ALEF

Security Report 2019

Trust the Strong
www.alef.com

Contents

3 Introduction

4 – 5 Security services in 2018

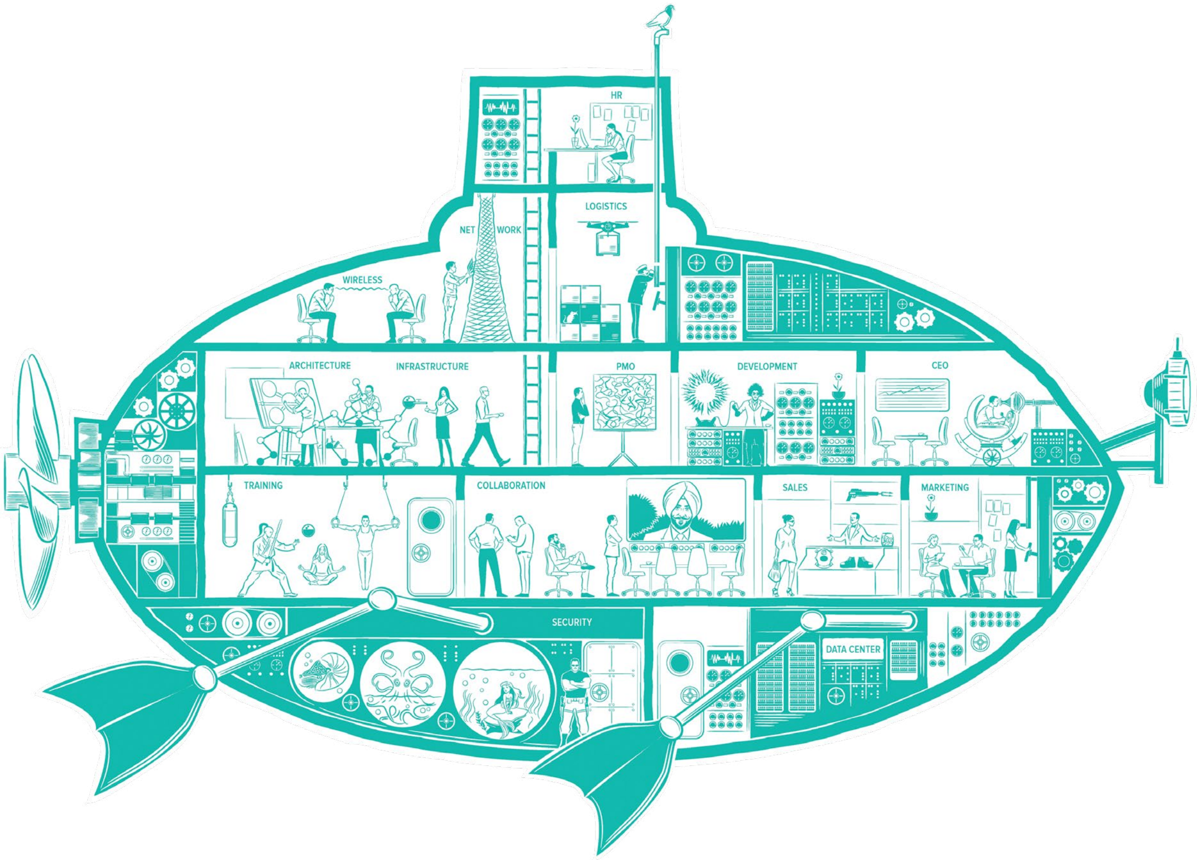
6 – 8 Attacks, incidents and other notable events in 2018

9 – 11 Analysis of data from e-mail gateways

12 – 13 Analysis of data from IPS - Q4 2018

14 – 19 Trends in security education

20 – 23 Selected ALEF CSIRT research activities in 2018



Thank you to Stanislav Novotný for translation.

Introduction

Data leaks, ransomware, phishing... Given the number of threats we face every single day, information security became an issue, which no modern organization can afford to ignore. Since the threats are constantly changing, we need to keep up with trends and developments in this area.

This report, created by members of ALEF CSIRT security team and other ALEF Group specialists, contains a summary of important developments in information security in 2018 – from changes in organizations' interest in specific types of security services, to trends in areas of threat evolution and security awareness education.

The text is unique because the vast majority of the data and statistics presented within it relate specifically to the environment of the Czech Republic. Thus, the analysis of trends can provide a good basis for decision-making on the implementation of new security measures for organizations operating in the Czech Republic.

For example, the available data shows that there has been a decline in the occurrence of various types of malicious code worldwide in 2018. Data for the Czech Republic, however, shows a noticeable increase in malware detections near the end of the year. Based on this information, it may be appropriate for domestic organizations to consider – for example – deployment of EDRs or other advanced anti-malware tools.

The part of the report, which covers security education in Czech organizations, or the summary of interest of local organizations in specific security services in 2018, can also be the source of inspiration for the decision-making process regarding implementation of new security measures.

There is no doubt that interest in various types of services and products will continue to be an interesting area to watch even in 2019, as some perceptible differences in comparison to the last year can already be seen. For example, in addition to the usual "top sellers", such as security audits and analyses or penetration tests, we have seen increasing demand for multi-factor authentication mechanisms. We have also noted an increased interest in security services and products for industrial systems and in the area of security monitoring and operations.

While on the subject of security monitoring, we would like to thank CESNET-CERTS and CSIRT.CZ security teams, who have kindly provided us with data and statistics from their monitoring tools and thus enabled us to analyze not only developments and trends in the Czech Republic, but global-level trends as well.

Security services in 2018

Jana Little

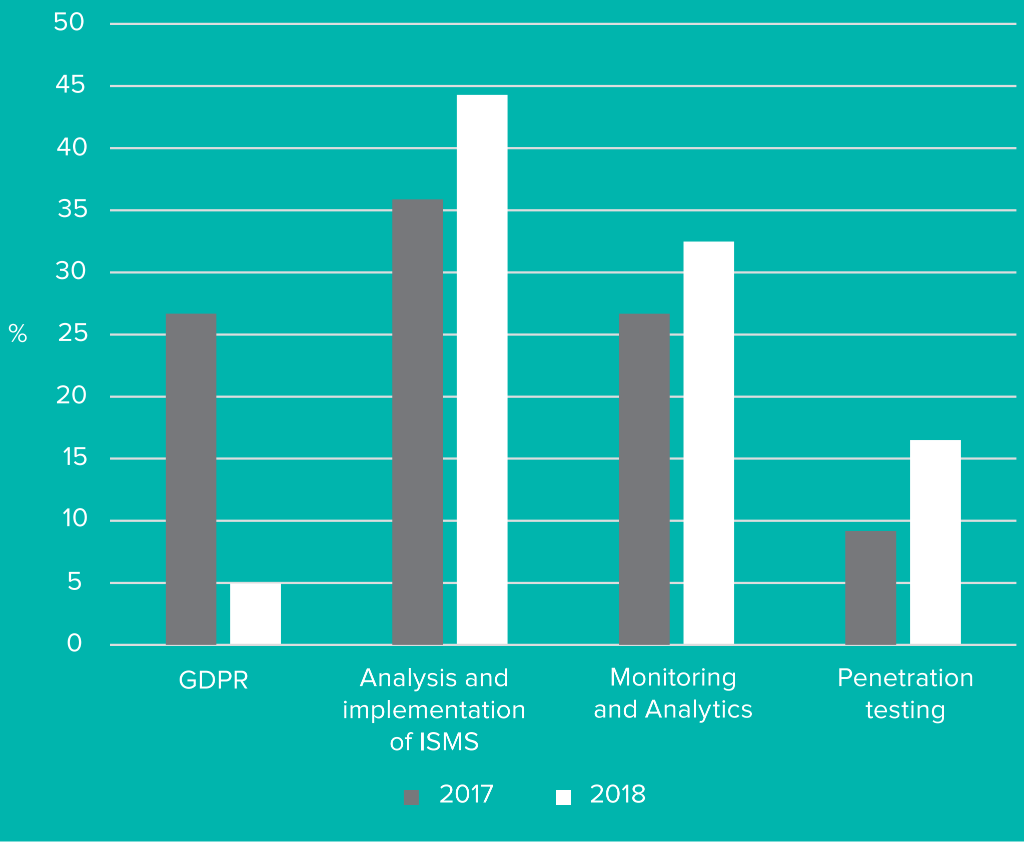
ALEF Security department works on a wide range of security projects every year. With rising requirements on organizational and technical security, we see a corresponding increase in demand of certain IT security services. Based on the analysis of our customer requirements in 2018, we can say that this year brought increased interest in services related to ensuring that organizations conform to the requirements of ISO 27 001 and the Czech Cyber Security Act. This heightened interest was probably related to the new implementing decree for Cyber Security Act, which was published in 2018. Nevertheless, this is not the only trend we have observed. In this part of the report, we will look at the changes in demand for the four most frequently ordered security products in 2017 and 2018.

Analysis of ALEF NULA Security Department shows that in the period 2017 - 2018, four security-related products were of main interest to customers. These are:

- analyses and other GDPR related products,
- analyses and implementation of ISMS,
- design and implementation of security monitoring and analytical platforms and
- penetration testing.

Generally speaking, there was a significant increase in interest in three of the above-mentioned types of services in 2018 when compared to the previous year, while the interest in services related to the GDPR decreased. More interesting than absolute values may be the ratio of interest in the most frequently ordered security products in 2017 - 2018, which is summarized in the following chart.

Interest in security products in 2017 and 2018



GDPR

In view of the General Data Protection Regulation of 25 May 2018 coming into effect, the Security Department saw increased demand for GDPR implementation consultations in 2017. In 2018, interest in these services fell sharply.

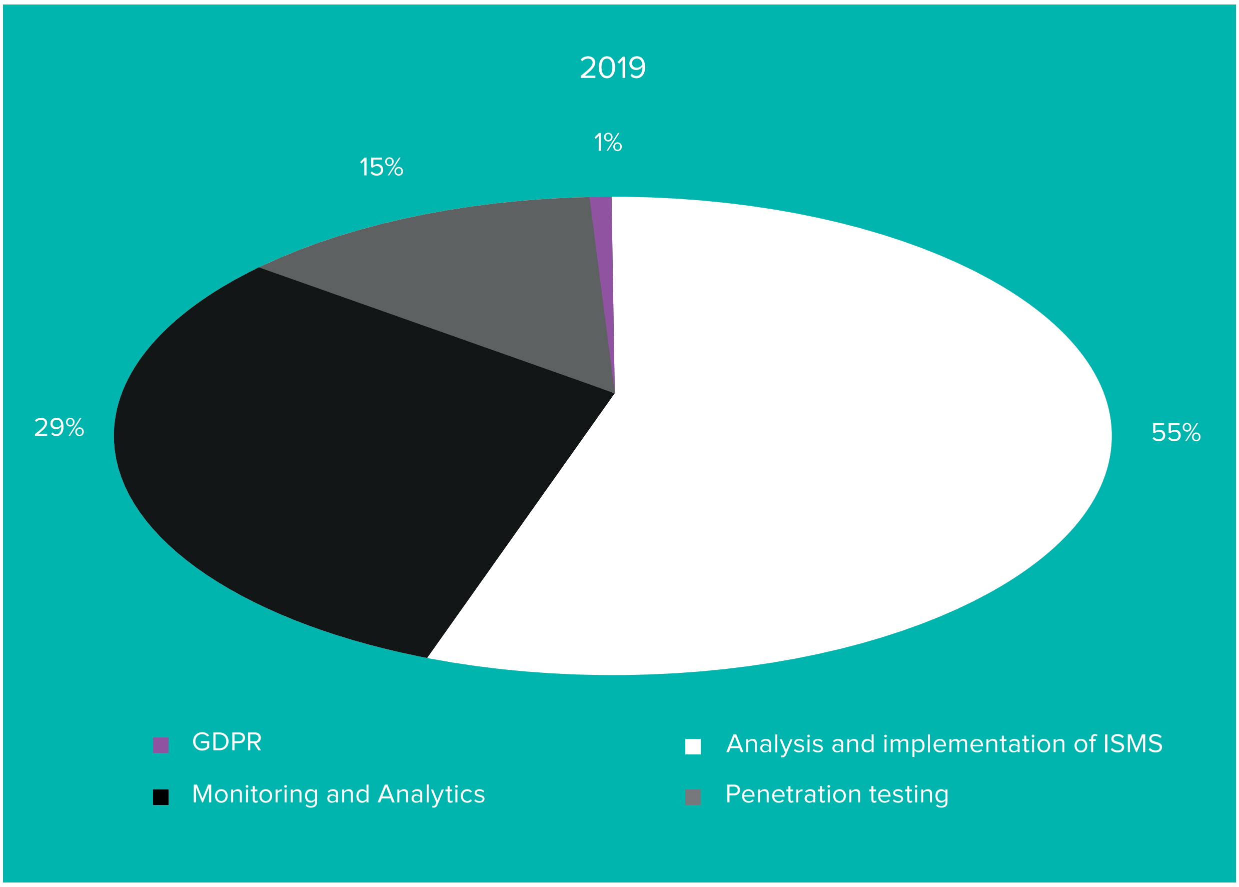
ISMS Analysis and Implementation

Under the umbrella term of ISMS Analysis and Implementation, we include orders for ISMS implementations according to various standards as well as the relevant gap analyses and audits. In 2018, we saw an increased interest in services related to the Czech Cyber Security Act, both for consultations and implementations of its requirements. In the area of gap analyses and audits (i.e. more or less formal assessments of the current environment against the requirements of the Cyber Security Act), the interest was relatively constant, as it was in implementation of corrective measures based on these analyses.

