are emerging that make life easier for a particular individual in such large, rapidly evolving businesses as described in this case study. In this regard, the use of the Internet and innovative technologies have allowed them to expand their capabilities, aided and abetted by the undeniable benefits such as accessibility, efficiency and awareness which the internet affords. Because of this, companies create their own networks with their services, from the corporate portal to the mail server.

With the advent of new technologies, people are appearing who attempt to take advantage of the ignorance, incomprehension and incompetence of some workers. Especially, malicious attempts to appropriate interesting data that is located in the corporate intranet: for example, employee personal data, customer data, corporate data, representing trade secret. To protect the corporate network, tests are needed to identify potential vulnerabilities that could cause a complete system failure and damage the business.

The structure of the thesis consists of 4 main parts: description of the problem, its solution, comparison and analysis, and summary. My role in the project is as follows: to analyze the shortcomings of the security system, compare existing solution methods, select the appropriate methods and incorporate them into the enterprise.

2 Description of the problems

2.1 Company description

The case study Company was founded in 1934, and specializes in complex technical retrofit projects, ‚newbuildings' outfitting projects, refit and refurbishment, and ship repair around the world.

Today the company staff consists of over 600 permanent highly skilled and experienced marine professionals, and is centrally managed from the head office in Tallinn, Estonia. Additionally, there are branch offices in Italy, France, and Germany where the company has large, long-term projects. This service is mainly offered in the form of outsourcers contracted to larger companies [1].

2.2 Current situation in the company

Within two years this company has grown very rapidly. A few years ago, there were about 80 computers in total in the company, compared to more than 250 today. There are simple solutions, such as a central high-end router and similar price ranges switches. Some computers come with separately purchased antivirus: some have a built-in antivirus for Windows. With the password is the same situation, some employees are using it, but some of them consider that it is unnecessary. In addition, the Wi-Fi network in very poor condition. For example, the Company's employees and guests are currently on one network, with printers, computers and switches situated in the local network. Security is minimal and equipment does not meet today's needs.

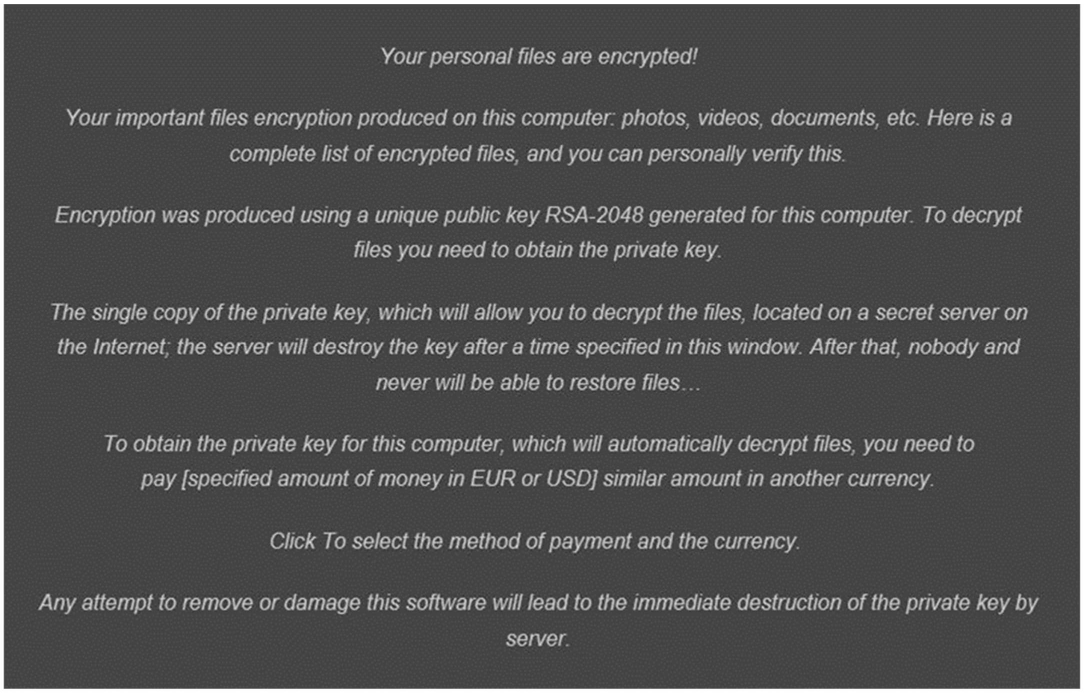
2.3 Workers as computer users

Employees read corporate emails, access corporate data and information systems on smart devices and laptops. The current existing security systems are simple and not effective. For example, in a best-practice model, all the screens should be locked (not all users do it), whereby locked screens data is protected in the event of a device being lost and getting into foreign hands.

In fact, not all users can differentiate between normal emails and malicious ones. On the Internet, there are links and sites full of viruses and Malware software.

2.4 What has happened

As seems to be relatively common, no one has thought about upgrading IT security since the first major incident happened, when the accounting server was hacked with a crypto virus (Crypto Locker). The entire database was encrypted and only the admin user was working. After logging in, the desktop had the following image (Figure 1):



Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files…

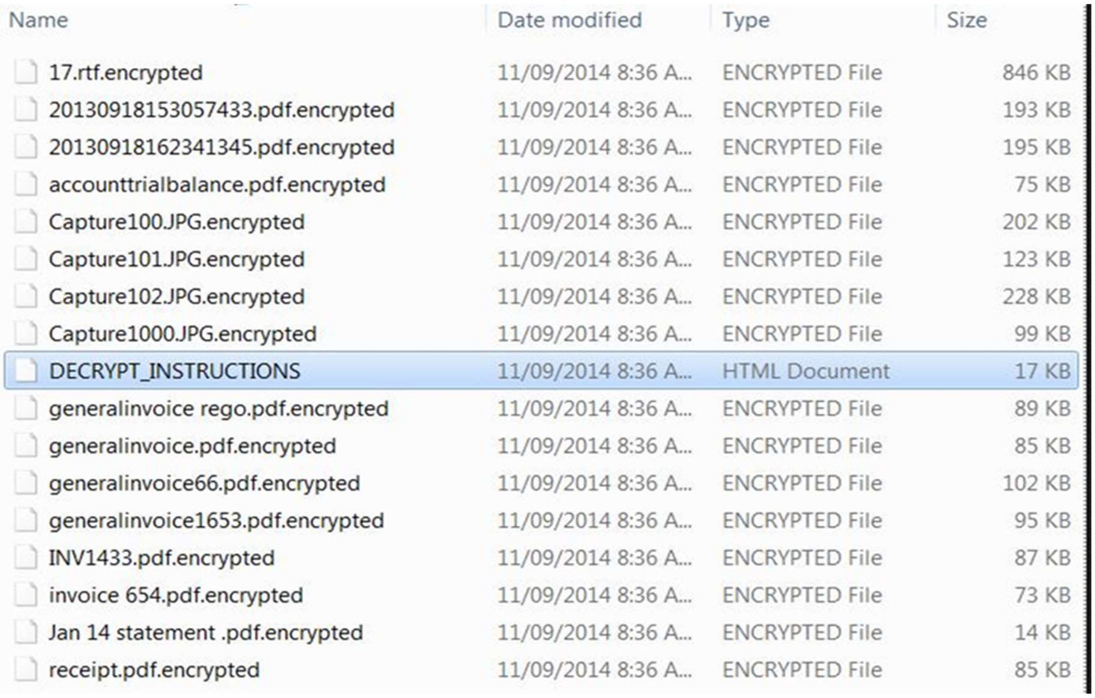
To obtain the private key for this computer, which will automatically decrypt files, you need to pay [specified amount of money in EUR or USD] similar amount in another currency.

Click To select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Figure 1. Crypto Locker info

This means that if we wanted the data back then we would have had to pay 2,000 US dollars through the Bitlocker system. Certainly, all the files were encrypted and not available for the users and admins. The Figure 2 shows what the file format was.

