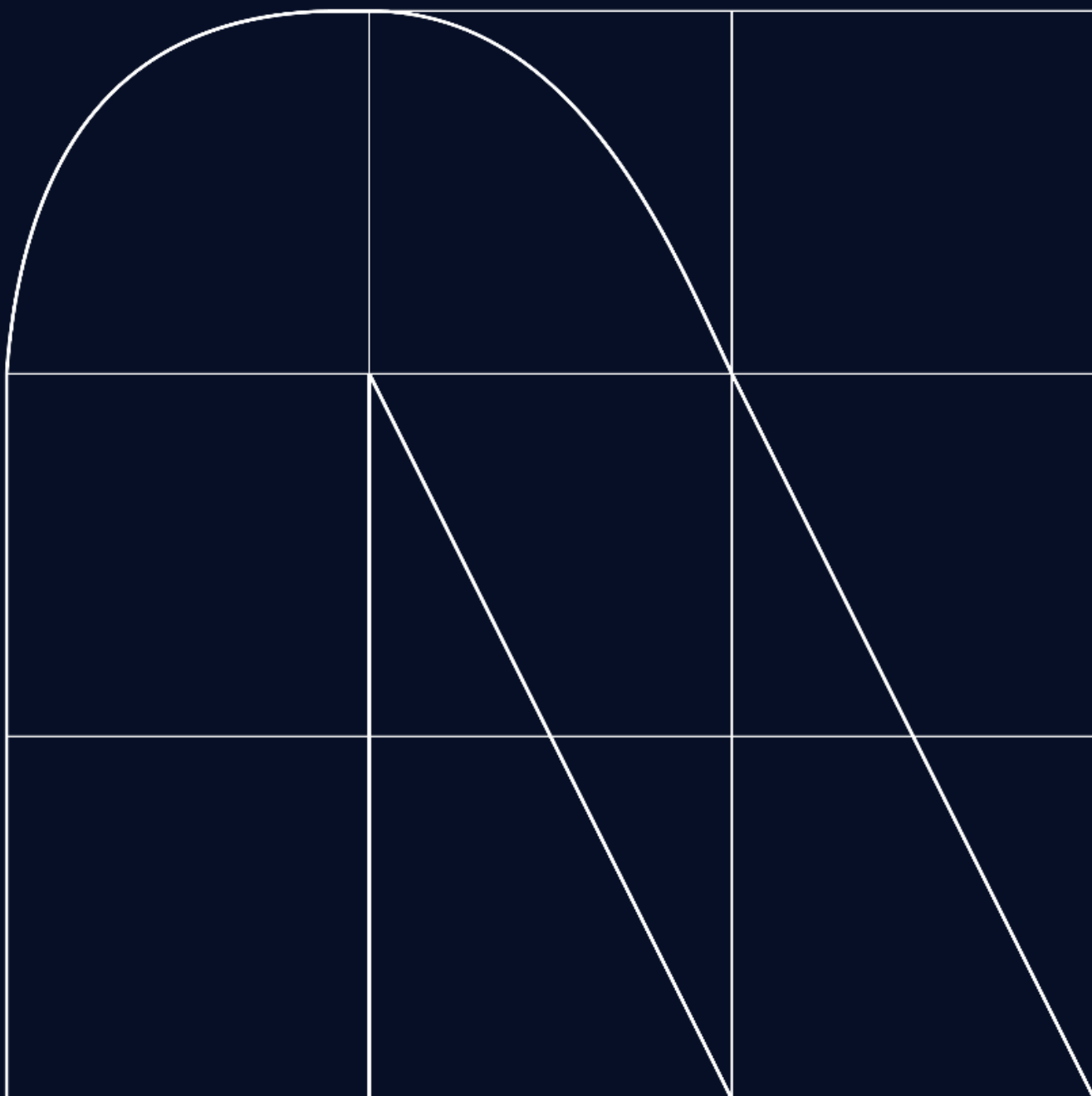
Issue 86 / January 2024

NTT DATA

Radar

The cybersecurity magazine



2024: A new beginning in the digital transformation process

By Maria Pilar Torres Bruna

We are starting a new year, 2024, and technologically speaking, everything points to it being an exciting year. Just when we thought that companies had taken a big step in their digital transformation (as a result of the pandemic and the modernisation it forced for remote work), and we were expecting a few years of stabilisation, we are once again getting the feeling that we are at a new beginning of the road. A new revolution is coming, which will be led by the adoption of artificial intelligence.

From the security areas, we have seen how new AI projects, even if they are in a proof of concept mode, are breaking into the business. The truth is that more than 70% of organisations, at least at the Latin American level, recognise AI as a driver of change in the transformation that is coming to us. There is a perceived concern from the point of view of security and privacy. Concern has become an occupation for various governments that are regulating the use of artificial intelligence and well-recognised entities such as NIST, the personal data protection agency in Spain, or the Ibero-American network of data protection.

And in this situation, it only remains for us to do what we have always done: make cybersecurity a key lever for digital transformation. And to be that lever of change, we believe that the following points must be very present in the upcoming year:

- We must accompany the adoption of AI projects by ensuring they comply with a framework of security and privacy that prevents biases and considers complete and reliable data sources. It does not matter if the country we are in does not have a regulation in place yet. Let's choose a solid framework of best practices to be prepared for future regulations and to position ourselves as promoters of responsible AI consumption in front of our clients.
- Let's embrace AI itself to enhance security levels within the company. Many technologies already involve the use of AI. It is necessary to maximise that use and detect points not yet covered by it in order to define how to make that functionality more efficient.
- Quantitative risk analysis can be a great ally to demonstrate that investment in security, in AI projects, and in projects in general, is not only not a cost, but also brings better results in the medium term. Perhaps it is time to carry out the analysis on the risk scenarios with the greatest impact for the organisation.
- Let's keep thinking about the future. Cybersecurity has ceased to be an aspect of the CISO to be a matter of organisational resilience. It is in everyone's hands.

