Security Risks of Cloud Computing Services from the New Cybernetics' Threats Perspective

Ioana PETCU, Ionuţ Bogdan CANDET, Costin ŞTEFĂNESCU, Cristian Ionel GRUIA, Vlad CRAIOVEANU
National Institute for Research and Development in Informatics – ICI Bucharest
ioana.petcu@ici.ro, ionut.candet@ici.ro, costin.stefanescu@ici.ro,
cristian.gruia@ici.ro, vlad.craioveanu@ici.ro

Abstract: Starting with the development of technology and the acceleration of the digital transformation process, the risks and threats of cloud computing data centers are on an exponential trend, with increased exposure to cyberattacks and security incidents. Cloud computing services and their security have entered a new era through the growing need for resilience, technological capacity building and the use of the highest standards of cyber security and digital autonomy. Both users and providers, and administrators of cloud computing will need to adapt quickly and continuously to new developments in cyber threats and develop their skills, responsiveness and cybersecurity capabilities. In the context of the new cyber threats posed by the new normal, in which old security practices have been deeply affected by the current pandemic, this article presents an analysis of new security risks and threats and the most important measures to prevent cyberattacks on cloud computing services seen from an agile and flexible approach to security.
Keywords: Cybernetics risk, New normal, Pandemic crisis, Awareness, Cloud computing, Data center, Cybersecurity, Threats, Vulnerability, Capability, Cyberattacks, Hacking, Control security

INTRODUCTION

This article is a part of a research project developed to improve cloud computing services and the proposed issue refers to the analysis of services security at the level of data centers and cloud computing in the new cyber threats perspective.

Cybersecurity is the state of normalcy of digital information, resources and services resulting from the application of a set of proactive and reactive measures, such as security policies, procedures, standards and guidelines, risk management, training and awareness-raising activities.

The implementation of technical solutions for the protection of cyber infrastructures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of digital information in cyberspace are necessary activities to protect networks and information systems affected by cyber threats, those events that may have negative impact to the computer networks [CEH V10 EC, 2018]. as shown in Figure 1.

Fig. 1: *Elements of Information Security, [source CEH V10 EC, 2018]*

Confidentiality is the protection of electronically stored information to which only certain authorized persons have access. Techniques such as data encryption, authentication and access control can be used as measures to control the risk of unauthorized access to information or identity theft.

Data integrity implies that access to data is available only to authorized persons. Data integrity risks mean that the information is no longer correct or reliable and fraud has occurred, in which case we have audit logs and the quality assurance process as a control measure.

In case of a malfunction or a cyberattack, the data must be available and can be accessed by authorized persons so that the continuity of the business does not suffer. Thus, the measures for planning and testing the back-up activity will be taken.

Authentication is the process of identifying the user to receive access, certain privileges, rules and policies, while ensuring the authentication of certain information initiated from a valid user who claims to be the source of information and message transactions.

Non-repudiation is one of the main pillars of information security that guarantees the transmission and reception of information between sender and receiver through various techniques, such as encryption or digital signatures. Digital contracts, signatures and e-mails use non-rejection techniques that ensure communication and authenticity, the sender cannot deny what he sent and the recipient cannot deny receipt.

In the next chapter we will present an analysis of the latest studies in the literature on the types of attacks and threats on data centers and cloud computing (malicious codes and scripts, viruses, spam and malware), vulnerabilities (unauthorized access, disclosure of confidential information, use and modification of sensitive data) and security measures that ensure the confidentiality, integrity and availability of data in the cloud and reduce permanent risks and exposure to attackers.

SECURITY OF CLOUD COMPUTING SERVICES

The security of cloud computing services involves processes, technologies, infrastructure, mechanisms that use security control, compliance and other risks of public, private or hybrid cloud systems.

The implementation models for cloud computing services are of three types:

• public cloud, hosted by a third party that offers different types of cloud services

• private cloud, individually hosted cloud, usually implemented by corporations due to security policies

• hybrid cloud, a mix between the two types of models presented above.

Interconnectivity, performance, data security, availability, efficiency, resilience, scalability, virtualization, on-demand self-service and distributed storage are key features of cloud computing products and services. The higher the number of devices connected to a data center, the lower the security and resilience vulnerability will be, due to the fact that they are not sufficiently integrated by design, and lead to insufficient cyber security [Barbu, 2016].

