CERT·IS

ANNUAL OVERVIEW 2021

CERT-IS is a department within Electronic Communications Office of Iceland.
Matters related to cybersecurity are the remit of Ministry of Higher Education, Science and Innovation (HVIN)

CERT·IS

ANNUAL OVERVIEW 2021

TABLE OF CONTENTS

Address by Director of CERT-IS

September 1 of 2020, the Act implementing the NIS Directive came into force in Iceland, more commonly known as the NIS Act. At this turning point, the role and structure of CERT-IS cybersecurity team was significantly strengthened, and it has grown in step with increased emphases and responsibility.

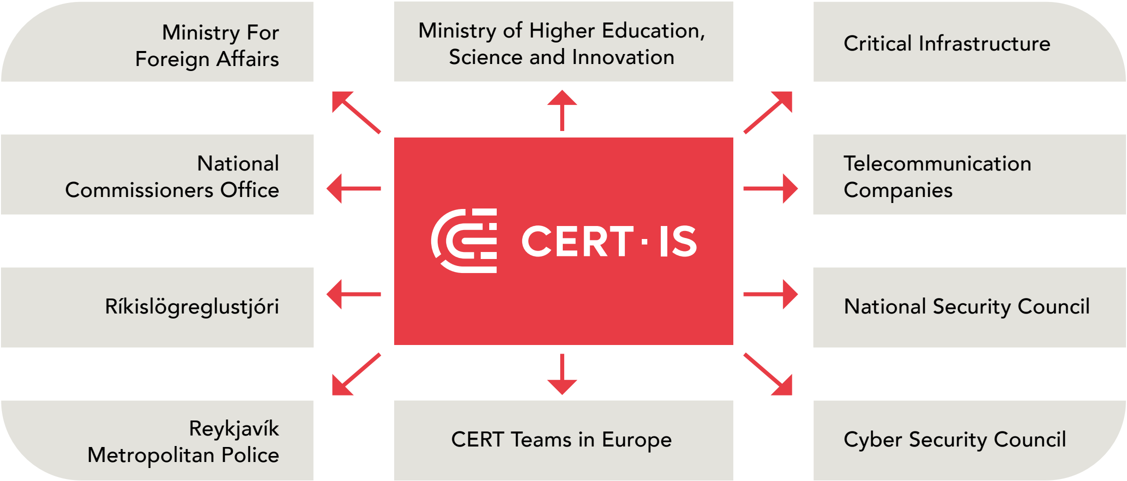
In the light of the fact that the NIS Act was implemented at a late stage in this country, one could argue that Icelanders have lagged behind other countries when it comes to developing official measures to respond to cybersecurity events. In the assessment of the International Telecommunication Union (ITU), Icelanders are leaders among nations in use of network and information technology, while cybersecurity issues need improvement. This position could be a threat to public and national security, and thus every reason to react and support without delay, the full development of measures that the NIS Act allows for.

In the new government charter, one of the major challenges is to embark on digital transformation which among other things will entail a focused effort on enhancing network and telecommunication security. In the opinion of CERT-IS, cybersecurity is the fundamental prerequisite for digital transformation. The cybersecurity team has a well defined coordination role for disseminating information and for advice on handling of events in critical infrastructure. It also maintains appropriate awareness of cybersecurity issues at a national level and disseminates this within the Icelandic cyber jurisdiction and to cybersecurity teams abroad.

To support powerful event response, CERT-IS has recently been providing sector-specific groups with necessary service. Sector specific groups have been activated for financial infrastructure, electronic communications infrastructure and energy infrastructure. Activating sector-specific groups enables the parties responsible for critical infrastructure to be more united in their cyber defences through increased cooperation.

A very significant increase in all kinds of cyber attacks can be observed, which echoes developments in our neighbouring countries. Increasing attacks can among other things be attributed to the fact that the technical threshold that must be crossed before implementing various types of attacks has lowered and it is becoming continuously less expensive to purchase access to systems to deliver such attacks. Whereas previously one needed substantial knowledge of network and computer systems and direct access to equipment to perform the attacks, it is now possible to use legal and illegal cloud computing and purchase specialised knowledge and services from criminal groups.

Responsible parties and operators of critical infrastructure are aware of this development and one can discern increased momentum in the discussion on cybersecurity and on enhancing general cybersecurity awareness. It is gratifying to observe increased willingness to openly discuss the nature and consequences of attacks. It is in everyone’s interests to share knowledge of events.


