CERT·IS

Annual summary 2022

CERT-IS is a department of the Electronic Communications Office of Iceland (ECOI). Cybersecurity issues are under the purview of the Ministry of Higher Education, Science and Innovation.

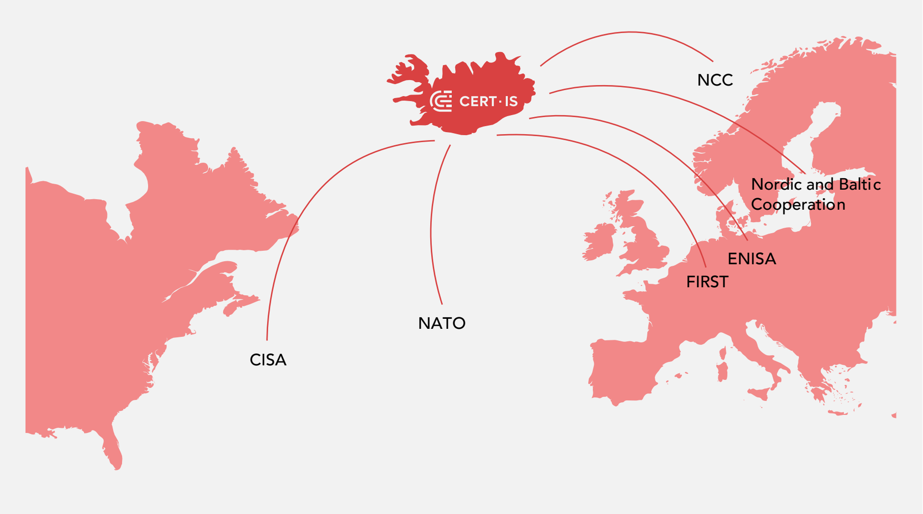
Efni

Managing Director's Address

The year 2022 will be remembered as a year of great upheaval. Residents of Europe awakened to a bad dream on the 24th of February to the news that Russia's full-scale invasion of Ukraine had begun. Although many have had a difficult time believing the new reality, the invasion had nevertheless had a considerable lead up. During that time, Western intelligence agencies freely shared information with the Ukrainian government and others that a Russian invasion was imminent. It can also be said that the invasion by Russian forces and groups loyal to them began even earlier, with targeted cyberattacks on the Ukrainian infrastructure whose primary objective seemed to be to cause as much damage as possible.

The Western world was facing a new reality, and responses were swift. In the aftermath, NATO member states - including Iceland - and other nations condemned the invasion and imposed economic sanctions of an unprecedented scale on Russia. Russia responded by making it clear that those countries participating in the sanctions would be considered hostile and could expect consequences. For Iceland, this necessitated a reassessment of the threats facing our infrastructure. What was once regarded as a distant reality had all of a sudden become a genuine risk and threat affecting the CERT-IS Cybersecurity Team's plans. The team has followed a three-year development plan that covers full-time equivalent positions, introduction of equipment and knowledge acquisition, that will maximise the team's capabilities, in light of resources, in order to support Icelandic infrastructure and administration. There was occasion to review these plans and to further expedite development in order to reach the defined objectives ahead of schedule. With the support of the Ministry of Higher Education, Science and Innovation, the implementation of departmental groups for all of the most vital infrastructures has been successfully expedited. The aim of the departmental groups is to ensure the coordination of related parties with regard to responding to and informing about vulnerabilities, attacks and other threats they might face, as well as administering joint cybersecurity exercises. Mobilising the departmental groups was one CERT-IS's most important tasks of 2022.

With an increase in employee numbers during the past two years, CERT-IS has reached a certain breadth regarding these issues. Now is the time to go deep. The next objectives involve increasing the team's analytical capabilities by implementing the right tools and improved cooperation with sister agencies in other countries. With the necessary and adequate support of the government, it has been possible to implement tools and systems that give CERT-IS even better access to information in order to identify foreign, advanced persistent threat groups within Icelandic online jurisdiction along with a detailed analysis of major threat indicators. It is important for the team to familiarise itself with and fully utilise this information so that it may be of the greatest value to the Icelandic online jurisdiction.