At NTT DATA we are confident that an exciting year is ahead for those of us working in cybersecurity. We look forward to partnering with you to continue to grow this wonderful field. Happy new year 2024! We wish you a cyber-secure year!

Maria Pilar Torres Bruna
Cybersecurity Director

Cyber-attacks threaten the security of medical infrastructure

Cyberchronicles

In the global healthcare landscape, a silent digital threat has unleashed an unprecedented vulnerability at the intersection of technology and healthcare. At the end of 2023, cyber-attacks have increased dramatically, with critical health infrastructures being one of the most affected, endangering the stability of clinics, hospitals, health service providers and laboratories. Health advocates must protect a fragile system that seeks to strengthen global health.

As November came to a close in New Jersey, the local healthcare system announced disruptions, marking another episode in the chain of events that has affected medical infrastructure. The prioritisation of surgeries according to urgency highlights the raw vulnerability of an essential system that supports not only diagnoses and treatments, but existence itself.

Simultaneously, in Tulsa, Oklahoma, Hillcrest Medical Centre became the epicentre of a devastating ransomware attack, postponing vital procedures and plunging thousands of patients into uncertainty about their health. The reality that our lives are intertwined with the digital complexities of healthcare was becoming more pressing than ever.

> These attacks pose a direct threat to the lives and health of millions, leaving patients on hold and generating devastating economic costs

It continued to expand to Nashville, Tennessee, when Ardent Health Services, responsible for 30 hospitals in six states, disconnected its network after a cyber-attack also in late November. Ambulances diverted, procedures suspended; the backbone of society, medical care, incapacitated in the face of attacks. The same heartbreaking threat became present in Colombia in September 2023, when more than 50 state institutions, including the National Superintendency of Health, reported cyber-attacks under the ominous ransomware modality, seriously affecting the provision of services to citizens by several health institutions.

These critical events reveal a chilling truth: the beating heart of healthcare is vulnerable to digital attacks that threaten not only infrastructure, but directly the health and well-being of communities. In this scenario, cybersecurity is not only an additional layer, but an essential line of defence to protect the integrity of global healthcare. While these incidents highlight the cracks in the system, they also call for collective and immediate action to preserve the trust and effectiveness of health services, ensuring cyber threats do not overshadow our ability to heal and care.

Worldwide, hundreds of cyber-attacks have emerged, from developed to less favoured nations, in a dance executed by cybercriminals with objectives beyond economic profit, seeking to destabilise and terrorise society. The gravity of the situation demands immediate action.

These attacks pose a direct threat to the lives and health of millions, leaving patients on hold and generating devastating economic costs. International collaboration stands as a fundamental pillar in this battle, where threat information must be shared quickly and transparently to strengthen collective defences.

The implementation of **rapid response strategies, artificial intelligence technologies and machine learning** becomes essential to detect patterns of attacks before they materialise. The fight against this dark digital threat requires not only technological innovation, but also a cultural change and constant awareness at all levels of healthcare. Investment in defensive innovations is imperative to build a robust shield against those who seek to bleed global health through dark digital nooks and crannies. The victory is celebrated not only in data protection, but in the preservation of the very essence of our existence - the health and well-being of humanity.

As we **move into 2024**, we face the challenge of turning past challenges into opportunities for change and improvement, especially in defending against cyber threats in healthcare. International collaboration and technological innovation are fundamental for a safer future, supported by a growing collective awareness about the importance of cybersecurity in the medical field.
This year urges us to translate lessons learned in the cyber battle into more effective measures and to build a stronger shield against digital threats. May 2024 be a period of positive transformation, where global togetherness, advanced technology and constant awareness will lead us to strengthened cybersecurity and, ultimately, to safer and more reliable healthcare for everyone.

But it is not only the health sector that is being affected by ruthless cybercriminals, as an old malware has returned with more strength and new and novel ways to breach public sectors, businesses and us as internet users. For this reason, it is worth mentioning a RAT that has made a strong comeback: **the NetSupport RAT**. Remote Access Trojans (Rats) are masters at orchestrating chaos, providing the attacker with absolute control over the infected machine. By infiltrating a system, this malware establishes a virtual bridge, allowing the intruder to direct the device remotely, in a way comparable to tools such as the Remote Desktop Protocol (RDP) or TeamViewer.

NetSupport RAT, once a legitimate remote management tool known as NetSupport Manager, has been reborn as a latent threat in the hands of malicious actors. Security experts are observing with concern its drastic increase in infections, with critical sectors such as education, government and business services falling victim. The spread of NetSupport RAT is carried out through various tricks, from fraudulent updates to clandestine downloads. This Trojan stands out for its versatility in affecting from cybernetic neophytes to seasoned adversaries, becoming a wide-ranging and subtle threat.

