FEASIBILITY STUDY:
THE CHANGING WORLD NEEDS NEW AGILE METHODS TO IMPROVE CYBERSECURITY - COMPANIES CYBERSECURITY CAN BE EASILY IMPROVED!

Contents

1 Foreword and presentation of key findings

The words "cybersecurity" and "easy" are rarely found in the same sentence. This is one of the key issues that the feasibility study nicknamed TONTTU by the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency Traficom aimed to change. The ease of doing things is at centre stage when the aim is to improve the overall security of society on a larger scale.

The overwhelming majority of Finnish companies are small or medium-sized. Hundreds or even thousands of them participate in implementing the critical functions of our society. The security solutions aimed at large companies rarely work for smaller companies that do not have special expertise or separate resources for cybersecurity. On the other hand, the schedules of the information security personnel of large companies are full of ongoing projects, which affects the availability of the existing resources.

Regardless of the size of the company, it is likely that the resources are low. People are interested in easy ways to develop cybersecurity. Do such ways exist? This is what the TONTTU project studied together with 11 organisations critical to emergency supply – and the results did not disappoint.

The project showed that the cybersecurity of society's critical services can be improved with methods that are easy to implement. The organisations themselves felt that the pilot brought them direct and immediate benefits.

The findings of the feasibility study included the following:

- Leaks in isolated information networks were found in nine organisations.
- Potential vulnerabilities were found in seven organisations' own or their suppliers' services.
- In two cases, suspicions of exploitation were also related to the vulnerabilities, one of which was confirmed for the working group. The suspected data breaches were not related to the operative networks.
- Data leaks in internet services becoming more common also affected the participants of the project.
- Seven organisations identified victims of data leaks among their personnel. Some of the participants had already identified the victims of a data leak earlier and started to train their personnel regularly to protect themselves and their working environment from the harmful effects of the leaks.

The participants of the project identified their assets to be protected automatically, received data on the information security of the assets automatically and tested how the isolation of networks functioned. In light of the project's findings, it is encouraging that all respondents are thinking about using similar capabilities in the future. A good thing was that three participants implemented the measures mentioned above immediately.

As a part of the project's findings, it came up that organisations should increase their visibility towards services provided by third parties so that they could demand that suppliers take action to improve security. Concrete observations improve the ability of organisations to assess the suppliers' level of cybersecurity, while the suppliers can gain a competitive advantage by acting in a way that ensures cybersecurity.

The vulnerabilities detected by the project helped the participants understand their suppliers' ability to react with regard to cybersecurity. Concrete requests for clarification related to leaks and vulnerabilities separated suppliers and service providers with a rapid response from those who were not able to react to the issues discovered quickly enough. Competent suppliers and service providers reacted quickly. The responses were clear and logical. As for the suppliers that performed poorly, they acted slowly, gave unclear responses if they responded at all, or attempted to downplay the problems.

Affecting the supply chain's ability to react to cybersecurity issues may have multiplier effects, because one supplier may serve several organisations critical to emergency supply. When the suppliers improve their own operations, it benefits customers critical to emergency supply. Organisations critical to emergency supply play an essential role here. The companies themselves or external parties should be able to make observations related to cybersecurity. This is the only way they can assess their suppliers' ability to react to cybersecurity issues and exchange experiences with other operators critical to emergency supply in society. An open comparison gives a competitive advantage to operators who ensure their cybersecurity.

The situation picture of the National Cyber Security Centre Finland (NCSC-FI) is assembled from several pieces. With the TONTTU project, the NCSC-FI can improve its own situation picture in cooperation with companies. The companies are happy to participate in the cooperation, as long as it does not burden them/their personnel too much. Automation and tools that are easy to use play a key role in building a situation picture of this type.

In addition to the situation picture, the results show that lasting benefits can be gained by taking care of basic cybersecurity issues. The organisations critical to emergency supply that participated in the TONTTU project considered it important and hoped that similar work would also be done in the future.

When asked to evaluate the importance of the NCSC-FI organising similar pilots in the future on a scale from 1 to 5, every participant gave the full five points.