In 2018, customers were especially interested in:

- defining a methodology for identifying and evaluating assets,
- definition of a risk analysis methodology,
- asset identification and evaluation,
- risk analysis,
- developing a risk management plan,
- developing a security awareness plan,
- creating a business continuity management strategy,
- modification of the existing Cyber Security Act documentation.

For the list to be complete, it is worth mentioning that we have also noted growing interest in implementations of TOGAF and ITIL frameworks. Many of the security services ordered in 2018 fall within the area of security monitoring and analysis. These were consultations, implementation and delivery of relevant tools. The area of penetration testing services recorded the sharpest growth. More and more organizations seem to be interested in evaluating security resilience of their information and communication systems in a practical manner. It is of note that results of penetration tests usually show that there is a “room for improvement” when it comes to security.
The chart below summarizes the current (1Q 2019) distribution of interest in the four most popular security products of 2017 and 2018.



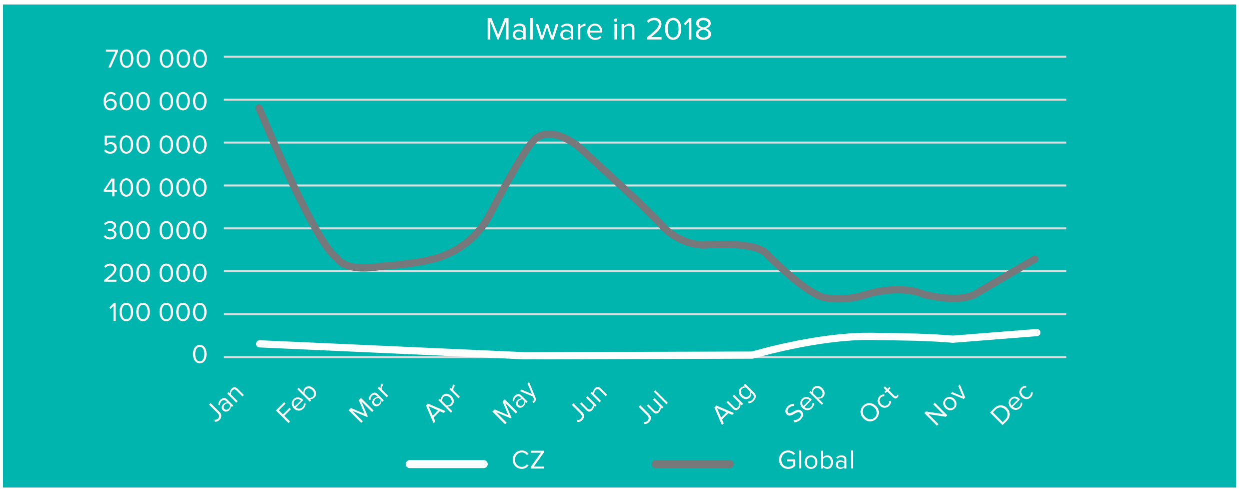
Attacks, incidents and other notable events in 2018

Jan Kopřiva

The year 2018 was undoubtedly very rich for attacks, incidents and new threats. The occurrence of both negative and positive events was not evenly distributed throughout the year and many interesting trends can therefore be observed at the global level as well as within the Czech Republic.
A more detailed analysis of specific types of attacks and notable events from the last quarter of 2018 is provided in the following two chapters. In this section, however, we will first focus on specific trends from the entire year 2018.
The data used in this part of the report comes from the PROKI system, operated by the national security team of the Czech Republic, CSIRT.CZ, the Warden system, operated by the CESNET-CERTS security team, and from various security and analytical tools operated and maintained by ALEF Groups' specialists within the infrastructure of ALEF and its customers. We would like to, once again, thank both of the security teams mentioned above for providing us with the data from their systems.

Malicious code

Malware is rightly considered one of the greatest current cyber threats. Although it was possible to observe a significant decrease in the use of ransomware in 2018 (predominantly in favor of spreading cryptomining / cryptojacking malicious code), it does not mean that this threat is no longer relevant. New types of crypto ransomware, as well as many other types of malicious code, have accompanied us throughout 2018 and allowing even one infected machine in an organizational network could have meant potential unavailability of critical services, loss of all data on network drives or a significant information breach.
According to available data, the most active month for malware detections in 2018 was January with nearly 578,000 identified malware-related detections worldwide. In the next few months, there was a noticeable decrease in global detections, with the data for the Czech Republic copying this trend.
In May, which – from the global point of view – was the richest month on malicious code detections after January, the Czech Republic registered the lowest number of detections of the whole year. After that, a gradual decrease in detections was noticeable until September globally, with gradual increase in detections on the domestic scene. Although it cannot be ruled out that these differences in data, related to global trends and the situation in the Czech Republic, were caused only by the limited number of monitored systems, their presence is interesting to say at least.
From the month of September to the end of the year 2018, the domestic situation followed a global trend, with the number of malicious code detections staying leveled until the end of November and increasing slightly during December. It is worth mentioning that, according to the available data, December was the richest month of the year for malware detections in the Czech Republic, with more than 52,000 detections logged.



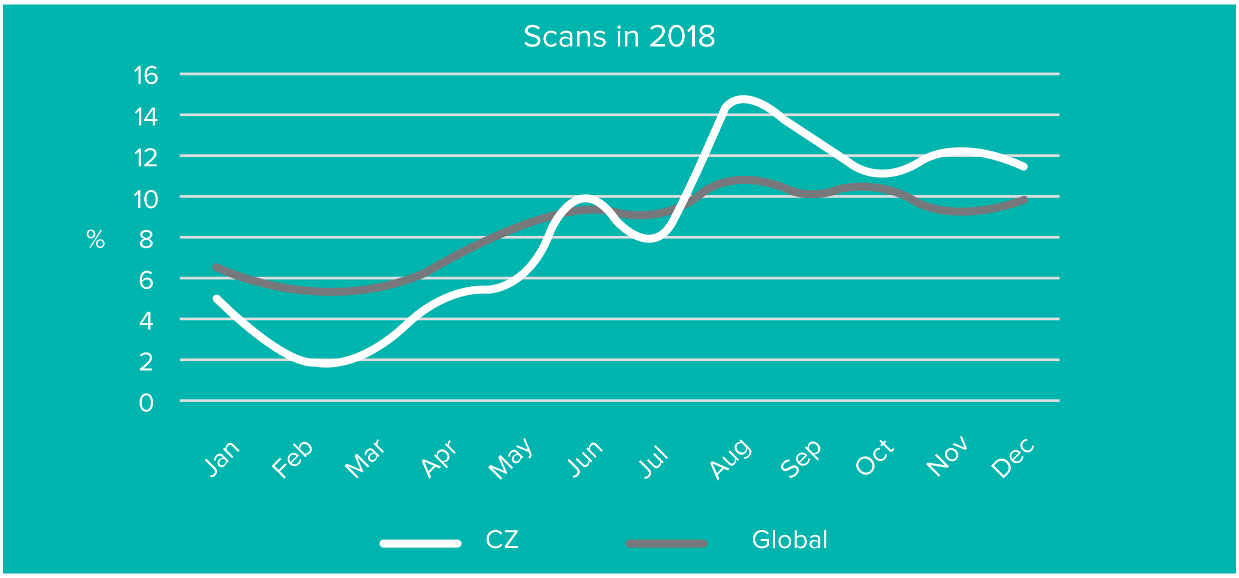
Scans

Almost every system, which is accessible from the Internet, is "scanned" by various automated tools several times every day. Many of these scans are completely legitimate, or at least done without any malicious intent. Most of them are, however, used by attackers to find vulnerable or poorly protected systems. Scans performed by automated tools have a variety of forms – from detection of open ports and running services to identifying vulnerabilities in web applications.

Due to the huge difference between the number of scans detected for the global and Czech environment, it is meaningless to compare these values directly. Comparison of percentages of detected scans in individual months can however be significantly more meaningful.

Data from tracking scans worldwide shows a slight drop in their first quarter detections, followed by a slow increase in their numbers until August when the number of detected scans reached its peak. From then on, until November, when there was a slight drop in detected scans (followed by another increase in December), the numbers remained very high.

Data for the Czech environment from the first 9 months of the year follow the trends described above, although both the initial fall and the subsequent increase in detections are significantly more pronounced. An interesting fact is that in the last quarter the situation in the Czech Republic was completely contrary to the global trend, i.e. there was a slight drop in the number of scans detected in October, increase in November and – again – a slight decline in December.



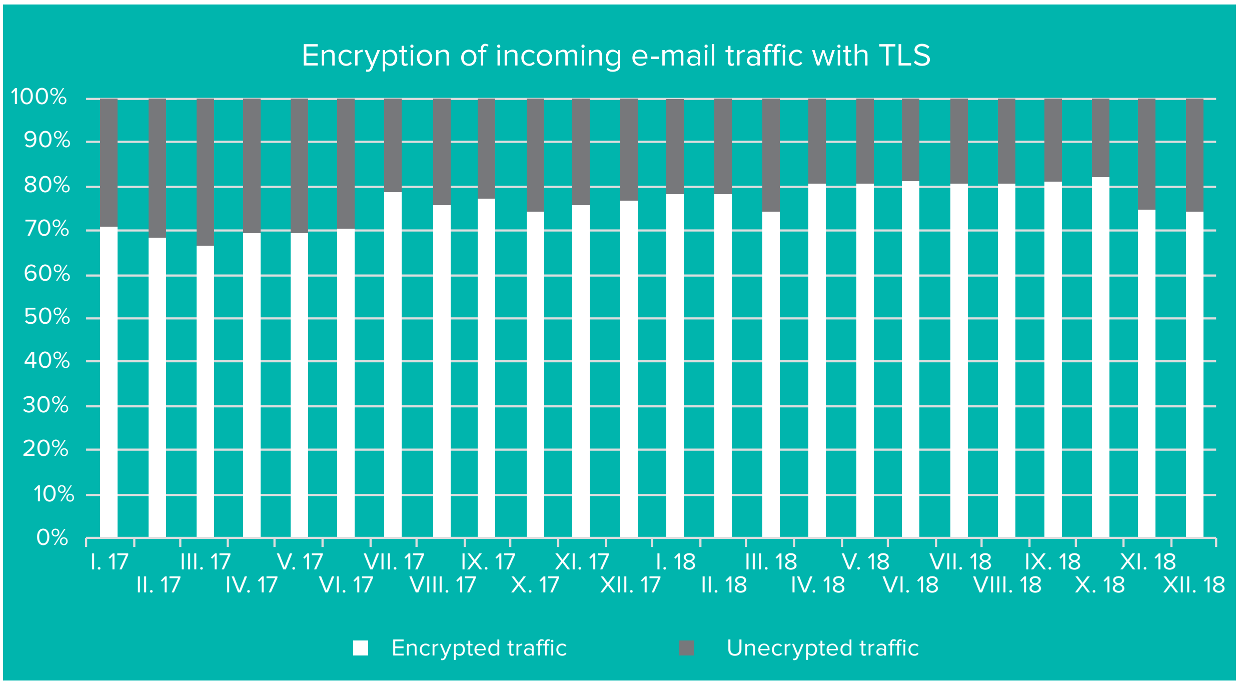
E-mail

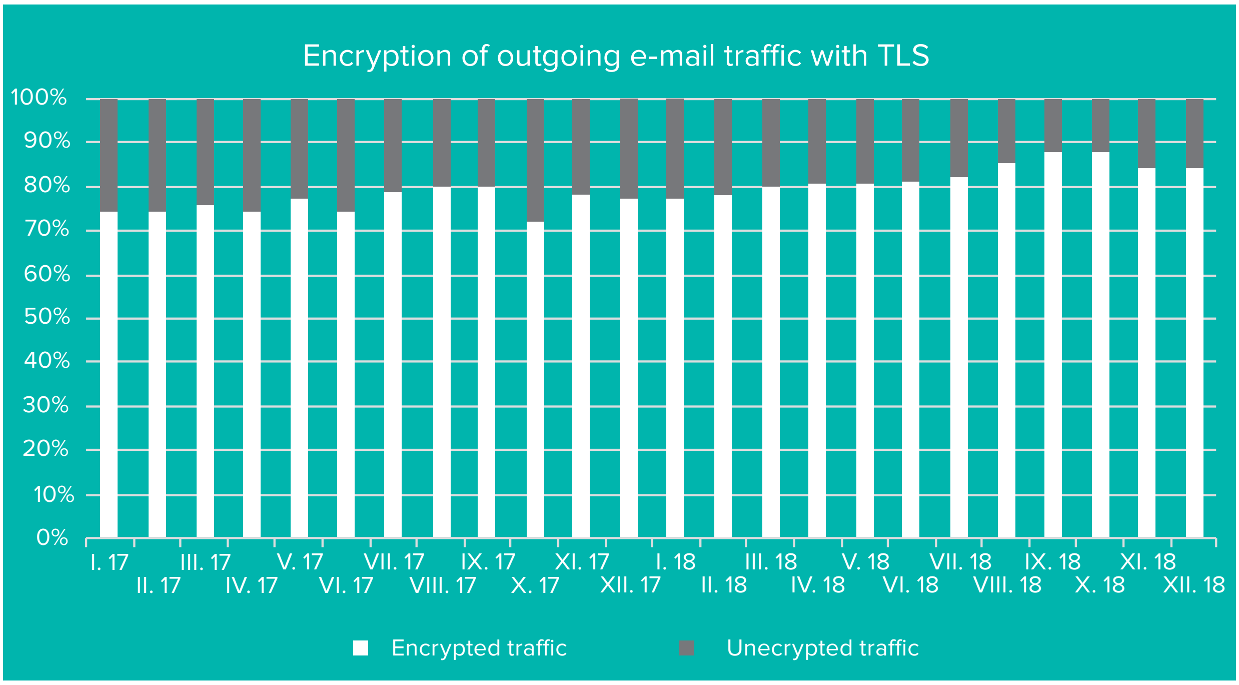
Spam, phishing, and other e-mail threats are covered in the following chapter. It would however be interesting to look at least at one area of e-mail security in our discussion of long-term trends. Namely the use of TLS protocol to encrypt message transmissions between servers.