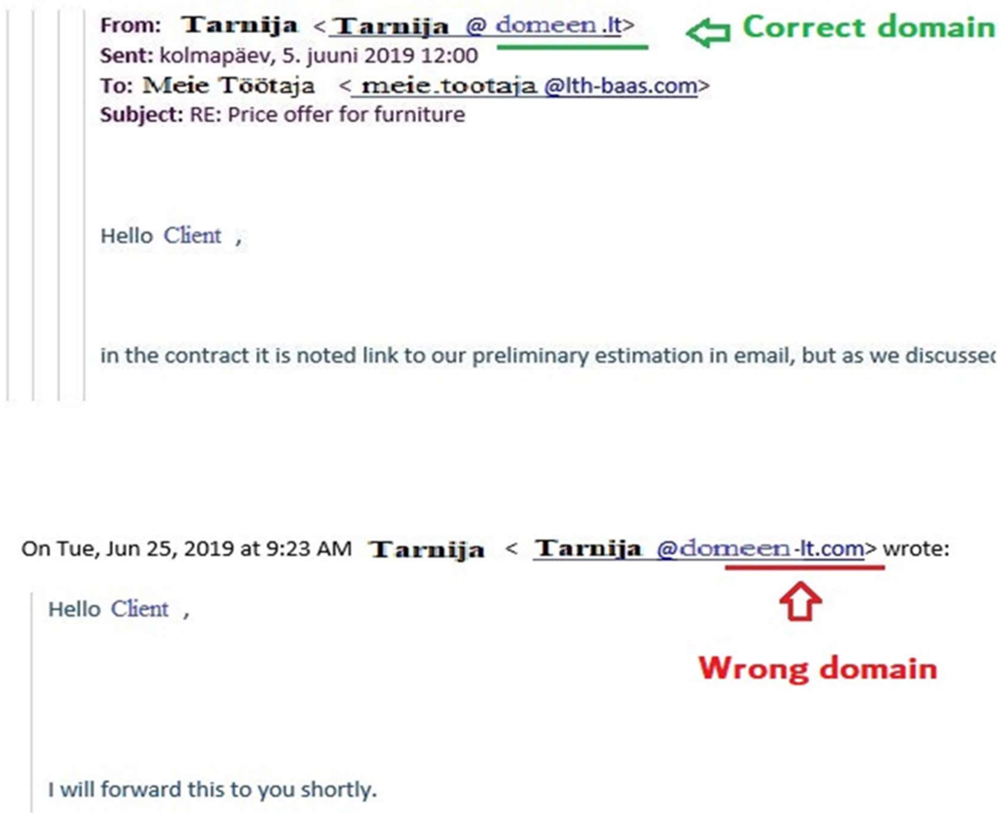


Name	Date modified	Type	Size
17.rtf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	846 KB
20130918153057433.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	193 KB
20130918162341345.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	195 KB
accounttrialbalance.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	75 KB
Capture100.JPG.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	202 KB
Capture101.JPG.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	123 KB
Capture102.JPG.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	228 KB
Capture1000.JPG.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	99 KB
DECRYPT_INSTRUCTIONS	11/09/2014 8:36 A...	HTML Document	17 KB
generalinvoice rego.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	89 KB
generalinvoice.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	85 KB
generalinvoice66.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	102 KB
generalinvoice1653.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	95 KB
INV1433.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	87 KB
invoice 654.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	73 KB
Jan 14 statement .pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	14 KB
receipt.pdf.encrypted	11/09/2014 8:36 A...	ENCRYPTED File	85 KB

Figure 2. Encrypted files (example).

Fortunately, as a backup was done the previous night, the data was restored, but one working day was lost and accountants had to rebuild the data base manually throughout the day.

In another significant case, a project manager talked to one supplier via email concerning an agreement that the supplier would load the ordered goods onto the ship. There was a contract and quite a lot of correspondence about it, including the last letter requesting an advance payment (approximately € 20,000). Subsequently, a prepayment bill was duly drawn up and sent to the accountant who paid it. A week later, the supplier reported that no monies had been received, whereupon a check was duly carried out and it was found that somewhere in the middle of correspondence, the domain of the exploits had changed and the conversation was already with other people (the hacker). In the Figure 3, it is shown how the domain was changed.



From: Tarnija < Tarnija @ domeen .lt>
Sent: kolmapäev, 5. juuni 2019 12:00
To: Meie Töötaja < meie.tootaja @lth-baas.com>
Subject: RE: Price offer for furniture

Correct domain

Hello Client ,

in the contract it is noted link to our preliminary estimation in email, but as we discusse

On Tue, Jun 25, 2019 at 9:23 AM Tarnija < Tarnija @domeen-lt.com> wrote:

Hello Client ,

Wrong domain

I will forward this to you shortly.

Figure 3. Correspondence with the supplier.

2.5 The Cause

A thorough analysis and investigation into the cause of both cases was subsequently carried out with the aim of identifying any mistakes and weak links in the security 'chain'. In the first case, related to an accounting server, it was found that under one of the users was installed Crypto Locker. This means that all users had complex passwords, but one had a very weak password. Table 1 shows this:

Name	**User**	**Pass**	
User 1	user1	StrongPassword1	
User 2	user2	StrongPassword2	
User 3	user3	StrongPassword3	
User 4	user4	12345	**weak password**
User 5	user5	StrongPassword5	
User 6	user6	StrongPassword6	
User 7	user7	StrongPassword7	
User 8	user8	StrongPassword8	
User 9	user9	StrongPassword9	

Tabel 1. List of users and passwords.

The second case was ultimately attributed to basic human error. Inevitably, with a typical rate of 200 emails per day, someone might not notice that two letters in the address had changed, which was what occurred in this case.

3 Solution

3.1 IT Audit

In order to improve the situation in the company, it is essential first to know what the solutions and devices currently in use are, and to understand what the current situation with the network is. To this end, an IT audit is required.

This company is audited in three parts:

a) Server room and network audit (routers, switches, servers, WiFi APs, NASs)

b) Auditing of laptops and desktops

c) Software audit

In fact, the audit shows that security is very weak. All computers, printers, telephones, tablets, guest devices are all on the same network and connect to Internet directly with a regular Provider router (Illustrative Figure 4).

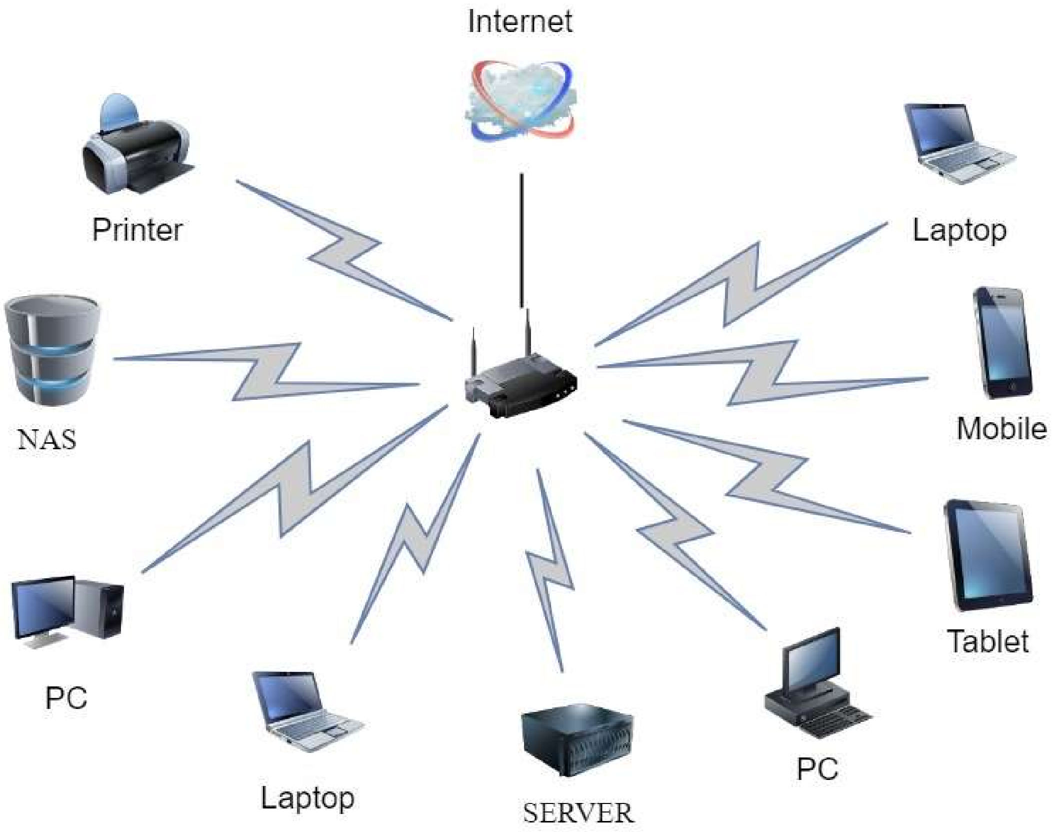


Figure 4. Today’s intranet in the company.