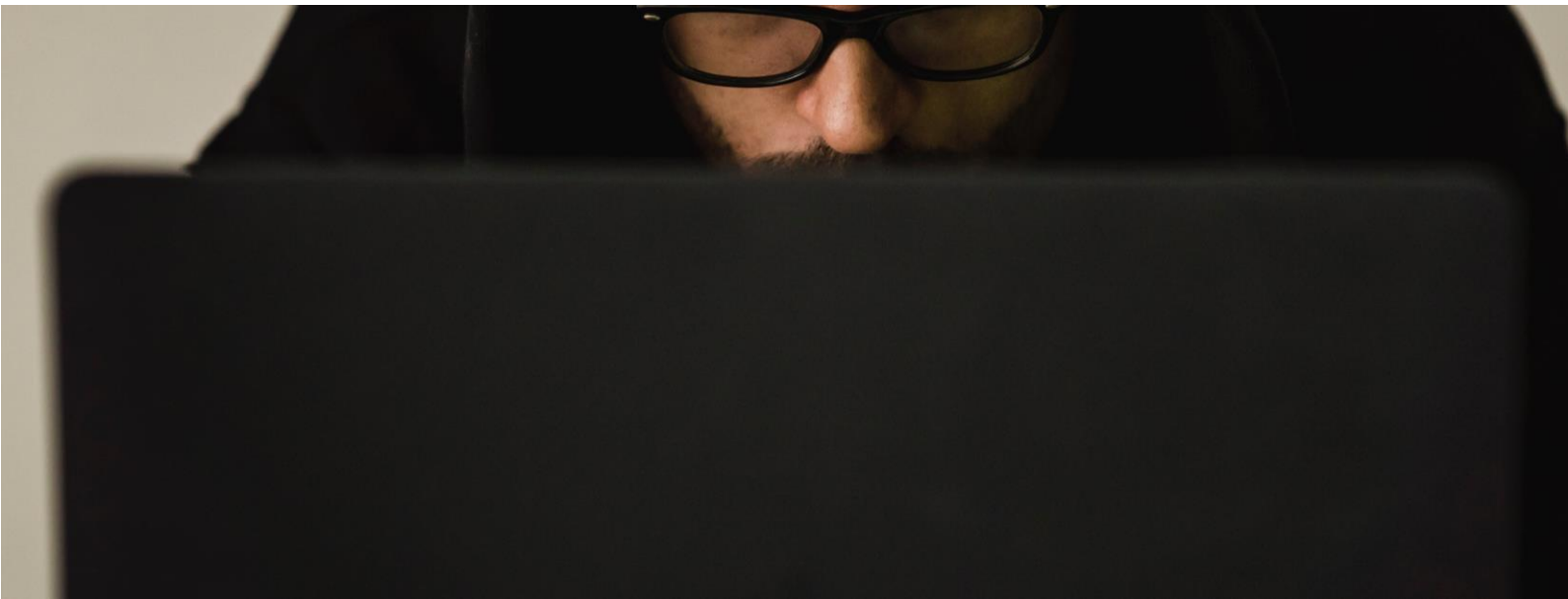
NetSupport RAT's modus operandi involves tricking victims, persuading them to download fake browser updates from compromised platforms. This adaptable and cunning infection tactic leaves a subtle but unmistakable imprint on the ever-changing canvas of cybersecurity. Faced with this stealthy resurgence, cybersecurity demands a vigilant and strategic approach. User awareness stands as an essential shield, educating them about phishing tactics and caution when downloading updates. Implementing advanced security solutions and keeping the technological infrastructure up-to-date become crucial barriers to stopping the onslaught of NetSupport RAT.

The NetSupport RAT can trigger devastating consequences once it manages to infiltrate a system. Attackers, armed with this malware, can execute various malicious actions, such as stealing sensitive data, remotely controlling the affected system, and even interrupting essential services. This set of capabilities threatens not only the confidentiality of information, but also to cause financial losses and damage the reputation of victims. The presence of NetSupport RAT has been detected in various sectors, from education to business services. Schools, universities, government entities and businesses have been targeted by this remote access Trojan, underscoring the breadth of its threat. NetSupport RAT employs a variety of methods to spread, including phishing, code injection and manual downloading of the malware. The diversity of strategies makes detection and prevention constant challenges in this strategic game in cyberspace.

In this scenario, **the defence against the rebirth of NetSupport RAT** requires strong preventive measures. User awareness, a strict policy of updates, investment in advanced security solutions, constant updating of systems and the implementation of continuous monitoring systems are key recommendations to mitigate risk and protect the cyber environment. The collaboration between the cybersecurity community stands as a shared strength, joining forces to understand and neutralise emerging threats. In this dynamic game between attackers and defenders, every mitigation measure constitutes a crucial step towards preserving digital integrity in this interconnected world.

Martín Bedoya
Cybersecurity Lead Analyst

Orlando Ospina
Cybersecurity Analyst



WELCOME, YEAR 2024. WILL CYBERSECURITY TRENDS CHANGE?

TRENDS

As the year draws to a close, it becomes customary for us to assess the cyber security outlook of companies and find that despite having ongoing risk assessment processes, they are failing to reduce their exposure to threats. This is due to the fact that unrealistic, isolated and tool-centric approaches still persist.

Forbes has indicated that, by the end of 2024, the cost of cyber attacks on the global economy will exceed $10.5 trillion. These numbers demonstrate a growing need on the topic of cybersecurity, and its strategic priority at the individual and organisational level.
We have been preparing ourselves to face new trends and technologies in our organisations, talking about the Internet of Things (IoT), Big Data, 5G and now Artificial Intelligence (AI). This leads us to think not only about new business opportunities, but also about new ways in which cybercriminals can attack us. However, nothing could be further from the truth when we observe that these "new ways" are still the same ones we "fight" year after year:

For example, organisations such as CISA (Cybersecurity & Infrastructure Security Agency) and ENISA (European Union Agency for Cybersecurity) agree that considering the impact and the frequency with which the various threats can be made or identified, we can consider them in the following groups:

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats to availability
- Manipulation of information
- Supply chain attacks

As organisations face a struggle to keep up with an ever-evolving threat landscape, cybersecurity leaders often resort to reactive approaches that only constantly pursue threats and seek to reduce any potential incidents. This is contrary to a strategy of initiating and maturing programs with a new approach to be able to more proactively understand the attack surface to which they are exposed, we believe that this would allow them to better prioritise their efforts and measure progress over time.