In addition to end-to-end encryption (S/MIME or PGP), which secures communication between a sender and a receiver of the message, an encryption of communication between e-mail servers using the STARTTLS mechanism (or rather the TLS protocol) is often used to protect contents of e mail messages.

While simply encrypting the channel, that the servers communicate through, does not offer the same level of protection for data as does a user-encrypted e-mail (only data transmitted between the servers is protected – an e-mail stored in a mailbox or data transmitted between a server and a user are not), it has one undeniable advantage. From the users' point of view, it is completely transparent. Additionally, the encryption is applied opportunistically whenever possible, i.e. if encryption is supported by both the sending and receiving server, their communication (including the transmitted e-mail) will be secured.

Not all e-mail servers support this opportunistic encryption, but the number of those that do grows every year. This also proportionately increases the number of e-mails, which are automatically encrypted when they are transferred between servers. This trend is evident in the data available for the CZ for the past two years, as is shown in the following charts. Based on available data, on average 72.8% of incoming and 76.7% of outgoing e-mails were encrypted using TLS in 2017, while 78.9% of incoming and 82.6% of outgoing messages were encrypted using TLS in 2018.





CSIRT.CZ

cesnet certs

Analysis of data from e-mail gateways

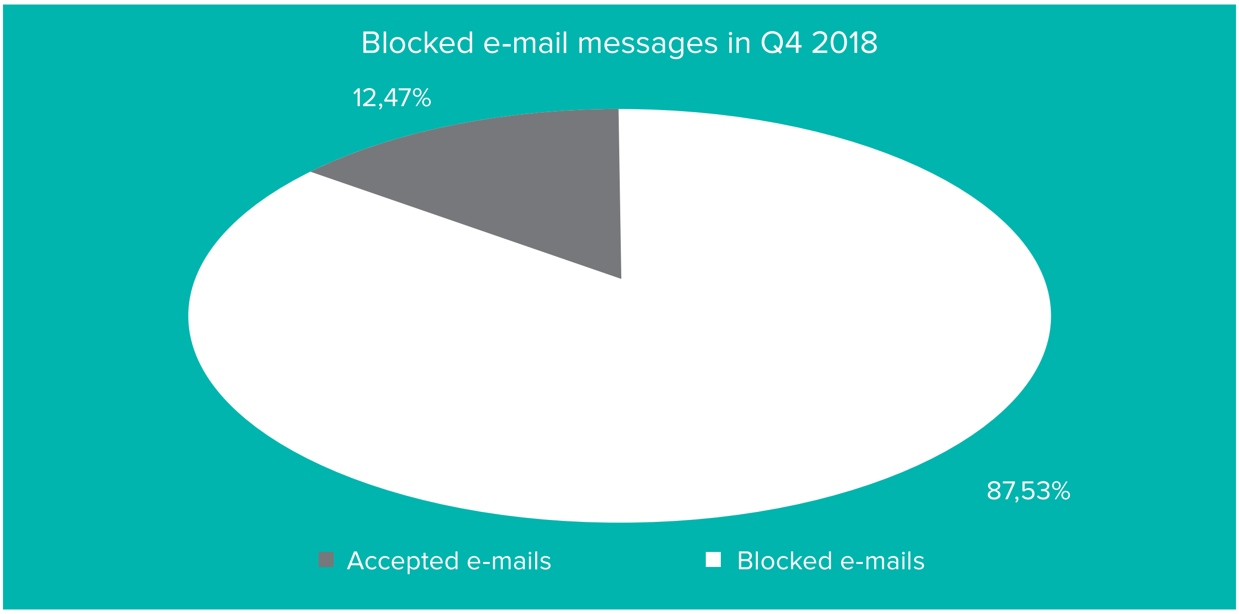
Milan Habrcetl

This part of the report discusses results of our analysis of data obtained from e-mail gateways of ALEF Nula and other organizations from the last three months of 2018. The total number of e-mail messages processed by these gateways in the monitored timespan was greater than 31 million.

In the last quarter of 2018, most e-mails that were processed in the monitored e-mail gateways were blocked. Of the nearly 31 million e-mail messages, more than 87 percent have been blocked.

Analysis of reasons for blocking e-mail messages

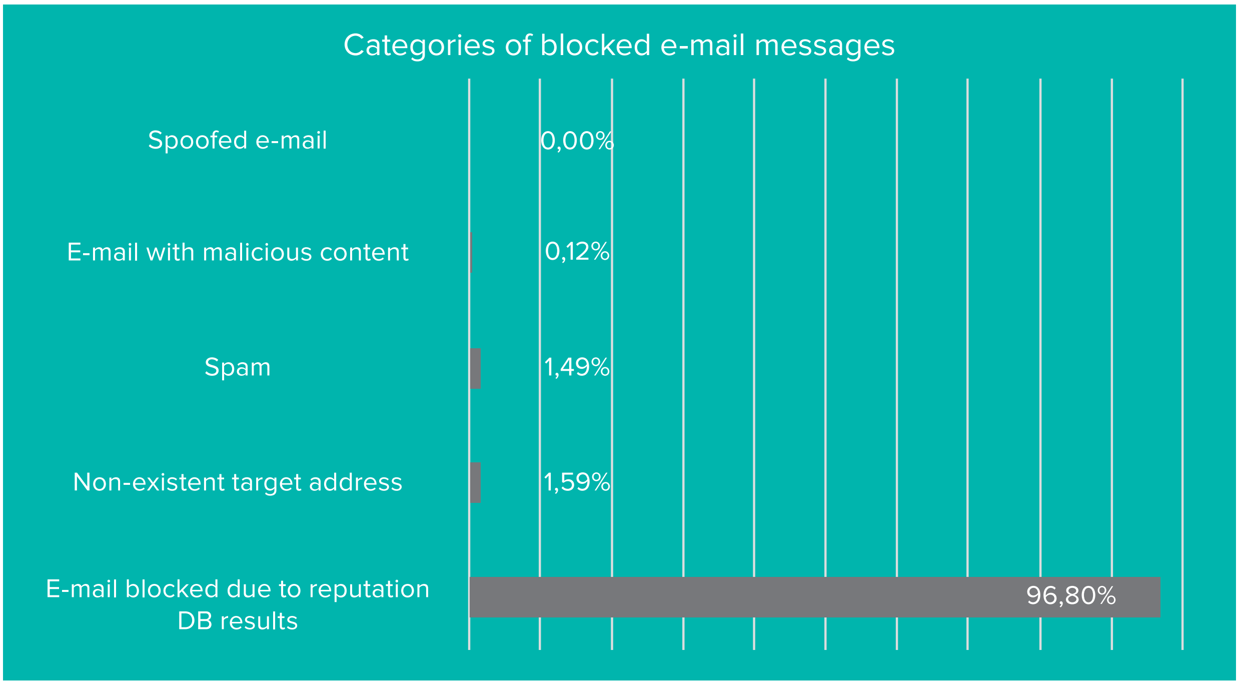
When analyzing the reasons for blocking e-mail messages on the monitored e-mail gateways, we have found that almost all rejected e-mail messages were blocked based on information, which is retrieved from reputation databases, about the servers from which the e-mail messages arrived. In a reputation database, servers are assigned a score, and if the score is low or negative, communication from the corresponding server is blocked.



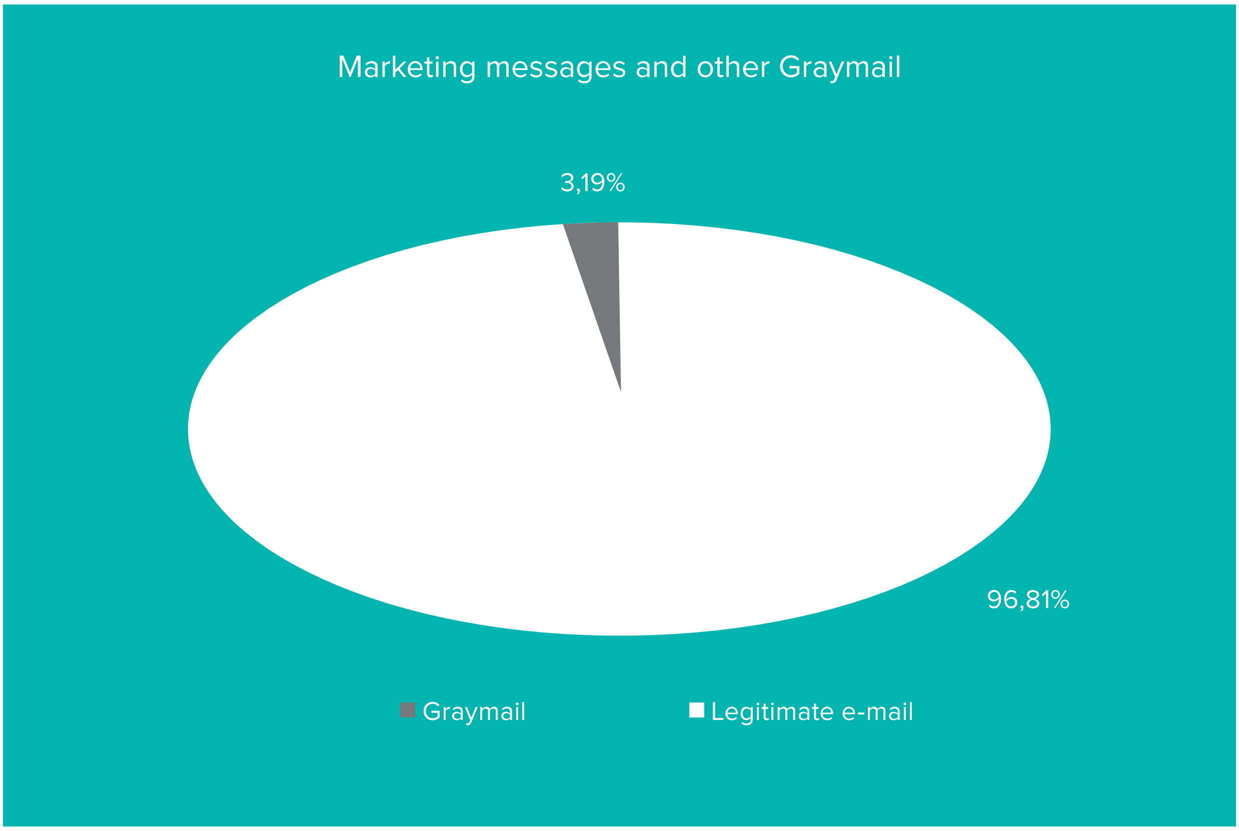
Some e-mail messages have been blocked because e-mail address of recipients did not exist – most often, this was due to typos in the address of the receiver. In other cases, these blocks were due to the use of an e-mail address, which existed in the past but was deleted since then.

Other e-mail messages have been blocked because they have been classified as spam or carried some sort of malicious content. Most of the blocked e-mail messages with malicious content contained a URL address that pointed to a malicious websites. The rest of the blocked messages with malicious content contained an attachment with malicious code.