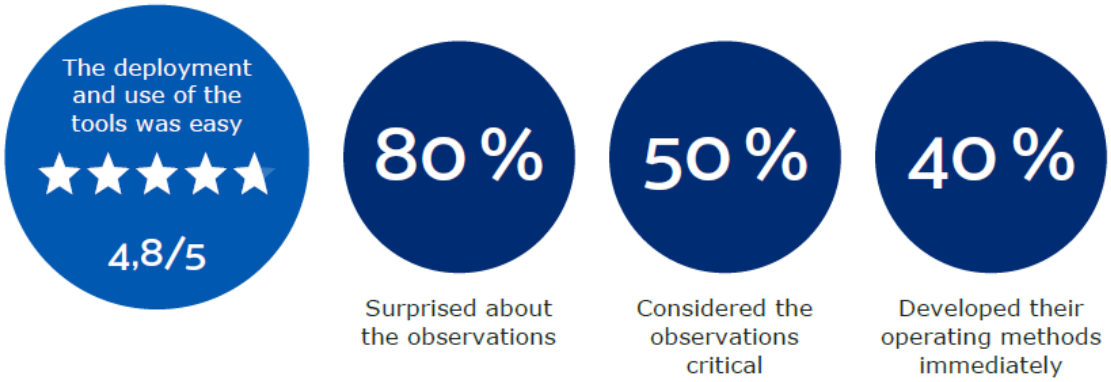


Image: The participants valued the ease of use of the tools and the usefulness of the observations.

2 Previous lessons learned included in the new study

Lessons learned from HAVARO and the Autoreporter service

The fully automated Autoreporter service of the NCSC-FI and the related cooperation with telecommunications operators have kept the Finnish networks clean for more than 15 years. The Autoreporter automatically sends information to network administrators on phenomena endangering information security that have been detected in their networks. The purpose of the service is to provide the administrators with information that they can use to address information security incidents that endanger data processing in general. Autoreporter has taught how simple things can have a great impact when they are implemented on a large scale. Every year, Finnish networks are among the cleanest in the world.

HAVARO is a national monitoring and early warning system for severe information security violations; it has protected Finnish organisations critical to emergency supply already since 2011. HAVARO is a service offered by the NCSC-FI especially to the vital organisation for the security of supply and the central government, in which an organisation's network traffic is monitored to find traffic that has been identified as harmful or abnormal based on identifiers of information security threats obtained from different sources.

HAVARO has innovated a model in which the benefits of cooperation for both authorities and organisations are considered even more carefully than before. Once the first participants told other organisations critical to emergency supply about HAVARO's concrete benefits, HAVARO started to grow rapidly. The growth improved both the situation picture of the NCSC-FI as well as the usefulness of HAVARO, as the observations from one organisation helped the other companies protect themselves even better.

The world keeps changing and innovations have a use-by date

The aim in the planning of the TONTTU project was to take advantage of the great lessons learned from Autoreporter and HAVARO. At the same time, development needs were discovered, and their improvement started in the TONTTU project. The Autoreporter and HAVARO services are based on the assumption that the assetss to be protected are located in Finland. This assumption is no longer entirely true. The change in technologies also brings along a changing operating environment, which presents new requirements on the monitoring of the operating environment and the tools available there.

The trends related to cloud services are already visible in the most advanced organisations related to critical infrastructure. IT is moving rapidly into the cloud. The first signs of operative functions being implemented with cloud services are already in use. In connection with the TONTTU project, ways to renew operations and meet new challenges were tested.