Ministry For Foreign Affairs
Ministry of Higher Education, Science and Innovation
Critical Infrastructure
National Commissioners Office
CERT·IS
Telecommunication Companies
Ríkislögreglustjóri
National Security Council
Reykjavík Metropolitan Police
CERT Teams in Europe
Cyber Security Council

To fulfil the CERT-IS role or maintaining awareness of the issues in Iceland, CERT-IS intends to emphasise the preparation of detailed information from indications received by the team, to be presented to the public and to sector-specific groups through e.g. reports like this. Emphasis will be placed on strengthening co-operation with foreign cybersecurity teams, which is important in the light of the fact that attacks in a digital world do not usually respect traditional borders. It is important that Iceland can make its contribution in international cooperation.

Last year was eventful for CERT-IS. The team has more than doubled with its increased responsibility and newly defined roles. But more has to be done. Development of the cybersecurity team CERT-IS is expected to take at least 3 years, given that lack of resources does not cause delay. Development of the cybersecurity team is a complex process which among other things, requires implementation and development of a regulatory framework; appointment and training of staff; acquiring accredited and secure working facilities; elaborating work processes and rules of procedure; introducing defined service procedures and service levels 24/7 and all year round; acquiring necessary systems and hardware; initiating and developing international contacts and developing sector-specific groups at a national level for all groups of critical infrastructure.

It is extremely important that government solidly support the development of the cybersecurity team such that Iceland succeeds in matching our neighbouring nations as soon as possible in this critical field, in such a manner that the relevant government objectives are achieved.

Respectfully.
Guðmundur Arnar Sigmundsson
Director if CERT-IS

Year 2021 in numbers

12 incidents

Information security

Access to information by illegal methods, data loss and data leaks.

446 incidents

Fraud

A system and service can be made unavailable by external action, e.g. DDoS attacks when the service of computer systems is deliberately impaired by causing overloading.

23 incidents

Vulnerabilities

Vulnerabilities that can be used to break into, or have an impact on computer systems belonging to other parties.

16 incidents

Malicious code

Computer viruses or other code used to spoil or take over control of computer systems.

6 incidents

Information gathering

Unauthorised gathering of information on vulnerability and network traffic.

22 incidents

Availability

A system and service can be made unavailable by external action, e.g. DDoS attacks when the service of computer systems is deliberately impaired by causing overloading.

6 incidents

Abusive content

Bullying, harassment and stalking. Child abuse content and the glorification of violence also belong to this category.

16 incidents

Intrusion

Intrusion into a computer system, whether that of home users, companies or operators.

10 incidents

Intrusion attempt

Attempts to take over a victim's computer system that were not successful.