The recommendations in this situation are as follows:

Ensuring that the results of exposure management contribute to multiple parts of the security and IT organisations by designing a programme to manage a broader set of exposures.

Considering threat exposure scenarios using areas that are emerging and are associated with your attack surface management and security posture.

Integrating continuous threat exposure management and have each cycle adhere to a five-step process (scoping, discovery, prioritisation, validation and mobilisation) associated with your incident management flow.

Jorge Trujillo
CyberSecurity Specialist

Application-layer encryption as a strategy to strengthen the security posture

Encryption has established itself as a fundamental tool to safeguard the confidentiality of information. Through mathematical mechanisms, it is possible to transform a set of data to prevent unauthorised actors from being able to understand them. This process is fundamental when it comes to protecting the traffic of the systems that are deployed over the internet.

The TLS protocol (Transport Layer Security) plays a crucial role in securing the information transmitted in communications between a server and a client, it is responsible for adding the padlock to the browser in what is known as HTTPS. Operating at the transport layer, this protocol is responsible for encrypting the entire communication channel using encryption suites.

Activities such as key exchange, mutual authentication, encryption and integrity review using hashes are processes that are carried out thanks to TLS, which allows to guarantee confidentiality, integrity and non-repudiation, verifying that the parties involved are who they say they are and cannot deny the authenticity of the information exchanged. This comprehensive encryption process is an essential component in the protection against threats and enables a secure exchange of data.

Although the TLS protocol guarantees an encrypted communication channel over the internet, it is important to note that encryption applies exclusively to the channel. This means that, in practice, there is the possibility of capturing and manipulating information by abusing the trust of the TLS protocol. Therefore, as a defence-in-depth measure, application-layer encryption allows you to add additional control to protect data from requests travelling over the internet.

HTTPS Proxies are tools that allow to execute attacks known as "Man In The Middle" (Man in The Middle), because they have the ability to interfere in the TLS protocol by abusing its excessive trust in the browser. These proxies allow an attacker to observe and alter the parameters that are sent from a client to the server in a web or mobile application even when the information is protected by TLS. Since these tools are widely known by adversaries, it is necessary to consider additional security strategies that allow traffic to be protected.

The capture of the network traffic of a web or mobile application introduces a series of threats that must be taken into account from the design of the solution. Code injections, brute force attacks, user enumeration or session hijackings are commonly known attacks that can be carried out thanks to the possibility of inspecting application traffic.

To counteract these potential threats, it is possible to implement encryption at the application layer. This control focuses on protecting the confidentiality of the parameters that are sent in server requests and responses. To achieve this, software factories must implement this control directly in the application, that is, in the backend and frontend source code.

Programmers can use two fundamental concepts of cryptography: symmetric and asymmetric encryption. A symmetric encryption algorithm involves the use of a single key for both the encryption and decryption process. This approach, although efficient, poses the challenge of securely sharing the key between the parties of the communication. On the other hand, asymmetric ciphers use a pair of keys: one public and one private. The public key is shared openly, while the private key is kept secret. Information encrypted with the public key can only be effectively decrypted with the corresponding private key.

The choice of the type of encryption algorithm to be used should be defined from the design phase of the application. On the one hand, symmetric encryption, being lighter, allows data to be encrypted faster. However, it carries the risk that the shared key will be captured and the adversary will manage to decrypt the communication.

To solve this problem, programmers can implement dark obfuscation mechanisms to hide the key. In its counterpart, asymmetric encryption provides greater security, since the decryption key is not shared. Despite this, asymmetric encryption algorithms require a higher computing capacity due to algorithmic complexity, which can seriously impact the performance and user experience of the application. Hence, the implementation of encryption at the application layer should be a control that should be implemented based on an analysis and in-depth knowledge of business needs.

It is important to consider that not applying encryption at the application layer introduces various threats to applications. However, the OWASP Foundation, which is an open community related to application security, does not elaborate on this control in its different methodological frameworks. This may be due to the impact on the performance of the application and the cost of implementation for the software factory.

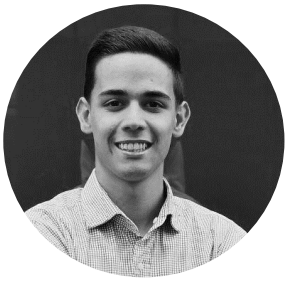
Historically, security and performance have gone in opposite ways. However, in recent years, computing capabilities have experienced a significant increase in power and a considerable reduction in costs thanks to the cloud, making the implementation of encryption at the application layer more viable.

On the other hand, finding programmers who implement cryptography can be a challenge for software factories, the need for more experienced programmers increases the cost per hour-development, these costs have been a significant barrier to the widespread adoption of application layer encryption. However, there is currently a change in this panorama thanks to the increase in Open-Source libraries and related documentation on how to encrypt in programming languages for the web.