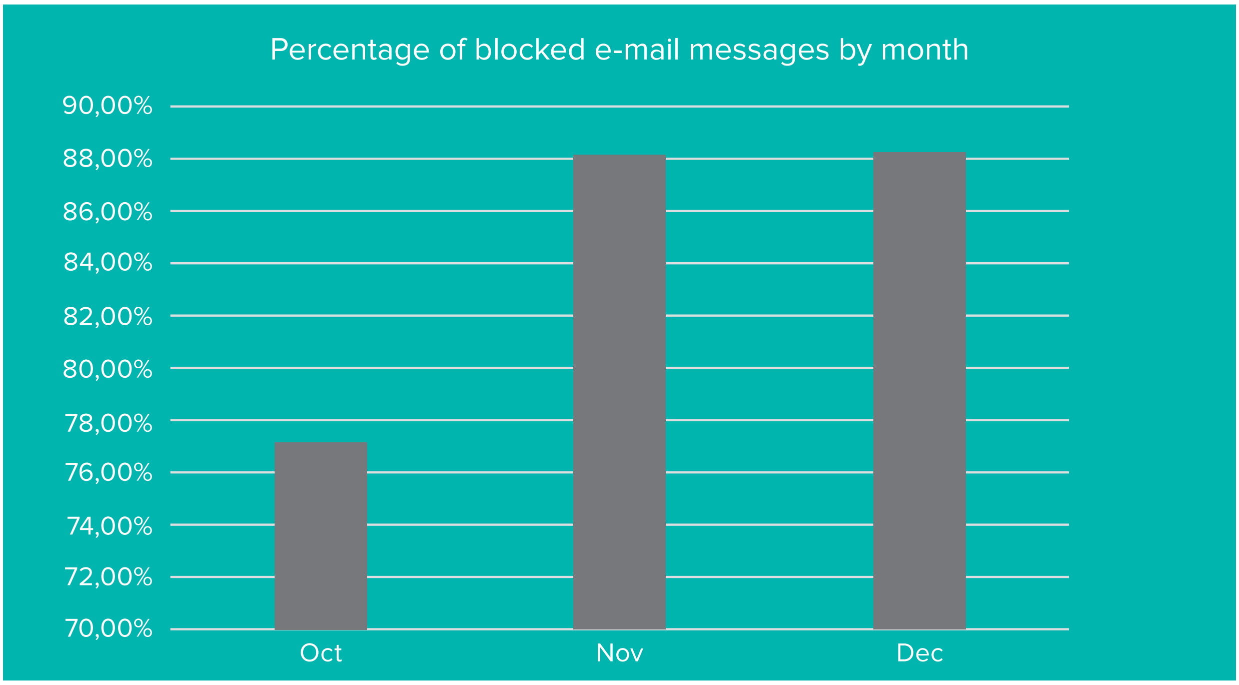
Although the adoption of DMARC (Domain-Based Message Authentication, Reporting and Conformance), an authentication mechanism for outgoing e-mail messages, is still increasing, no e-mail has been blocked based on it during the period in question.



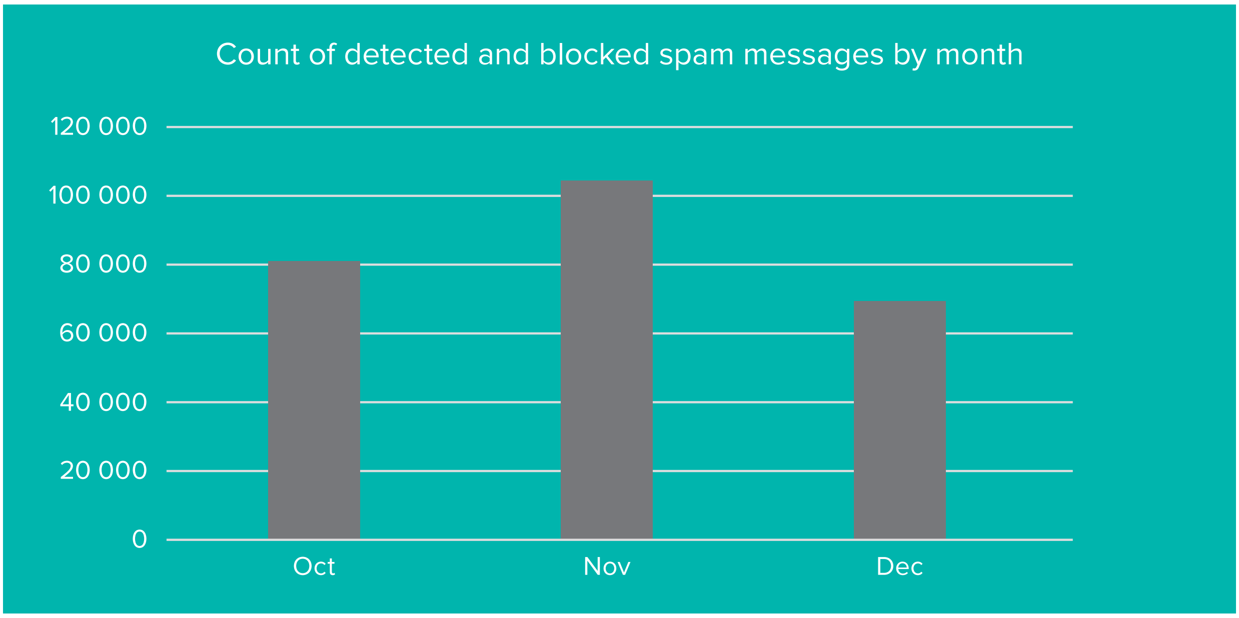
Typically, e-mail gateways are configured to mark marketing content or social networking messages in a certain way. These types of e-mail messages are commonly referred to as “Graymail” because some users consider them spam, but for others they are completely legitimate. Since it is not possible to determine automatically whether they are undesired e-mails, these messages are usually not blocked out of hand, but only marked in certain way. For example by inserting “[Marketing]” in the subject line of the e-mail message. The e-mail messages marked in this way accounted for more than 3 percent of all unblocked e-mails in our sample.



Increase of attacks during the holiday season
As Christmas preparations begin in the last months of the year, attackers use this period to increase their chances of getting sensitive information or money from users by sending out e-mail messages that offer cheap merchandise and contain links to fraudulent sites. During this time, attackers also step up phishing attacks on organizations and try to take advantage of the increased inattention of users during the holidays. Thus, the chart below shows a large increase in blocked e-mails starting in November, when holiday preparations and gift shopping are underway, and continuing to the end of the year.



A large increase in spam messages was also detected in November, followed by a significant decrease in December. This may be due to the addition of newly discovered spam sending servers to reputation databases and subsequent blocking of e-mail messages from these servers based on reputation database scores rather than spam blacklists.

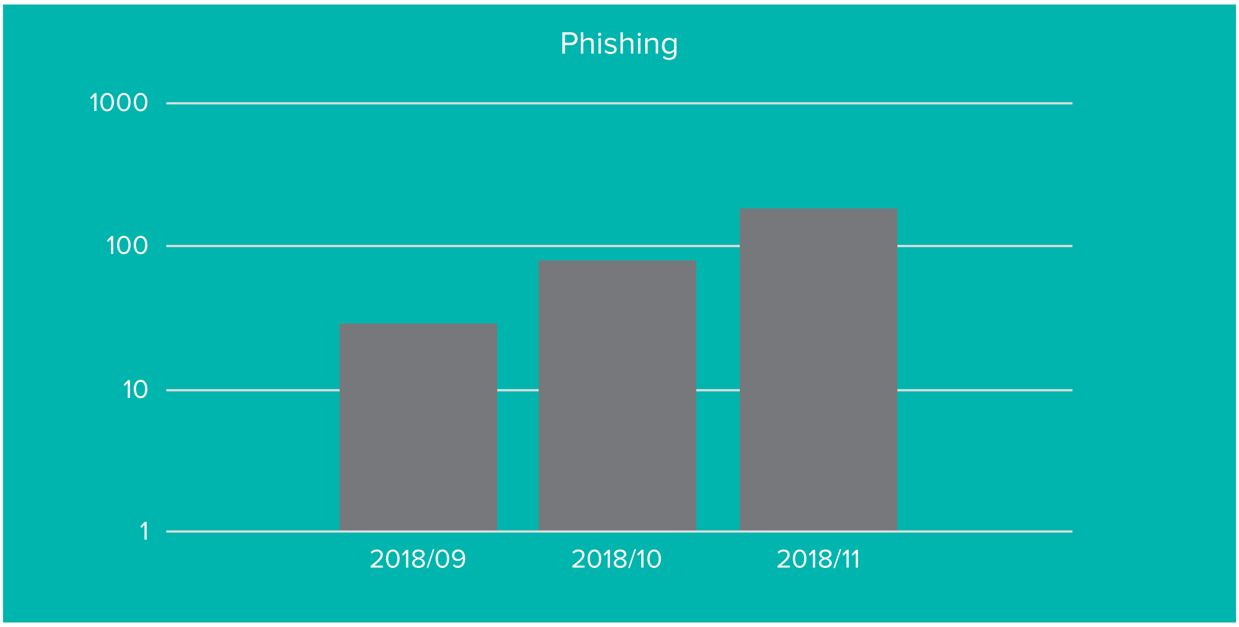


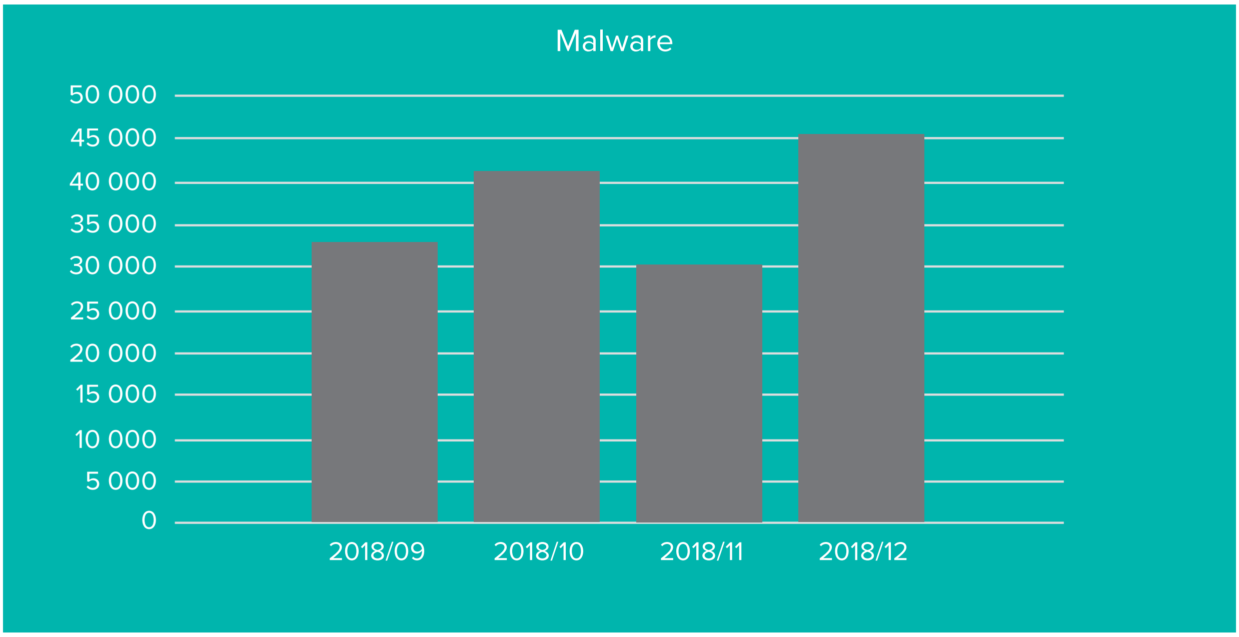
Analysis of data from IPS - Q4 2018

Stanislav Techlovský

This part of the report discusses result of our analysis of data from IPS systems and monitoring sensors deployed within our own infrastructure and infrastructures of our clients. The analysis will focus on data from the last four months of 2018.

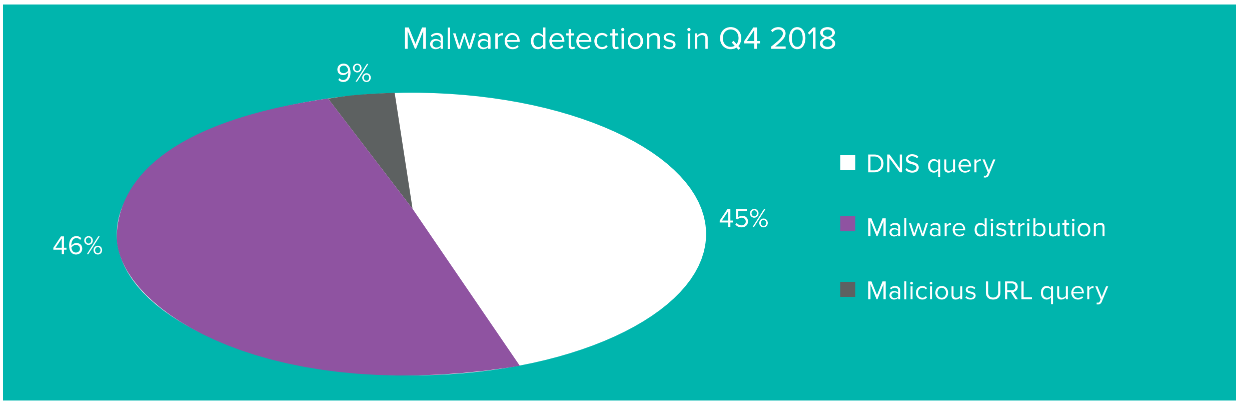
In the first part of the analysis, we will take a closer look at phishing, which has been increasing from September up to the end of a year. Intrusion prevention systems detect phishing-related events whenever a user tries to visit blocked phishing sites, thus the data refers to fluctuations in user vigilance towards the end of the year, rather than the number of fraudulent messages sent out by threat actors.