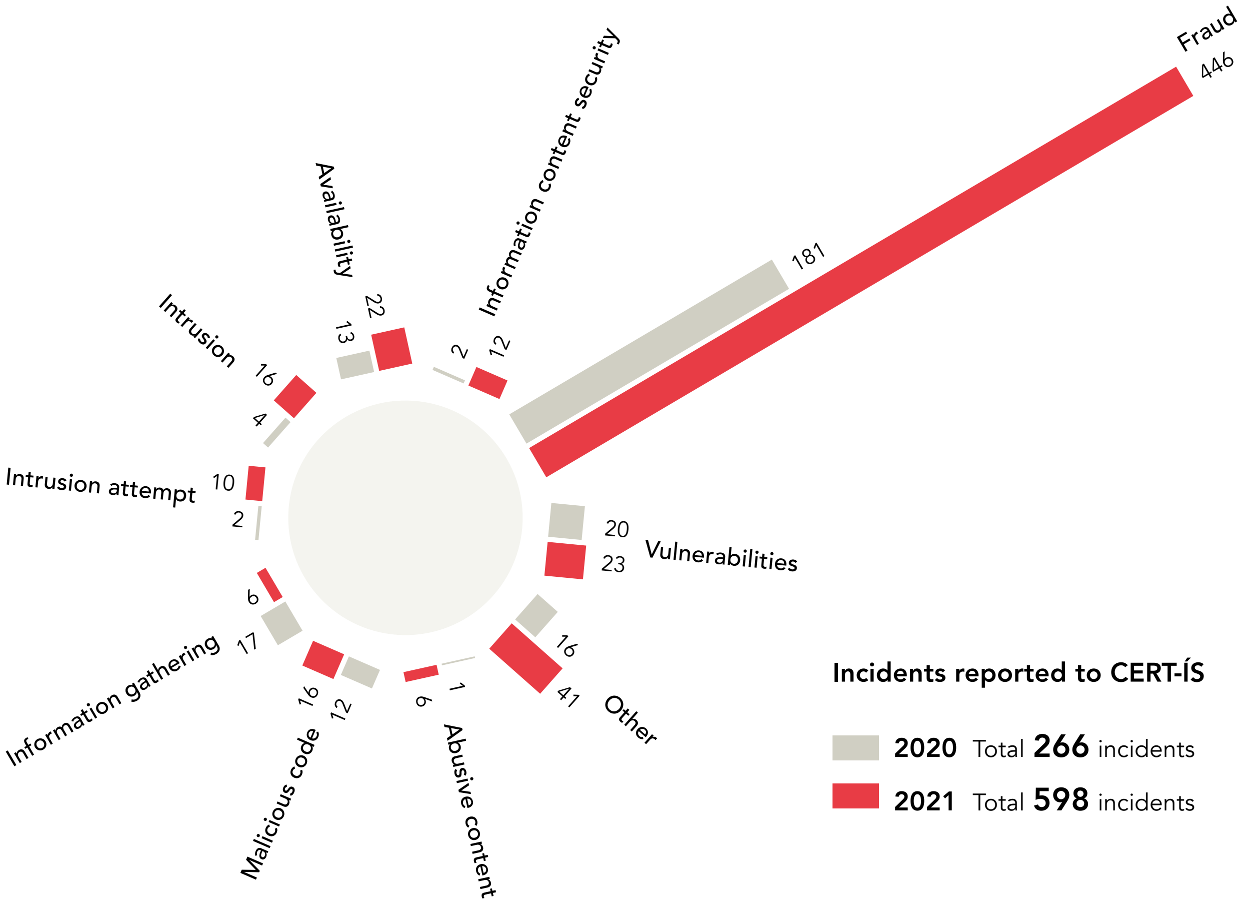
41 incidents

Other

Events which cannot be allocated to the above categories.

Total: 598 incidents

Statistics give us good indications of current developments in cyber attacks in Iceland. It is appropriate to note that these are only reported events, and that they could be more than indicated here. It is important that all events are notified to CERT-IS.



There are no official statistics on the number of computers in use in Iceland. It is however certain that most jobs today depend on a safe computer system and access to the Internet. Almost all business is transacted through computer systems; access and key systems are based on computers; the media depend on computer systems to be able to disseminate news and control of traffic at sea and in the air depends on information technology in one way or another.

In the year 2021, 598 notifications of events were registered by CERT-IS. This is more than double the number of attacks in 2020. It is likely that this huge increase in notifications can be attributed to two factors, on the one hand, the general increase in events related to cybersecurity worldwide, and on the other hand, that there is greater willingness among companies and institutions to notify events that take place in their systems.

It is striking that the greatest increase in notifications is in the fraud category. This includes, for example phishing where attempts are made to collect sensitive information by pretending to be someone else, through for example email, or with a duplicate of a well-known web page. One reason for this substantial increase is proxy services in the domain registration operated in Iceland that not only hide personal information of ordinary people but also of those who conduct dubious business. Events related to proxy services established in Iceland are received by CERT-IS, even where there is no hosting or other known connection with the country. CERT-IS does not have legal remedies to respond to such notifications.

Privacy and proxy service can be used to hide personal information that is required when registering a domain. Contact information of the proxy service is entered instead of information of the party registering the domain. There are no rules or legal requirements about such operations in Iceland, which means it can prove difficult to send messages to the parties that are in reality behind the domain.

According to the law, critical infrastructure and operators of essential service are obliged to notify events to CERT-IS. In addition to this, CERT-IS encourages other institutions and companies to notify events related to cybersecurity in order that they can maintain as accurate a picture as possible of the status of cybersecurity in Iceland and any given time.

It is difficult to calculate financial loss incurred as a result of cybercrime. This is particularly the case where direct financial loss does not give a true picture of the actual loss resulting from a cyber attack. Loss of data, stoppage of work and processing that can result from a cyber attack can lead to enormous costs for the victim, which can be difficult to recoup. International research shows that up to 60% of smaller companies that are victims of cyber attack, cease operations within 6 months of the attack having been made. Suffering such an attack also results in shock, mental pressure and stress which must also be handled.

The European Union Agency for Cybersecurity (ENISA), estimated that states in Europe lost about 1.6% of GDP per annum as a result of cybercrime. Two years later in 2018, the Australian government estimated that their society lost 1.9% of GDP per annum as a result of cybercrime.