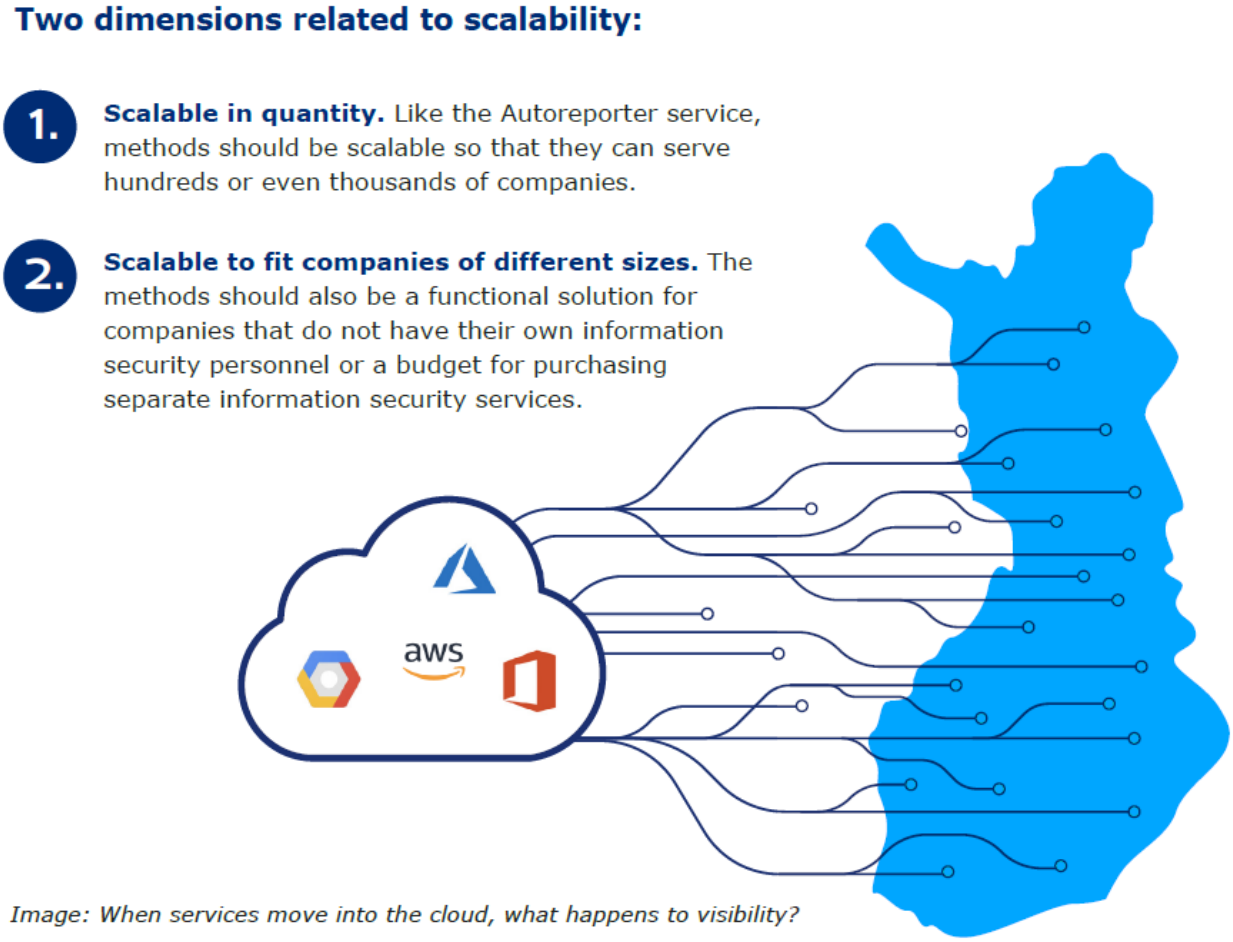


Image: When services move into the cloud, what happens to visibility?

Effectiveness requires scalability, and scalability requires almost complete automation

New methods, lighter than previous ones, were tested during the TONTTU Project; they simultaneously improved the safety of the organisations critical to emergency supply and expanded the situation picture of the NCSC-FI to cover the organisation's assets to be protected. The methods were scaled to fit both the number of participants and the size of the participant organisations.

The previous observations and lessons learned described above created a framework for the TONTTU project, which gave rise to five statements that should be realised in the project. They could also be applied to similar projects in the future:

1. **It must be easy for the organisation to decide to participate**. Making an agreement between the parties must be simple: if agreements are needed, they must be brief and clear.

   In this study, the parties were the National Cyber Security Centre Finland of the Finnish Transport and Communications Agency Traficom as well as

the organisation critical to emergency supply. The project reinforced the assumption that trialling the cooperation must not require the participant to go through a laborious procurement process, either.

