UNIVERSITETET I AGDER

Project report in engineering and systems thinking,TFL200

Faculty of Engineering and Science, Grimstad

Title: **Data surveillance for companies**	**No of pages: 20** **Distribution: Open**
Authors: **Bendik Egenes Dyrli, Einar Larsen, Nicolai Prebensen, Ørjan Solli**	**Semester:** **Autumn 2017**
4 keywords: **Privacy, Surveillance, Security, Ethics**	

Abstract: <approximately 150 words>

Surveillance is an important factor in information security. Both to protect a company's data and it's infrastructure from attacks, as well as preventing personal information of individuals from being leaked. Data collection introduces issues regarding legislation, ethics and innovation.

This report discusses to what extent a company can legally perform data surveillance and will account for the issues related to ethics, innovation and law based on experience obtained through information security related work, as well as research performed by the group as a whole. In order to confirm the various statements regarding legislation, the group researched the Norwegian Laws to investigate the terms and conditions for data surveillance.

Result of the problem statement shows that existing security solutions have the ability to log and collect almost all network traffic originating from the company's network, but must be modified to comply with the law. The law states that a company can collect large amounts of data as long as the reason behind the data collection is for information security and that employees must be informed about the surveillance. Possible solutions that can help improve personal privacy and ethical issues regarding surveillance has also been discussed.

Phone: +47 37 23 30 00	Jon Lilletuns vei 9, 4879 Grimstad	Telefax: +47 38 14 10 01

University Of Agder

TFL 200

Data surveillance for companies

Author:
Bendik Egenes Dyrli
Einar Larsen
Nicolai Prebensen
Ørjan Solli

Supervisor: Gunvor Sofia Almlie

2017


UNIVERSITY OF AGDER

Abstract

Surveillance is an important factor in information security. Both to protect a company's data and it's infrastructure from attacks, as well as preventing personal information of individuals from being leaked. Data collection introduces issues regarding legislation, ethics and innovation.

This report discusses to what extent a company can legally perform data surveillance and will account for the issues related to ethics, innovation and law based on experience obtained through information security related work, as well as research performed by the group as a whole. In order to confirm the various statements regarding legislation, the group researched the Norwegian Laws to investigate the terms and conditions for data surveillance.

Result of the problem statement shows that existing security solutions have the ability to log and collect almost all network traffic originating from the company's network, but must be modified to comply with the law. The law states that a company can collect large amounts of data as long as the reason behind the data collection is for information security and that employees must be informed about the surveillance. Possible solutions that can help improve personal privacy and ethical issues regarding surveillance has also been discussed.

Contents

0.1 Introduction

Surveillance is an important factor in information security. Both to protect a company's data and it's infrastructure from attacks, as well as preventing personal information of individuals from being leaked to untrusted or unauthorized third-parties.

When collecting sensitive data, the privacy of individuals could get violated if the correct procedures have not been followed. This introduces multiple ethical issues related to handling the collected data in an appropriate manner.

Today everything is being digitalized, which leaves large amounts of data vulnerable to hackers if security solutions are not kept up to date and maintained. This means companies have to innovate in data protection in order to mitigate possible attacks and various threats. Data surveillance is a viable defense solution.

For a company, the ideal idea would be to surveil without restrictions. This is however not the case. Multiple laws exist due to i.e privacy of individuals, where privacy must be maintained and therefore regulated by law and company policies.

Chapter 1

Research question

Issue: To what extent can companies perform data surveillance without breaking the law? This question will be answered with regard to innovation, law, and ethics.

Companies today have a larger focus on IT-security than before, and are starting to collect data to monitor usage and traffic of employees in the company. Such data could for instance include email and Internet traffic. But to what extent can a company legally monitor employee data traffic before violating the law, and improve ethical issues?

Chapter 2

Theory and Method

2.1 Theory

System theory is a way of segregating a system into sections by limiting it to certain topics, to reduce complexity and explaining how the different topics interact with each other. This provides an overall picture of the system and at the same time, gives a detailed understanding in the complex workings of the system. [6]

The topics are technology, ethics, legislation and innovation, with main focus on the technology. As subsections, the remaining topics are connected to technology with two different types of connections; A-(subsystem) and B-(interconnections) connections.

A-connections are direct connections between technology and the subsections, while B-connections are connections between the various subsections, for instance between legislation and innovation

2.2 Method

This report is based on experience obtained through information security related work as two of the group members are working in an information security company as a part time job, as well as research performed by the group as a whole.