3.2 New infrastructure planning

In this company, it is essential to eliminate completely all security loopholes. In order to achieve this, it is necessary to devise a plan and a diagram of how to proceed in the future. Based on the findings of the audit, a plan of action has been devised. As follows:

a) Obtain new network hardware and software.

b) Develop a detailed plan for deploying Active Directory (domain) and security systems in the company.

c) DC licenses, configuration, connection, testing.

d) Configure a centralized WIFI system.

e) Integrate head office users in to the domain (configuring each computer, configuring offline folders and other procedures associated with this step).

f) Connect German branches to the company's internal network, connecting to the head office and employees' computers in to the DC.

g) Connect French branch to the company's internal network; connecting to the head office and employees' computers in to the DC.

h) Set up a centralized security system (prohibiting the use of personal memory sticks, hard drives and other devices which could damage computer equipment, data and the company's internal network). Computer’s Hard Drives Encryption.

i) Set up monitoring for all network devices, servers, and anti-virus (24-hour device monitoring).

The diagram of the new, future and secure network is determined in Figure 5:

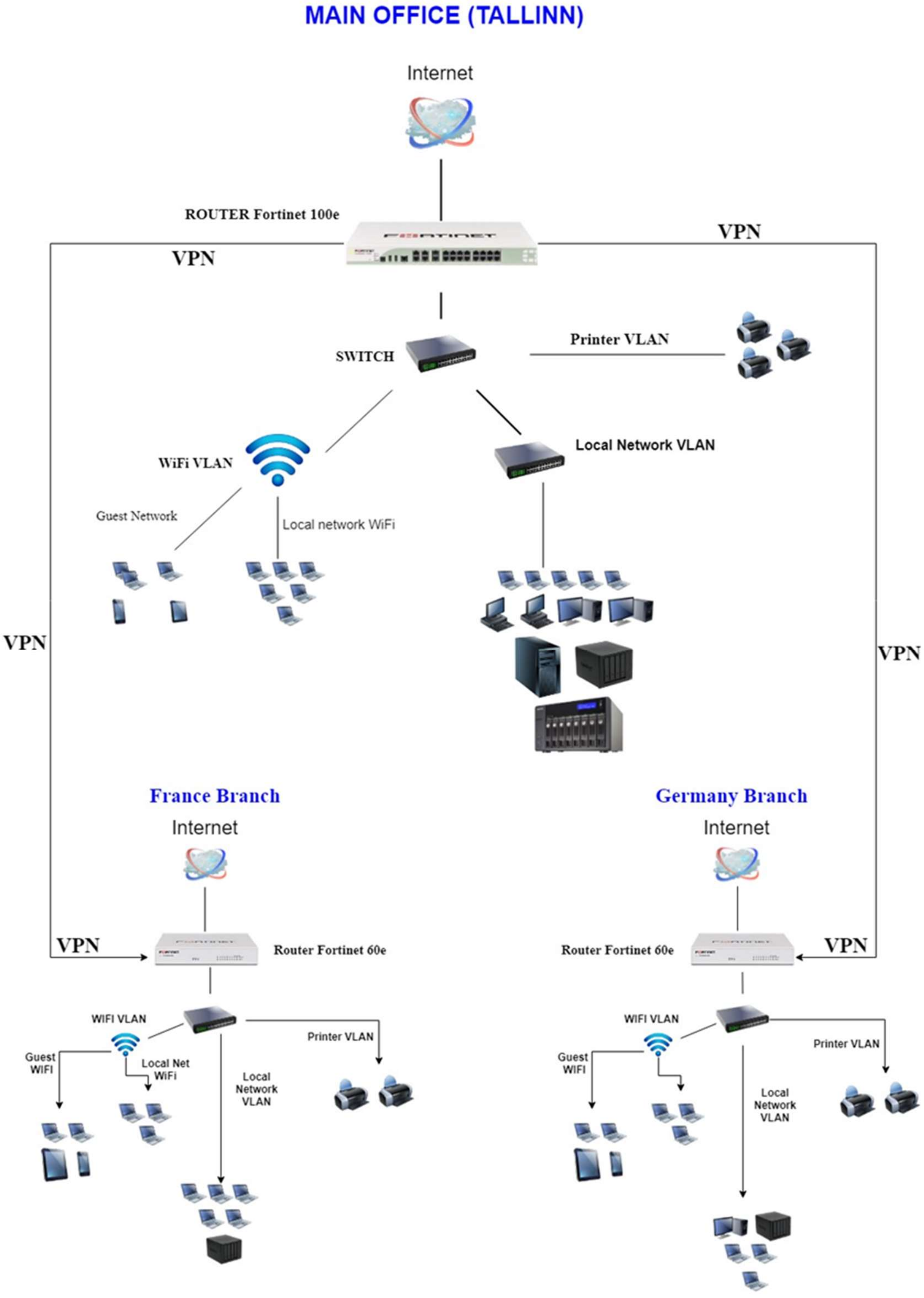


Figure 5. Schematic of a future intranet.

3.3 Obtaining Hardware and Software

The Network hardware of the company is somewhat outdated and insecure. As a result, a request for new equipment and licenses has been sent. The choice of equipment was based on three main criteria: price, quality and functionality. Accordingly, the following equipment and licenses were planned to be purchased:

- FortiGate 100E - head router to Tallinn office
- FortiCare with 3-year support 24x7 - Provides firmware upgrades, tech support and FortiGuard subscriptions (included with Fortigate 100E)
- Ubiquiti Unifi Switch 8-60W - PoE switch for wireless AP'd through the LAN cable. 1 pc to Tallinn, 1 pc to France and 1 pc to Germany.
- Ubiquiti UniFi AC High Density - Wireless AP'd. 6 pieces to Tallinn, 3 pieces to France and 3 pieces to Germany.
- Ubiquiti Unifi Cloud Key - AP'd control center. 1 pc to Tallinn, 1 pc to France and 1 pc to Germany.
- 28-Port Gigabit Smart Switch, D-Link - 1 pc for France and 1 pc for Germany.
- 48-Port Gigabit Smart Switch, D-Link - 1 pc Tallinn
- Synology DS418 NAS 8TB - Network File Server. 1 pc to Tallinn, 1 pc to France and 1 pc to Germany.
- UPS APC Back 700VA / 390W BX70 - Uninterruptible Power Supply for Network Equipment 1 pc to Tallinn, 1 pc to France and 1 pc to Germany.
- Dell PE T440 2X4114 SILV H730P - Server for Domain and Active Director in Tallinn.

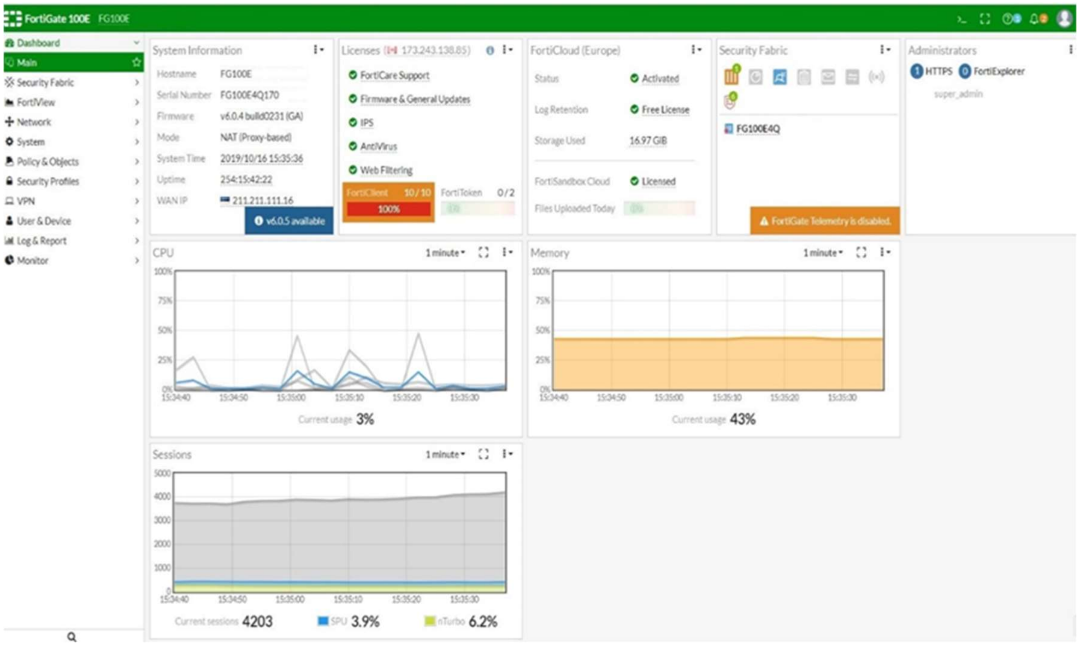
From Table 2, you can see the prices and suppliers' information.