2. **The participants' time is valuable.** The project must not take up a significant amount of the participants' time. Few meetings, tools that are easy to deploy and operate constantly in the background instead of requiring constant management.

3. **Cooperation must be based on automation**. Manual exchange of information works in exceptional situations, but continuous cooperation requires automated exchange of information.

4. **The foundation of information security is built on the basics.** The project supports taking care of the basics. Many are looking for solutions to the most current problems. By taking care of the basics of information security, the company can also prepare comprehensively for future threats.

5. **People's time should be spent on thinking about repairs and solutions.** The project focuses on clear observations. The scalability goals of the project cannot be met cost-effectively, if the observations themselves require analysis or interpretation by a human being.

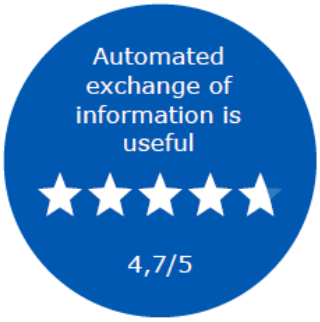
3 Light methods for improving information security

Identifying assets to be protected and sharing necessary information

"We need to inventory the services that are visible to the public network more carefully."

The systems, the services used by personnel, subcontracting chains and the related responsibilities have become so complex that identifying the assets to be protected in a network is difficult. The assets that need to be identified vary from user information vulnerable to data leaks to technical cloud service resources.

In the project, organisations critical to emergency supply identified their assets to be protected and shared information about the critical resources of their cloud services to help the NCSC-FI to focus the national work on information security on the protection of these assets. When the NCSC-FI knows automatically and in real time where society's services critical to emergency supply are specifically located, it can transmit the information security community's warnings related to the assets directly and automatically to the owners of the assets.



"The exchange of information has to be automated, otherwise it just won't work"

In the study, methods developed by technology providers Badrap Oy and SensorFu Oy were combined with the services of the NCSC-FI. Badrap.io service made it possible for the producers and transmitters of information security data to reach companies with focused information security data. The service itself helps companies to correct the problems identified. For example, when one of the companies' users has become exposed to a user data leak, the immediate and focused training and instructions offered by the service may prevent negative consequences of the leak. In practice, the service links companies and information security content producers together while also ensuring that there is a script ready for typical repairs. The companies use the service to protect both their personnel as well as their cloud services.

The SensorFu Beacon product offers an ability to monitor the functioning of network isolation continuously. Network isolation is one of the most important information security controls in high security information networks. The Beacon automates the isolation testing that is normally carried out manually and generates alerts on the leaks detected. The alerts make it possible for the network owner to react quickly. Network leaks may occur by accident, such as in connection with changes of configuration, due to human error, or caused by hostile parties.

