NUMBER 65 | ARPIL 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

THE ISO/IEC 27002:2022 STANDARD HAS BEEN UPDATED

ISO27002 has just released an update eight years after the last revision, and what many of us are wondering is what relevant changes are in this new version. It is worth remembering that ISO 27002 is a complementary standard for organisations that have implemented ISO 27001, which helps to implement the most effective best practices and controls to prevent attacks or breaches of organisations' information and privacy and those of their stakeholders.

For most organisations, ISO/IEC 27002:2013 was perceived as a compendium of practices that was set in a rigid framework of domains and was not adapted to organisations' needs and requirements in a global environment. The context of teleworking, cloud management, the incursion of new forms of security and cryptology, etc. has made it necessary for ISO 27002 to focus more effectively on the attributes of controls than on the control domain itself.

Attributes can be defined according to:

- The type of control and its function: preventive, detective, or corrective.
- Information requirements, which may be confidentiality, integrity, and availability. In this section, it is necessary to review the regulations of each geographical region.
- The cybersecurity purpose or objective, which may be to identify, protect, detect, respond, and recover.
- Operational capabilities such as asset management, HR security, governance, information protection, application security, access controls, risk, threats and vulnerabilities, regulatory compliance, and security in provider relationships, among others.
- Security domains.

For this reason, the new version of ISO/IEC 27002:20022 has fallen into place, not only as a security option, but also as a solution for this new reality, due to all the major changes it presents.

One of the changes that is giving us more things to consider is the simplification of the classification of controls into 4 domains. In practice, no controls have been eliminated. They have only been merged, split, or renamed, with the aim of reducing efforts in the implementation of the standard, all in collaboration with the ISMS.

Through this simplification, the important things in security are quickly perceived: organisation, people, physical environment, and technological environment. Perhaps the part of organisation, physical environment and technological environment is clearly accepted, and many organisations focus their investments there, but we particularly like the fact that the focus of another domain is on people.

This point is very relevant and is clearly aligned with what we think: the individual is the key factor in cybersecurity and the main focus of vulnerabilities within organisations. As we have already written about this topic in previous RADAR articles, in this issue we will focus a little more on the evolution of ISO27002 and once again remind you of the key points of cloud security.

María Isabel Patón

Cybersecurity Technical Manager at NTT Data Europe & Latam

CYBER NEWS

Today we begin our cyberchronicle with an eye on the war between Russia and Ukraine, not only because of the videos of bombings and displacement of people, but also because of the cyberwar that has been developing in its wake.

Russian-allied hacker groups, such as Fancy Bear and Mustang Panda, have launched several phishing campaigns against Ukraine and Poland, targeting company officials and citizens by impersonating members of the Ukrainian mail service UKR.net, compromising their credentials and then stealing confidential information or using them as mechanisms to publish fake news and send emails with links to fraudulent portals. A real targeted social engineering campaign.

> “Mykhailo Fedorov, posted on his twitter account: *We are creating a digital army, there will be tasks for everyone.*”.

Also, DDoS attacks on Ukrainian government sites such as the Ministry of Foreign Affairs, Ministry of Defence, Security Services (SBU) and banks such as PrivatBank were confirmed by Netblock and later by Cloudflare.

These actions are being carried out by Russian-allied hacker groups after Ukraine was admitted to NATO’s Cooperative Cyber Defence Centre of Excellence (CCDCOE).

But Ukraine is not far behind, the Ukrainian deputy prime minister and also minister of digital transformation Mykhailo Fedorov, posted on his twitter account: “We are creating a digital army, there will be tasks for everyone.” for any volunteers with computer defence skills to help guard the country’s cyber infrastructure.

And in addition to this, a telegram link to the “IT army of Ukraine” group, which now has thousands of subscribers, brings together hackers to attack some 31 Russian targets included in a list distributed within the group, as well as manuals for generating denial-of-service attacks that include how to hide identity through public VPN services or the use of sockets.