NAME	PCS	PRICE/PC (€)	PRICE TOTAL (€)	SUPPLIER
FortiGate 100E	1	1 999	1 999	ATEA
FortiGate 60E	2	470	940	ATEA
Ubiquiti UniFi Switch 8-60W	3	100,15	300	ATEA
Ubiquiti UniFi AC HD	12	269,9	3 239	ATEA
Ubiquiti UniFi Cloud Key	3	67,4	202	ATEA
28-Port Gb Smart Switch, D-Link	2	264,1	528	ATEA
48-Port Gigabit Smart Switch, D-Link	1	899	899	ATEA
Synology DS418 NAS 8TB	3	754	2 262	ORDI
UPS APC Back 700VA/390W	3	80	240	ORDI
Dell PE T440 2X4114 H730P Server	1	4820	4 820	DATAGATE
FortiCare 3 year support 24x7	1	3520	3 520	ATEA
Total:			**18 950 € + VAT**	

Tabel 2. Equipment and Licensing Offer.

3.4 Domain, Active Directory and Enterprise Security Deployment

Subsequently, all equipment was purchased. The next step is to configure the Domain Controller. It was decided to do this on the Linux platform. There is no need to buy a separate license for this, and the system itself is more stable. On the new DELL server, a VMWare ESX platform was installed. This means that DC is installed on the virtual server. Once the first step is complete, it is necessary to perform a security system analysis, in order to ascertain what to do next and in what order. Next, it is necessary to build a new intranet, starting by installing and configuring the router and switches. Since it is envisaged to make at least three VLANs, a complicated configuration will be required. In this respect, The Fortinet interface is very friendly (Figure 6) and quite easy to configure.



System Information

Hostname FG100E
Serial Number FG100E4Q170
Firmware v6.0.4 build0231 (GA)
Mode NAT (Proxy-based)
System Time 2019/10/16 15:35:36
Uptime 254:15:42:22
WAN IP 211.211.111.16

Licenses (173.243.138.85)

- FortiCare Support
- Firmware & General Updates
- IPS
- AntiVirus
- Web Filtering

FortiClient 10/10 100%
FortiToken 0/2

FortiCloud (Europe)

Status Activated
Log Retention Free License
Storage Used 16.97 GIB
FortiSandbox Cloud Licensed
Files Uploaded Today 0%

Security Fabric

FG100E4Q

Administrators

1 HTTPS 0 FortiExplorer
super_admin

Current usage 3%

Current usage 43%

Current sessions 4203 SPU 3.9% nTurbo 6.2%

Figure 6. Fortinet interface

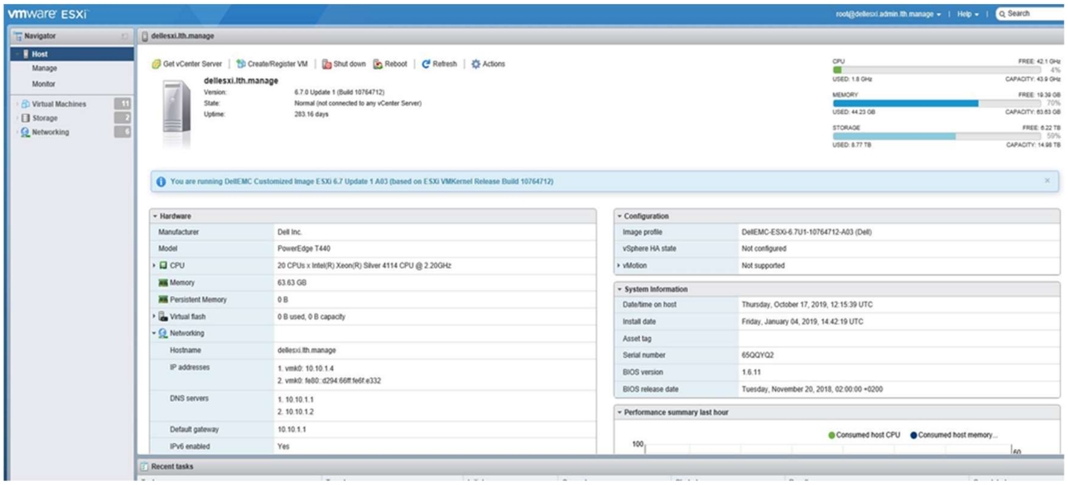
VLANi interfaces:

- VLAN1 has subnet 192.168.1.254 for the intranet
- VLAN2 is a wireless network with a subnet 10.10.5.1
- VLAN3 has a subnet for printers with 10.10.4.254

Now our network is separated. On the switches, we configure same VLANs. After that, we can move on.

3.5 Configuring the Domain Controller

On the ESXi's platform (Figure 7) a new virtual machine has been created where Linux was installed. We used the CentOS 7 platform.



dellesxi.lth.manage

Version:	6.7.0 Update 1 (Build 10764712)
State:	Normal (not connected to any vCenter Server)
Uptime:	283.16 days

CPU FREE: 42.1 GHz 4% USED: 1.8 GHz CAPACITY: 43.9 GHz

MEMORY FREE: 19.39 GB 70% USED: 44.23 GB CAPACITY: 63.63 GB

STORAGE FREE: 6.22 TB 59% USED: 8.77 TB CAPACITY: 14.98 TB

You are running DellEMC Customized Image ESXi 6.7 Update 1 A03 (based on ESXi VMKernel Release Build 10764712)

Hardware

Manufacturer	Dell Inc.
Model	PowerEdge T440
CPU	20 CPUs x Intel(R) Xeon(R) Silver 4114 CPU @ 2.20GHz
Memory	63.63 GB
Persistent Memory	0 B
Virtual flash	0 B used, 0 B capacity
Networking	
Hostname	dellesxi.lth.manage
IP addresses	1. vmk0: 10.10.1.4 2. vmk0: fe80::d294:66ff:fe6f:e332
DNS servers	1. 10.10.1.1 2. 10.10.1.2
Default gateway	10.10.1.1
IPv6 enabled	Yes

Configuration

Image profile	DellEMC-ESXi-6.7U1-10764712-A03 (Dell)
vSphere HA state	Not configured
vMotion	Not supported

System Information

Date/time on host	Thursday, October 17, 2019, 12:15:39 UTC
Install date	Friday, January 04, 2019, 14:42:19 UTC
Asset tag	
Serial number	65QQYQ2
BIOS version	1.6.11
BIOS release date	Tuesday, November 20, 2018, 02:00:00 +0200

Performance summary last hour

Figure 7. The ESXi platform.

CentOS underwent all the necessary preparations and the domain manager panel was connected to a Windows 10 virtual machine. This is easier to manage with users and group politicians. Three groups were created at AD's: Tallinn, France and Germany. There is a common certification system for users and computers. The following logic was used for users:

For example, there is an employee in Tallinn, Peeter Saarapuu. To create domain account for this user, we took his initials and the first letter of the branch - TPSPC, which stands for Tallinn Peeter Saarapuu Personal Computer.