The major benefits of cloud data security include smaller investigations with efficient management of patches and security updates, disaster recovery, dynamic scaling of defensive resources and other security services that provide protection against cyber threats in the cloud.

Cyber security is not only a technology issue, but also a link to human behavior [Vevera, 2018]. Thus we speak of cyber hygiene, of those simple, routine measures, which, when implemented and carried out regularly by users, organizations or companies, minimize their exposure to the risks of cyber threats.

There are 5 major stakeholders in the cloud computing services:

• Cloud Consumer (user), the one who maintains the business relationship and uses the services of the cloud provider,

• Cloud Provider provides cloud services to stakeholders,

• Cloud Auditor, which can perform an independent evaluation of cloud services, information system operations, cloud deployment performance and security,

• Cloud Carrier, the intermediary that provides connectivity and transport of cloud services from providers to cloud consumers,

• Cloud Broker manages the use, performance and delivery of cloud services and negotiates the relationship between cloud providers and cloud consumers.

Cloud service users should have accurate information about the level of assurance with which the security of IaaS, PaaS or SaaS products and services has been certified, provided that it is known that no IT product or service is completely secure, which is why the basic rules of cyber hygiene need to be promoted and prioritized.

The most common types of cloud computing services [Barbu et al., 2019] are:

• Infrastructure-as-a-Service (IaaS), provides cloud-based infrastructure to deploy a remote data center,

• Platform-as-a-Service (PaaS), allows users to develop, run and manage applications,

• Software-as-a-Service (SaaS), through which on-demand software is hosted to be accessible to users who use the „client" through browsers.

A study published in the journal Economica.net shows that the data centers infrastructure market in Romania will grow in 2021 by 20-30% over the value of 25 million euros recorded in 2020. The growth is determined by factors such as new facilities built by companies private and government institutions, increasing the power needs of current cloud players and colocation, interest in increasing energy performance in the context of the emergence of new solutions and technologies, the existence of funding through projects on European funds. In 2021, the local data center market has become increasingly diversified, both in terms of

public and private investment, the structure and technologies used modularly and edge and the locations chosen by beneficiaries.

Starting with the increasing use of cloud computing services by state institutions but also by private companies, the exposure to security risks has also increased, with cyber threats exploiting human, technical or procedural vulnerabilities. We are encountering more and more cyberattacks against public utility infrastructures, hospitals, universities through unauthorized access, modification, deletion or unauthorized damage of computer data or illegal restriction of access to such data or cyber espionage.

Applications used by cloud computing providers involve services, including e-mail and social networking, provided to end users, which collect and store a large volume of data of the order of terabytes of information and personal data, in data centers throughout the world, data that is exposed to cyberattacks.

The old cyber security practices had to be updated to the new normal in the current context of the pandemic generated by the health crisis. The new normal in which most users have worked from home has generated an agile and flexible approach in the field of cybersecurity. In this context, users of cloud computing services have increasingly relied on mobile devices, and the use of smartphones and tablets has not been limited only to personal use, but also in the interest of service, thus increasing the risks posed by user's unwanted behavior.

Emerging smartphone technology has caught the attention of hackers to steal commercial and personal information. The most common threats are data leaks, insecure Wi-Fi, network spoofing, phishing attacks, spyware, cracked encryption or incorrect session management. COVID-19-related phishing is one of the biggest threats to mobile users last year, with attackers trying to take advantage of people's fears.

Another type of attack is Man-in-the-Middle (MitM) which affects smartphone users with internet access through the WI-FI network can be achieved by gaining physical control of the network infrastructure through fake Wi-Fi hotspots, allowing hackers to spy on internet traffic, or by manipulating the network protocol that provides encryption, exposing data that needs to be protected.

Attackers use applications that contain malware, fraudulent advertisements, adware with approved applications through official checks in the application store, which contain pop-ups that take over the screen of a device making the application unusable.

Information security in the cloud is ensured by the existence of three levels of security: network security, server security and application security. Level of security is a measure of the security power in the system, functionality and usability, known as the Security, Functionality and Usability triangle.

The system becomes nonuser-friendly, thus decreasing its performance by implementing a high security process that impacts quite easily the level of functionality and usability. It is recommended that cybersecurity experts should ensure a balance between the development and integration of security measures and functionality and ease of operation.