International cooperation is a matter of grave importance to CERT-IS. The team is an active participant in Nordic CERT Cooperation (NCC), a collaboration of CERT teams across the Nordic countries. A great deal of energy and determination is evident in the extent to which the Nordic countries stand together when it comes to matters of cyberdefence. Iceland is now on an equal footing with its Nordic neighbours in this field and has contributed to the collaborative effort in a way it can be proud of. Furthermore, Iceland participates in international defensive cooperation with other NATO members. NATO has defined cyberattacks as one of the fastest growing threats to its member countries, and unlike physical dangers by land, sea and air, it is to a greater extent up to the member countries themselves to ensure correct cyberdefence practices within their own borders. CERT-IS thanks the Ministry of Foreign Affairs for its outstanding and professional initiative in connecting the team with important collaborators within NATO, thus ensuring the common interests of Iceland and the alliance to an even greater extent.

CERT-IS's development has exceeded expectations and we're excited for the future. We are now reaching the end of the three-year process of bringing the CERT-IS Cybersecurity Team into full operation and are making the initial plans for our priorities for the next years, with the aim of benefitting the Icelandic public and its infrastructures.

Respectfully,
Guðmundur Arnar Sigmundsson
Managing Director of the CERT-IS Cybersecurity Team

The year in numbers

Numerous cybersecurity incidents occur every year, and it is CERT-IS's job to maintain statistics for Iceland's online jurisdiction about what types of incidents take place domestically. Cybersecurity incidents can take many forms, ranging from system updates and power outages to opportunistic attacks by cybercriminals or targeted, organised attacks on businesses or institutions.

Statistics are based only on incidents reported to CERT-IS. It is therefore extremely important to report all incidents that arise. These statistics provide CERT-IS with vital clues about the development of domestic incidents that enable us to offer preventative advice to institutions, businesses and individuals.

As was the case last year, cyberfraud comprised the vast majority of incidents in Iceland. It is most apparent that the campaigns launched against Icelanders in 2022 were more sophisticated and better organised than we've seen before. Cyberfraud will be explained in greater depth later.

Reports of attempted takeover doubled between the two years. This suggests that attempts to break into computer systems in Iceland are more frequent. There is no way to know with certainty how often attempts were made to attack businesses or institutions, as many technological defences interrupt most attempted attacks before they're noticed. Once an attempted break-in is detected, the attacker has already penetrated the first defences but is discovered before any significant damage is done.

The fact that attackers are coming closer to causing damage within computer systems with greater frequency is a matter of concern. It only takes one successful attempt to paralyse an entire business or institution. It is therefore necessary to be on constant guard when it comes to computer system defence.

Several instances of malicious code or malware found in systems in Iceland were reported to CERT-IS in 2022. Malicious codes are created by attackers and may look harmless until they enter the computer system. Malware can be of various types, but is often used to destroy data, take over systems or for espionage.

Finally, the slight increase in incidents due to attackers taking advantage of vulnerabilities in computer systems bears mention. CERT-IS draws attention to confirmed serious vulnerabilities with announcements on the CERT-IS homepage as well as through a subscriber mailing list. It is important that businesses and institutions keep up with new updates and implement them quickly and efficiently.

8 Incidents

Information security

Access to information through illegal channels, data loss and data leaks.

26 Incidents

Availability

Systems and services not accessible due to external circumstances, e.g. distributed denial-of-service (DDoS) attacks, when computer systems are deliberately overloaded.

422 Incidents

Fraud

Phishing, whereby attackers attempt to get hold of sensitive information such as credit card numbers or passwords

9 Incidents

Abusive material

Bullying, harassment or stalking. This includes material involving child abuse and incitement of bullying.

28 Incidents

Vulnerabilities

Vulnerabilities that can be exploited in order to break into or influence other computer systems.

18 Incidents

Break-ins

Break-ins into computer systems of home users, businesses or economic operators.

26 Incidents

Malicious code

Viruses and other codes used to destroy or take control of computer systems.

34 Incidents

Attempted takeover

Unsuccessful attempts to take over victims' computer systems.

15 Incidents

Information gathering

Unauthorised gathering of information about vulnerabilities and internet traffic.