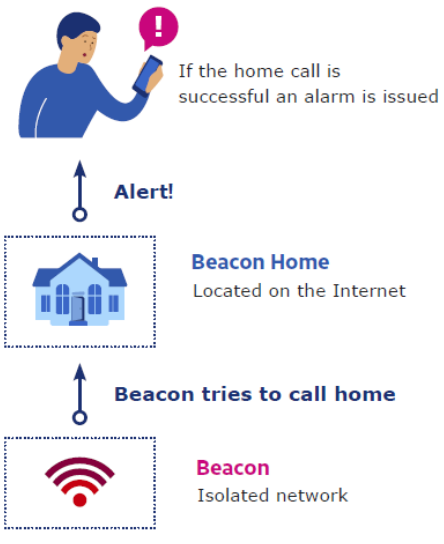


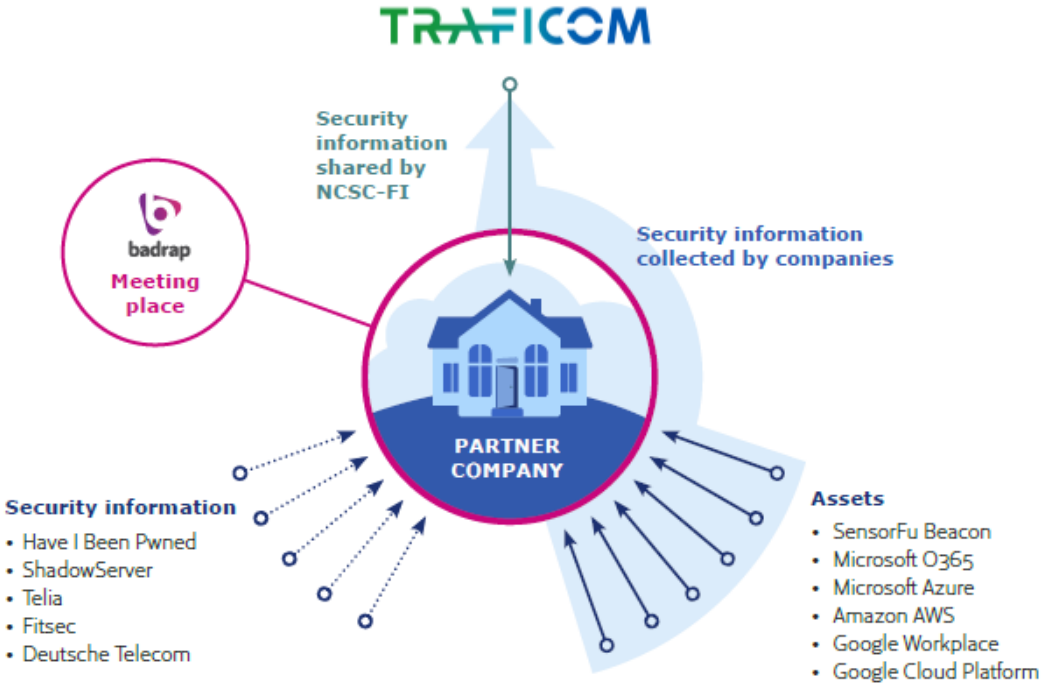
Image: SensorFu Beacons test isolated networks and generate alerts about leaks.

The continuous identification of office networks was implemented by placing SensorFu´s Beacon software intended for testing isolated networks exceptionally into an open office network. The source addresses of Beacon's handshakes were marked automatically as assets to be protected. The participants shared the information automatically with the NCSC-FI in the Badrap.io service with the Traficom application.

In the project,the Badrap.io online service acted as an application platform and meeting place, where the Beacon application adapted for use in mapping by SensorFu and the monitoring of assets in popular cloud platforms (Microsoft, Google, Amazon) generated real-time asset information for the

company. This also allowed companies to share the asset information voluntarily with the NCSC-FI by using the service's Traficom application.

Producers of information security data, such as the NCSC-FI and SensorFu that participated in the project, can publish integration applications in the Badrap.io service that organisations can use to improve their security. Among other things, the participants appreciated the ease of use of the service and the automated information sharing.



The Badrap.io online service acted as a meeting place, where companies identified their assets and shared information voluntarily with the NCSC-FI.

Know what you are protecting

It is important to know your own operating environment so that you can avoid factors that threaten it or prepare for them. The participants estimated that identifying the assets had a significant effect on the organisation's security. On a scale from 1 to 5, where 5 was "completely agree", the average estimated impact on IT networks was 4.3, while the same value for operative networks was 4.6. Based on the responses, the respondents either completely or somewhat agreed that identifying the assets to be protected affects the safety of the organisation significantly. The small difference in emphasis may be explained by the fact that several of the participants had recently identified the visibility of OT networks as a development target in the year in question.

Improved visibility offers surprising benefits

"You helped us trace a pretty tricky network malfunction."

The visibility for its own assets improves the organisation's ability to handle unexpected incidents. For example, an organisation that participated in the project was able to track down the root cause of network problems that had lasted for two weeks thanks to the additional visibility offered by the project. An office network IP address in the list of assets by the Badrap.io service had changed exactly at the same time as when the network problems began. The change in IP address in turn prevented access to certain external services that required a specific IP address as the source of data traffic.