SECURITY CONTROLS IN CLOUD COMPUTING

Cloud Computing Security refers to the security deployments and prevention against security threats. The cloud computing services security includes control policies, the implementation of security devices, such as firewalls and next-generation IPS devices and the strengthening of cloud computing infrastructure.

When it comes to application-level cloud security control layers, web application firewalls are implemented to filter and observe traffic behavior.

To ensure the confidentiality and integrity of information that is communicated between the client and the server, various policies are

configured at the cloud computing level to monitor any data loss, including Data Loss prevention (DLP) and Content Management Framework (CMF). Data Loss Prevention (DLP) prevents the leakage of confidential, financial, off-network information by enforcing rules and regulations, using data loss prevention policies that prevent the user from intentionally or unintentionally sending this confidential information.

Cloud computing services can be secured by filtering emails, including backup and spam system, web content filtering and vulnerability management. Some threats are better managed by a larger data center. Applications running in the cloud are less vulnerable to Distributed Denial of Service attacks that involve trying to prevent a website or service from working. Identity, access management and associated policies for cloud services use must be equivalent to current business practices and ensure interoperability with existing applications.

Data encryption in cloud computing is not a complete solution because data must be decrypted in certain situations - so that it can be processed and perform the normal functions of data management, indexing and sorting. Although data in transit and stored data are actually encrypted, the need for decryption by the cloud service provider can be a security issue.

Cloud Computing security management includes Governance, Risk Management and Compliance (GRC), Identity and Access Management (IAM), patch and configuration management, approaches that can help secure access and managing resources.

To secure the network layer at the cloud computing level, there are several solutions available such as the implementation of state-of-the-art IDS / IPS devices, Firewalls, DNSSec, Anti-DDoS, OAuth and Deep Packet Inspection (DPI).

Next-Generation Intrusion Prevention System (NGIPS) is one of the most effective proactive component in the integrated security solution against threats, offering a stronger security layer with deep network visibility, automation, improved security information and advanced protection against emerging threats to secure complex network infrastructures. NGIPS uses the most advanced and effective intrusion prevention capabilities to stop complex emerging network attacks and continuously collects network information, including operating system information, file and application information, devices and user information that helps to determine network maps and profiles that lead to contextual information to make better decisions about intrusive events.

Regarding Trusted Computing, Root of Trust (RoT) is established by validating each hardware and software component from the final entity to the source certificate, ensuring only the use of reliable software and hardware, while maintaining flexibility. Data migration and data replication in cloud computing can be secured by implementing HIDS / HIPS host-based intrusion detection or prevention systems, integrity check configuration, file system monitoring and log file analysis, connection analysis. Data storage security uses different encryption algorithms.

Using IDS / IPS, the cloud computing provider can identify the attacks or the illegitimate data traffic that have as foundation the resources of cloud computing user, without his knowledge, and the target being the services outside the cloud. IPS / IDS works together with the operating system kernel creating a filter layer against any malicious application.

Physical security is always necessary, being the first level in the OSI model, and includes protection against hacker attack such as theft, damage, unauthorized physical access, or the impact of environmental factors such as rain, dust, power blackout, fire. If the device is not physically secured, any security configuration will not be effective.

Responsibilities for cloud computing security are shared between cloud service

providers and users. Thus, if we refer to the responsibilities of a cloud service provider, they include the performance of the following security controls [CEH V10 EC, 2018]:

- Web Application Firewall (WAF)
- Real Traffic Grabber (RTG)
- Firewall
- Data Loss Prevention (DLP)
- Intrusion Prevention Systems
- Secure Web Gateway (SWG)
- Application Security (App Sec)
- Virtual Private Network (VPN)
- Load Balancer
- CoS/QoS
- Trusted Platform Module
- NetFlow and others

The responsibilities of a cloud service consumer include performing the following security controls:

- Public Key Infrastructure (PKI)
- Security Development Life Cycle (SDLC)
- Web Application Firewall (WAF)
- Firewall
- Encryption
- Intrusion Prevention Systems
- Secure Web Gateway
- Application Security
- Virtual Private Network (VPN) and others.

