ROMANIAN NATIONAL COMPUTER SECURITY
INCIDENT RESPONSE TEAM

THREATS EVOLUTION IN
THE ROMANIAN CYBERSPACE
2018

BUCHAREST, 2019

[ABSTRACT]

The CERT-RO analysis of the evolution of cyber threats in the Romanian cyber space is the result of the processing of the information collected and processed by the institution during 2018. An element of novelty to previous years' reports is the move to a new, "custom-global" concept, mainly due to the entry into force of Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures to a high common level of network and information security in the Union.

CERT-RO has switched to a new work paradigm on its areas of competence, by initiating a redefining process of the workflows, in order to ensure a proportional response to cyber security incidents, depending on the impact and the magnitude of the incident.

Also, our own data sources on cyber security incidents, namely sensors, Darknet mechanisms, and honeypots, have been developed.

As a result of this new approach, in 2018, attacks from all continents, from over 190 states/territories were identified, compared to 60 states/territories in 2017, an element that reflects the "lack of borders" in cyberspace, and the universality of cyber attacks.

New types of malware have been identified in the Romanian cyber space, Monerominer, VPNFilter and Eitest. Also, there were no more clues of activity for other types of malware that operated in 2017, such as Palevo.

Romania is generating cyber security incidents, but it is a target in the same time.

Regarding cyber malware attacks, the # 1 position is held by Andromeda malware.

* * *

THREAT EVOLUTION AT NATIONAL LEVEL

Romanian National Computer Security Incident Response Team - CERT-RO, as an independent structure of expertise, research and development in the field of cybersecurity, is a public institution with legal personality, coordinated by the Ministry of Communications and Information Society. CERT-RO operates in accordance with the legislation in force, in order to prevent, analyze, identify and respond to incidents within cyber infrastructures that provide public utility functionality or provide information society services.

CERT-RO organizes and maintains the database system on threats, vulnerabilities and cyber security incidents, identified or reported.

According to the Law no. 362/2018 which fully transposes the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016, on measures to achieve a high common level of security of network and information systems across the Union, CERT-RO has become the National Authority for Network and Information Security, National Single Point of Contact and National CSIRT, within the scope of the NIS Directive.

In this context, the results obtained through own sources, as well as the notifications received by CERT-RO through the classical sources, were used with priority for this analysis.

The report presents an overview of threats and vulnerabilities in the national cyber space as well as recommendations for strengthening prevention and response capabilities, that can be used in defining public, organizational and individual policies as well.

In order to assess the state of the national cyberspace security, CERT-RO initiated the transfer process from the security analysis using the "general-specific" phrase to the security analysis using the "custom-global" syntax. Using its own sources (sensors, Darknet, honeypot mechanisms, etc.), the implementation of the new concept aims mainly to identify the events / incidents specific to the national cyberspace that have a global impact and where Romania is also a target of cyber attacks .

Stages addressed in achieving the proposed goal (new concept):

- The implementation of its own sensors by sectors / fields of activity.
  - In order to identify the latest cyber incidents/events, a procedure has been initiated to implement its own sensors that collect and relate data on cyber-security alerts, depending on the sectors / domains established by Directive (EU) 2016/1148.
- The implementing of some complex cyber security mechanisms.
  - To identify and investigate security incidents that target the national cyber space, honeypot cyber security mechanisms, as well as network-type telescope mechanisms (Darknet) have been implemented.
- The identifying and implementing of new data feeds, OSINT type.

As a first observation of the new analytical approach, we can see the decrease in automated cyber security alerts from global suppliers (*general information*), along with a significant increase in the volume of data collected from its own sources (*customized information*).

A specific and correct analysis will be carried out at the end of 2019, when the new "custom-global" concept will be fully implemented and the statistical analysis will be based mainly on data collected from its own sources.

The global trend towards the diversification of cyber threats and vulnerabilities was reflected in 2018, in the national cyber space, with the emergence of new types of cyber attacks and the disappearance of others.

While most alerts automatically processed by CERT-RO (other sources than its own) refer to vulnerable computer systems (*not up-to-date, insecure or improperly configured*) compromised or infected with various malware variants, which may indicate a low level of cyber security culture among users in Romania, most of the alerts from our own sources - *complex security mechanisms* refer to *Information Gathering* attacks, through which requests are sent to a system to discover weaknesses and try to collect information about hosts, services and accounts.