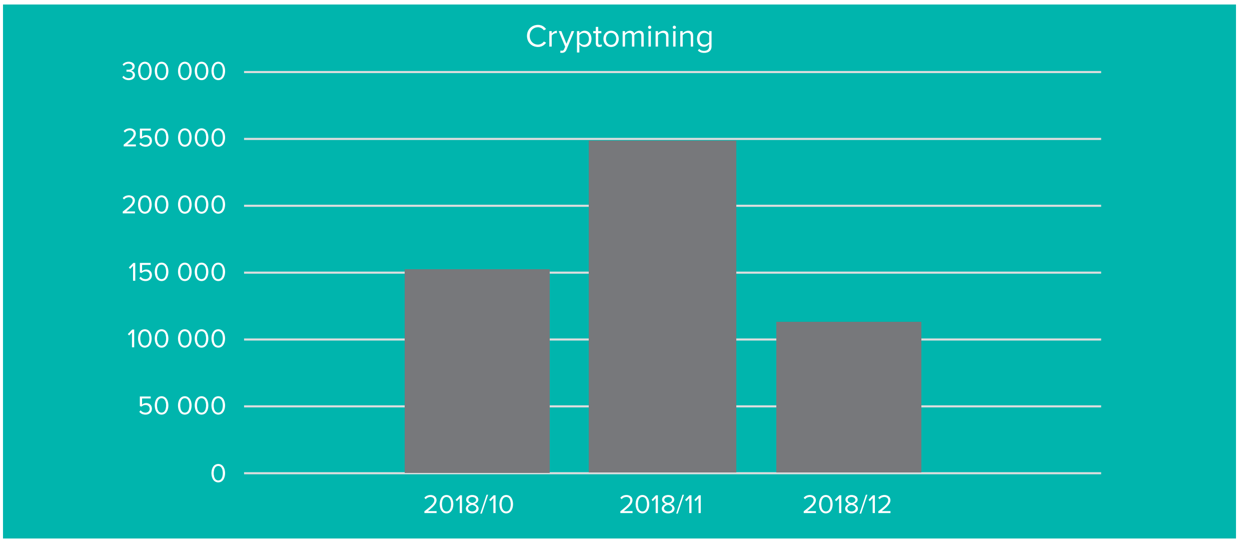
In the fourth quarter of 2018, malware detections were highest in December, when the total number of logged events exceeded 45,000, which was an increase of 47% over the previous month.

IPS probes and tools used to collect this data divide malicious code detection into three basic categories. In the malware distribution category, there are events in which communication with IP address contained within the IPS reputation database has been detected. The database contains IP addresses of machines, which were/ are used for spreading malware, and these records are used to check the source and destination IP address of any communication. The Malicious URL query category contains attempts to access URLs, where malware has been detected. Detection of such attempts is performed by probes, which inspect web traffic (HTTP or HTTPS). The last category is DNS query. In this category are logged attempts at communication with domains, which are used to spread malicious code based on a reputation database check. Thus, DNS queries for domains used by malware to spread are detected. The structure of detections of malicious code during the last quarter of 2018 is summarized in the following chart.



One of the major trends in 2018 was an increasing interest of attackers in mining cryptocurrencies with the help of their victims' machines. Therefore, it is not surprising that the number of detections associated with unwanted cryptomining was very high in the last quarter of 2018.

Events in the "Cryptomining" category were detected by IPS probes, using a reputation database of IP addresses used in cryptomining attacks. The protection mechanisms are also able to detect and analyze downloads of relevant binary data or use of specific web clients, mining protocols, and communication with domains on blacklists, based on interception of SSL / TLS certificates. The highest number of cryptomining attempts was detected in November 2018 with a more than 245,000 attempts detected. Compared to the previous month, this was a 63% increase. In December, cryptomining attempts decreased by 54% over the previous month.



Trends in security education

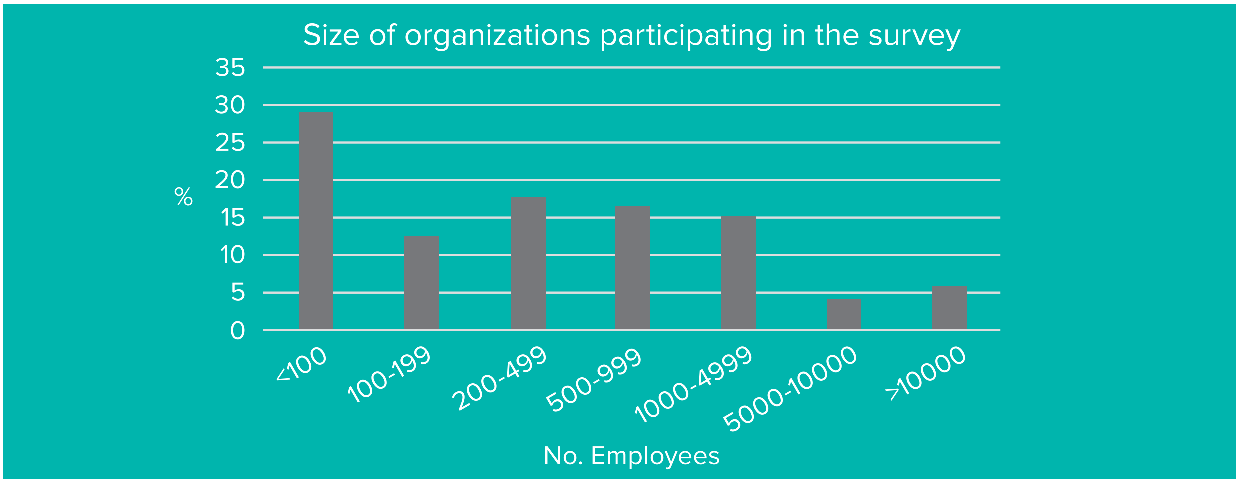
Jan Kopřiva

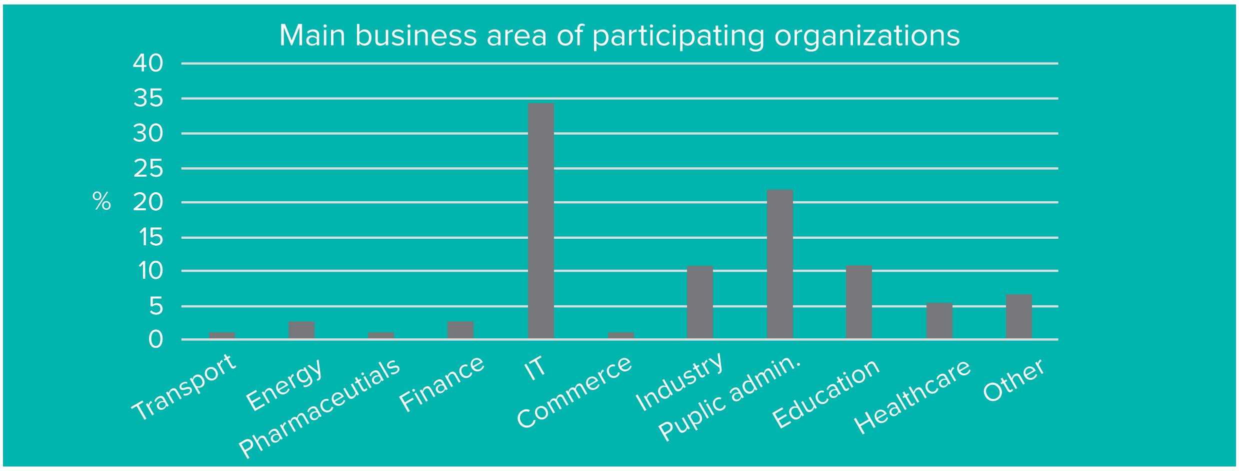
It is a well-known fact that in most cases, human factor is the weakest link in the proverbial security chain. Both IT and security specialists often lack deeper understanding of current threats, making them unable to protect their organizations effectively, and ordinary users often click without forethought on any link in e-mails that lands in their inbox.

On the other hand, a second generally accepted fact is that a human has the potential to be the most effective security mechanism. Users who are familiar with the techniques traditionally used to create phishing emails are generally able to quickly identify fraudulent messages, and well-trained technical specialists can effectively analyze circumstances of security incidents and implement appropriate measures in response to them.

Increasing security awareness and relevant professional competencies in employees is therefore a priority for many organizations. Although their aim is the same, the focus of educational programs as well as their scopes can differ significantly between different organizations.

In order to be able to analyze trends in this area in the Czech Republic in more detail, than just in very general terms, ALEF CSIRT together with the ALEF TRAINING department conducted a survey focusing on educational programs and activities implemented or planned by domestic organizations in January 2019. Representatives of 73 organizations of various sizes and operating in different fields participated in the survey, as the following charts show.

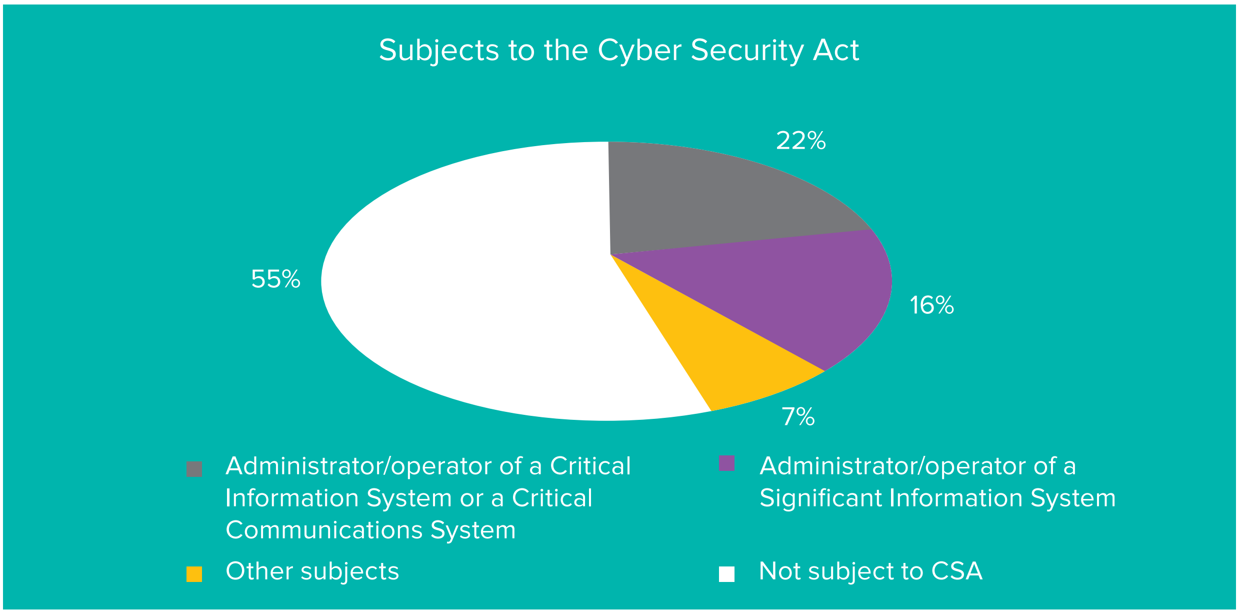




For the sake of completeness, it should be noted that 45% of surveyed organizations were subject to the requirements of the Cyber Security Act.