The Ukrainian minister’s initiative has been joined by the hacktivist collective Anonymous, which has confirmed its support for Ukraine against Russia, attacking civilian organisations such as the TASS news agency and the Kommersant newspaper, in which a message could be read against the military operation led by Vladimir Putin and which they referred to as “madness”.

Days later, a video circulated on Twitter in which the live television services of channels such as Russia 24, Channel One and Moscow 24 were interrupted in order to broadcast images of the results of the Russian invasion, and this was also taken to platforms such as Wink and Ivi, similar to Netflix.

The distraction generated by the cyberwar between Russia and Ukraine has allowed cybercriminals like the LAPSUS$ group, who, not content with the attack on the multinational NVIDIA, chose Samsung and MercadoLibre as their next targets; in the first case, they requested the release of the limit applied to NVIDIA's GPUs to increase their mining power, this was demanded as a reward for not disclosing a terabyte of exfiltrated data.

Meanwhile, the South Korean company had part of the source code of its Galaxy line of mobile phones extracted. The Argentinian e-commerce company MercadoLibre confirmed the compromise of the data of at least 300,000 of its 140 million registered users.

In times of war, the sophistication of attacks can increase, and the rewards demanded by cyber-criminals or even ransoms can be outrageous, so it is important that organisations maintain a conscious and proactive cybersecurity posture from all sides, with a cross-cutting approach to all areas of the company, including monitoring exercises of exposed systems, audits of vital technology components and awareness-raising activities for operational staff.

CYBERSECURITY AS A CROSS-CUTTING ISSUE WHEN MIGRATING TO THE CLOUD.

By: NTT DATA

Switching to cloud computing is nowadays a strategic objective for companies, due to the multiple benefits it contains for the business, such as remaining profitable in the long term, reducing costs, and offering more and better services to their customers.

Migrating to a cloud space has become an essential step that needs to be achieved as quickly as possible to take advantage of the benefits it offers rapid scalability to meet demand, cost reduction as you can pay only for what you use and agility to adapt to change and the ability to innovate.

However, although the benefits and advantages are already known, there is still uncertainty about how to start this transformation process and all that it implies: migration, costs, risks. Step-by-step migration can become an option for companies to start their operations in the cloud, thus reducing risk and identifying gains in a short time.

It is important to consider that throughout this transition process, which often involves a radical change for the company, cybersecurity should not be lost from sight and its management should be considered as a cross-cutting issue throughout the transformation. Most cloud transition programs carry with them the risk of creating inconsistencies and can lead to security breaches due to the complexity of managing the migration.