Our group proceeded with setting up a graphical system overview (see figure and table 4.1 in section 4.1) where the various connections between the main parts of the project were discussed and created.

To answer the thesis question, a relatively small number of sources have been used, due to the fact that multiple group members are highly experienced with information security technology. Therefore, the majority of the sources referenced are related to legislation regarding data surveillance in the Norwegian law. These sources have been analyzed and investigated to the terms and conditions for data surveillance.

Chapter 3

Results and Discussion

3.1 Graphic overview of interacting systems

In figure 4.1, the connections between the interacting systems are shown. The different connections has been specified and explained in table 4.1.

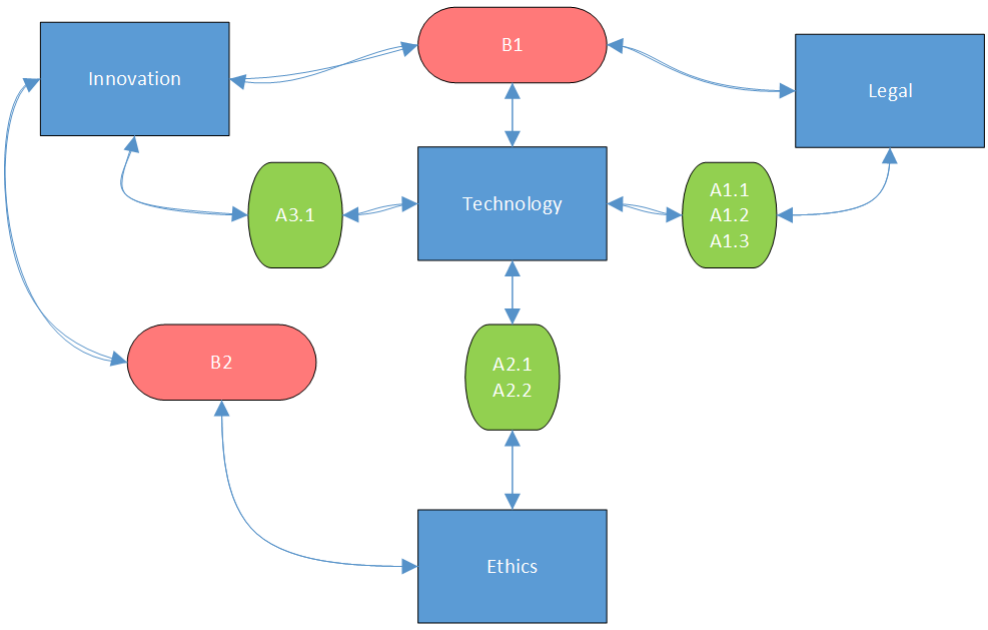

Figure 3.1: System overview showing A-connections and B-connections

Connection	Issue
A1.1	Privacy
A1.2	Corporate protection
A1.3	Storing data
A2.1	Data abuse
A2.2	Abuse of permissions
A3.1	Surveillance by AI
B1	Lawful AI utilization
B2	Privacy not violated by AI

Table 3.1: Description of connections represented graphically in figure 4.1

.

3.2 Technology

Due to large amounts of threats originating from the Internet, companies now need broader data protection to mitigate potential incoming attacks, some of which could be devastating for a company. Such threats may include major data breaches where classified customer or personal data is leaked or locked. The list below describes the most critical threats among companies

- Ransomware - Encrypts all files on a machine and holds them for ransom
- Virus/Malware/Trojan - Machine infected with malicious software
- Spearphishing - Email-spoofing attack that targets a specific organization or individual
- DDOS - Distributed Denial of Service

For a company, an employee or a user in the internal network could potentially be the weakest link, and if vulnerable, lead to total compromise of a companys infrastructure and data. The most common way that client machines get infected is by receiving emails containing malicious attachments or links to malicious web pages, or simply by being redirected towards malicious web pages when surfing the Internet. Therefore employee/client traffic needs to be collected and monitored in order to mitigate and limit potential infections and damages.

To mitigate threats from the Internet, companies need to monitor and collect log data from incoming and outgoing data traffic as well as data exchange from within the company. To prevent most critical threats described above, various security appliances may be used. These normally include intrusion detection systems (IDS), intrusion prevention systems (IPS), anti-virus/anti-malware software, airgapped networks (i.e. separate internal/corporate network) and log correlation from machine logs.