If we apply these numbers to Iceland, we can see that they represent a significant amount of money. By allowing for 1.5% of GDP in Iceland being lost through cybercrime, we would reach the figure of ISK 40 billion being lost per annum. The nature of cybercrime means that it is a communal project of society as a whole to adopt defences against cyber threats.

There were two major cases that occurred last year that will be specifically dealt with in this report. They are DDoS attacks on the financial sector and Log4j vulnerability. It is a fact that serious weaknesses or risks can come to light at any given time and also that our infrastructure has been a target for cyber criminals It is therefore important to be always prepared to respond.

Vulnerabilities in Log4j

The first time that the civil defence alert phase was activated because of a cyber threat in Iceland was in 2021, when a serious vulnerability in the Log4j code package came to light. The vulnerability had an impact across the world and in the large majority of systems one can find some hardware or programme that needs to be upgraded or removed.

It was on 10 December that it was made public that a vulnerability with a of 10 of 10 had been found in the code package and a fix was released. System administrators subsequently began work in most companies in the world to find all programmes that used the package, upgrade them, remove or prevent the impact in another manner. As is often the case with vulnerability, two smaller vulnerabilities were found in the same code package and upgrading had to be repeated in many systems. Suppliers in the information technology sector were still issuing upgrades until the beginning of 2022.

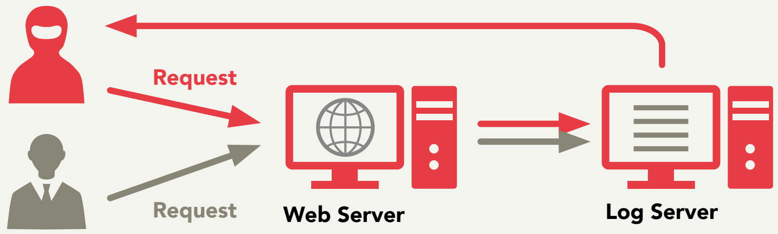
An example of how vulnerability in Log4j was misused was through installing ransomware and then sending a ransom demand, through stealing system identities, taking control of weak systems and stealing data from them. Two large events abroad are directly traced to this vulnerability.

As the spread of common programmes and code packages is extensive, it is only a matter of time until a similar major vulnerability will come to light. Iceland needs to be prepared to respond with effective measures, as operators did last December, where tens if not hundreds of Icelandic technicians worked day and night as Christmas approached in order to respond and protect their systems. One can furthermore argue that one should seek methods to reduce work like this on the next occasion when such a serious vulnerability emerges.

One of the tools we have at our disposal to tackle a widespread event like this is to activate the protection alert level in accordance with Act no. 82/2008. There are three levels defined in the response plan: alert level, danger level and emergency level. Cooperation commences at the alert level between the civil defence and CERT-IS. CERT-IS has the coordination role and regularly conducts status assessment. At the risk and emergency levels, the coordination and command centre of the civil defence is activated, which is responsible for coordination and management of all measures, with advice and status assessment from CERT-IS.

Why do so many systems use log4j?
The code package greatly facilitates entering records in an event log, and instead of having each programmer write his own version for such functionality, it is much less time-consuming and usually more secure to use what already exists. Not to reinvent the wheel.

Examples of attacks that used the Log4j vulnerability.



Distributed denial of service attacks on Icelandic financial infrastructure

DDoS – Distributed Denial of Service are attacks that disrupt access and service over the Internet.

Recent years have seen an enormous increase in the use of ransom DDoS/RDDoS by criminal groups for the purpose of demanding ransoms from their victims. The most common scenario is for criminal groups to implement a short attack to show their capability of making a DDoS. A threat of further attacks if the victim does not pay a financial ransom is then sent. There are known instances of parties purchasing RDDoS attacks from specialised criminal groups, in order to attack a specific company.

Botnet

It can be extremely difficult to identify the party behind a DDoS, except in those instances where threatening letters are sent. The reason why it can be difficult to identify the party making a DDoS attack is that such attacks are often implemented with the help of botnets, or by using web servers with vulnerabilities to redirect traffic to victims of reflection or amplification attacks. The attack appears to originate from a number of varying starting points that have little or nothing in common, where the real perpetrators are hidden behind a chain of Internet servers in varying jurisdictions, making them difficult to trace. In those instances, it can prove unclear how the attacks will develop.