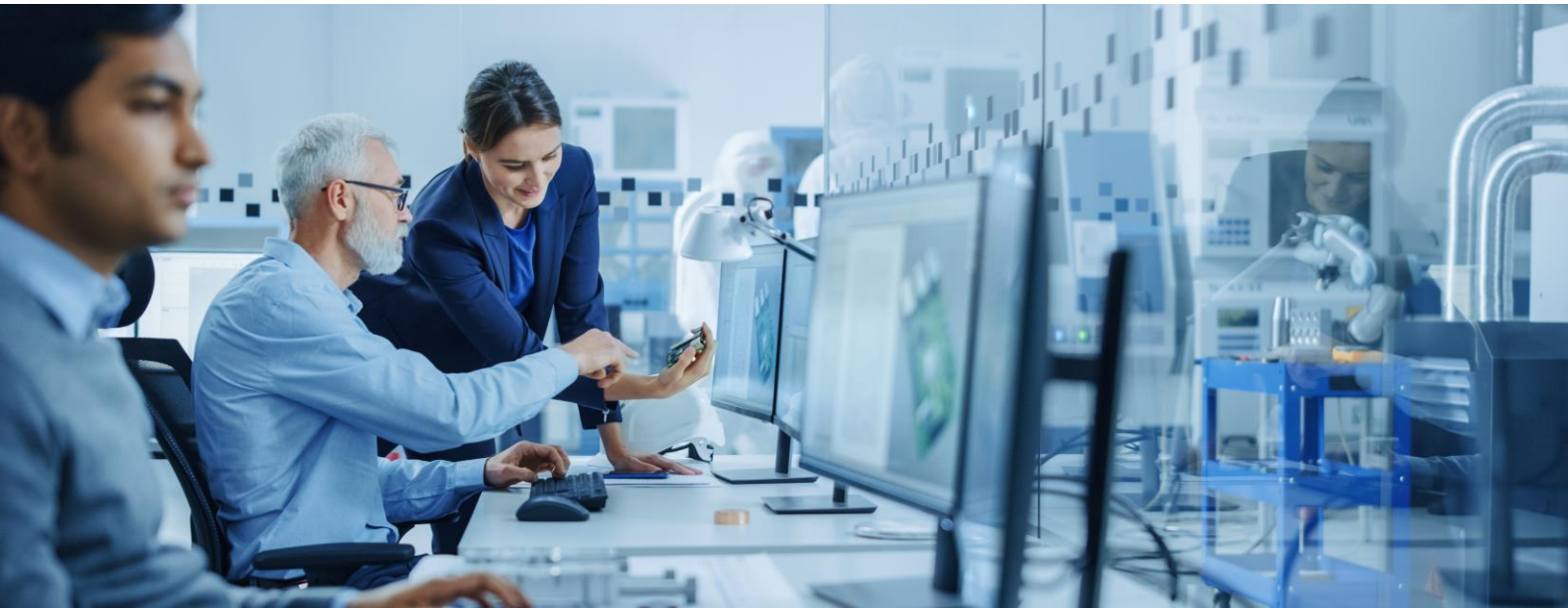
Despite this progress, OWASP has not yet included traffic interception as a vulnerability criterion for web applications; it did at the time for mobile applications, however, it is a control that they subsequently depreciated. Security priorities and approaches change over time as technologies and cyber threats evolve. It is crucial for software factories to follow up-to-date security practices and anticipate changes in the technological environment that introduce new threats. It is likely that OWASP will incorporate this control in its next updates.

In summary, the TLS protocol, although valuable for the protection of the communications channel, is not sufficient to guarantee the protection of information against interceptions. Therefore, the implementation of encryption at the application layer is a security strategy that can be used by software factories to strengthen their security posture and raise the level of application security maturity. Every day the implementation of this control is more economical and its benefits are easily measurable, because the motivation of an adversary to compromise an application can be diminished when they must not only evade TLS, but an additional layer of encryption.

Martín Bedoya
Cybersecurity Lead Analyst



José Cianci
Cybersecurity Analyst



Neobanks and trends in cybersecurity: challenges and opportunities

In recent years the financial industry has undergone a great digital transformation which has led, among other aspects, to the arrival of neobanks. These are financial institutions that offer their services under a totally digital scheme, without the traditional physical branches, betting on a differentiation in the agility and practicality for the enrolment of users, as well as in the acquisition and use of their products.

As neobanks are positioning themselves in the market and are adding more and more users, cybersecurity is emerging as a key element in this new financial landscape. In this article, we will explore some of the main challenges and opportunities facing neobanks today, in the field of cybersecurity:

Challenges that Neobanks should take into account

Strong authentication: Secure authentication is essential in a fully digital financial environment, implementing measures such as multi-factor authentication and biometric technologies becomes crucial to ensure users' identity validation processes as well as the secure execution of transactions.

Increase and evolution of cyber threats: their 100% digital value proposition makes them a very attractive target for cyber attacks such as phishing, Ransomware, denial of services, online fraud, among others; which could seriously compromise the security of users' financial and personal information.

Cloud storage: the vast majority of neobanks store data in the cloud in order to facilitate access and agility in their services, which requires implementing more advanced security measures to protect this data.

Privacy of personal data: the collection and handling of data are fundamental for the operation of neobanks, ensuring the privacy and security of this personal information is crucial to build and maintain the trust of their customers.

Regulatory compliance: as neobanks expand, they face challenges in terms of regulatory compliance since cybersecurity and privacy regulations are also evolving and becoming increasingly demanding with these types of innovative proposals in the financial market; in that sense, neobanks must adapt and ensure compliance with such regulations in order to avoid possible fines or penalties.

User education: user awareness and education are key components in the defence against cyber threats. Neobanks should provide clear information on security best practices, identification of potential threats and how users can protect themselves.

Opportunities in the midst of challenges

Just as there are multiple challenges in cybersecurity, neobanks also have the opportunity to stand out and build user trust by taking proactive measures.

They have a wide range of options to invest in security tools and emerging technologies, such as artificial intelligence, machine learning, threat intelligence, among others, to anticipate threats and strengthen their defences.

In addition, they can add and/or improve their capabilities through expert providers that offer specialised knowledge and advanced solutions for the different challenges they must address in terms of cybersecurity.

In conclusion, as neobanks open up new possibilities in the financial landscape, cybersecurity becomes a fundamental pillar of their success and sustainability. The adoption of emerging technologies and support in cybersecurity expert providers will allow them to thrive in an increasingly dynamic and threatening environment. The key lies in the ability to maintain a balance between innovation and security to offer reliable digital financial services.