Possible approaches

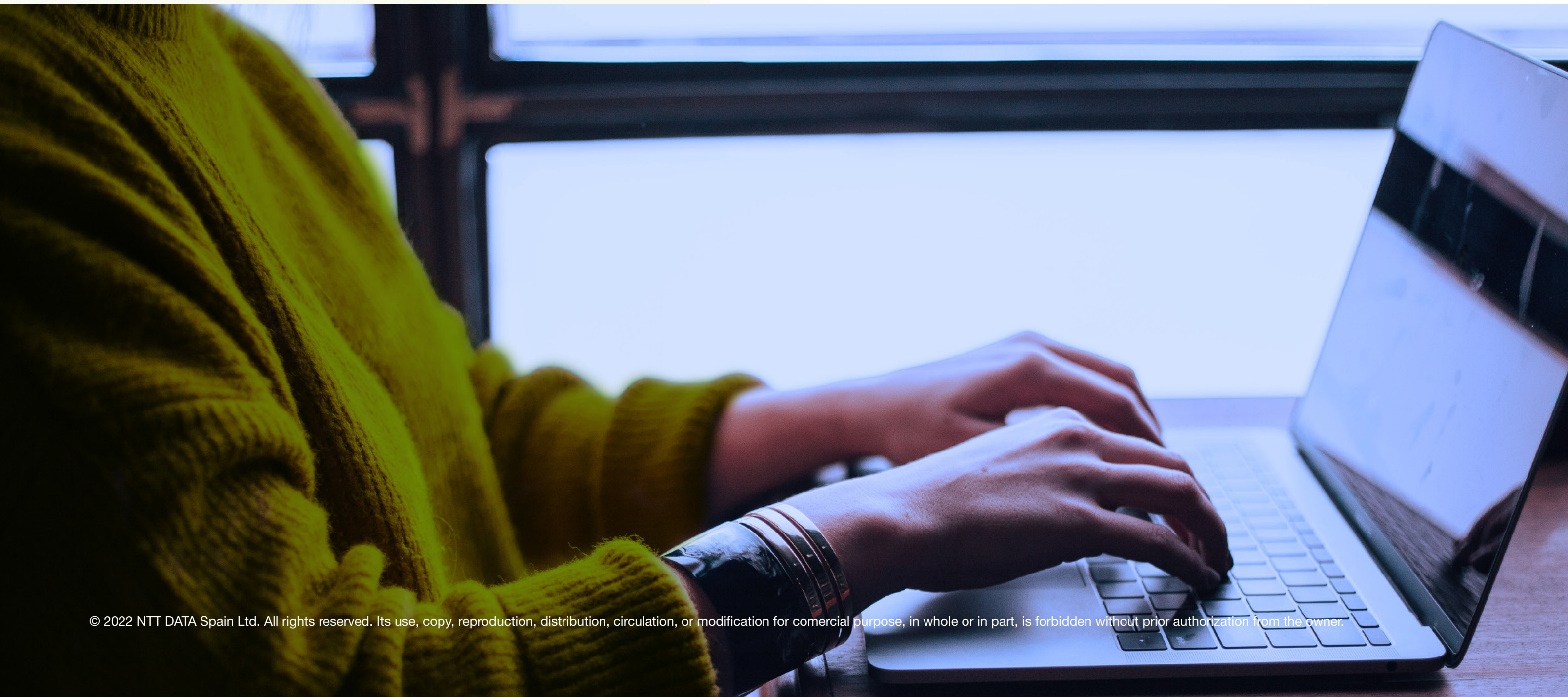
There are three approaches and multiple solutions that companies can follow through different methods to migrate to the cloud:

- Software as a Service (SaaS)

This approach offers a competitive advantage, because companies can use standardised commercial software solutions to quickly access the benefits of cloud services. These commercial solutions can be ERP or CRM systems, which, although they already exist in the market, can be beneficial due to their constant evolution by improving their functionalities, as well as sector-specific and customisable software platforms, which allow companies to gain benefits faster compared to a conventional process. On the other hand, SaaS can also be leveraged to develop services for end customers.

- Application migration

This approach involves studying the company's current portfolio of applications, so that decisions can be made as to which applications are eliminated, replaced, or migrated; achieving greater operational efficiency. It aims to create environments that optimise business operations and therefore achieve long-term competitive advantage.



- DevOps model

In this approach, the company has a potential advantage as the application portfolio is cloud-native, work is more agile as it allows the development team to access innovations quickly, all based on the DevOps model with all the benefits that entails. The disadvantage of this model is that there can be a certain decentralisation of control when security is not prioritised. Therefore, this approach seeks to add security using the DevSecOps model, where this aspect represents a fundamental responsibility of each member of the team and therefore must be properly managed.

Threats to consider

Although migrating to the cloud is a challenge with expectations of multiple benefits, it is important to consider that, in every process, security represents a key element to ensure that these benefits are achieved, which is why its consequences must be identified and managed with full responsibility.

- Data usage: This is the most well-known risk when migrating to the cloud. There are policies and regulations such as the General Data Protection Regulation, so companies are required to take special care with its storage, access, and use, preventing a possible loss of data.
- Identity management: Secure access to applications according to a role, responsibility, and privileges of each user in the organisation will ensure that access to data is not vulnerable to failures that allow easy access to intruders.
- Interfaces: In the cloud, the possibility of developing interfaces is scalable, multidimensional, and flexible. Shared platforms and corporate environments are used. Most APIs offer services through a common portal, which is a point that can be exploited by cybercriminals, as they can access the API's main code and thereby obtain service and customer data.
- Interconnection and Information Sharing: The use of shared technology saves costs and provides speed in development, but the company can be implicated in problems caused by other companies using the same software. Strict security management must be in place to ensure that the benefits of shared environments are not compromised by security breaches.
- Malicious attacks: There are three factors: online crime, countries with hostile intentions, and dissatisfied customers and employees, all of which can lead to security incidents that can cause attacks on the security infrastructure of enterprises.
- Organisational transformation: The transformation of the company through the migration to the cloud is a process that brings security risks, and it is important that these can be identified, quantified, and mitigated during this transformation process.