Distributed denial of service attacks on Icelandic financial infrastructure

In September 2021, the Icelandic payment systems were subjected to repeated DDoS attacks that resulted in all payment cards being unusable for a short period of time on Saturday evening, 11 September.

Payment processors, banks and financial enterprises responded quickly to these attacks and their specialists worked on countering the attacks over a period of a number of weeks. One could say that although there had been a significant impact, they were successfully contained because of this response.

When such attacks are made to one or more service companies, one should not forget the wider reach of the damage caused. Saturday evening is peak time for restaurants and if there are delays in payment, this means that e.g. tables are not being vacated at the right time. It is difficult to assess total costs or losses resulting from such events.

It has not been possible to determine who made the attacks against the financial systems, nor the purpose of the attacks.

Volume-based attacks

Objective:
to fully utilise bandwidth

- UDP flood
- ICMP flood
- Spoofed packet flood

Protocol attacks

Objective:
to fully utilise resources

- SYN flood
- Fragmented packets attack
- Ping of death attack
- Smurf DDoS attack

Application layer attack

Objective:
to cause system collapse

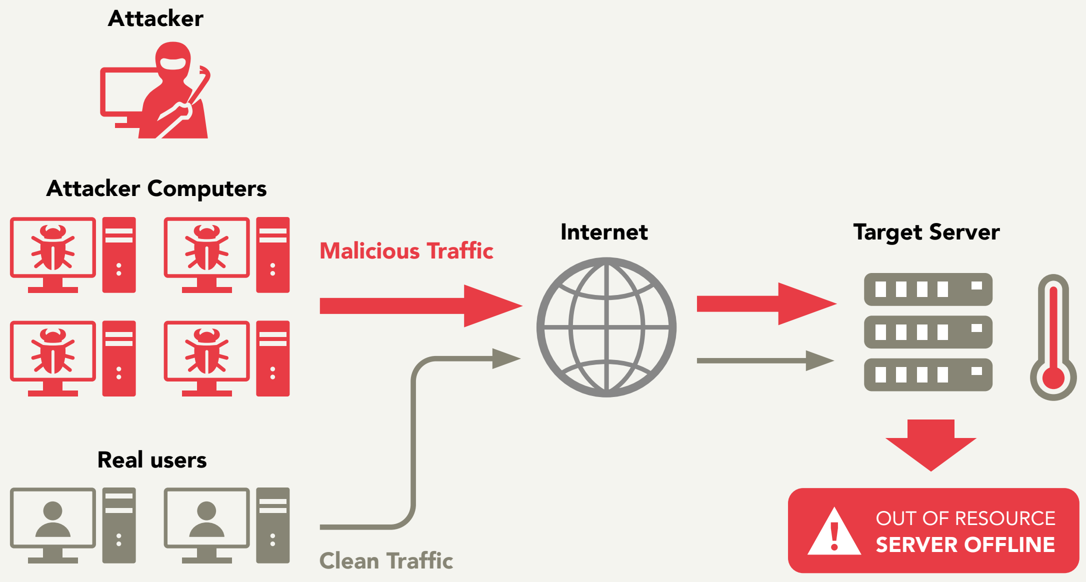
- Low-and-slow attack
- GET/POST flood
- Vulnerability attack

Development of attacks

DDoS attacks have developed in recent years to being tailor-made for the victim and more multi-vector attacks are being used than was previously known. In other words, the attacker implements an attack that he considers adequate to disrupt the victim's capacity to provide service, but if that attack proves insufficient, then the type of attack is changed, and its intensity, until it has achieved its goal. CERT-IS has seen tailor-made DDoS implemented in Iceland.

According to a Netscout analysis, 5.4 million DDoS attacks were made across the world in the first half of 2021. Most attacks were made with the help of botnets. It was also remarkable that multi-vector attacks more than doubled in number. CERT-IS conducted a status survey during the latter half of 2021 on the nature of DDoS attack defences in this country and on attitudes to threats. All respondents agreed that it was likely that the number of DDoS attacks would increase in coming years and that DDoS attacks would continue to make technological advances.

Operation of DDoS Attack



Security in remote working

There has been an increase in recent years in the practice of institutions and companies offering staff the opportunity to work from home. The Covid 19 pandemic has doubtless accelerated this development.

This is a development that brings new challenges in various fields, among other things in the field of computer security. Staff need to work with confidential data on their computers, e.g. personal data, business documents and a variety of documents on intellectual property which is in continuous development.