Planned changes

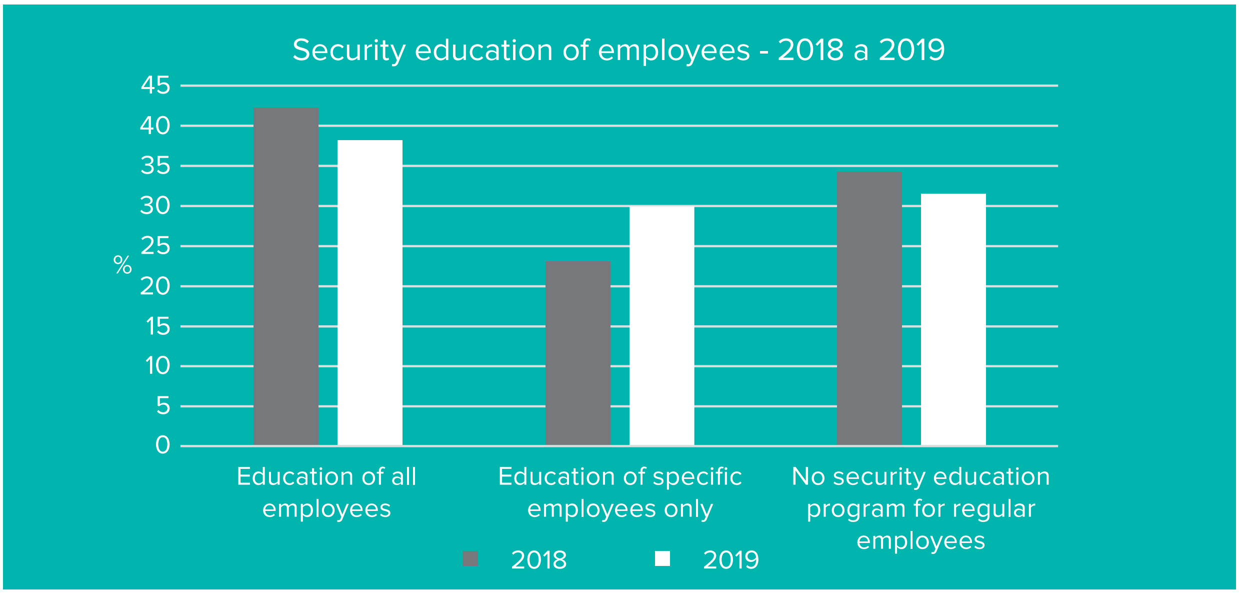
In the survey, respondents commented on the implemented security training programs in their organizations in 2018 and on any planned educational activities for 2019.



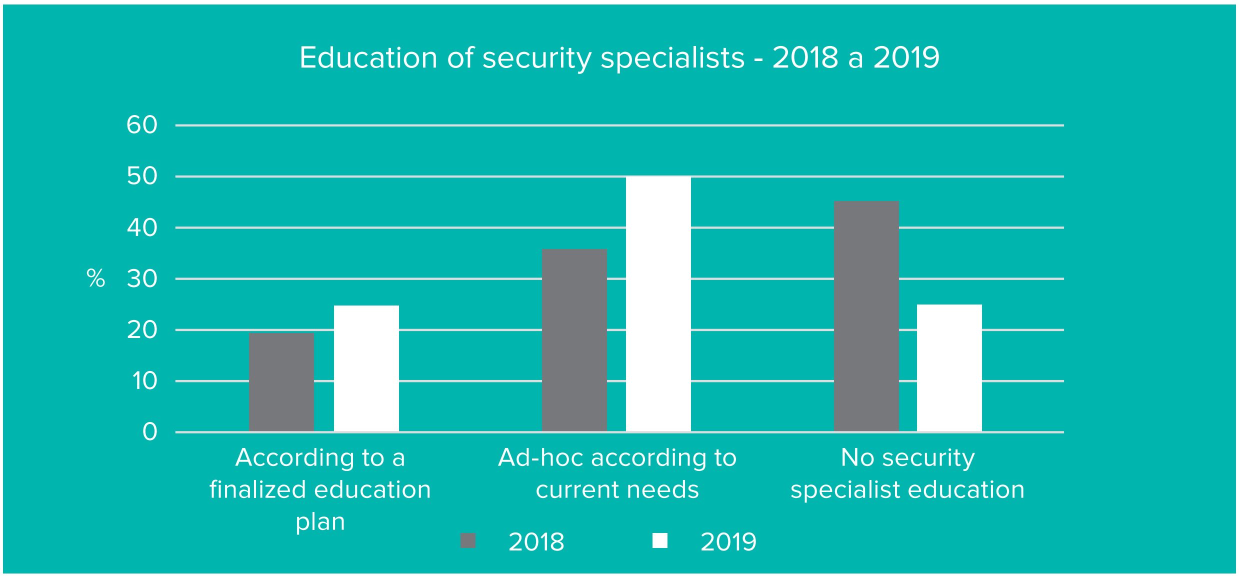
Despite the limited sample size, based on the answers obtained in the survey, trends in the Czech Republic seem to follow a global trend as increasing number of organizations is introducing at least some form of security education for ordinary employees and professional security specialists.

As is shown in the following chart, less than 66% of the organizations provided some form of employee security education in 2018, while almost 68.5% of them planned to actively educate at least some of their employees in 2019.

In addition to the aforementioned general positive trend, the chart also suggests a slight shift away from general education of all employees in favor of training only specific employees in 2019. Although this trend cannot be considered as representative for the situation in the Czech Republic due to the limited size of the sample available to us, its presence in the obtained data is certainly interesting.

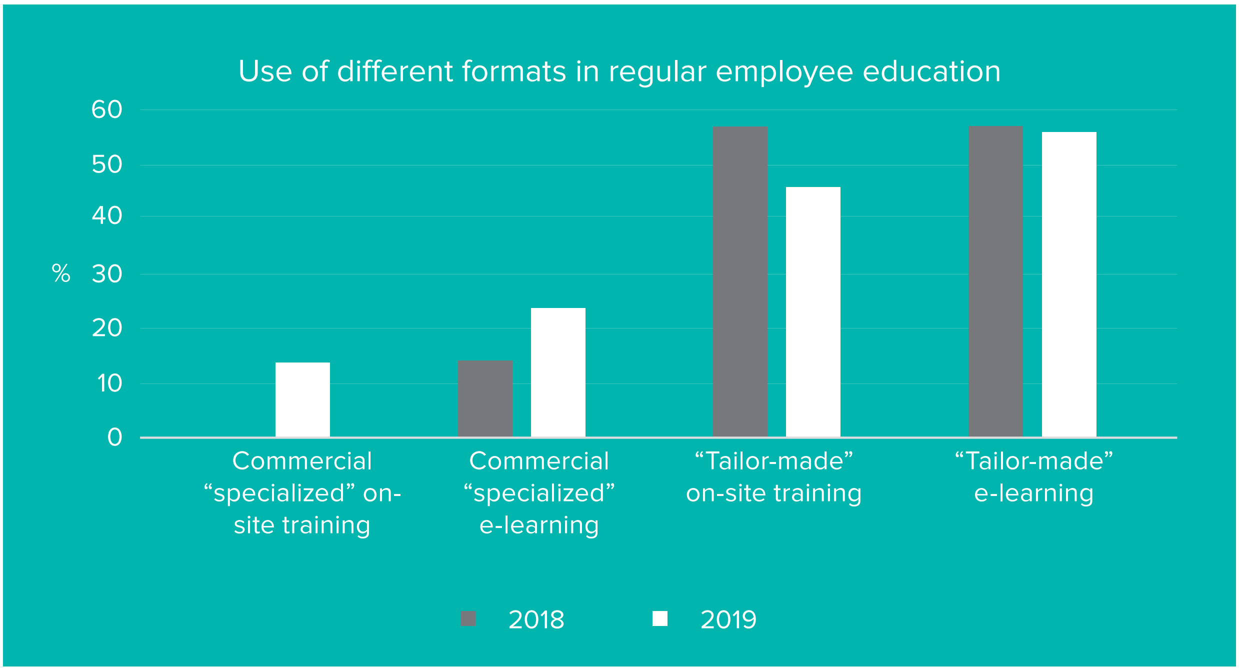


An even more positive trend than in the education of regular employees is evident in the data on education of security specialists (i.e. cyber security managers and architects and other infosec-oriented employees). While, according to respondents, only a little under 55% of companies educated their security specialists in 2018, in 2019, full 75% of organizations surveyed planned to do so.

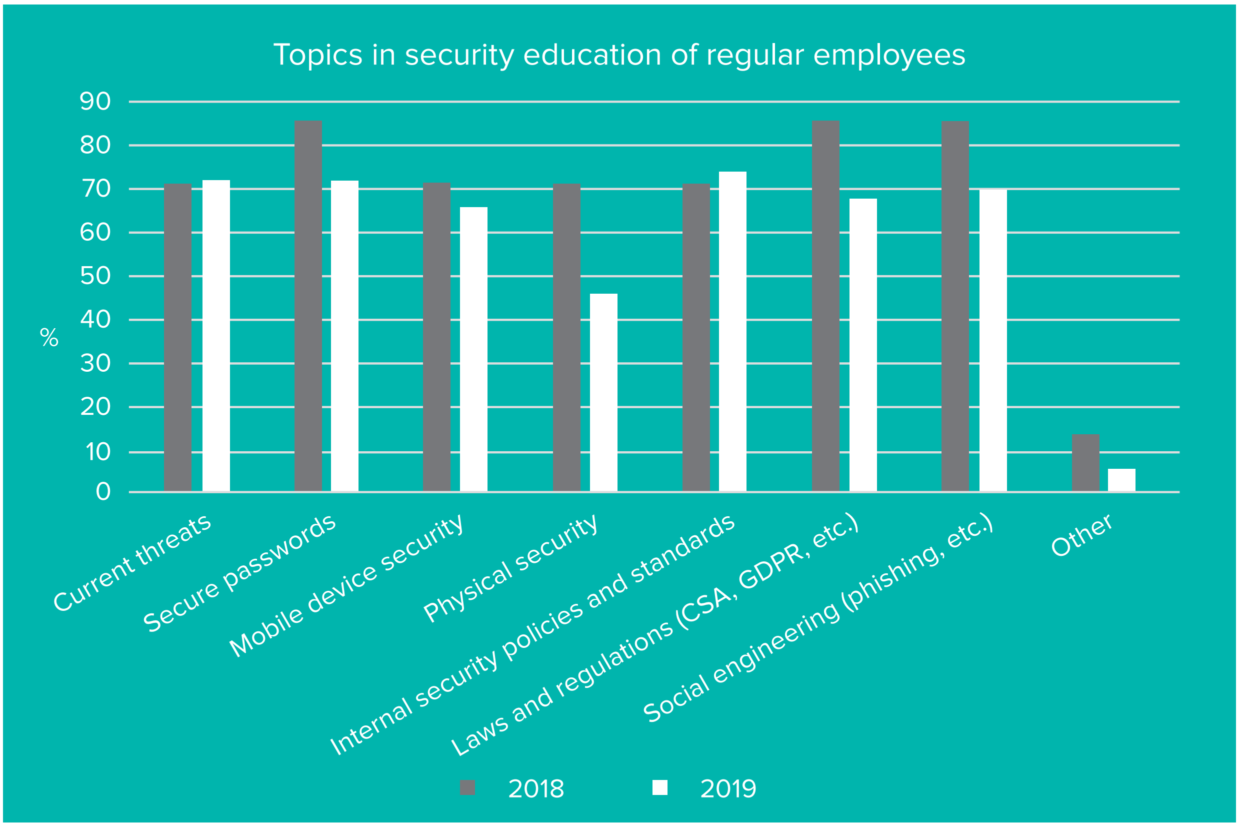


Employee Education

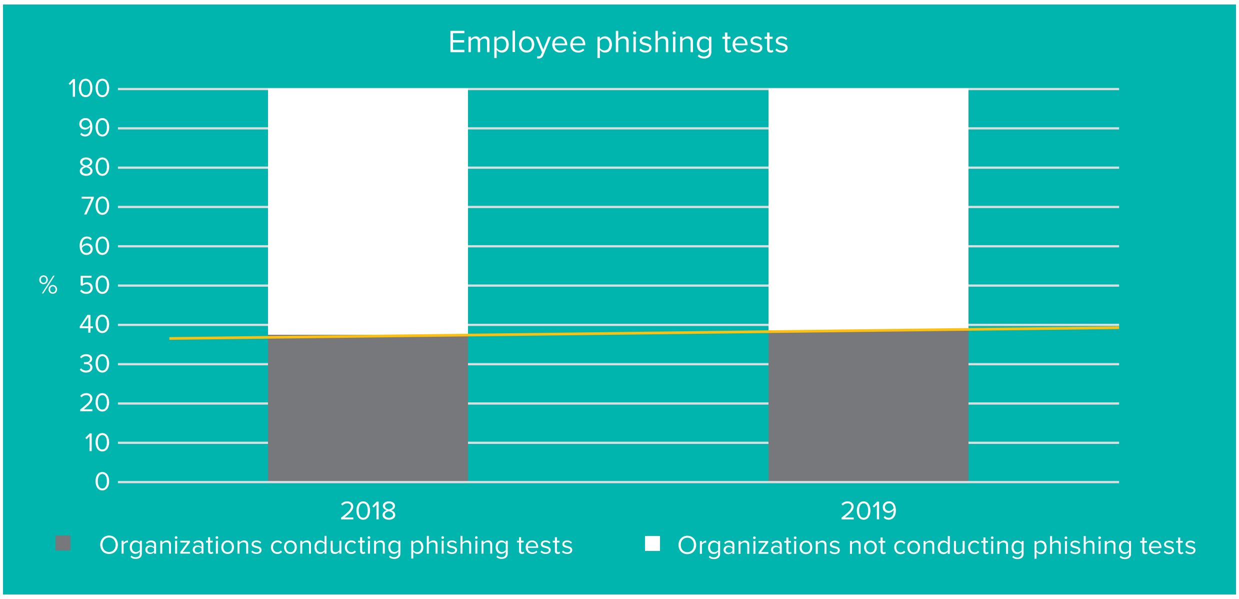
Perhaps the biggest change planned by organizations for 2019 in the area of general security employee education seems to be an increase in the use of standardized commercial trainings, both in the form of on-site courses and e-learning. In most cases, the wider use of standardized courses was to be implemented at the expense of tailor-made training (mostly in-house tailor-made training). In spite of this shift towards standardized security courses, trainings created according to the specific needs of particular organizations will remain the dominant form of employee education in 2019. 46% of organizations are planning to use tailor-made courses in their on-site trainings and 56% in e-learning format in 2019.