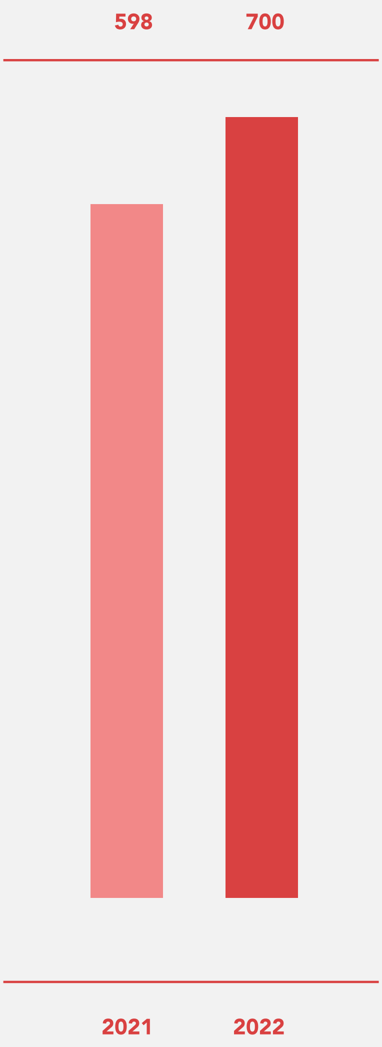
114 Incidents

Other

Activity that does not fall into any of the above categories.

Total: 700 Incidents

Statistics



Phishing

Nearly all necessary services have recently become accessible online, and electronic ID makes them easier to access. Before, it was necessary to pay monthly bills at commercial bank branches, but now banking services are mostly available online or in smart apps.

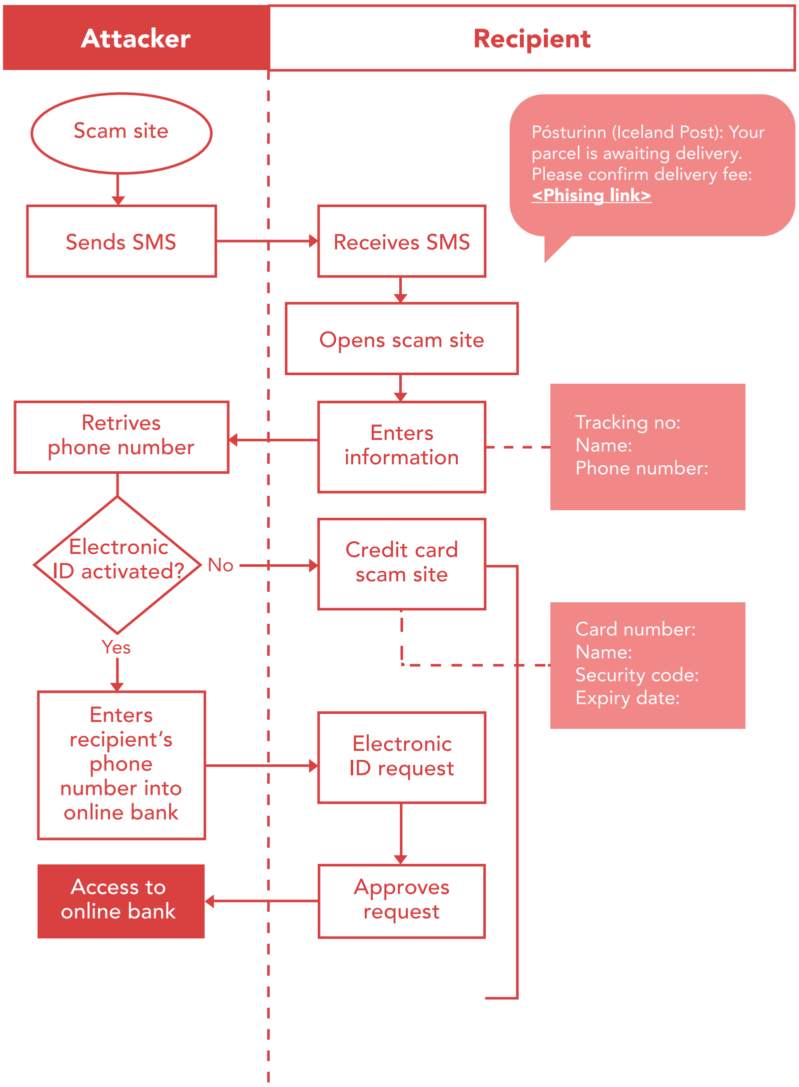
In recent years, phishing activity has increased. Unscrupulous parties are constantly looking for new ways to scam people, changing their methods quickly according to what works best each time. Phishing can take various forms and is directed both at individuals or specific targets, e.g. a business's finance director.