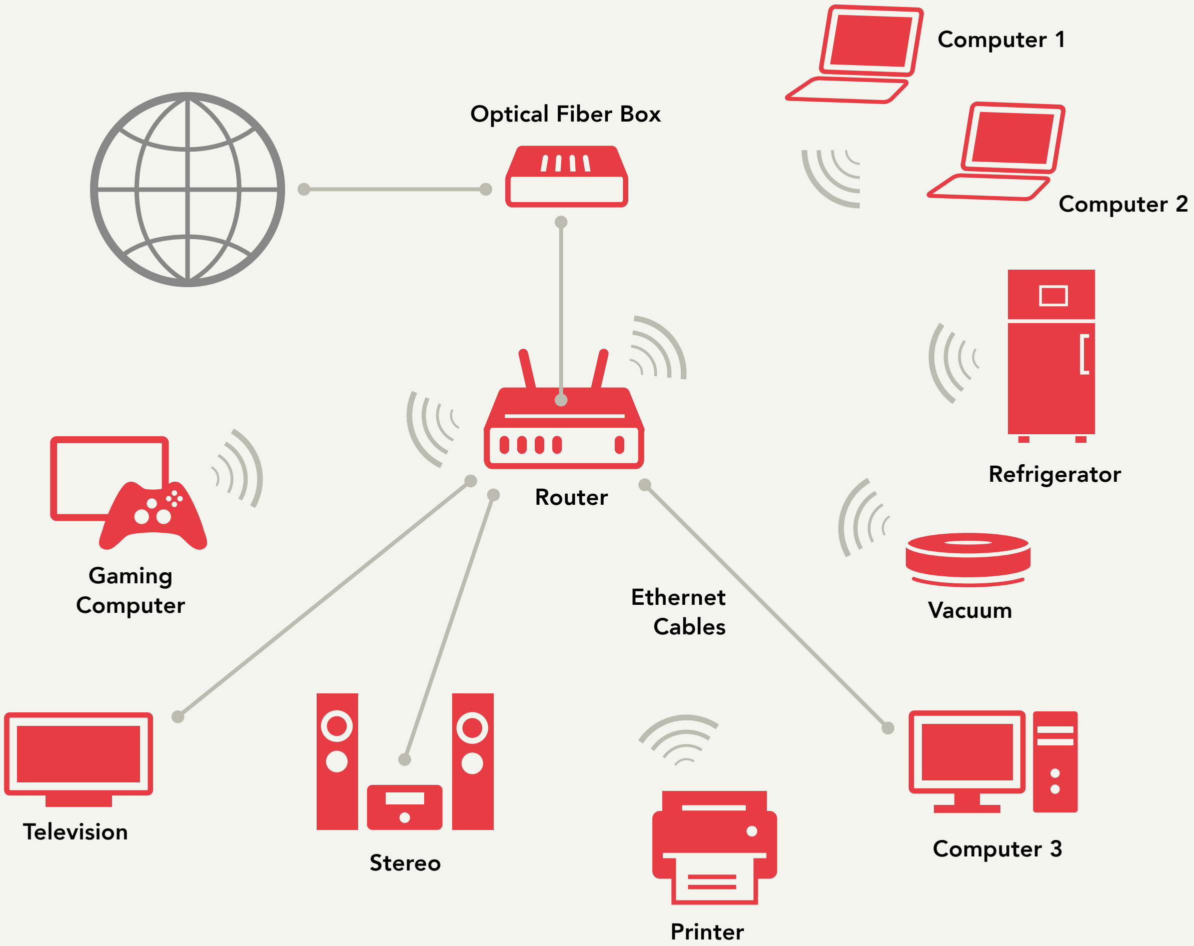
When the working day takes place in the offices of companies or institutions, measures are in place to ensure the security of computer and network systems for the staff who are handling sensitive data. This does not apply when working from home, as the staff connect through their own home network to do their work. It is important that employers give network and computer security some thought when people are working from home.

It is important that access to the computer is limited, that it should only be used by the employee himself. Data stored on the computer should also be encrypted if it should be lost, which is offered by all the main operating systems today. It is also important to remember that access to the most sensitive data and programmes may need to be limited. Where possible, multi-factor authentication should be used, or identification that makes theft of authentication more difficult.

Employees' home Internet connections and the smart devices connected to the same home Wi-Fi can be a route into all the computers of a company or institution. When many parties use the same network, it matters what each and everyone does, e.g. is some member of the household downloading unknown software or visiting insecure sites. If a virus infects one computer, it can spread to other computers or equipment connected to the same network. It is important that hardware has active firewalls and defences against viruses, where the best solutions today are called endpoint protection that provide significant security if they are properly configured and monitored.