Milagros Silvia
Cybersecurity Expert Consultant

If you want to receive this PDF monthly in your mail, subscribe to the RADAR newsletter to stay up to date with all the news about cybersecurity.

Business Continuity Management: IT and OT

Business Continuity Management (BCM) is the set of activities, processes, tools, people and controls previously defined, structured, documented and tested, which aim to guarantee the minimum continuity, previously agreed, of the services and / or areas that support the business, when one or more relevant resources for the organisation are not available. The BCM allows the organisation to have a lower impact, a certain predictability and an adequate continuity of its activities.

Corporate governance has principles. One of them demands sustainability. As such, the existence of the BCM is the responsibility of the Management Body and/or the Board of Directors.
1. Transparency: To inform and make the information available correctly.
2. Equity: Fair and non-discriminatory treatment.
3. Accountability: Responsibility.
4. Corporate continuity: Sustainability of the organisation.

Types of resources

For a better structuring, implementation and maintenance of the BCM, it is important to identify which types of resources exist and which should be considered.

Information Technology (IT) resources: they are resources in which information or data are the main elements to be considered in their various forms and presentations. This set of resources is the most well-known and used in organisations. It is the most advanced in terms of processing and communication. It has a high maturity in terms of security.

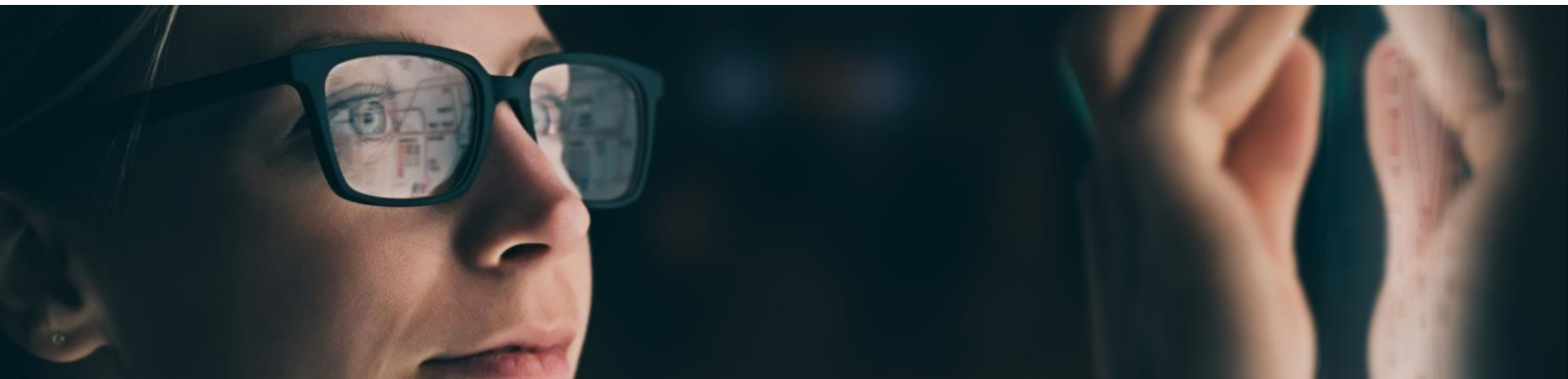
Operational Technology (OT) Resources: when the resource to be considered is not, essentially, of an information or data nature. In this group, equipment with some processing for industrial, sanitary and agro-industrial areas are considered. They are resources of the Internet of Things (IoT). There are many types of equipment.

Considering the controls of confidentiality, integrity, availability, legality, non-repudiation and reliability, all of them are important for the functioning of organisations. However, there is a security router for each type of technology. For information technology, the priority is confidentiality. For operational technologies, the priority is availability. Then there are the other controls.

Information Technology security is more mature and has defined equipment, applications, legislation and standards. Security for Operational Technology is less mature, due to its need for security. Until recently, Operational Technology dealt with the environment of industrial machines, with operation very limited to one piece of equipment or groups of equipment normally in a factory. With the development of the Internet of Things (IoT), the field of Operational Technology has become more sophisticated and has gone beyond the industrial environment. Agribusiness is using soil sensors to indicate humidity and other factors in large fields, as well as to control its machinery. The healthcare sector is using examination equipment, remote operations with robots or intra-corporeal machines such as pacemakers and chips that collect information from the body. Smart cities are growing, generating facilities and taking care of citizens' privacy.

However, whether it is Information Technology or Operational Technology, Business Continuity Plans must be in place. The macro controls are the same. However, in each of them there will be a specific application for information or smart "things".

The steps described below are indicative and should always be used taking into account the characteristics of the environment that you want to protect. They are as follows (next page)



Identification of threats: all possible threats must be identified. However, the threats that will be considered for the plan must be defined.

Scope and scenario
The scope is the range of resources and environments that will be taken into account. The scenario is the time and the concrete conditions of the possible unavailability situation.

Prioritisation of resources
It is the definition of the order of priority and time for the recovery of resources. The Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) are identified taking into account the data loss. This prioritisation can be identified by a Business Impact Analysis (BIA) process, a contractual requirement, a legal requirement or a Board of Directors definition.

Selection of the strategy
It is about defining the alternative solution for the resource or the environment. The priorities and the cost of implementing the alternative solution will be taken into account.

Structuring and elaboration of the plan
It is about designing the teams, the flow, the activities, the responsibilities and the documentation.

Planning and conducting of tests
It is about the planning, preparation, structuring, authorisation, execution and evaluation of the tests.

Maintenance of the plan
It is about the planning and the rules of regular updating and specific updating.

Crisis plan and communication plan
From the point of view of the BCM, the Crisis Plan and the Communication Plan exist to support and enable the holistic action of all areas of the organisation. Of course, they can have an independent life, but in practice they complement and enable the effectiveness of other plans.