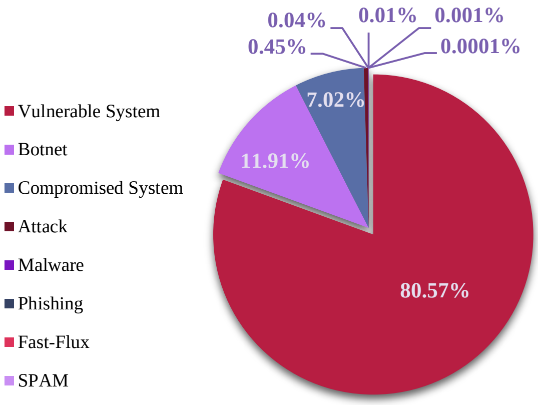
STATISTICS

1. AUTOMATICALLY PROCESSED ALERTS
2. MANUAL PROCESSED ALERTS
3. COMPLEX SECURITY MECHANISMS - DARKNET
4. OWN SENSORS / SOURCES

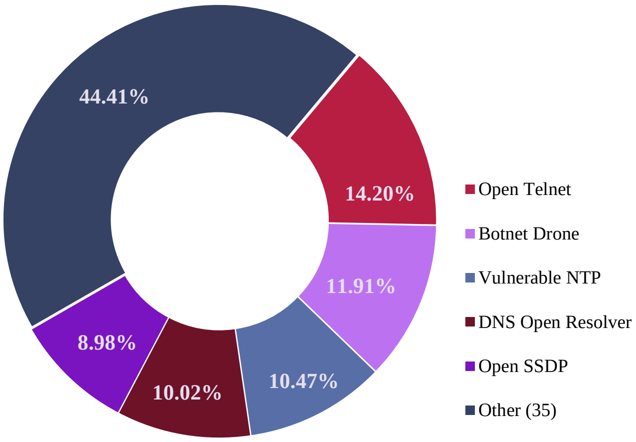
1. AUTOMATICALLY PROCESSED ALERTS

Threat distribution based on alert / incident class

Main incident class -> Vulnerabilities: 80,57%.



Threat distribution based on alert/incident type



«Top 5 incident types » represented: 55,59%.

In 2018, attacks / alerts of all kinds of predefined incidents were identified: 40.

As in the previous year, the first position is occupied by Open Telnet attacks..

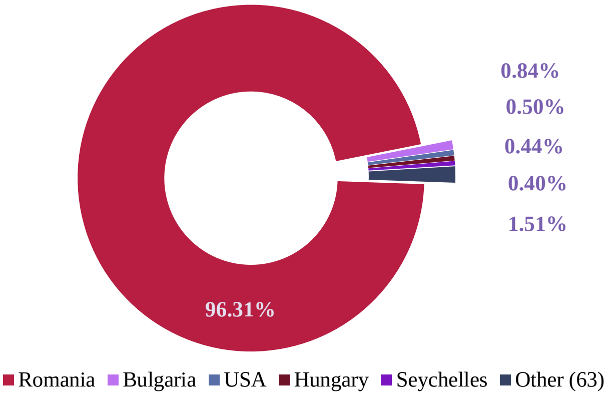
Threat distribution depending on the country of origin of the alert/incident

«Top 5 countries – attack source» represented: 98,49%.

Total number of states as origin of attacks: 68.

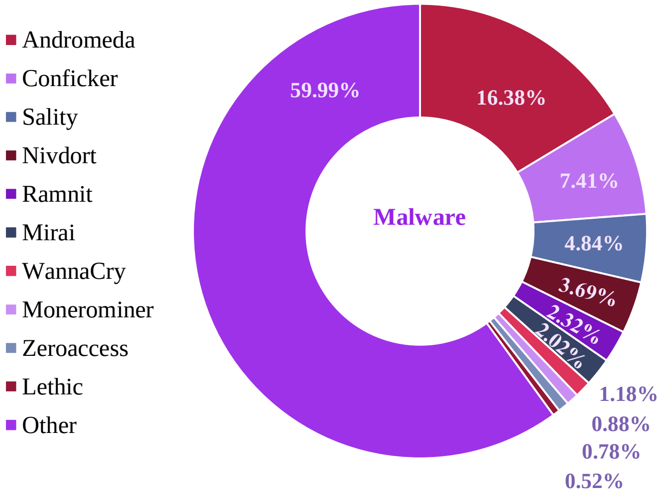
As a particularity, attacks from 25 new states were identified for the first time compared to 2017 (examples: Afghanistan, Armenia, Aruba, Algeria, Estonia, Philippines, Indonesia, Syria, etc.).