Perpetrators use text messages (SMS) to a great extent in phishing activities. Various factors encourage the use of this method. The likelihood of someone opening a text message is 98%, as opposed to 20% for a typical e-mail. On average, a minute and a half elapses between someone receiving a text message and opening it, versus 90 minutes for an e-mail. What's more, individuals are more likely to trust text messages than e-mails from an unknown party. Finally, there are a number of security systems and spam filters available for e-mail systems, but not so much for text messages.

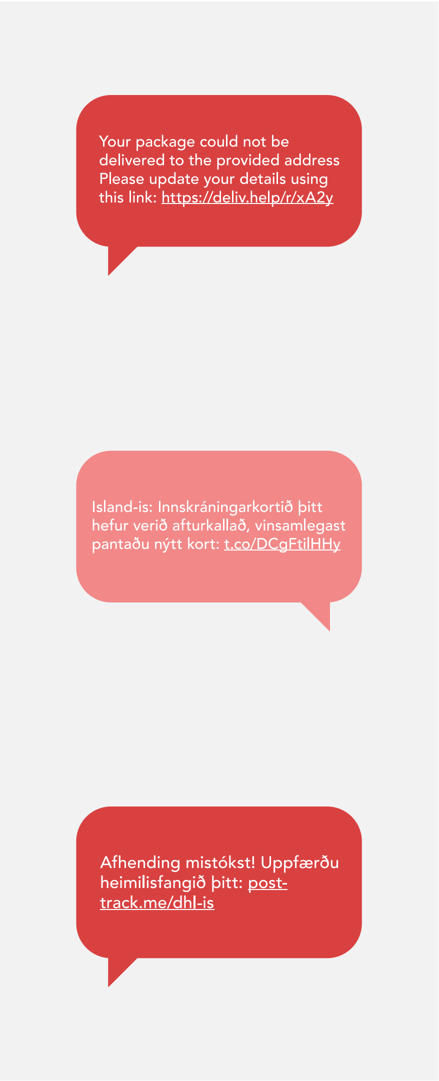
Most of us recognise suspicious e-mails. They're usually poorly composed and strangely worded. However, this can be expected to change with the advent of language models such as ChatGPT. SMS is a simpler medium than e-mail. Messages are generally short, with strings of numbers or links, and thus an ideal way for attackers to impersonate others. These messages often claim that "your delivery has been stopped" or "your card has been blocked", accompanied by a link that the recipient must click immediately in order to respond.

Once the recipient clicks the link, the attacker's first goal is achieved - to capture the person's attention and lure them to their own website. These sites usually request payments of small amounts in order to process or display information on the status of a delivery, and ask for the victim's name, address and phone number. This is normal information to request in such a context, but what the attacker is doing behind the scenes is checking whether the phone number is connected to an electronic ID. If not, a further request is sent for credit card information. If the phone number is connected to an electronic ID, the associated ID can be used to attempt to log into any system that supports it. These include online banking services or the services of public institutions, to name a few.

Some campaigns put a good deal of effort into setting up the scam, and it's obvious that a lot of work has gone into learning how to avoid detection by the institutions or businesses being exploited.



Pósturinn (Iceland Post): Your parcel is awaiting delivery. Please confirm delivery fee: <Phising link>



Your package could not be delivered to the provided address Please update your details using this link: https://deliv.help/r/xA2y

Island-is: Innskráningarkortið þitt hefur verið afturkallað, vinsamlegast pantaðu nýtt kort: t.co/DCgFtilHHy

Afhending mistókst! Uppfærðu heimilisfangið þitt: post-track.me/dhl-is

What we can do to protect ourselves against these scams is to stop and consider the authenticity of the messages. If a message claims to be from a business or institution, it is always possible to contact the business/institution and verify the message's authenticity. Our phone numbers are no longer just phone numbers, and attackers know this.