In order to increase their security, many workplaces use virtual private networks, which means that part or all of the traffic from the computer is encrypted and sent through the employer's network. When using VPN, it is possible to use systems that are specifically protected. If all traffic passes through a VPN, this provides certain defence against surveillance and alterations, and security monitoring becomes more effective.

Multiple connections to the home internet



Critical Infrastructure and exchange of information

CERT-IS is responsible for the sector-specific groups for critical infrastructure, where the emphasis is placed on strengthening Icelandic cybersecurity defences and response capability to cybersecurity events. These objectives are achieved among other things, by encouraging technical consultation and exchange of information in the field of network and information security. The groups will form a mutual view of the development of cybersecurity issues within their field in Iceland, for example about the information that would be useful to share; they would prepare coordinated responses to serious events and take part in related exercises.

Cooperation and sharing information are extremely important when it comes to network and information security. What threatens one can also threaten others. Sharing information supports improved security for everyone who takes part in the cooperation. Sharing information also prevents the situation where many different parties repeat the same analysis work, which could prove time-consuming. In return, everyone shares information to enhance understanding and defences within the group as a whole.

One reason for sharing information is for there to be trust between all participants. The parties need to see a gain for themselves in participating in sharing information. This means that all parties make their contribution so that the cooperation can achieve desired results, and respect trust and confidentiality of the others.

Though email and network chatting are in many ways useful, such free communication forms have certain weaknesses when it comes to response. By using a formal information structure and a specialised tool to disseminate, it is possible to facilitate various work such as more controlled distribution; automatic processing such as for warnings and for links other events and to older cases.

When taking part in the formal information network with CERT-IS, our ability to disseminate the most accurate picture of the status in Iceland in Iceland is enhanced.

Sviðshópar

Energy

Healthcare

Telecommunications

Utilities

Transportation

Banking

Paswoord Manager

In daily life we rely on user names and passwords to connect to most of our access on the Internet, whether to social media, email service, image and data storage or other service or apps. There are many data leaks every year where user passwords are leaked. Criminal groups can then take advantage of the passwords to enter through their victims' access. People's tendency to reuse their passwords or use very similar passwords, makes it easier for criminal groups to acquire other victim access than those that were compromised in the data leak.

There are many methods to protect one's access, such as having complex passwords, multi-factor authentication and by having a password manager.

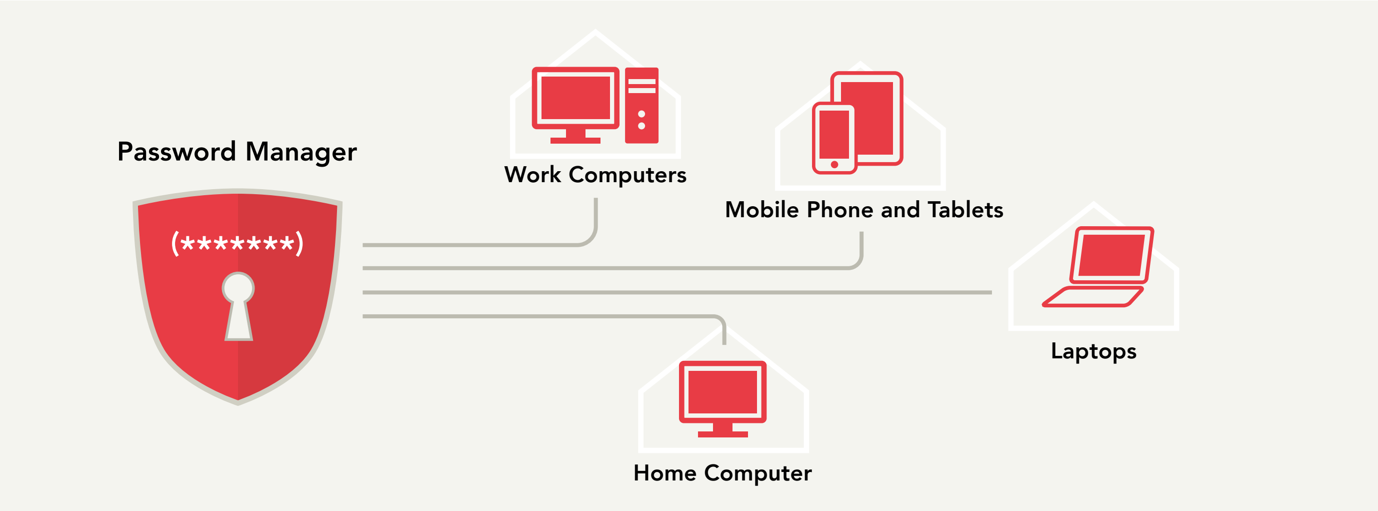
Password managers enable people to save their access information for all sites and services in one secure location. If an individual uses a password manager, he can enable the bank to fill out the user names and passwords for access. This means that each and every password can be much longer and more complex, as the password manager remembers them for the user. Some password managers also offer to create new passwords and one does not then have to use one's imagination, but can get a complex password of appropriate length automatically. One only has to remember one password, the password for the password manager itself. It is then important to protect the password manager password with multi-factor authentication.