Testing the isolation of specially protected networks

Network isolation is one of the cornerstones of information security. A typical data breach is not particularly targeted; instead, it is rather opportunistic, and criminals are interested in easy marks. By isolating networks, it is possible to ensure that the business critical systems have been protected in their separate network segments. If a criminal can access the organisation's network, the whole operation is not endangered, only a section of it. The project offered its participants a chance to test the durability of their isolations.

During the pilot, SensorFu Beacons were delivered to the critical networks of 11 organisations. Networks included operation critical ICS/OT -environments, which means that they should be completely isolated from the internet. These critical networks include SCADA, ADMS and HVAC systems, among other things. The Beacon was deployed in four networks per customer on average.

"There were long discussions on how to fix this based on the observations."

4 Successful cooperation with the participants

Ten companies reached production in three months

"The deployment was easy."

There can be many twists and turns involved in starting out, making decisions and agreements, deployment and operation that may not have been taken into account in the plans. Scalability involves much more than just technology. The project's first aim was to find 10 interested companies and bring the capabilities to production in three months so that the initial results of the project would be available during the sixth month.

The NCSC-FI informed its stakeholders about the project via e-mail. In addition, the working group identified target organisations that were of direct interest to the project. The aim was to find both large and as small as possible participants for the project.

Based on the contacts and its own identifications, the working group listed 25 organisations whose interest in participating was investigated more closely. Two of these companies were not reached in time, two were willing to participate later, and the matter was discussed with ten companies without receiving confirmation for the participation before the places were filled. The remaining 11 were included in the project.

The size of ten of the companies has been illustrated in the image below. Of the eleven companies that participated, ten responded to the survey concerning things such as the size of the organisation.

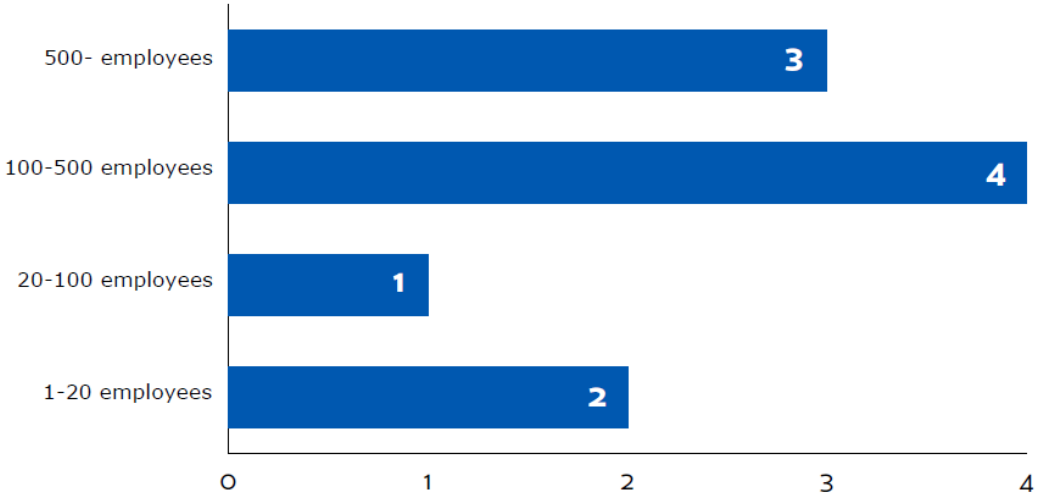


Image: Size of the organisations that participated in the project.

Observations right from the start

The first observations on network isolation tests were made almost immediately after the Beacon software for testing isolation was deployed in production. In the end, leaks were found in nine of the eleven companies.

"I'm sure that we couldn't have made these observations ourselves, they only became possible with the project's methods."

People are still at the core of security. Because most network attacks are focused on the users, the employees play two roles: not only are they assets to be protected, they are also operators that protect the company. Victims of data leaks also have a heightened risk of becoming targeted by scams. The reuse of passwords has led to leaked passwords being used in attacks. As for the misuse of other leaked personal information, it increases the credibility of attacks on employees.

"There may always be vulnerabilities that your own or your partner's abilities can't detect. Knowledge and attitude did change due to the project."

As the visibility to the organisations' assets to be protected improved, the working group conducted light basic checks on the IT systems.