As well compared with 2017, attacks from China, Belgium, Israel and Japan have diminished.



It can be noticed that, in the case of the old "*general-regional*" concept, the impact of the threats on the Romanian cyberspace has a strong territorial character. The lack of complex cyber security systems and mechanisms can not generate a proper analysis of the threats from the national cyber space, which led to the implementation of the new analytical "*custom-global*" concept aimed to increase the national cyber security

Malware attacks distribution



Alerts processed at CERT-RO level contained information about the associated malware type (botnet alerts or malicious URLs).

Position # 1 is owned by Andromeda malware

Rank # 1 of Top10 / Malware Downadup (Conficker) fell to # 2.

New types of malware have been identified: **Monerominer**, **VPNFilter** and **Eitest**; and the disappearance of the others: **Palevo**.

In 2018 there was a significant increase in the cryptojacking attack phenomenon. In Romania, the malware applications MoneroMiner type (0.88% of the total associated malware), CoinMiner type (0.015%) and BitcoinMiner type (0.007%) were identified.

EITest. One of the oldest networks of malware in the world, the EITest infection network was closed in 2018 (after being discovered in 2011). Malware was distributed through a private exploitation kit and aimed to direct web traffic from the infected server to malicious and scam sites. Although the EITest spreading network is closed, the infection is still active and can affect vulnerable servers that are running the malicious code**.**

WannaCry has not yet died. Although at the beginning of the year it seemed that WannaCry became history, in 2018 IPs from Romania were infected with this type of malware.

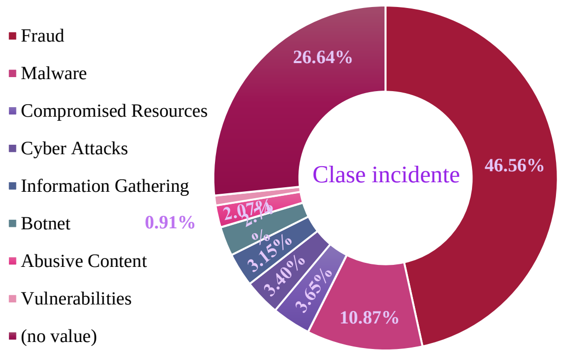
As statistics come from global information providers, it has not been identified if real damage has occurred in Romania. However, the number of attempts to infect computers with this malware in 2018 suggests that WannaCry is still active. So, computers can still be infected with this ransomware.

Locky. If at the end of 2017, it was predicted that the Locky ransomware would be abandoned by its creators and will disappear. In 2018 a new developing campaign was noticed, IPs being identified, including from Romania.

VPNFilter. In May 2018, Cisco Systems announced that over 500,000 routers and storage devices were infected by hackers in 54 countries. In Romania, the IPs involved were identified, both in attacks and in casualties.

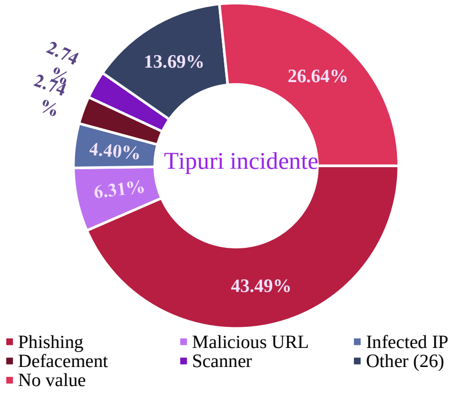
2. MANUAL PROCESSED ALERTS

Representative data on manually collected alerts



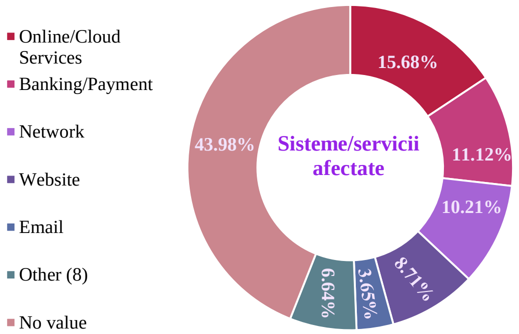
In 2018, attacks / alerts were identified for all classes of incidents used by CERT-RO to classify them. Events were managed using **Request Tracker for Incident Response (RTIR)**.