When one makes a password for the password manager, it is important to choose a strong password which can be remembered. It is a common myth that passwords need to be complex random letters and symbols, where it is hardly possible to remember their order. Long simple passwords are considered stronger than short complex ones today. In this way is better to use a sentence with no context composed of a number of words with numbers of varying lengths in between, rather than to choose a few letters and symbols that are difficult to remember.

Common and weak passwords

1. 123456
2. Qwerty
3. Password
4. Name of children/ partner/pets
5. Favourite football team/ /band
6. <word><number>

✗ GK"$/45gS
✓ Santaclaus323loveseasterfood84i109october



Ransomware attack

It is increasingly common that criminals use threats and financial blackmail to get money from companies, e.g. with a ransomware attack. Criminals have then succeeded in capturing a company's data, encrypting it or deleting from the web server. They then send payment instructions to the company and promise, against payment, that the victim will gain access to his data. It is also common to threaten to publish the data if the company does not pay the demand, which could have serious consequences in the case of sensitive data, e.g. sensitive personal information. Management and owners of companies must therefore be introspective and consider how prepared the company is to respond to this type of attack.

It is not possible to require that management and supervisors of companies engage in an extremely technical dialogue when it comes to their company's computer security. There are however several questions that one has to have in mind, particularly when companies are entangled in financial blackmail attempts:

1. **Does the company have a backup of the data that is necessary to ensure company operations and is the backup hosted in a secure location?**
   - Has the data been defined that is critical for operations; how often are backups taken of these data?
   - Where are the backups stored; are they accessible to criminals; are they on off-line machines or in cloud solutions? How long would it take to get access to the backups?
2. **Are there detailed procedures that are activated when a ransomware attempt is made on the company?**
   - Do the procedures specify when contact should be made with all the departments covered by the plan? e.g. managers, attorneys and the marketing department?
   - Are everyone's functions defined; when the marketing department should prepare a press release; what regulatory authorities should be contacted?
3. **Who should make the final decision on whether the company pays the ransom demand or not?**
   - How long can the company operate without the data that was taken?
   - If data should leak, could the company's reputation survive?

It is appropriate to note that CERT-IS advises to never pay criminals who try to coerce a ransom from companies. There is no guarantee, even if the ransom is paid, that the company's data will be returned or that the data will not be leaked. It could also increase the likelihood that the company will be a target at a later date.

Cyber criminals have over a period of many years been developing the best methods to force companies to accede to their demands. This means that the criminals often have knowledge of the size of ransom that the victim can pay. This could mean that it is tempting for a company to pay the demand in the hope that it can continue operations unhindered. It is not unusual on the other hand, that data is en route from the criminals for several weeks or that it is returned damaged, after a payment has been made. There is therefore no guarantee that they will be able to start operations immediately if they accede to the criminals' financial blackmail.

All companies can be subjected to a ransomware attack. The size and operating environment of the company is irrelevant. This means that all managers and owners of companies should elaborate a policy, a response plan and procedures that are activated in the event of cyber attacks.

Ransomware Attack

2021

JANUARY 5 employees

- Operators of essential services designated
- New regulation on CERT-IS (480/2021)
- Law on Icelandic national domain (54/2021)
- New law on The Electronic Communications Office of Iceland (ECOI) (75/2021)
- CERT-IS moves to new premises
- DDoS attacks on Icelandic Financial infrastructure
- Sector-specific group for the financial infrastructure begins to operate
- Intrusion into the email service at University of Reykjavík
- Cyber Security Policy for Iceland 2021–2036
- Log4j vulnerability
- Intrusion into Strætó bs computer system

DECEMBER 8 employees