As a result, large amounts of data regarding a clients computer usage will be search-able in analytic tools in order to perform analysis of any potential security threatening events. However, there is a limit to what extent a company can monitor their employees. This will be described in the subsections below, regarding what is legal, what is ethically correct, and how data surveillance can be improved.

3.3 Legislation

Multiple entries regarding personal privacy and human rights exist in the Norwegian laws. In cases where a company or an individual wants to perform data surveillance, the collecting and storing of data must correspond with the law.

A company or organization with multiple employees must also inform and sign contracts with each employee respectively, before collecting and storing personal data. The individual has the right to get insight in what information the registrar/company has stored at any time. [1].

Companies must also stay up to date with the legislation as new privacy rules are introduces in the upcoming year 2018. *"The EU Privacy Statement will be Norwegian law in 2018. This means that new privacy rules will be introduced in Norway. The new regulations give businesses new duties. The persons who receive their personal data will be granted new rights."* [4].

Failure to comply with, or violation of the law and regulations of data surveillance will result in various penalties. The various penalties can be seen as referenced in section 48 of "Personal Data Act".

Section 48 Penalties

"Anyone who wilfully or through gross negligence
[...]
e) processes personal data contrary to sections 13, [...]
shall be liable to fines or imprisonment for a term not exceeding one year or both. In particularly aggravating circumstances, a sentence of imprisonment for a term not exceeding three years may be imposed. In deciding whether there are particularly aggravating circumstances, emphasis shall be placed, inter alia on the risk of great damage or inconvenience to the data subject, the gain sought by means of the violation, the duration and scope of the violation, manifest fault, and on whether the controller has previously been convicted of violating similar provisions. An accomplice shall be liable to similar penalties. In regulations issued pursuant to this Act, it may be prescribed that any person who wilfully or through gross negligence violates such regulations shall be liable to fines or imprisonment for a term not exceeding one year or both." [1].

3.4 Ethics

With large data sets of sensitive information comes great responsibilities. Ethics plays a large part when it comes to sensitive information, and especially how one should handle this information appropriately. In general, ethics functions as a guideline to what is right and wrong, but in some cases varies from person to person. For a company it is important to operate ethically, both to keep the trust of customers and clients, as well as the employees working for the company. This is beneficial for all parties.

In a security setting collection of data is used when investigating an incident or reviewing large data logs for security audits. This data often contains raw logs of network traffic and can potentially contain information about employees such as emails, chat logs and browser history. As this data is considered sensitive and possibly personal, the availability of this data should be limited to only authorized personnel who are ethically qualified and trustworthy for this type of access. Providing access to such large amounts of data could be a challenge, as the people authorized to view this data at any time can look into what other employees are doing online.

A major concern, which is also why not every individual is suitable for a job within computer security is the amount of data that becomes available. This data is highly valuable to some, and catastrophic consequences could occur if sensitive information end up in the wrong hands. Such cases occur especially when large amounts of money is at stake, where employees in example could sell data secretly to third-parties.

Abusing permissions for personal gain is unethical. The abuse of permissions in data surveillance context can have large impact on the employees being affected. If an individual with the right kind of permissions have access to the data of an employee and abuse it for his or hers personal gain, it could potentially destroy the victims career. For instance in a blackmail attempt for a rapid corporate advancement where negative personal information about the victim is disclosed/leaked.

3.5 Innovation

As of today, the majority of the security appliances are used to detect and log possible threats, analysing data flowing through the network and storing it in a searchable management system. Such systems can, upon successful detection of a threat, also perform actions based on pre-configured settings in order to mitigate/block assumed malicious traffic, but on the other hand requires constant tuning and maintenance to perform optimally and ensure that only legitimate traffic is allowed. This is done by human interaction, which also is needed to perform a proper analysis of data traffic.

One example of such a system is "Security Information and Event Management" (SIEM). SIEM is a system which rely on large amount of logs across a company's data environment to aggregate data from multiple log sources such as Intrusion Detections Systems (IDS) / Intrusion Prevention Systems (IPS), employee computers, servers etc.. Having these logs aggregated using the SIEM system provides the ability to correlate potential malicious events across devices/log sources in the network and generate alerts. [2]

A future innovation to the security industry, which already is being worked on is the use of artificial intelligence (AI). The usage of artificial intelligence to perform monitoring and analysis will require less human interaction with collected data, which also results in less human mistakes and misinterpretation when handling collected data.