Hybrid environments

During the process of migrating from an on-premises environment to a cloud-native environment and given its complexity, the organisation may need to plan strategies and have the resources in place to deal with threats fully and effectively. Services and processes must be operated by data centre, network and cloud providers that are able to adapt, scale and grow with the business, and given these circumstances, security must be present in hybrid cloud-network systems.

The proposed architecture consists of 4 types of platforms: Foundations, referring to network topology resources and services, storage architecture and basic management systems. Catalogue, to offer customised services and individual resources. Models, a platform with programming resources and Digital Capabilities that provides access to development resources and accelerates the launch of new services.

The reference architecture is based on three vertical management areas that apply to the described platforms: observation for the control of all processes, capabilities and resources and connection between them; reliability that includes all systems and processes related to business plans and disaster recovery; and finally, security, an area dedicated to governance and management to maintain security throughout the environment.

Cybersecurity strategy

Business operations are constantly changing based on customers, ecosystem interactions and the balance between on-premises and cloud actions. Security measures must be implemented across all platforms (foundations, catalogue, models, and digital capabilities) applied across the corporate environment and in the cloud-native ecosystem, bearing in mind that security must be tailored according to the needs of the business. There are three key components to security management: an effective and consistent governance system, rigorous identity and access management, and methodologies and practices across the security lifecycle, all of which must be seriously considered before strategies can be implemented

Key solutions

To operate in a cloud environment, regardless of the size of the company, a certain level of security automation is required across the entire operating environment and while effective solutions exist for security management and monitoring, companies have a continuous battle to anticipate threats and adapt to the complexity of these environments.

The key solutions are:

- Infrastructure as Code (IAC), allowing security policies to be programmed and adopted automatically.
- Cloud Security Posture Management (CSPM), which automates the identification and remediation of risks anywhere in the cloud system.
- Work protection platforms, a tool that protects the security of specific tasks performed in multiple cloud environments.
- It is clear that cloud computing systems represent an advantage for companies to take full advantage of, which is why cybersecurity becomes a key and strategic point for the success of cloud migrations, as efficient security management is important.

WHAT ARE THE RELEVANT CHANGES IN THE UPDATE OF THE ISO/IEC 27002:2022 STANDARD?

By: NTT DATA

Undoubtedly, this is one of the questions that thousands of professionals dedicated to security issues within companies have asked themselves the most. For most organisations, the ISO/IEC 27002:2013 standard exuded an aroma of stagnation and did not fit the new environment in which organisations were operating globally. On the other hand, in the last 18 months, organisations have accelerated their digital transformation, and together with the rise of remote working, this has forced abrupt changes within them.

For this reason, the new version of ISO/IEC 27002:20022 comes at the right time, not only as a security option but also as a solution for this new reality, due to all the major changes it presents.

But how did this standard come about? what process does it follow? when is it published? what are its main changes?

In the midst of 2021, significant progress was made on the current ISO/IEC 27002:2022 standard, and a number of advances have been released. In 2022, the final updated version was published.

The new version brings with it important changes, the most representative being:

- Constant name changes (due to the names of the established committees being updated)
- Incorporation of new terms and definitions
- The new structure of information security topics
- The new structure of control attributes
- Changes in controls since ISO 27002:2013 version

Name change.

The development of the standard is established under a specific committee, for the development of each draft issued according to the code of stages of the standard.

The first ISO/IEC JTC 1/SC 27 committee named "Information Security, Cybersecurity and Privacy Protection", adopted its name in a first draft, thus remaining behind the context of Information Technologies, specifically in security techniques.