The cloud computing service client should evaluate the security controls of the provided data, such as:

- Data encryption in rest
- Measures to prevent unauthorized user access - including restrictions on access to data by CSP system administrators
- Database encryption
- Two-factor / multi-factor authentication (2FA / MFA)
- Monitoring data access and reporting violations

THREATS IN CLOUD COMPUTING AND TYPES OF ATTACK

The computer networks, data centers and cloud computing services are able to support all aspects of our economic, social, cultural and security life and stimulate economic growth, being most often exposed to cyberattacks and threats.

A cyberattack involves three main components: reason, method and vulnerability [CEH V10 EC, 2018], as shown in Figure 2.

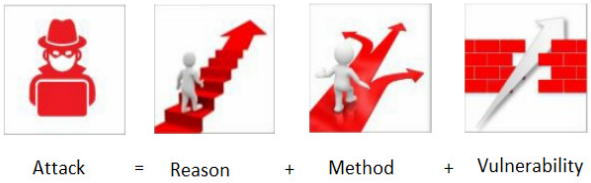

Fig. 2: *Information Security Attack [source CEH V10 EC, 2018]*

The target of a cyberattack can be information theft, data manipulation, disruption, the spread of political or religious beliefs, the attack on the target's reputation or revenge. These are some of the most common reasons for a hacker to focus on attacking a computer system or data center, using various tools and techniques to exploit a system vulnerability or breach security policy to achieve their goals.

A major threat to the security of cloud computing services is the data security breach that can lead to losses, allowing the hacker to access multiple records in cloud computing. This is the worst situation where compromising a single entity leads to compromising multiple records. Data loss is one of the most common potential threats and is a security vulnerability in cloud computing. Encrypted improperly or loss of encrypting keys can lead to data modification, deletion, data theft and data misuse.

An example of abuse of cloud services that used malicious services is when Dropbox cloud service has been abused by an attacker to spread a massive phishing campaign and hosted malicious data. Data loss may be due to intentional or accidental actions, may be large-scale or small-scale; however, the massive loss of data is catastrophic and expensive.

Another major threat to cloud computing is cloud account hijacking. Applications running in cloud computing with poor encryption performance, gaps and vulnerabilities allow the hacker to control data, access and account information using malicious or unauthorized activity.

There are many others threats to which cloud computing is vulnerable like data loss and security breach, insecure interfaces and APIs, malicious information, escalated privileges, natural disasters, authentication's failure, attacks on virtual machines, denial of services, trojan, poor security, as shown in Figure 3.