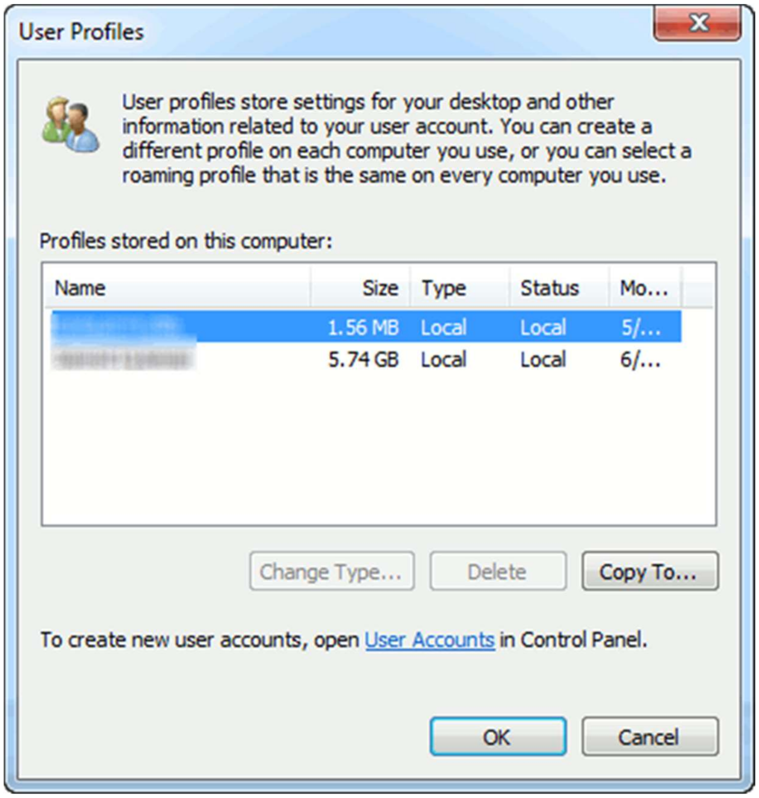
This process was replicated in Germany and France. The first passwords are automatically generated. There are ten symbols in the password; at least one uppercase and one lowercase letter, one number. Mandatory monthly password change (decision of owner of the company). Table 3 gives an example.

Employee	User	Computer	Password
TALLINN			
Peeter Saarapuu	tps	TPSPC	fN5RvkZLYv
Aare Keel	tak	TAKPC	UZbyFM4WdF
Georg Ots	tgo	TGOPC	en3QLfgFxy
Mikk Saar	tms	TMSPC	9jjW7X6X4z
Evely Sepp	tes	TESPC	Rb5a97C7WA
FRANCE			
Abella Caron	fac	FACPC	sZXgPuVrw4
Felipan Berger	ffb	FFBPC	LhFrqfbxKv
Geneva Couture	fgc	FGCPC	96nVg6kv4z
Hazard Segal	fhs	FHSPC	xYhSgju8Es
Marian Mullins	fmm	FMMPC	rWTnBCdaw6
GERMANY			
Ben Müller	gbm	GBMPC	PvH7bVCJ3k
Paul Schmidt	gps	GPSPC	hD65NJ59ge
Jonas Schneider	gjs	GJSPC	zK7PQREJHb
Elias Meyer	gem	GEMPC	sXg7FU56dj
Leon Becker	Glb	GLBPC	wHpP9RQ6jV

Tabel 3. Example of employees, users, computers, and passwords.

3.6 Enterprise Integration and Testing

All preparations with domain controller are complete, and employee computers are now being integrated into the domain. The computer test proved satisfactory. However, the ultimate test will be how these new systems and procedures perform in practice when used by the actual staff. Five users were selected and work started. The easiest step is to connect a user to DC. After initial login, users should change their temporary passwords, thereby allowing user access into the domain system. Now all data, documents and profiles need to be moved to the domain profile. Unfortunately, in Windows 10, there is no longer a feature whereby you can simply copy the user profile (Figure 8). Therefore, all data was copied manually. After this, users will begin testing it and provide information to the IT department if any problems arise.



User Profiles

User profiles store settings for your desktop and other information related to your user account. You can create a different profile on each computer you use, or you can select a roaming profile that is the same on every computer you use.

Profiles stored on this computer:

Name	Size	Type	Status	Mo...
[redacted]	1.56 MB	Local	Local	5/...
[redacted]	5.74 GB	Local	Local	6/...

To create new user accounts, open User Accounts in Control Panel.

Figure 8. Profile migration in Windows 7.

3.7 Configuring a Centralized WiFi System

For the Wireless network, four manufacturers were reviewed: Ubiquiti, Aruba, Ruckus, Meraki and. Ubiquiti hardware has been chosen. Why was such a manufacturer chosen? As you can see in Figure 9, Ubiqiuti's has the best specification throughput [2].

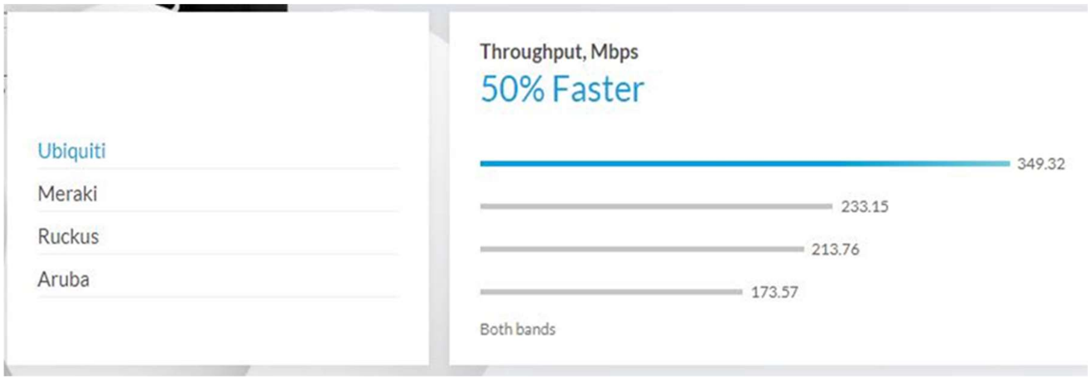


Figure 9. Comparison of wireless APs.

Under the Unifi controller system (Figure 10), independent physical sites with unique network monitoring, configurations, maps, statistics and administrator accounts can be created and managed. Unifi controller dashboard displays an overview of the state of enterprise networks, as well as complete statistics, analytics and other data understanding. The UniFi Controller can be employed to configure and provide Ubiquti APs, switches and gateways with basic, industry-standard settings such as VLAN, POE and more, while taking full advantage of Wi-Fi scanning of the patented Ubiquiti tools and Packet deep control. In addition, UniFi simplifies bandwidth control, traffic planning and network access policies for different users, such as guests.

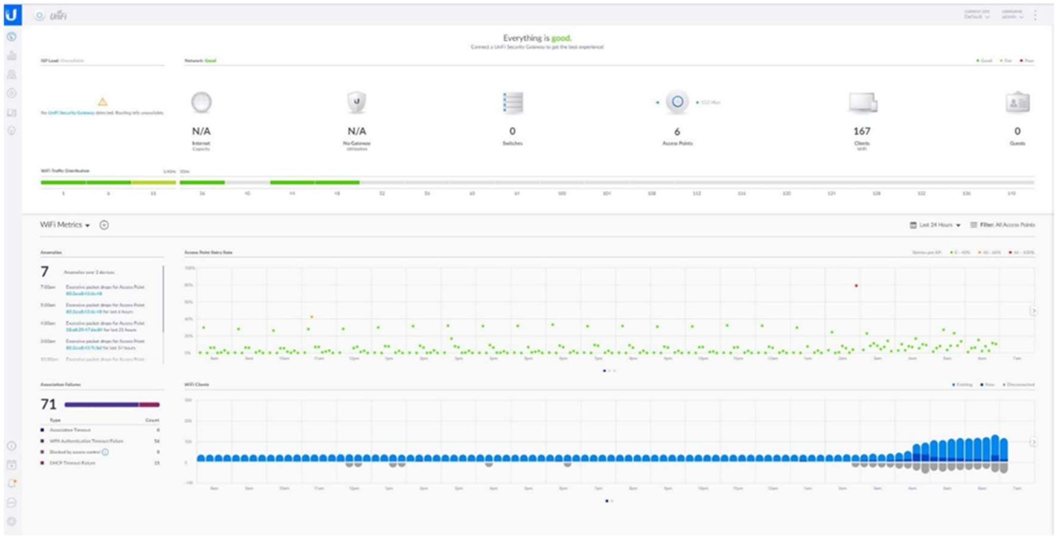


Figure 10. UniFi controller interface.