The second interesting trend in general employee education for 2019 seems to be focus on a narrower scope, which will cover only areas critical to the organization. This trend is most evident in physical security. In 2018, physical security was part of 71% of educational programs, while it is expected to be a part of only 46% of them in 2019.



It is worth noting that the number of organizations, which use phishing tests as a tool for verification of the effectiveness of their security awareness programs, will probably not increase significantly in 2019 compared to the previous year. 37.5% of organizations conducted phishing tests in 2018, according to the survey, and in 2019 a little under 39% of organizations plan to conduct such tests.

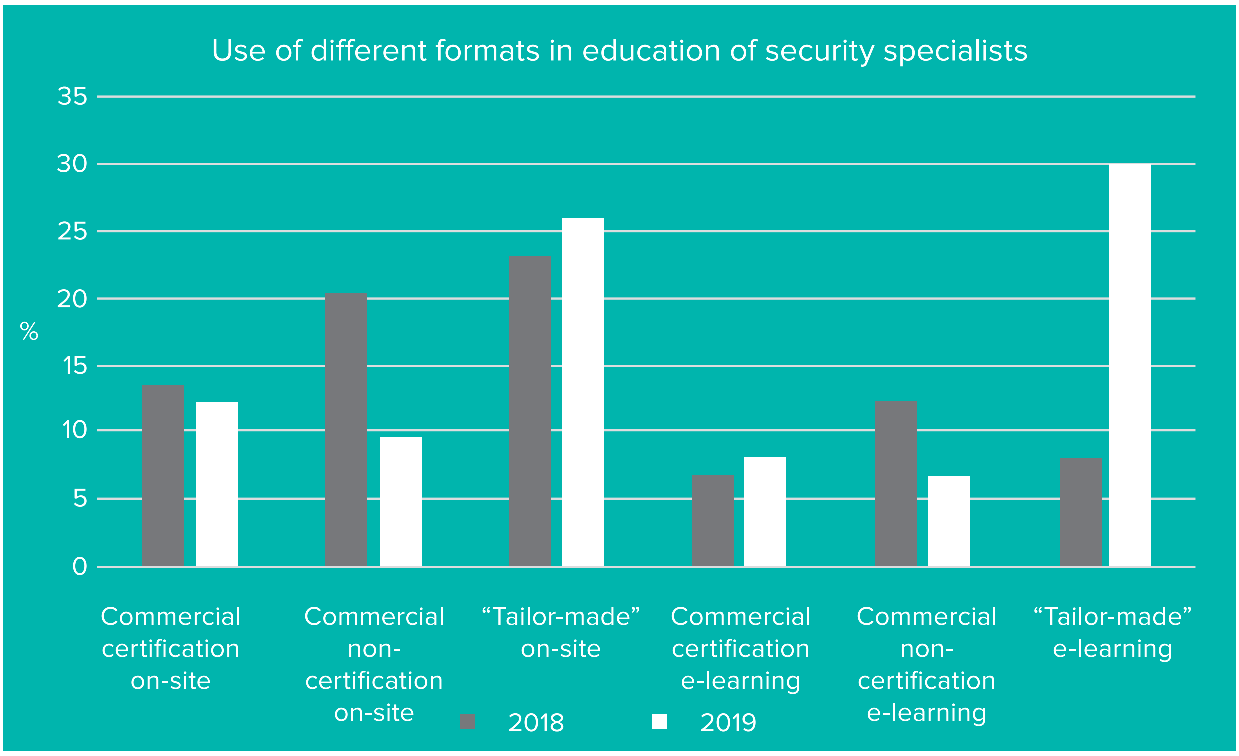


Training of security professionals

As is mentioned above, according to the results of the survey, three out of four organizations were planning to educate their security specialists in 2019. This is a 55% increase over the previous year.

The main tool for security specialist education, which most organizations planned to employ in 2019, were tailor-made courses in both e-learning (30% of organizations) and on-site formats (26% of organizations).

Apart from the extremely large increase in interest in 'tailor-made' e-learning courses, the most noticeable differences between 2018 and 2019 may be seen in reduced interest in non certification training in both the on-site and e-learning courses.

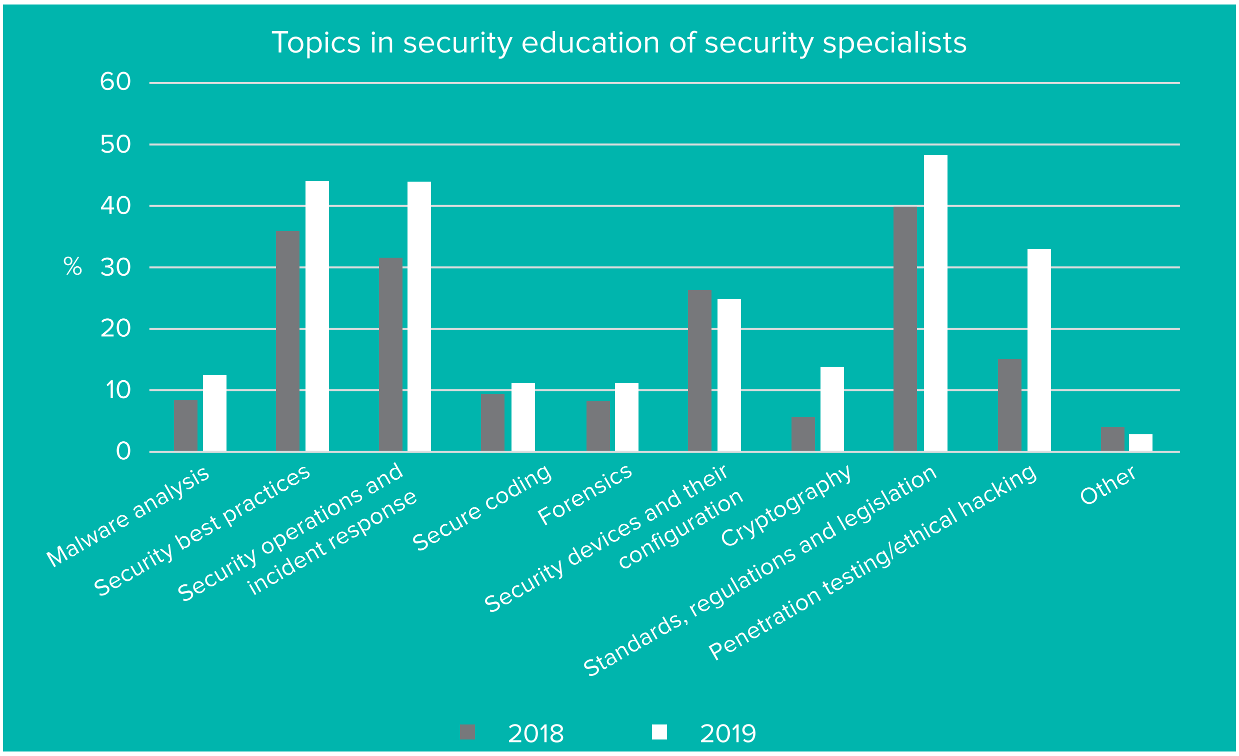


Unlike with general employee education, which will be – according to the survey – more limited in scope in 2019 in many organizations, education of security specialists should be much wider in its scope.

The highest interest in specialized training for 2019 was indicated in the area of security standards, regulations and legislation. Almost 48% of organizations planned to train their specialists in this area in 2019, according to the survey.

The biggest year-over-year increases in interest seen in the survey are related to penetration testing and ethical hacking (15% of organizations educated their specialists in 2018 in this area and in 2019 almost 33% of organizations plan to do so). A large increase in interest can also be seen in the area of security operations and incident response (security specialists in 31.5% of organizations were trained in this area in 2018, while 44% of organizations plan to educate their experts in it in 2019).

The increased interest in training of internal security specialists in the areas of penetration testing and incident response is quite understandable – the reasons for it can be found in the current situation on the job market, where the lack of competent specialists in both of these areas has been noticeable for a long time.


Topics in security education of security specialists
%
60
50
40
30
20
10
0
Malware analysis
Security best practices
Security operations and incident response
Secure coding
Forensics
Security devices and their configuration
Cryptography
Standards, regulations and legislation
Penetration testing/ethical hacking
Other
2018
2019

Selected ALEF CSIRT research activities in 2018

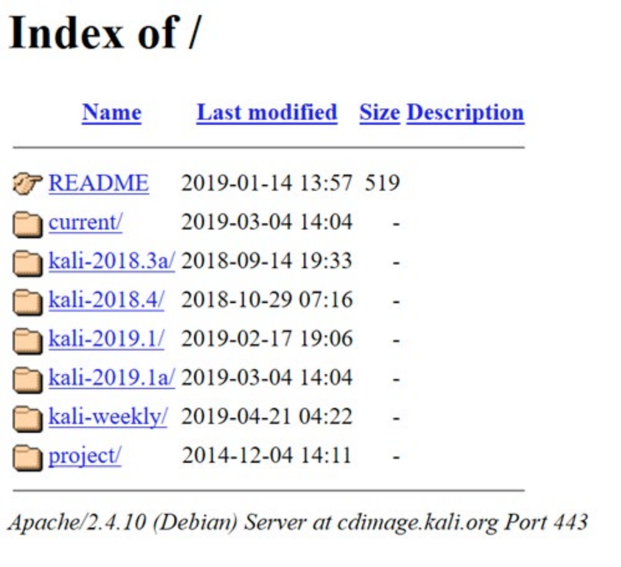
Jan Kopřiva

In 2018, ALEF CSIRT carried out – among other activities – two researches focused on the analysis of various security aspects of web servers operated within the top-level domain CZ. The goal of the first research was to identify servers containing sensitive data in freely accessible directories. The second research dealt with identification of web applications affected by open redirect vulnerabilities.

Sensitive data on the Czech web

Automatically generated directory listing pages are sometimes used by administrators as a simple way to allow users access to the contents of specific folders on a server, without the need to manually create corresponding webpages.

However, due to an administrative error or user ignorance, it is sometimes the case that sensitive personal or organizational files are made available to virtually anyone on the Internet using similar “open” directories.



Index of /

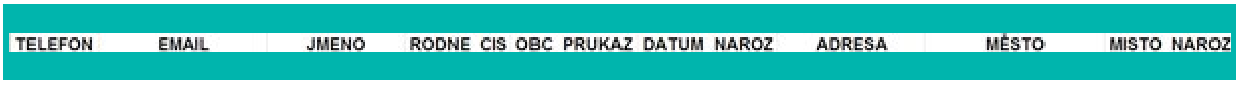
Name	Last modified	Size	Description
README	2019-01-14 13:57	519	
current/	2019-03-04 14:04	-	
kali-2018.3a/	2018-09-14 19:33	-	
kali-2018.4/	2018-10-29 07:16	-	
kali-2019.1/	2019-02-17 19:06	-	
kali-2019.1a/	2019-03-04 14:04	-	
kali-weekly/	2019-04-21 04:22	-	
project/	2014-12-04 14:11	-	

Apache/2.4.10 (Debian) Server at cdimage.kali.org Port 443

ALEF CSIRT’s specialists focused on searching for such data during the third quarter of 2018, and after analyzing the contents of several thousand open directories, they identified 159 servers in the CZ domain where sensitive files were freely accessible.

The most numerous (probably) unintentionally shared type of data found were music files. These were found at 22.6% of the 159 web servers. The second most frequently found type of data was much more problematic – personal data. Personally identifiable information (PII) could be found on 25 servers.

In many cases, these were only lists of relatively innocuous identifiers, such as e-mails and names, but several servers contained files that held a considerably wider amount of information (see the header of one of the discovered Excel tables in the following figure).



TELEFON	EMAIL	JMENO	RODNE CIS	OBC PRUKAZ	DATUM NAROZ	ADRESA	MĚSTO	MISTO NAROZ

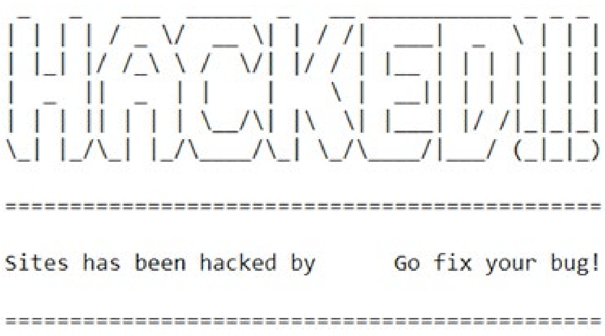
On other servers, we identified potentially not-fully-legal software (in 18.2% of cases), movies, TV series and other audiovisual content (on almost 14% of servers), e-books and audio books (in less than 7% of cases) personal photos of variously sensitive or intimate nature (less than 17% of servers) or explicit pornographic content (5% of servers).