- In seven cases, suspected vulnerabilities were found in the organisation's own or the suppliers' services that the participants investigated with their suppliers.
- In two organisations, a subdomain takeover vulnerability was discovered; such a vulnerability makes it possible to use the company's name in scams targeting the company or external parties.

Two of the observations presented above also led to suspicions of data breaches, one of which was confirmed during the project. The data breaches were not related to operative networks. Data leaks in different internet services becoming more common also affected the participants of the project.

Seven organisations identified victims of data leaks among their personnel. Some of the participants had already identified the victims of a data leak earlier and started to train their personnel regularly to protect themselves and their working environment from the consequences of the leaks.

It is noteworthy that during the project no security incidents at all were observed in the companies whose operating methods included checking the services regularly with regard to name service records and firewall rules. This shows, therefore, that the basic grassroots work is very important and rewarding in the form of an improved level of security.

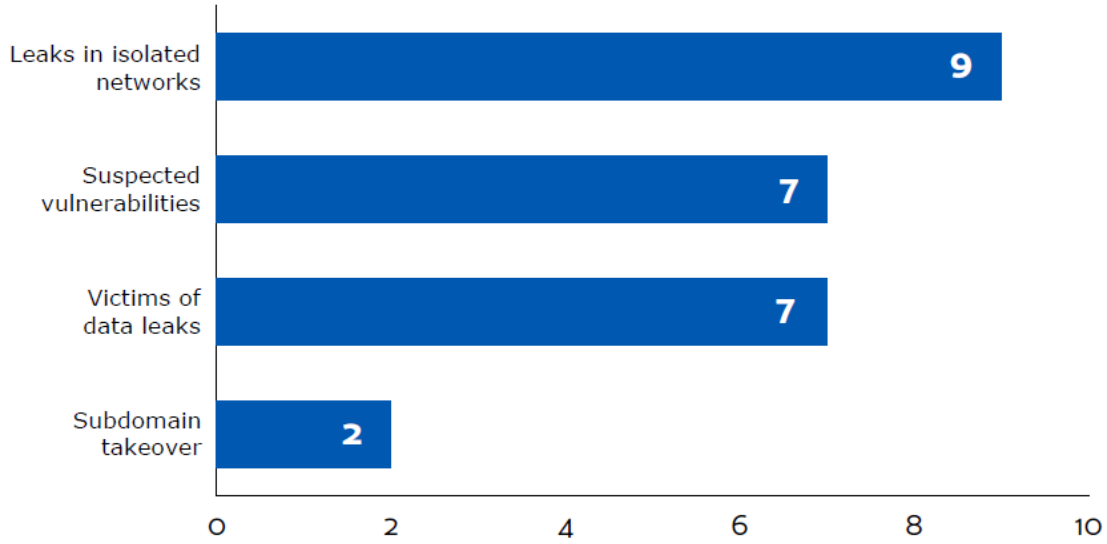


Image: Different types of security incidents detected in the organisations

5 Results and conclusions

The project proved the following:

- The cybersecurity of services critical to society can be improved with scalable methods that can be deployed lightly. The companies thought that the pilot methods gave them immediate benefits.
- The National Cyber Security Centre Finland can improve its own situation picture in cooperation with the companies. The companies are happy to participate in the cooperation, as long as it does not burden them too much. Automation and easy-to-use tools play a key role.
- The results also show that sustainable benefits can be gained by taking care of the basics of cybersecurity.
- Companies should also invest in monitoring the functionality of production networks' important information security controls, such as network isolation. The need is illustrated by the finding made in the project, in which 81% of the participant organisations' networks that were intended to be isolated leaked in unexpected ways.
- Companies should improve visibility towards the vulnerabilities of services provided by their partners. Almost all of the vulnerabilities visible to the outside were related to services provided by suppliers that are not monitored actively.
- Companies should train their personnel to prepare for data leaks and the potential attacks and scams that result from them. If a company

has to prioritise its training, the measures should be targeted first at key persons and the victims of data leaks.

All participants are considering taking advantage of similar capabilities in the future. Three organisations took action immediately, obtaining similar capabilities.