The new WiFi system installation starts with the installing of the PoE Switch, Unifi Cloud Key and six Ubiquiti AP'd in Tallinn office. The UniFi controller is located on the Cloud Key and is configured for WiFi. An internal network of employees has been created, for example, MAIN NETWORK and guest network, for example, GUEST NETWORK, which gives access only to the web pages and some of the services such as Exchange, WhatsApp and Viber. The Guest network is located under separate VLAN, and both networks are protected by complicated passwords and WPA-PSK encryption. Once the configuration is ready, the WiFi Access Points will be connected, after which it is necessary to upgrade them and download the configuration to each wireless access point. We used Ubiquiti High Density AP. The selection was stopped on these devices because they use MU-MIMO technology (Figure 11). This means that each wireless hub communicates with multiple clients at once - significantly increasing multi-user throughput and overall user experience [3].

Figure 11. MU-MIMO technology.

After the Wi-Fi network was completed, it was necessary to test it with actual users. Phones and tablets were connected to a guest network, laptops and desktops were connected to a regular network. The results were encouraging: computers do not interfere with each other because of MU-MIMO technology. The UniFi controller itself will decide which AP to connect to with a client that has a better signal and shows clearly how much data each client is using. A similar system is installed in both branches: France and Germany. Figure 12 shows the overall state of the Wi-Fi network in the company.

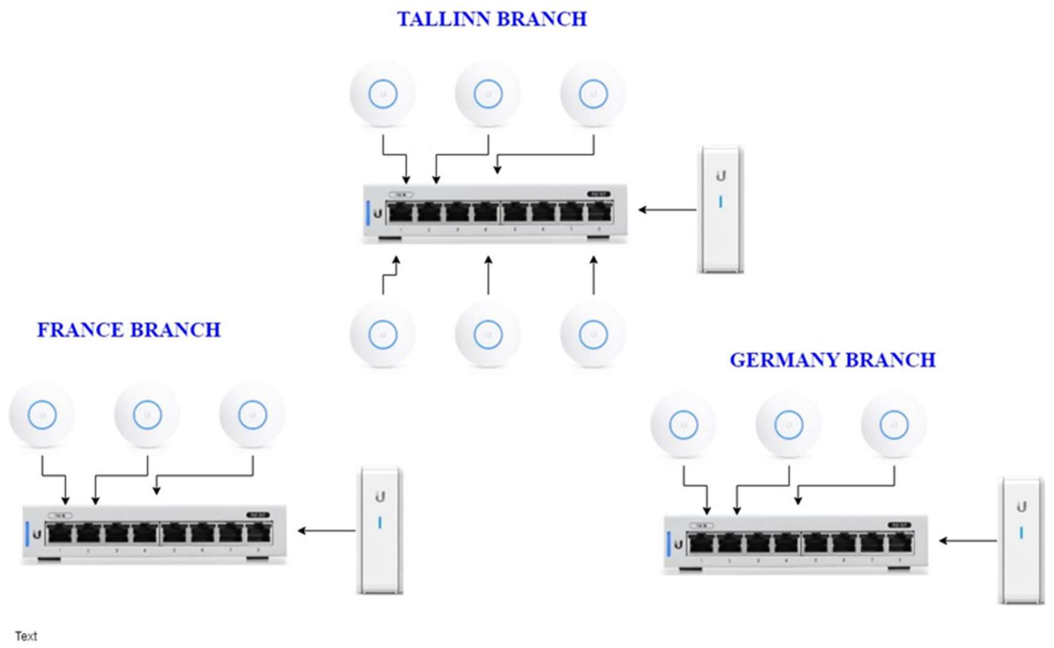
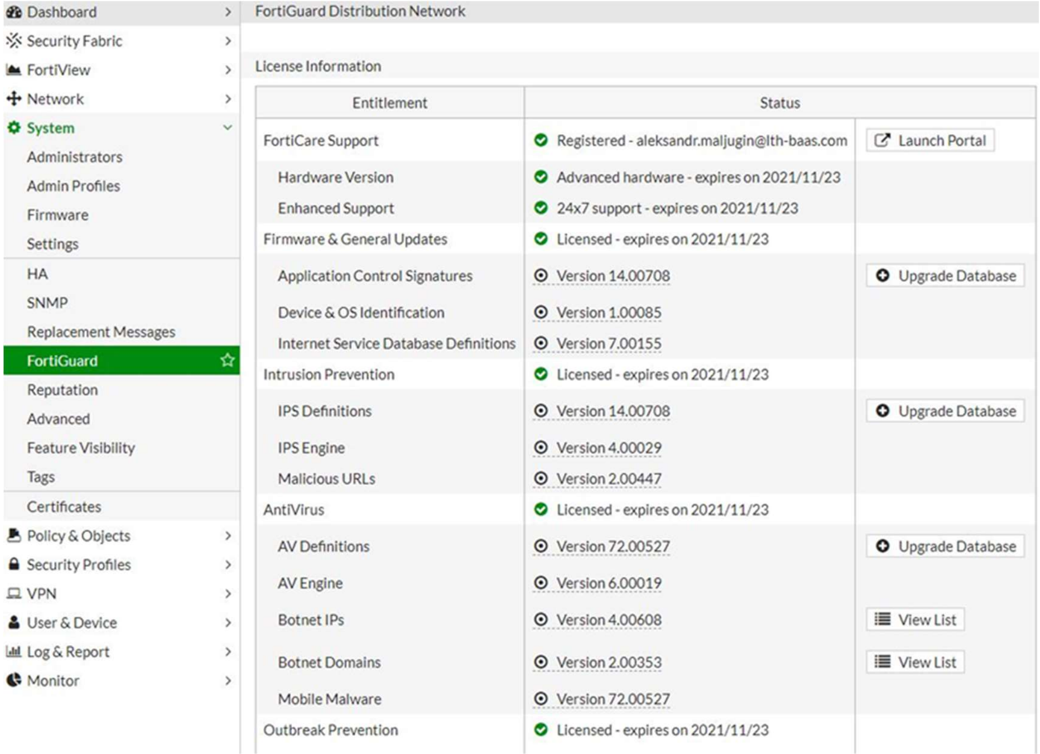


Figure 12. Architecture of WiFi networks.

3.8 Setting up a centralized security system

The intranet is more or less ready and protected. After that, it is necessary to protect one's business computers. The first firewall that protects the intranet is located on a router called FortiGuard (Figure 13).