The most common class of incidents: Fraud (561)



Depending on the type of incidents, 31 types of alerts (out of 36 types defined in the RTIR) were identified / collected.

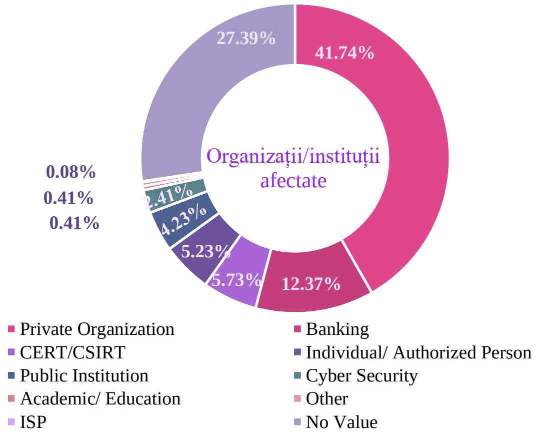
The most common type of incident in 2018 remains Phishing (524), the Fraud Incident class.



Regarding services / systems affected 13 types were identified (out of the 14 predefined types).

Position # 1 affected systems / services are *Online / Cloud Services*.

For the first time, alerts that affected ERP / CRM and Database services were identified.



For affected organizations / institutions, 9 types (out of 10 predefined types) were identified.

The first position is represented by private companies (503).

Alerts / vouchers processed involved a total of 107 430 unique IPs and 175 890 alerts / notifications have been issued.

3. COMPLEX SECURITY MECHANISMS - DARKNET.

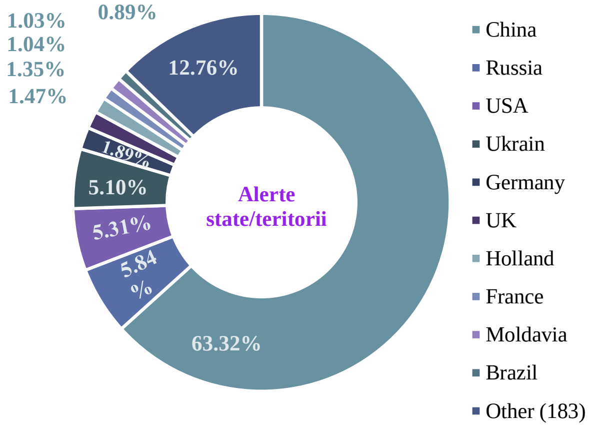
All attacks detected through this mechanism were part of the "*Information Gathering*" alert class and they were "Scanning" type.

Attacks were identified from 193 states / territories, including Romania (0.28% of total attacks).

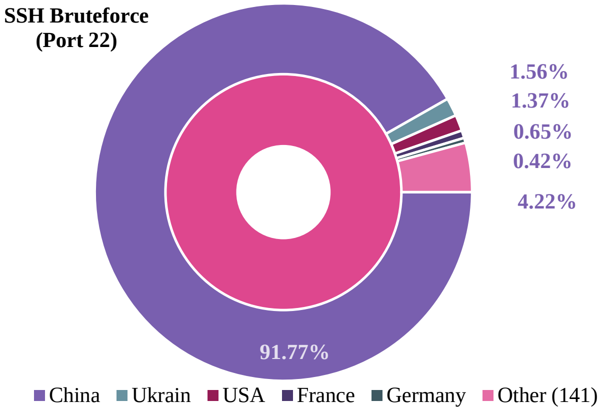
Position # 1 is held by China (63.32% of total attacks).

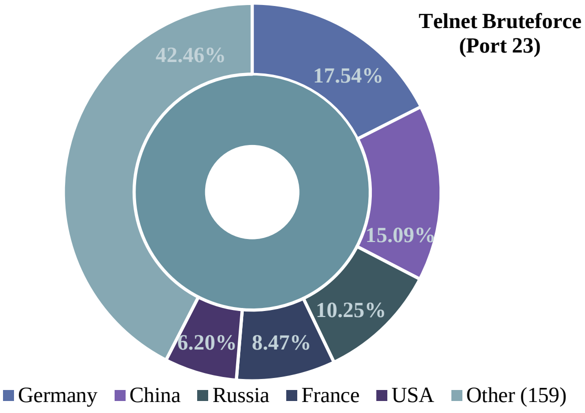
If in the case of external sources / feeds (to which CERT-RO is subscribed) it is observed that the identified attacks have a zonal impact; in case of own sources it is identified that the impact is global.