Artificial intelligence is not a new concept, but in recent times there has been a larger focus on developing new solutions using artificial intelligence. Some projects and solutions already exist claiming that their appliances are utilizing artificial intelligence and machine learning to prevent Cyber attacks. [3]

Chapter 4

Connections

4.1 A - Connections

A1.1 Privacy

When it comes to personal privacy, there is a limit to what kind of information that legally can be logged. This is regulated by the local law for privacy, and must be complied by any party that wants to perform data surveillance according to Personal Data Act §8.

Any party can store or view personal information about a consenting person according to Personal Data Act §9. In Norway, anyone can manage sensitive personal information if the person in question has allowed it according to section 9.

Section 8 Conditions for the processing of personal data

"Personal data (cf. section 2, no. 1) may only be processed if the data subject has consented thereto, or there is statutory authority for such processing, or the processing is necessary in order
a) to fulfil a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into such a contract,
b) to enable the controller to fulfil a legal obligation,
c) to protect the vital interests of the data subject,
d) to perform a task in the public interest, [...]" [1].

Section 9 Processing of sensitive personal data

"Sensitive personal data (cf. section 2, no.8) may only be processed if the processing satisfies one of the conditions set out in section 8 and
a) the data subject consents to the processing,
b) there is statutory authority for such processing, [...]" [1].

A1.2 Corporate protection

Individuals can be surveilled without knowledge of exactly what data is being collected. This occurs in cases where informing the individual of the surveillance potentially can be damaging, and the party performing the surveillance will in such cases be protected by §23.

Section 23 Exceptions to the right to information

"The right to access pursuant to sections 18 and 22 and the obligation to provide information pursuant to sections 19, 20 and 21 do not encompass data
a) which, if known, might endanger national security, national defence or the relationship to foreign powers or international organizations,
b) regarding which secrecy is required in the interests of the prevention, investigation, exposure and prosecution of criminal acts,
c) which it must be regarded as inadvisable for the data subject to gain knowledge of, out of consideration for the health of the person concerned or for the relationship to persons close to the person concerned,
d) to which a statutory obligation of professional secrecy applies,
e) which are solely to be found in texts drawn up for internal preparatory purposes and which have not been disclosed to other persons,
f) regarding which it will be contrary to obvious and fundamental private or public interests to provide information, including the interests of the data subject himself.
Data pursuant to the first paragraph, litra c, may nonetheless on request be made known to a representative of the data subject when there are no special reasons for not doing so. Any person who refuses to provide access to data pursuant to the first paragraph must give the reason for this in writing with a precise reference to the provision governing exceptions. The King may prescribe regulations regarding other exceptions from the right of access and the obligation to provide information and regarding conditions for the use of right of access" [1].

A1.3 Storing data

The company shall not store personal data longer than necessary to carry out the purpose of the data collection. However the company can store personal data for historical, statistical or scientific purposes. In this case the company must honor this

by securing any personal data the company possesses and if keeping the data stored for longer periods of time ensure that the subject is not identifiable.

Section 28 Prohibition against storing unnecessary personal data

"The controller shall not store personal data longer than is necessary to carry out the purpose of the processing. If the personal data shall not thereafter be stored in pursuance of the Archives Act or other legislation, they shall be erased. The controller may, notwithstanding the first paragraph, store personal data for historical, statistical or scientific purposes, if the public interest in the data being stored clearly exceeds the disadvantages this may entail for the person concerned. In this case, the controller shall ensure that the data are not stored in ways which make it possible to identify the data subject longer than necessary.

The data subject may demand that data which are strongly disadvantageous to him or her shall be blocked or erased if this

a) is not contrary to another statute, and

b) is justifiable on the basis of an overall assessment of, inter alia the needs of other persons for documentation, the interests of the data subject, cultural historical interests and the resources required to carry out the demand.

After the Director General of the National Archives of Norway has been consulted, the Data Inspectorate may decide that the right to erase data pursuant to the third paragraph shall take precedence over the provisions of sections 9 and 18 of the Archives Act of 4 December 1992 No. 126. If the document which contained the erased data gives a clearly misleading picture after the erasure, the entire document shall be erased." [1].