FortiGuard Distribution Network

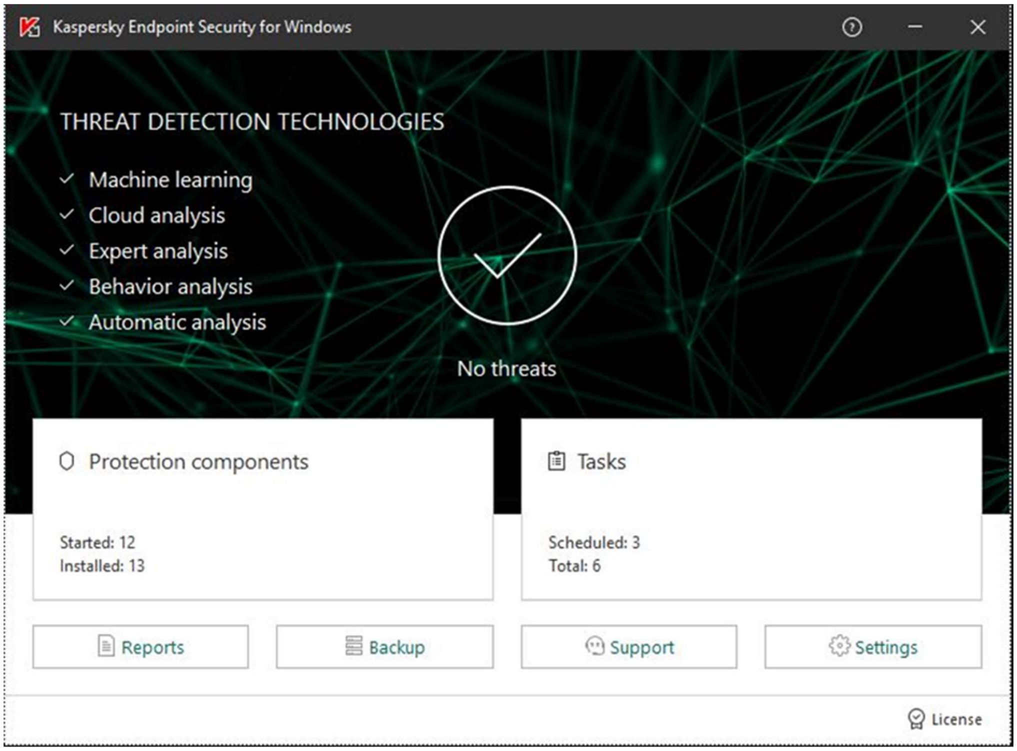
License Information

Entitlement	Status
FortiCare Support	✓ Registered - aleksandr.maljugin@lth-baas.com
Hardware Version	✓ Advanced hardware - expires on 2021/11/23
Enhanced Support	✓ 24x7 support - expires on 2021/11/23
Firmware & General Updates	✓ Licensed - expires on 2021/11/23
Application Control Signatures	Version 14.00708
Device & OS Identification	Version 1.00085
Internet Service Database Definitions	Version 7.00155
Intrusion Prevention	✓ Licensed - expires on 2021/11/23
IPS Definitions	Version 14.00708
IPS Engine	Version 4.00029
Malicious URLs	Version 2.00447
AntiVirus	✓ Licensed - expires on 2021/11/23
AV Definitions	Version 72.00527
AV Engine	Version 6.00019
Botnet IPs	Version 4.00608
Botnet Domains	Version 2.00353
Mobile Malware	Version 72.00527
Outbreak Prevention	✓ Licensed - expires on 2021/11/23

Figure 13. FortiGuard – router firewall.

FortiGuard already scans incoming and outgoing Internet traffic. The following objects are scanned: viruses, malware, mobile software, BOTNET domains, BOTNET IP addresses, mails etc.

All computers need to have antivirus installed as well. The choice was made to install Kaspersky Endpoint Security (Figure 14).



THREAT DETECTION TECHNOLOGIES

- ✓ Machine learning
- ✓ Cloud analysis
- ✓ Expert analysis
- ✓ Behavior analysis
- ✓ Automatic analysis

No threats

Protection components

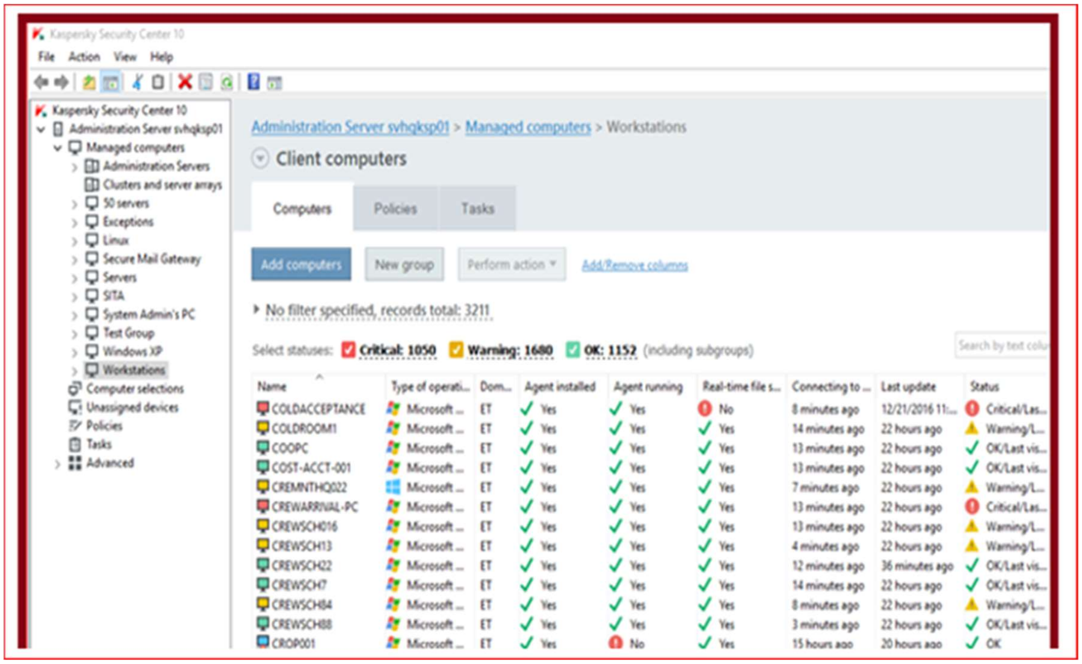
Started: 12
Installed: 13

Tasks

Scheduled: 3
Total: 6

Figure 14. Kaspersky Endpoint Security.

We can purchase a corporate license for this antivirus. This means that we are sent one electronic key (license) with which we can activate. For example, a hundred licenses on personal computers. However, installing the program on hundreds of computers manually takes too much time, and for this reason, Kaspersky has a very effective solution that works beautifully on both the intranet and the domain: Kaspersky Security Center. It can view computers online, install and update antivirus licenses, one at a time or one by one and remove software from computers that may harm your internal network or operating system. It can be seen if a computer was hacked or infected with a virus [4]. An example of Kaspersky Security Center is shown in Figure 15.



Administration Server svhqksp01 > Managed computers > Workstations

Client computers

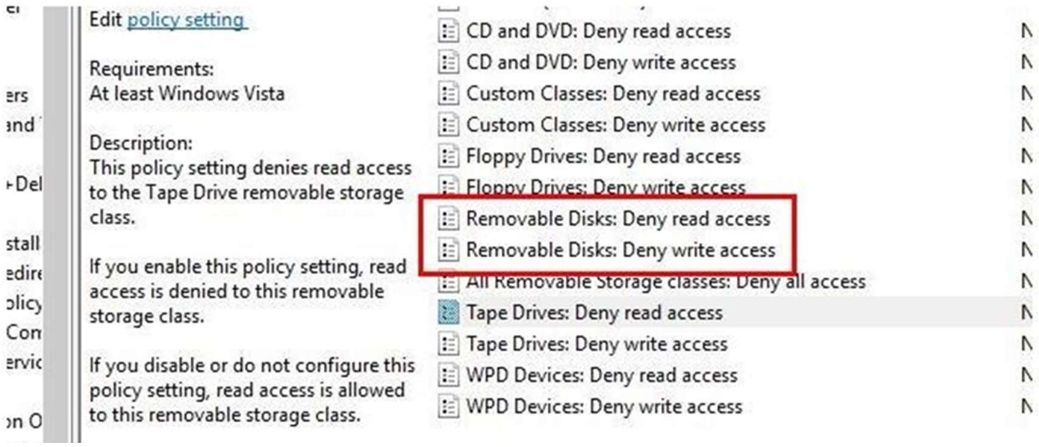
No filter specified, records total: 3211

Select statuses: ☑ Critical: 1050 ☑ Warning: 1680 ☑ OK: 1152 (including subgroups)

Name	Type of operati...	Dom...	Agent installed	Agent running	Real-time file s...	Connecting to ...	Last update	Status
COLDACCEPTANCE	Microsoft ...	ET	✓ Yes	✓ Yes	! No	8 minutes ago	12/21/2016 11:...	! Critical/Las...
COLDROOM1	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	14 minutes ago	22 hours ago	⚠ Warning/L...
COOPC	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	13 minutes ago	22 hours ago	✓ OK/Last vis...
COST-ACCT-001	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	13 minutes ago	22 hours ago	✓ OK/Last vis...
CREMNTHQ022	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	7 minutes ago	22 hours ago	⚠ Warning/L...
CREWARRIVAL-PC	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	13 minutes ago	22 hours ago	! Critical/Las...
CREWSCH016	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	13 minutes ago	22 hours ago	⚠ Warning/L...
CREWSCH13	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	4 minutes ago	22 hours ago	⚠ Warning/L...
CREWSCH22	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	12 minutes ago	36 minutes ago	✓ OK/Last vis...
CREWSCH7	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	14 minutes ago	22 hours ago	✓ OK/Last vis...
CREWSCH84	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	8 minutes ago	22 hours ago	⚠ Warning/L...
CREWSCH88	Microsoft ...	ET	✓ Yes	✓ Yes	✓ Yes	3 minutes ago	22 hours ago	✓ OK/Last vis...
CROP001	Microsoft ...	ET	✓ Yes	! No	✓ Yes	15 hours ago	20 hours ago	✓ OK

Figure 15. An example of Kaspersky Security Center.

Another important setting required is to disable the use of personal memory sticks, hard drives, and other devices on your work computer, making it impossible to use them without IT department permissions. This can be done in the GPO's domain (Figure 16).