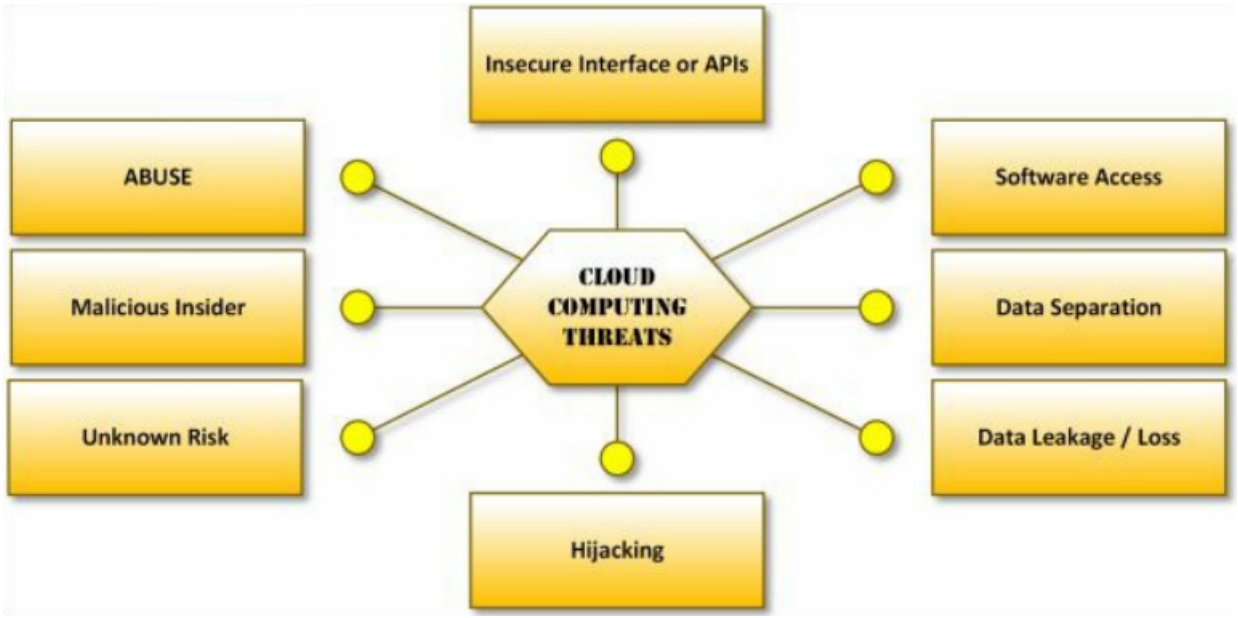

Fig. 3: *Cloud Computing Threats*
[source CEH V10 EC, 2018]

Personal data protection and the privacy management issues can lead to the success or failure for many cloud services, due to problems with the location of data centers in several places with different levels of security. Commercial espionage, intellectual property protection - copyright protection - are also considered high security issues for cloud computing services.

Software User Interface (UI) and Application Programming Interface (API) are interfaces used by customers to interact with the cloud service and can be secured by monitoring, orchestrating, managing and provisioning. These interfaces must be secured against malicious attempts.

The many types of cyber threats can be classified according to their data effects such as disclosure, modification, destruction or denial of access. Cyber threats can be classified according to the basic principles of information security in threats concerning unauthorized access, data availability, data confidentiality or data integrity: When there is a data disclosure threat, the security of data confidentiality is compromised. If the information changes data security and data integrity is compromised due to unauthorized access or corruption. Data availability security is affected when data is deleted or blocked. Attacker's design and malware and malicious software use, such as viruses, trojans, ransomware, worms, adware, and spyware, to disrupt the operation of computer networks, earn money, or steal information.

Ransomware encrypt data programs, prevent users from accessing their files until a ransom is paid, usually in cryptocurrency, or until a certain action is taken. According to

Europol, the number of ransomware attacks has increased in last years. [ECA EU, 2019].

One of the worst types of threats is Advanced Persistent Threats (APT), the attacker monitors for a long time and steals data or destroys it in order to keep hackers undetected for as long as possible. APT threats are often associated with a state and target particularly sensitive sectors, critical infrastructure or government cloud computing services. The most common types of attacks in cloud computing are those used by an attacker to extract sensitive information, such as credentials or gain unauthorized access, with cyber espionage and it is estimated to account for at least a quarter of the total number of cyber incidents.

Service Hijacking using Social Engineering Attacks, using social engineering techniques, the attack tries to guess the password resulting in unauthorized access and exposure of sensitive information depending on the privileged level of the compromised user.

Service Hijacking using Network Sniffing refers to the attacker's capture of sensitive information (passwords, session IDs, cookies) and other information related to web services (UDDI, SOAP and WSDL). By launching Cross-Site Scripting (XSS), the attacker can steal cookies by injecting malicious code into the site.

Session Hijacking using Session Riding hijacks sessions by which the attacker can exploit a system trying to falsify the application between sites. The attacker uses the currently active session and browses it by executing requests such as changing data, deleting data, online transactions and changing the password, tracking the user to access a malicious link.

Domain Name System (DNS) Attack include DNS manipulation, Cybersquatting, domain hijacking, and fragmentation. An attacker can try to fake by manipulating the DNS server or cache to obtain internal user credentials. DNS hijacking involves stealing the domain name of the cloud service, through phishing scams, where users can be redirected to a fake site.

Side Channel Attacks or Cross-Guest VM Breach is an attack that requires the implementation of a malicious virtual machine on the same host. For example, a physical host hosts a virtual machine that provides cloud services, therefore the target of an attacker is to install a malicious virtual machine on the same host to take advantage of the resource sharing, such as processor cache or cryptographic keys. The installation can be done by a malicious user or an attacker by imitating a legitimate user.

Other attacks types used for cloud computing are: SQL Injection Attack - injection of malicious SQL statements for extracting information, Cryptanalysis Attacks - weak or outdated encryption, The Packet Attack - message body duplication, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks.