The data collected is only for 2018, so we can not make a comparative analysis, but this will lead to a more correct interpretation of the phenomenon next year.



For the first two types of attack identified (SSH Bruteforce and Telnet Bruteforce), depending on the source of the sources of attack, the situation is as follows:





4. OWN SOURCES / SENSORS

The analysis of the data collected through these mechanisms presents **the state of the national cyber space security in the area of Local Public Administration** (the domain under the responsibility of CERT-RO in accordance with GD No. 494/2011 on the establishment of the Romanian National Computer Security Incident Response Team - CERT-RO).

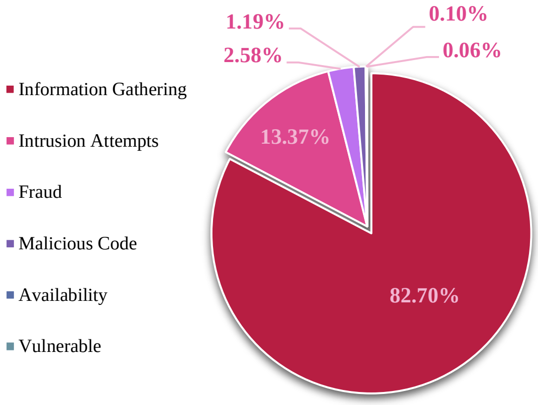
Threat distribution by class and type of incident

The main class of incidents -> Information Gathering[1]: **82,70%**.

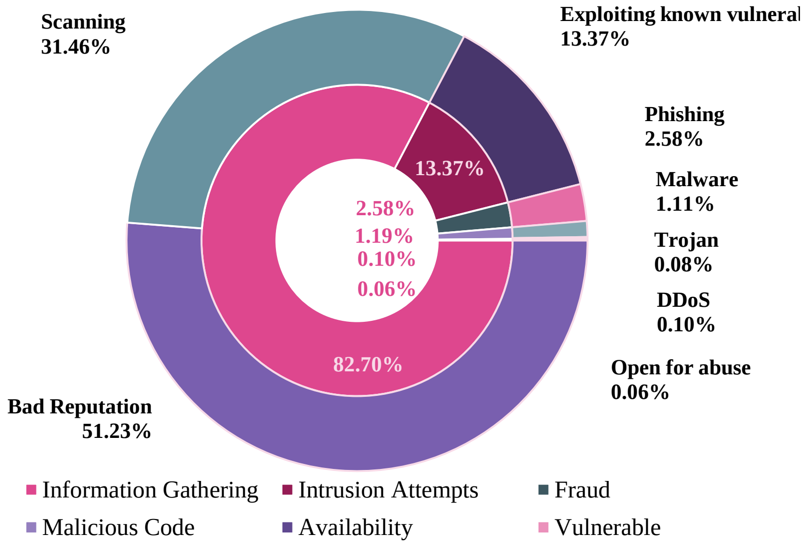
Cyber attacks: 3,87% .

Compared to data collected from external sources, it can be noticed: the Vulnerable class is placed on the last position (0,06%).

So the data obtained from our own sources provides more relevant information about the state of the national cyber space security.



The situation regarding the distribution of types of attacks depending on their class.

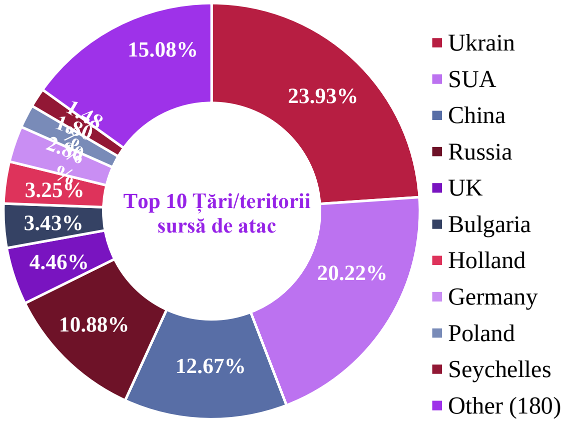


More than half of the data collected were "*Bad Reputation*"[2] attacks (*51,23%*).

2.58% were Phishing attacks, 1.11% Malware attacks and 0.08% Trojan type.