CERT-IS receives all phishing emails and screenshots of phishing scams at **phishing@cert.is**. E-mail notifications to CERT-IS help ensure a better overview of scam e-mails and campaigns aimed at Iceland.

The war in Ukraine

When Russia's full-scale attack on Ukraine began in February of 2022, there was immediately significant reason to believe that, alongside conventional means of attack, a number of cyberattacks on Ukrainian infrastructure and even that of their allies would follow. The attacks would come from the Russian government or their allies.

Many experts believed that Russia would use cyberattacks to try to paralyse Ukraine during the invasion. In 2017, Russia did exactly that - bring daily life in Ukraine to a standstill with wiper malware called NotPetya. The country's financial system ground to a halt and hospitals lost internet connection as well as most government institutions. The malware also extended far beyond Ukrainian borders and impacted businesses across the world, e.g. Britain's NHS.

Although there have been fewer cyberattacks in the news during and about the war than many expected, such attacks have certainly been used. During the early days of the war, Russia used cyberattacks to incite rioting and create division. One such example is an attack on a satellite partly responsible for communication within the Ukrainian military, which began an hour before the invasion. The day after the invasion began, Russia also targeted the government websites and border crossing points to prevent people from escaping. Furthermore, Russia made use of deep fakes of Ukrainian president Zelensky in order to spread fake news of disarmament.

Most striking is the use of wiper malware against Ukrainian infrastructure. Wiper malware was first used in 2012 and was employed eight times before the war commenced. In 2022, wipers were used thirteen times against Ukrainian infrastructure. This is a massive jump in the use of a malware that is exclusively used to destroy, unlike other means of attack where it is often possible to retrieve data in at least some form.

Ukrainian authorities immediately called for the support of cybersecurity experts from both the public and private sectors, and the response was swift. For the first time to our knowledge, cybersecurity companies in Ukraine were present and active participants in the war effort in cooperation with the country's government.

If you would like to learn more about the impact of cyberattacks on Ukraine since the invasion, a detailed article can be found on our website at **www.cert.is**.

14/2
70 government institutions attacked, "Wait for the worst" appears on their websites

24/2
KA-SAT satellite attacked

25/2
Border crossing points attacked with a wiper

4/3
Aid organisations within Ukraine attacked

16/3
Television stations attacked, deep fake of Zelensky

8/4
Attempted attack on Ukraine's energy sector

Wiper: a type of malware designed to erase - or wipe - a computer's hard disk. All stored data is deleted and cannot be retrieved again unless a copy has been saved on another machine.

Cybersecurity in Iceland

All of Europe's security landscape changed with the invasion of Ukraine. Until now, Iceland has been safer than other countries during conventional conflicts due to its status as an island in the middle of the North Atlantic. But the times are changing. The internet has no borders, and all countries can fall victim to cyberattacks.

Alongside the invasion of Ukraine, Russia and their allies have committed cyberattacks against Ukraine's infrastructure. They haven't stopped there, and have directed cyberattacks against Ukraine's allies in the war. These attacks are aimed in particular at current and prospective members of NATO. Owing to Finland and Sweden's applications for NATO membership, attention has turned to the Nordic countries.

All of the Nordic countries have been attacked by groups loyal to Russia. Most common are distributed denial-of-service (DDoS) attacks designed to take down websites and temporarily paralyse the operations of businesses or institutions. In Iceland, scanning of the online jurisdiction increased six times during the first weeks and months of the invasion in comparison to the normal situation. Scanning of online jurisdictions is done the hope of identifying vulnerabilities that can be exploited in cyberattacks.

Iceland is often said to lag behind its neighbouring countries in terms of cybersecurity. This claim finds support in a list from the International Telecommunication Union (ITU), where Iceland ranks 58th It is worth noting, however, that the list was last updated in 2020 and many positive changes have been made since then.