Crisis plan: a set of actions and controls that the organisation must plan when an unexpected event occurs that may have a negative impact on the organisation.

Communication plan: this plan guarantees the existence of internal communication within the organisation and also (mainly) the communication of the organisation with the external environment, such as the press, customers, shareholders, supervisory bodies or the like.

Business Continuity Management it should be designed and built specifically for each organisation and each organisational situation. There is no such thing as a "ready-made plan." Professionals involved in business continuity management must have knowledge and experience in contingency plans and situations.

Edison Goncalves
Cybersecurity Evangelist

Vulnerabilities

Multiple vulnerabilities in Dell devices

Date: December 4, 2023
CVE: CVE-2023-44304 and 1 more

SSQ: 9.8

CRITICAL

Description

Dell has reported multiple vulnerabilities in its "Dell DM5500" product, in all versions prior to 5.14.0.0. Among them, two critical vulnerabilities stand out.

One of these vulnerabilities, CVE-2023-44302, allows an attacker to gain access to the device without first authenticating on it, there being the possibility of executing remote code and obtaining control of the affected computer.

In addition, the other critical vulnerability discovered on this device is given the identifier CVE-2023-44304. This vulnerability is focused on elevation of privilege, allowing an attacker with low security privileges to bypass the restrictions it contains by its role, allowing access to the root of the device and view its contents.

In addition, other vulnerabilities of lesser severity have also been discovered focused also on privilege escalation.

Affected products

This vulnerability affects the following versions:

- All versions prior to 5.14.0.0.

Solution

Dell has published a notice (DSA 2023-425), which indicates that the main solution to solve this vulnerability is to update to the latest version of the device.

Links

- www.dell.com
- nvd.nist.gov
- www.cvedetails.com

Critical vulnerability in Apache Struts software

Date: December 7, 2023
CVE: CVE-2023-50164

SSQ: 9.8

CRITICAL

Description

On December 7, 2023, a vulnerability was published in the Apache Struts software, a support tool for the development of web applications using Java.

The critical vulnerability, once exploited, may allow an attacker to execute remote code on the affected device.

In order to perform the remote code execution, an attacker must take advantage of an incorrect configuration on the server, performing a “Transverse Path” type attack. From this point, there is the possibility of uploading a file to the web server itself that allows a remote code execution on it.

This vulnerability has been identified as CVE-2023-50164, and Apache has recommended its users to upgrade to the new versions to fix these security flaws as soon as possible.

Affected products

The different products affected by this vulnerability are as follows:

- Versions prior to 2.5.33.
- Versions prior to 6.3.0.2.

Solution

The solution proposed by the manufacturer consists of updating to the aforementioned versions:

- Version 2.5.33.
- Version 6.3.0.2.

Links

- www.incibe.es
- lists.apache.org

Patches

CRITICAL **Multiple security patches for Android devices**

Date: December 4, 2023
CVE: CVE-2023-40077 and 4 more

Description

Android has published new security patches that fix a large number of vulnerabilities in all its devices, some of them being categorised as critical.

The following are the four critical vulnerabilities:

- CVE-2023-40077: privilege escalation vulnerability.
- CVE-2023-40076: which allows access to other users' credentials.
- CVE-2023-40088: vulnerability that allows memory corruption.
- CVE-2023-45866: vulnerability that allows the injection of HID messages.
- CVE-2022-40507: vulnerability that allows memory corruption.

The vulnerabilities affect both the operating system, as well as system components, the structure, MediaTek and Qualcomm.

Affected products

The following products have been affected by these vulnerabilities:

- Android (version 14)
- Android (version 13)
- Android (version 12L)
- Android (version 12)
- Android (version 11)

Solution

The solution consists in updating the security patches published in the December newsletter (depending on the version of the operating system installed in each case).

Links

- source.android.com
- www.csa.gov.sg
- www.incibe.es

CRITICAL **New security patches for Microsoft products**

Date: December 12, 2023
CVE: CVE-2023-35618 and 1 more

Description

On December 12, Microsoft released a series of updates to remedy multiple security vulnerabilities in its Windows operating systems and other *softwares*. In total, 36 vulnerabilities have been published, of which 2 are critical, 23 important and 11 of medium severity.

The following are the vulnerabilities categorised as critical:

- CVE-2023-35618: Vulnerability affecting Microsoft Edge. Once this application has been compromised, the necessary privileges can be obtained to execute code on the compromised machine.
- CVE-2023-36019: This vulnerability affects Microsoft Power Platform and Azure Logic Apps services. It focuses on a “spoofing” type attack that originates when clicking on a link provided by the attacker to redirect the victim to another malicious link or file.

The rest of the vulnerabilities belong to several types: denial of service, privilege escalation, information disclosure, remote code execution and phishing.

Affected products

These vulnerabilities cover a large number of Microsoft products. These products can be consulted in: msrc.microsoft.com

Solution

Apply the corresponding security patch on the affected products.

Links

- msrc.microsoft.com
- thehackernews.com

Events

SANS Cloud Defender 2024 (Live Online) (8 - 13 January)

The SANS Cloud Defender 2024 will take place online from January 8th to 13th. This course offers an immersion training designed so that interested security and/or IT professionals can learn how to build, deploy and manage secure infrastructures, platforms and applications in the cloud.

Link

CSA AI Summit (17 - 18 January)

The CSA AI Summit is an outstanding event that seeks to bring together industry experts in order to provide guidance on critical Artificial Intelligence (AI) issues and their impact on cybersecurity. For 2 days, it offers key information on how generative AI can benefit cybersecurity, how cyber attackers are using it and the guidelines that should be considered for responsible use.