Also, DDoS attacks accounted for 0.1% of all cyber attacks on Local Public Administration.

Threat distribution by country / territory of origin of attacks



The analysis of the attacks carried out at the level of the local public administration reveals the following::

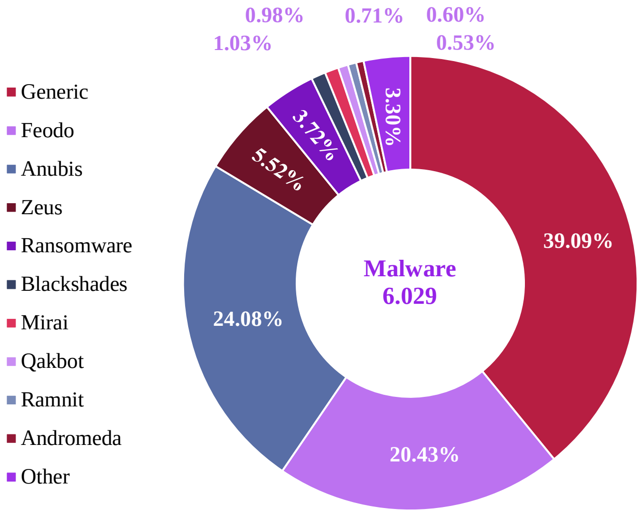
- The vast majority of attacks come from China (12.67%) and the former Soviet space, mainly from Ukraine (23.93%) and Russia (10.88%).
- Attacks came from 190 states / territories, and those from the top 10 countries ("Top 10") accounted for 84.92%.

[1] Information Gathering - Attacks that send requests to a system to discover weaknesses, including testing processes to collect information about hosts, services and accounts. Examples: fingerd, DNS, ICMP, SMTP (EXPN, RCPT...), port scan.

[2] Bad reputation - By means of sensors, connections have been identified from computer networks where they are placed to IP addresses known to be involved in malicious activities.

Also, based on the information provided by sensors, we estimate that about 20% of IT equipments in the Local Public Administration area are affected by various malware applications.

The distribution of malware attacks



6,82% of the alerts processed at CERT-RO level contained information about malware.

Position # 1 is owned by malware that has not yet been included in a dedicated category (*Generic malware*).

By comparing data collected from external and internal sources, some of the common types of malware, Mirai, Ramnit and Andromeda, are identified in 'Top 10 Malware'.

CONCLUSIONS

The analysis of collected and processed data implied a comparison of *external sources* versus *internal (own) sources*, ie *regional* vs. *global* character.

While in the first case attacks from 68 countries / territories were identified, in the second case (Darknet, respectively sensors) attacks from 193 states / territories, including Romania were found.

Under these circumstances, the orientation of the security analysis towards the "*custom-global*" concept and, mainly, the data collected from its own sensors, creates the premises of a thorough and extended approach to the cyber security issues under the competence of CERT-RO.

In the case of the new "*custom-global*" concept, it is noted that **the impact of threats on the Romanian cyberspace has a strong global character, and attacks come from almost all countries / territories of the world**. So, in the digital age "***distance does not prevail***" and attacks are made from anywhere in the Earth.

In conclusion, **the future of cyber defense is "*global cooperation*"** to ensure a secure cyber space, characterized by lack of borders, dynamism and anonymity.

By implementing its own sensors and detection systems, CERT-RO analysis is more accurate, highlighting the specificities of national cyber space.

Ensuring IT security involves a series of measures such as user awareness and training, risk analysis and assessment, vulnerability and security alerts management, access rights management, network and information system configuration management, and security plans at their level, compliance with European and international standards.

In this regard, CERT-RO, as the National Authority for Cyber Security, supports the creation of a national framework for cooperation between public/private environment and the academic environment, which will contribute to the exchange of information and good practices, as well as strengthening cyber security measures.

For this reason, we considered changing the way we approach the annual report so that it can provide specific data on the level of security in place in Romania, to encourage both reporting to CERT-RO and the exchange of good practices regarding the cyber security measures.

We also appreciate that, in the near future, besides the activities specific to the implementation of the NIS Directive, an important role will be played by the awareness and education activities that we intend to run on age and education level, so that we ensure that cyber security is better understood by all internet users in our country, because THE CYBERSECURITY OF ROMANIA IS THE RESPONSIBILITY OF ALL ITS CITIZENS.