The way a company stores personal data about their emploees must be carefully planned and reported to a third-party

Section 13 Data security

"The controller and the processor shall by means of planned, systematic measures ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data. To achieve satisfactory data security, the controller and processor shall document the data system and the security measures. Such documentation shall be accessible to the employees of the controller and of the processor. The documentation shall also be accessible to the Data Inspectorate and the Privacy Appeals Board. Any controller who allows other persons to have access to personal data, e.g. a processor or other persons performing tasks in connection with the data system, shall ensure that the said persons fulfil the requirements set out in the first and second paragraphs." [1].

A2.1 Data abuse

An example of data abuse is sale of bulk email addresses to affiliate companies wanting to sell their products. This is not directly a security issue for the owner of the email address, but it is a possible violation of the company's ethical policy and could lead to malicious content or unwanted advertisement being sent to these addresses. This particular example happened in 2004 when a employee of America Online (AOL) one of the worlds largest Internet service provider (ISP), stole 92 million e-mail addresses of AOL customers and selling them to spammers. [5]

A2.2 Abuse of Permissions

Often, a more ethical approach to securing data would be to have an external source monitor the data, to respect all aspects of ethical rights. This prevents colleagues within the company from having their personal data exposed to fellow co-workers, and limits potential ethical violations, and limit the amount of co-workers having access to this type of data. That is not to say the company should not have any security department at all, but instead have a local IT group that will receive incidents from an external security company that only includes the viable data needed in order to handle the security threat for a given client. This approach can for instance work as an ethics filter.

A3.1 Surveillance by artificial intelligence

A possible innovative solution is the use of artificial intelligence to perform surveillance. An AI can be trained to perform tasks better than a human, and can function efficiently 24 hours per day, delivering a more accurate analysis.

4.2 B - Connections

B1 Lawful AI utilization

One of the benefits of using artificial intelligence to perform surveillance is that personal privacy will not be violated to the same extent as if a person was performing the analysis.

However, the law remains with the same procedure required before starting monitoring and log collection of individuals/employees data traffic.

B2 Privacy not violated by AI As artificial intelligence becomes better at tasks that previously only were done by humans, the need for human interaction therefore naturally decrease. In cases where a human would need to sign documents and agreements regarding confidentiality, a solution using artificial intelligence could be programmed and taught to keep the data secure, as well as being free from humans potentially abusing sensitive collected data.

Chapter 5

Conclusion

As a conclusion to the project, the existing security solutions have the ability to log and collect almost all network traffic originating from devices connected to a company's network. Therefore these technologies must be modified or configured to obey the law in relation to privacy rules for a company to perform this type of data collection.

The law states that a company can collect large amounts of data as long as the reason behind the data collection is for information security, for example protecting the company itself as well as employees against threats and data leakages originating from the usage of data networks eg. Internet.

The law also states that the employee must be informed about the surveillance, and has signed a contract stating that he or she has been informed and is aware of active company policies. The company also has to comply with the legislation of privacy rules when collecting and handling "private" and sensitive employee data.

It is also important to note that there is a rapid development of technology, therefore the law should be updated accordingly to the relevant technology and. Companies must also follow the last revision of the law accordingly and maintain their policies.

Handling this type of data does not come without ethical concerns and must be reviewed for handling the data with care and ethical ground lines in conjunction with legislation. The use of Artificial Intelligence could also be a positive factor regarding solving or improving ethical issues. It is in companies best interest to operate ethically to keep an image of trustworthiness for its employees and customers and other collaborators.

Bibliography

[1] Personal Data Act [Online]
http://app.uio.no/ub/ujur/oversatte-lover/data/lov-20000414-031-eng.pdf
[Accessed:12.Feburary 2017]

[2] Securosis - Blog [Online]
http://securosis.com/blog/understanding-and-selecting-siem-lm-use-cases-part-1
[Accessed:23.March 2017]

[3] Cylance — Advanced Threat Prevention Built on Artificial Intelligence [Online]
https://www.cylance.com/en_us/home.html
[Accessed:23.March 2017]

[4] Consequence of new law [Online]
https://www.datatilsynet.no/Regelverk/EUs-personvernforordning/hva-betyr/
[Accessed:26.March 2017]

[5] AOL employee sold email addresses to Spammer [Online]
http://www.information-age.com/aol-employee-sold-email-addresses-to-spammer-292581/
[Accessed:26.March 2017]

[6] Nilsen, T. V. "Forelesning i systemtenkning" Lecture. UiA, Grimstad