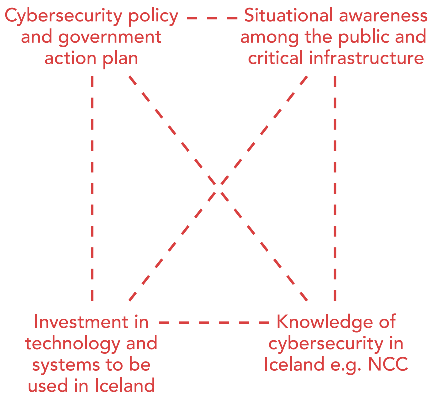
With the adoption of NIS-legislation along with an increase in the number of permanent CERT-IS positions from five to thirteen, the Icelandic government has added services to important infrastructure. A new cybersecurity policy for Iceland was published for the period between 2021 and 2036, as well as a specific action plan that shows how the government intends to achieve its cybersecurity goals beyond vital infrastructure. A watershed in Icelandic cybersecurity issues was reached with the establishment of NCC-IS, a collaborative platform for cybersecurity training, education and research. In the near future, a master's program in cybersecurity will be offered in Iceland.

In the past, Iceland had only a limited ability to identify advanced persistent threats (APTs) potentially directed at the country's online jurisdiction. Today, CERT-IS has made agreements with parties that specialise in identifying APTs and therefore has access to specialised tools that significantly improve CERT-IS's analytic capabilities.

While much has been done in recent years, cybersecurity can never be fully guaranteed. Cyber defences must be in constant development in accordance with attackers' changing behaviour. It is therefore necessary to follow up on the action plan in order to ensure Iceland's position in the forefront of cybersecurity issues.

APTs are well-organised groups of assailants often associated with nation states. The groups specialise in entering computer systems undetected, where they can destroy important functions or steal information for long periods of time.

Cybersecurity in Iceland divided among


Cybersecurity policy and government action plan

Situational awareness among the public and critical infrastructure

Investment in technology and systems to be used in Iceland

Knowledge of cybersecurity in Iceland e.g. NCC

Departmental groups - what they do and the vision for the future

One of the primary tasks of the CERT-IS Cybersecurity Team is to take care of vital infrastructures and economic operators of essential services in order to promote better preparedness against cyberthreats. In this way, CERT-IS has established interdisciplinary consultation groups for the infrastructures specified in the law. The year 2022 was a turning point for CERT-IS in that it was possible to establish and manage all six departmental groups, with over 50 operators of vital infrastructures and essential services.

CERT-IS's main objective with the departmental groups is to facilitate information exchange, increase situational awareness and strengthen communication channels between CERT-IS and vital infrastructures. Common to all infrastructures and services is the maintenance and operation of services vital to society, but they are nevertheless a diverse group with different needs and risks.

It thus bears mention that for some infrastructures, it is important to be informed of system updates and vulnerabilities or specialised vulnerability scans that CERT-IS offers. Other departmental groups have focused on employees and users of services, who are themselves the targets of phishing and scam campaigns. There are numerous examples from other countries where institutions such as hospitals and banks have fallen victim to massive attacks in which the first steps into the systems were the phishing of employees.

Stage group

Energy

Healthcare

Utilities

The objective for 2023 is to further develop cooperation vis-à-vis departmental groups. The plan is to hold cybersecurity exercises in order to strengthen communication channels between CERT-IS and participants in the departmental groups. This will be the first step of many in creating a more organised arrangement of cybersecurity exercises in Iceland.

Early in the winter of 2022, the European Parliament and the Council approved a new network and information security directive for critical infrastructure, the so-called NIS2. This is an updated version of the law according to which CERT-IS operates. The new NIS2 directive is expected to enter into Icelandic law in 2024, thereby increasing the number of groups of infrastructure and economic operators that are deemed both critical and essential.

Telecommunications

Transportation

Finance

Cybersecurity exercises

Cybersecurity exercises are organised exercises that cover what to do in the event of a compromise in the operation of network and information systems. Examples of such compromises range from system updates rendering important systems temporarily inactive to genuine attacks on information systems using e.g. ransomware or DDoS.