Distributed Denial of Service (DDoS) attacks aim to block certain cloud services or resources by flooding them with more requests than can be handled, users may be manipulated in such a way as to unintentionally perform a particular action or disclose confidential information. This strategy can be used in the case of data theft or cyber espionage, and it is known as social engineering. The method used is phishing, through e-mails that seem to come from trusted sources, users are tricked into revealing information or opening links that will infect their devices with downloaded malware.

CONCLUSIONS

The effects of identifying vulnerabilities exploited by hackers to compromise data centers can be mitigated by taking a series of measures such as: constantly updating operating systems, disabling external management skills, enabling secure login methods and powerful authentication functions, blocking protocols redundant present in the network and their organization within the system configuration.

Whenever a new device connects online or to other devices, the attack surface in

cybersecurity increases. The exponential development of cloud technologies, big data systems and the digitalization of the industry is accompanied by an increase in the exposure of vulnerabilities, allowing malicious attackers to target more and more victims. Given the variety of types of attacks and their increasing complexity, keeping up with new developments is a real challenge.

In order to create a sustainable cyber security environment, it is important that design security should be used as a principle in the process of developing, maintaining, operating and upgrading cloud computing infrastructures, cloud products and services, by supporting state-of-the-art secure development of appropriate security tests and audits, through remedial updates, known vulnerabilities or threats, and by enabling third parties to provide updates after the end of the product life cycle

Security by design should be ensured throughout the products life cycle and services, and through development processes that are constantly evolving in order to reduce the risk of damage by malicious exploitation.

AKNOWLEDGEMENTS

The work has been funded by the Nucleu Program PN 19 37 0201: Increasing the performance of Cloud services through the analysis and development of a Billing system, Phase 3: Analysis of security service at the level of data centers and cloud computing in the perspective of new threats

REFERENCE LIST

Barbu, D.C., Îmbunătăţirea protecţiei infrastructurilor critice din sectorul TIC prin creşterea rezilienţei, Revista Română de Informatică şi Automatică, nr 4, 2016

Barbu D.C., Sipica A., Candet I., Aspecte privind securitatea la nivelul SLA în serviciile de Cloud computing, Revista Română de Informatică şi Automatică , vol. 29(3), pp. 31-40, 2019

Barbu, D.C., Vevera, A.V., e-Documents - A Digital Freeway from a Cybersecurity Perspective, 12th International Technology, Education and Development Conference - INTED 2018 Proceedings, pp. 5311-5314

CEH V10 EC-Council Certified Ethical Hacker Complete training Guide with Practice Labsnet, IPSpecialist LTD, May 2018

Luna, J., Taha, A., Trapero, R., Suri, N. (2017). Quantitative reasoning about cloud security using service level agreements. IEEE Transactions on Cloud Computing, 5(3), 457-471

MIHAI, I.C., CIUCHI, C., PETRICĂ, Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu, Institutul European din România, 2018

MINCHEV, Z., Digital Transformation - An Extended Future Outlook for the Balkans Region, Romanian Cyber Security Journal, Fall 2020, No. 2, Vol. 2

SDF (2020). Securing Digital Future 21 Web Forum, http://securedfuture21.org

Strategia României pentru Cyber Security, 2013, https://cert.ro/vezi/document/NCSS-Ro

Smolenov, H. (2016). Sharing Genius with the Universe. The Light-Second Code & the Golden Ratio Tagarev, T. (Ed) (2020). DIGILIENCE 2020: Cyber Protection of Critical Infrastructure, Big Data & Artificial Intelligence, Information & Security. An International Journal, Vol. 47

Vevera, V. A., Albescu, A. R. (2018). Factorul uman vs. securitatea cibernetică. Romanian Journal of Information Technology and Automatic Control, Revista Română de Informatică și Automatică, Vol. 28, No. 4, 2018, 67-74

Vevera, A.V. (2014), Ameninţări cibernetice globale şi naţionale, Romanian Journal of Information Technology and Automatic Control, vol 24, Nr . 3

*** Ghid de securitate cibernetică, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO, CERT-RO, ANSSI, ARASEC, Ambasada SUA în România

*** PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")

*** Provocări pentru o politică eficace a UE în domeniul securității cibernetice, Document de informare, Curtea de Conturi Europeană, Martie 2019, https://eca.europa.eu