Edit policy setting

Requirements:
At least Windows Vista

Description:
This policy setting denies read access to the Tape Drive removable storage class.

If you enable this policy setting, read access is denied to this removable storage class.

If you disable or do not configure this policy setting, read access is allowed to this removable storage class.

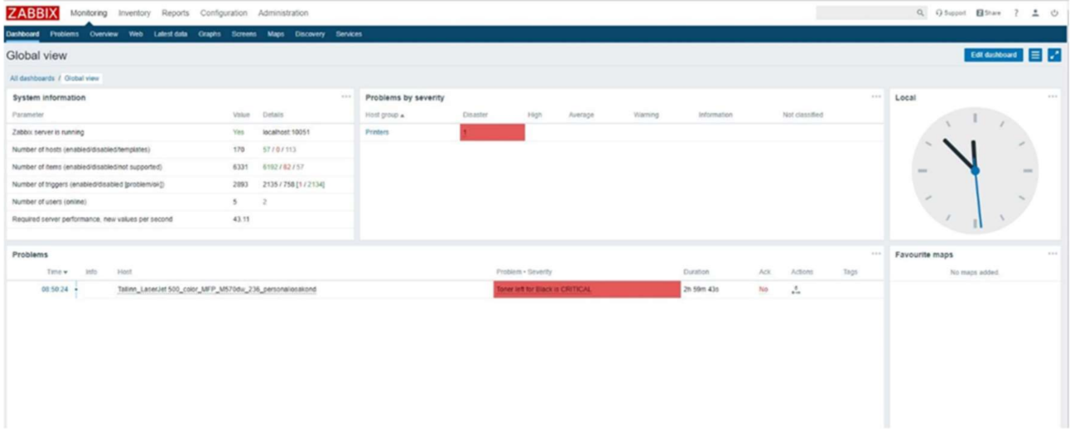
CD and DVD: Deny read access	N
CD and DVD: Deny write access	N
Custom Classes: Deny read access	N
Custom Classes: Deny write access	N
Floppy Drives: Deny read access	N
Floppy Drives: Deny write access	N
Removable Disks: Deny read access	N
Removable Disks: Deny write access	N
All Removable Storage classes: Deny all access	N
Tape Drives: Deny read access	N
Tape Drives: Deny write access	N
WPD Devices: Deny read access	N
WPD Devices: Deny write access	N

Figure 16. Turning off USB sticks in GPO.

As soon as it is ready, users will be notified that the use of memory sticks is prohibited.

3.9 Monitoring the Intranet

Intranet monitoring is a very important part of the IT infrastructure. Because of this, it was decided to make a separate virtual server on the Linux platform and install Zabbix Agent (Figure 17).



System information

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (enabled/disabled/templates)	170	57 / 0 / 113
Number of items (enabled/disabled/not supported)	6331	6192 / 82 / 57
Number of triggers (enabled/disabled [problem/ok])	2893	2135 / 758 [1 / 2134]
Number of users (online)	5	2
Required server performance, new values per second	43.11	

Problems by severity

Host group ▲	Disaster	High	Average	Warning	Information	Not classified
Printers	1					

Problems

Time ▾	Info	Host	Problem • Severity	Duration	Ack	Actions	Tags
08:50:24	•	Tallinn_LaserJet 500_color_MFP_M570dw_236_personaliosakond	Toner left for Black is CRITICAL	2h 59m 43s	No		

Figure 17. Zabbix Agent – monitoring software.

Zabbix agents are used for observational purposes to actively monitor local resources and applications (statistics on hard drives, memory, processors, etc.). The agent collects operational information locally and sends the data for further processing to the Zabbix server. In the event of problems (such as lack of free hard disk space or an unusual termination of the service process), the Zabbix server can quickly notify the administrators of the specific server that reported the error. Zabbix agents are extremely effective because they use native system calls to gather statistical information [5]. In Table 4 lists the checks that can be configured in the agent.

Network	Packets/bytes transfered
	Errors/dropped packets
	Collisions
CPU	Load average
	CPU idle/usage
	CPU utilization data per individual process
Memory	Free/used memory
	Swap/pagefile utilization
Disk	Space free/used
	Read and write I/O
Service	Process status
	Process memory usage
	Service status (ssh, ntp, ldap, smtp, ftp, http, pop, nntp, imap)
	Windows service status
	DNS resolution
	TCP connectivity
	TCP response time
File	File size/time
	File exists
	Checksum
	MD5 hash
	RegExp search
Log	Text log
	Windows eventlog
Other	System uptime
	System time
	Users connected
	Performance counter (Windows)

Tabel 4. Zabbix Agent Functions.

4 Comparison and analysis

Finally, now the task has been completed, it is possible to compare our previous IT infrastructure situation with a new, modern, secure solution.

In the beginning, a standard solution was used in our company, used by 80% of companies in Estonia, which comprised a service provider router with NAT system and enterprise equipment. Very rarely do people use quality security software (antivirus, firewall, etc.). Consequently, these companies do not have good IT protection from hackers and malicious attacks, which makes them highly vulnerable to losing commercially sensitive information, and invariably implies the payment of large sums of money to restore this data in the event of an attack.

In order to counteract this threat, the company’s intranet has been rebuilt, using modern and security hardware from manufacturers such as Dell, Fortinet and Ubiquity. DC, based on a Linux platform which was integrated into the local network. A WiFi network was realized according to plan, and all dangerous ports were closed. This means that it is now harder to hack a company's intranet and computers. In addition, antiviruses and firewalls were installed on the user’s PCs and external devices (flash drives, external hard drives, etc.) at the group policy level were blocked in the domain.

In comparison with the previous IT infrastructure with the modern one, it can confidently be stated that the company is now fully protected in terms of IT.

5 Summary

The aim of this work was to create a safe and secure intranet in a large and dynamically growing company.

Companies must defend themselves on three fronts:

a) Company protection: construction of lines of defense.

b) Optimization of the cyber security system: Priority will be given to rejecting ineffective solutions,

c) Supporting growth: increasing productivity and reinvesting in innovative technologies to improve the existing security system.

This work should be done in three directions at the same time [6]. Only under these conditions, is cyber security the key to growth. I can say that security = risk management (Figure 18) [7].

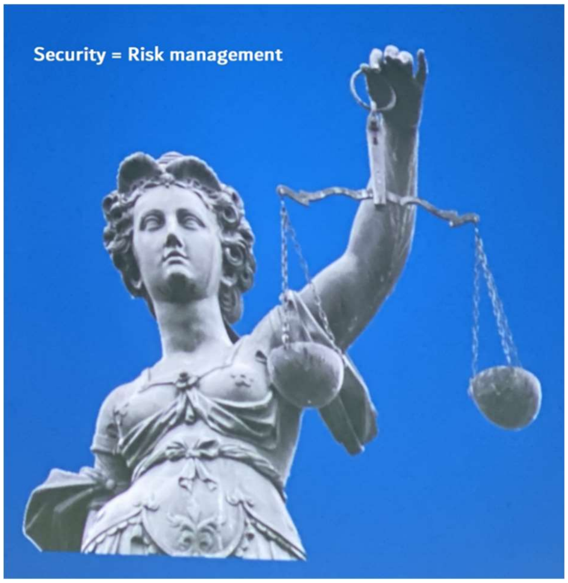


Figure 18. Security = Risk management.

References

[1] LTH-Baas As homepage, about info. Available: https://www.lth-baas.com/about-us/ [Accessed 15.11.2019]

[2] Ubiquiti corporation, Why Unifi? Available: https://www.ui.com/why-unifi/ [Accessed 15.11.2019]

[3] Ubiquiti corporation, MU-MIMO technology. Available: https://unifi-hd.ui.com/ [Accessed 15.11.2019]

[4] Kaspersky Labs. Available: https://www.antivirus.ee/ru/security-center [Accessed 15.11.2019]

[5] Zabbix Agent. Available: https://www.zabbix.com/zabbix_agent [Accessed 15.11.2019]

[6] 21st Global Information Security Survey 2018-19 “Is cybersecurity about more than protection?” Available: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-rus/$FILE/ey-global-information-security-survey-rus.pdf [Accessed 15.11.2019]

[7] ATEA Action 2019. Chester Wisniewski, Principle Research Scientist, SOPHOS. Available: https://www.atea.ee/sundmused/atea-action-2019/ [Accessed 15.11.2019]