Link

SANS Cyber Threat Intelligence Summit & Training 2024 (January 29 - February 5, 2024)

The SANS Cyber Threat Intelligence Summit & Training is an event that takes place in Washington DC, United States from January 29 to February 5. This event, which can also be accessed online, aims to enable those interested in the industry to acquire new perspectives and learn from case studies that challenge the assumptions of cyber threat intelligence, leading to a change in their understanding.

Link

Resources

Certificate of Competence in Zero Trust (CCZT) FAQ:
The Certificate of Competence Zero Trust (CCZT) is an industry-leading resource that provides technology professionals with the essential knowledge to understand and apply the Zero Trust principles. In the FAQ document prepared by the Cloud Security Alliance (CSA), you can find more information about the benefits of the CCZT and how to access it.

Link

Mitigation of security risks in applications based on Retrieval Augmented Generation (RAG) LLM

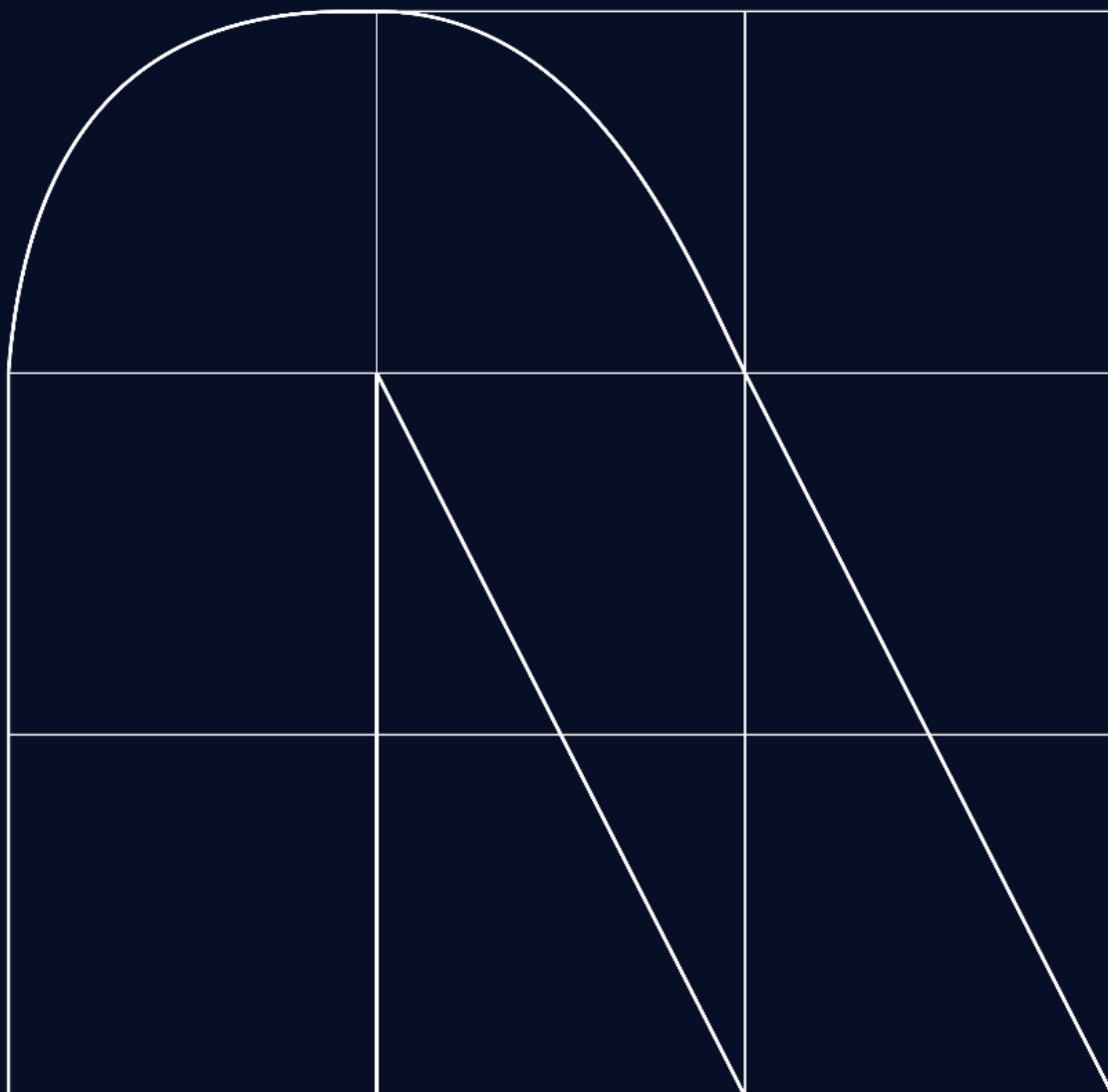
Retrieval Augmented Generation is an effective technique used by AI engineers to develop applications based on large linguistic models (LLM). However, it has been identified that the lack of security controls in RAG-based LLM applications can pose risks if not properly addressed. Due to this, the article prepared by the Cloud Security Alliance, has the following objectives: (i) analysing the RAG architecture, (ii) identifying the potential security risks at each stage; and, (iii) providing technical recommendations to mitigate said risks, thus serving as a practical guide for developers.

Link

GPT-4 Turbo

OpenAI announces the launch of GPT-4 Turbo, a new generation of the large language model, LLM in English, which promises to overcome the weaknesses of the previous ones, GPT-3.5 and GPT-4, to be faster and cheaper. This new version reaches a context length of 128,000 tokens, that is, the amount of text it supports and understands when the chatbot is asked a question. In addition, it can accept images as inputs in the Chat Completions API, allowing use cases such as generating captions, analysing real-world images in detail, and reading documents with figures.

Link



Powered by the Cybersecurity NTT DATA team

es.nttdata.com