Although files containing the data mentioned above were not shared deliberately in most cases, these cannot be considered so problematic as the aforementioned PII, or other "sensitive" information that was found on almost 16% of target servers. In this case, "sensitive" data is intended to mean files containing financial information of organizations and individuals (such as accounting records and tax returns), email communication backups or scanned personal documents – generally almost any data that is not personal information but whose publication can be unequivocally considered undesirable from the perspective of their owner.

In addition to personal data, passwords for various services and systems (found on nearly 4% of servers) and sensitive databases (accessible on 1.3% of target systems) were not included in the category of sensitive information.

Indicators of some form of malicious intrusion have also been discovered on – not insignificant – 5% of target servers.

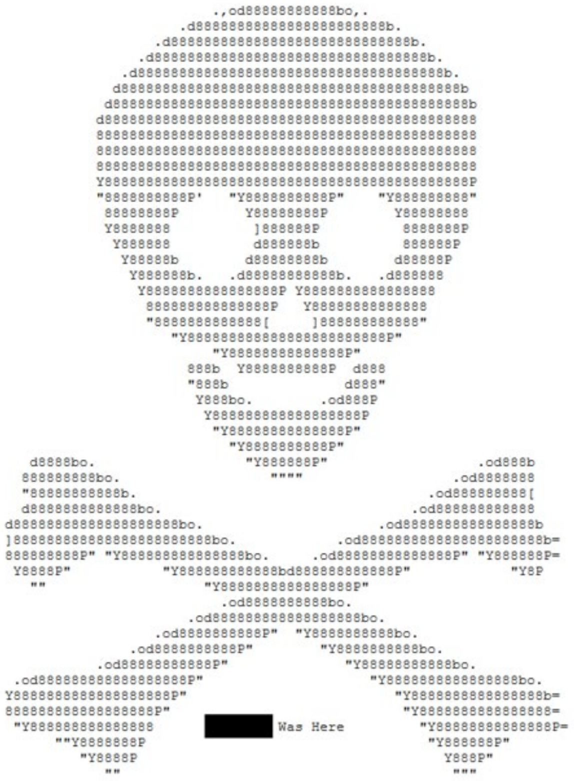
These indicators were mostly text-based or image-based "business cards" of various groups or individuals, predominantly ones trying to increase fame of their author or inform the servers' administrator about a successful "hack" of their system (see below).



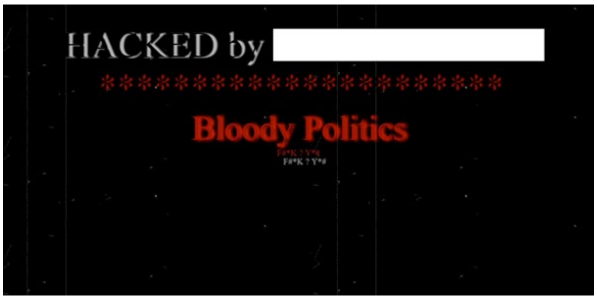
```
=============================================

Sites has been hacked by       Go fix your bug!

=============================================
```



[redacted] Was Here

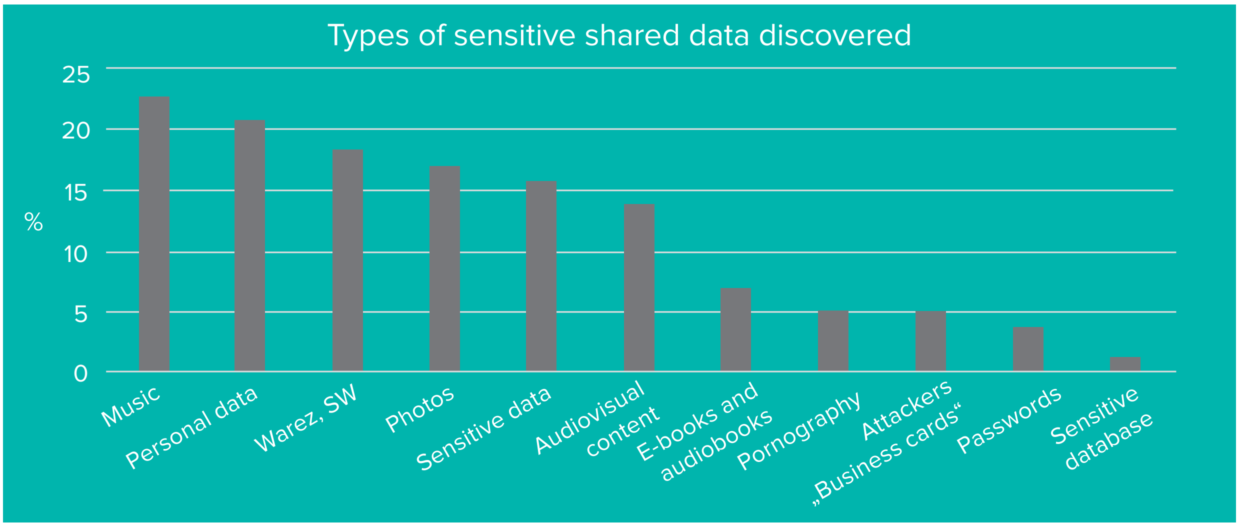


HACKED by [redacted]

****

Bloody Politics

The following chart summarizes the distribution of sensitive data found during this research. A more detailed description of the analysis – including discussion of data found on servers outside the CZ TLD – was published on Root.cz.



Open redirect on the Czech web

After the analysis of freely accessible sensitive data, ALEF CSIRT carried out another research in the last quarter of 2018. This time, the aim was to identify vulnerabilities in the Czech web.

During this research, ALEF Groups' specialists focused on searching for web applications, which allow for so-called open (or "unvalidated") redirects, within the CZ top-level domain.

Open redirect refers to a vulnerability that makes it possible to create a link to vulnerable web application, which – when opened – redirects a browser to some other URL specified by a parameter in the link.

An example that demonstrates the principle of open redirection is shown below.

hxxps://www.trustednetwork.tld/redirect?to=www.newsite.tld => https://www.newsite.tld
hxxps://www.trustednetwork.tld/redirect?to=www.newsite2.tld => https://www.newsite2.tld

The technique of redirecting users to new URLs with the help of an internal redirection script or other mechanism is often used by web application authors (especially for marketing purposes) as it allows to find out which links the site visitors click on. However, if there are no limitations on where a site may redirect a visitor, a malicious actor may create a link to this legitimate site, which will however redirect the victim to a fraudulent or malicious site. In such cases, malicious actors usually distribute these links using phishing campaigns.

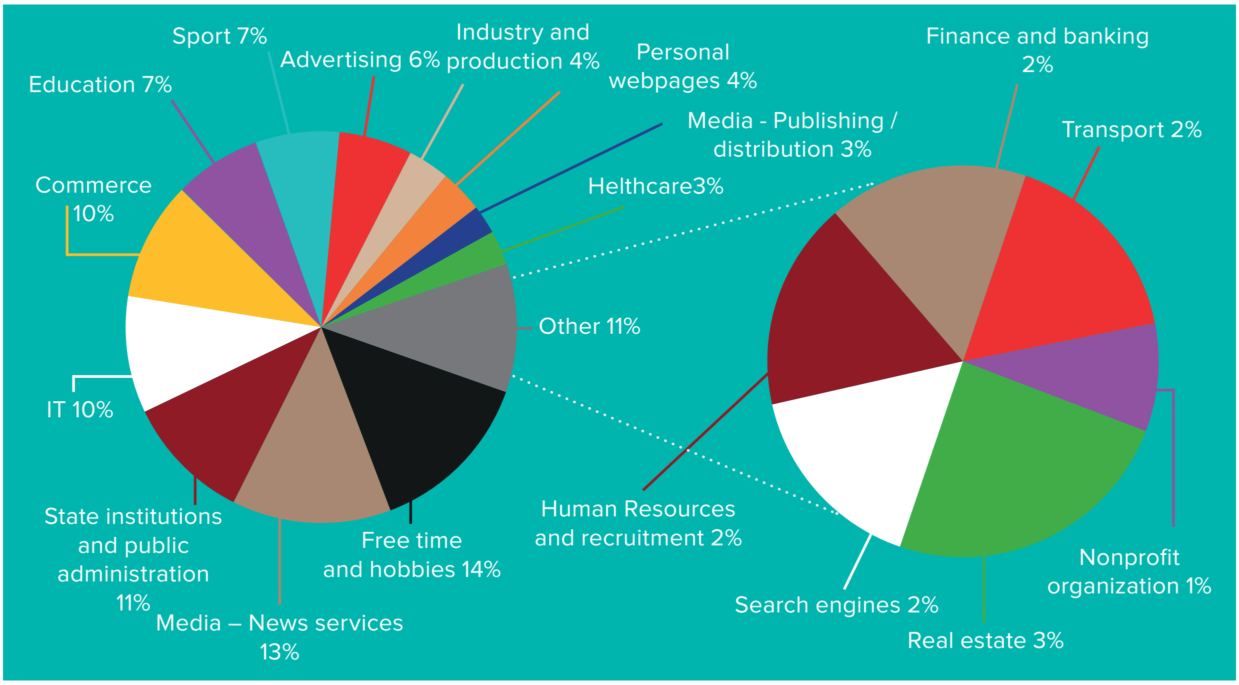
hxxps://www.trustednetwork.tld/redirect?to=www.untrustednetwork.tld => https://www.untrustednetwork.tld

Given the open redirection principle described above, it is clear that this vulnerability is not an overly big problem for most sites, but can pose a very perceptible danger to highly sensitive and trusted sites (such as sites of banks and other financial institutions) or – rather – to their users.

Within the CZ TLD, about 700 web pages, which use some redirection script or other mechanism, were examined during the research. 114 of these were vulnerable and allowed redirection to any URL.

The chart below summarizes types/focus of sites where the vulnerabilities have been discovered.

It should be noted that the vulnerabilities were identified in, among others, websites of two banks, one nationwide television station, one ministerial department and several other entities that are subject to the Czech Cyber Security Act.



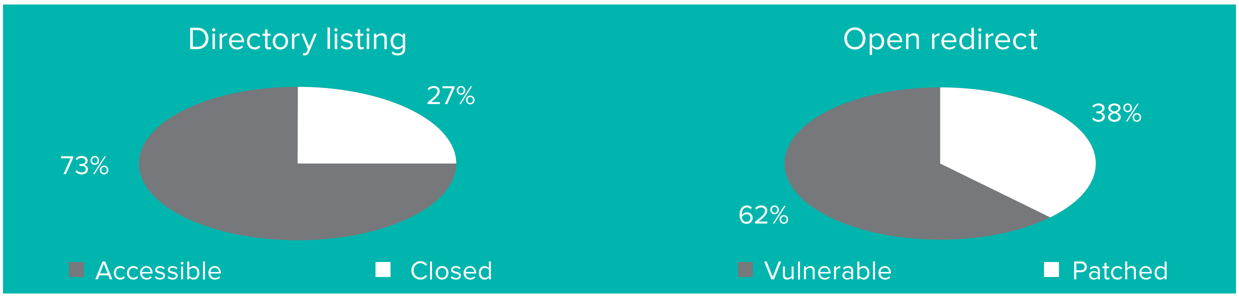
Also noteworthy is that as a part the above-described research, ALEF CSIRT specialists have been able to also uncover an open redirect vulnerability in Babel – a SW module, which provides multilingual content support to sites created with CMS Made Simple (CMSMS). The number of sites using this module worldwide was potentially in the order of thousands at the time when the vulnerability was identified.
A more detailed description of the research, including discussion of vulnerabilities found on servers outside the .CZ domain, was also published on Root.cz.

Contact of affected organizations

The operators and administrators of the above-mentioned vulnerable websites and/or servers, where sensitive data was accessible, were contacted after each research and informed about our findings, either by ourselves (by e-mail or using the Open Bug Bounty platform) or with the help of CZ.NIC, to whom we would like to – once again – express great thanks for their cooperation.

At the end of April 2019, the servers, which we identified as vulnerable or sharing sensitive content, were checked once again to determine whether there was some change following the report to their administrators/operators. It turned out that access to “open” directories on 27% of the systems, where sensitive data was originally found, was blocked. This number does not necessarily have to tell the whole story, because without deeper analysis of the data still available on the sites where directory browsing is still enabled, there is no way to tell whether the administrators haven’t removed the sensitive content from the sites while keeping access to the remaining data open.

For sites that were affected by open redirect vulnerabilities, responses of their administrators were more perceptible - by the end of April 2019, vulnerabilities had already been patched on nearly 38% of the initially identified vulnerable servers.



ALEF

For information please contact: cz-sales@alef.com or @ALEFSecurity