We're all familiar with exercises such as fire drills or safety protocols in the event of an air disaster. Different scenarios are addressed in an organised fashion and the responses and interactions of various parties are rehearsed. Such exercises may be as simple as turning on a fire alarm system to check if it works to staging an air crash where debris is set alight in order to actualise the technical implementation of security protocols on site.

Cybersecurity exercises can range from simple tabletop exercises in which a response is coordinated, better known as cyber incident response exercises, all the way to technical implementation exercises in which a technical response is reality tested. The core of the cybersecurity exercises is to rehearse communications and communication channels; if information is not delivered promptly and correctly, it can be difficult for specialised responders to respond properly. Technical implementation exercises, on the other hand, focus on technical responses to cyberthreats in real time, in which the "red team" launches an attack against which the "blue team" must defend.

Cybersecurity exercises do not need to be complicated in order to effectively teach how to respond to a cyberthreat. Answers to these questions are often simple, but sometimes certain processes must be followed in order to ensure not only operational continuity, but also adherence to law. Cybersecurity exercises involve not only preempting cyberthreats, but also minimising damage, expediting recovery and the entire process that a cybersecurity incident sets in motion.

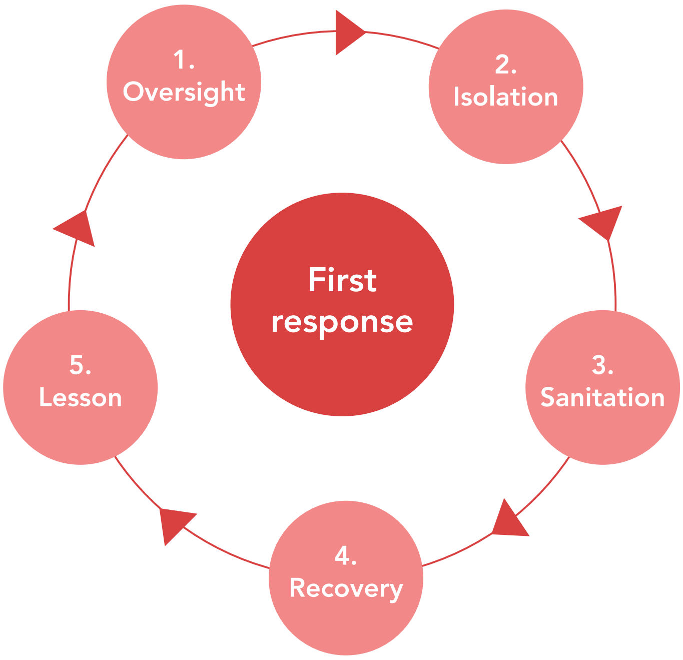
In this way, simple tabletop exercises in which responses to a cyberthreat are coordinated can be very useful in testing response plans and determining what can be improved. These exercises involve not only technical departments, but also managers, lawyers and representatives from human resources and the press.

The custom is to refer to the aggressors in the exercises as the "red team", and their role is to do their best to attack a designated victim. The "blue team" are those who must respond to the attack by employing technical measures.

The aim is to go through the process from beginning to end and to be able to answer questions such as:

- How and when did the incident become apparent?
- How did the relevant parties respond to the incident in order to stop it?
- Who was in charge of oversight and project management?
- How was information disseminated to management and staff?
- Was it necessary to report the incident to the police, CERT-IS, the Data Protection Authority or other supervisory bodies? If so, how was this done?
- What did we learn from the exercise?

A lot can be learned by rehearsing a scenario from beginning to end with whatever groups would be involved in solving such an incident. On the CERT-IS website you can find drafts of simple response exercises and further information about cybersecurity exercises.



Timeline since 2022

- War breaks out in Ukraine
- Departmental group for energy infrastructures engaged
- DDoS attack on Fréttablaðið
- Phishing@cert.is
- Ransomware attack on Tækniskólinn
- CERT-IS and SURF cybersecurity exercises
- Cybersecurity Month
- New homepage with a new notification portal
- Departmental group for healthcare infrastructures engaged
- Departmental group for transportation infrastructures engaged
- Government cybersecurity action plan.

CERT·IS