As a result, the prefix established in the standard was changed. The second name change to DIS was due to the international subcommittee by which it was revised and similarly adopted its name to ISO/IEC DIS 27002.

The name of the standard underwent a third alteration from "Code of Practice for Information Security Controls" to simply "Information Security Controls".

The updated standard is therefore named ISO/IEC 27002:2022 Information security, cybersecurity, and privacy protection - Information security controls.

1. Changes in categories and controls.

In our opinion, the most important change in the standard is the restructuring of the 14 domains of controls defined in ISO 27002:2013 to only four major themes and two annexes, as shown in the table below:

ISO/IEC 27002:2022	
Organisational controls:	37 organisational management controls
People-focused controls:	8 security controls focused on human resources
Physical controls:	14 security controls in the physical environment
Technological controls:	34 controls with security technology solutions
ANNEX A:	Matrix with the 93 controls and their attributes
ANNEX B:	Correspondence between the controls of the new version and the previous version.

Fuente: https://www.iso.org

his classification of functions is much simpler than that provided by the 2013 version of the standard and can be better covered by each area of organisations when they adopt this standard, which is much more oriented to the context of the application of the control (organisational, people, physical and technological). In the 2013 version, each domain established a series of control objectives (34) and then the information security controls (114); in this new version, there is no definition of control objectives (it is eliminated), with the new standard defining a total of 93 controls. However, the standard includes an attribute that allows for control-specific classification, whereby each control is classified into one or more of the 15 established categories, which will be explained later. This seems a rather positive change, as the establishment of controls according to their context of application makes the responsibilities of business personnel for managing information security, cybersecurity, and privacy protection much more evident. The elimination of control objectives is also a positive aspect, given that these are intrinsically defined in the control itself, being scarcely used in the 2013 version, providing very little value in practice. The main difference between the Draft International Standard (DIS) and the 2013 version is the structure of the set of controls. Most of the ISO 27002 controls remain unchanged but have now been regrouped from the existing 14 domains into 4 broad "Topics", depending on what the control refers to. In turn, four attributes have been associated with each control, which can be used to apply different grouping or filtering criteria and generate different "views" of the controls.

2. New structure of controls. One of the relevant aspects provided by the standard for each control is the structure of the controls, dividing this structure into 6 parts as we will see below:

Control Title	Name of the control
Table of Attributes	Values of each of the attributes for this control
Control	Description of the control
Purpose	Detailed explanation of the purpose of the control
Guidance	Guide for the implementation of the control
Other information	Bibliography or references to other documents with direct relevance to the control

New controls. In total, 11 controls were added plus 1 control that was restructured from the previous standard, corresponding to:

- Constant changes in the use of technology and data protection:

  5.7 Threat Intelligence.

  5.23 Information security for the use and services in the cloud.

  8.12 Data Leakage Prevention.

- Controls for sensitive data:

  8.10 Deletion of information.

  8.11 Data masking.

- Essential recognition of the role of technology in business resilience:

  5.30 Preparation of ICTs for business continuity.

  5.16 Identity Management

  7.40 Physical security monitoring

  8.1 User End Point Devices

  8.9 Configuration Management

  8.22 Web Filtering

  8.28 Secure Encryption

Controls that merge with the previous version:

NTTDATA CYBERSECURITY TEAM	
ISO/IEC 27002:2022	**ISO/IEC 27002:2013**
SOME CONTROLS HAVE BEEN INTEGRATED TO BECOME A MAIN CONTROL	
5.14 Information Transfer	13.2.1 Information transfer policies and procedures
	13.2.2 Information Transfer Agreements
8.24 Use of Cryptography	10.1.1 Policy on the Use of Cryptographic Controls
	10.1.2 Key management
	18.1.5 Regulation of Cryptographic Controls
THE OBJECTIVES OF SOME CONTROLS ARE SEPARATED IN ORDER TO EMPHASISE MONITORING	
8.15 Logging	12.4.1 Logging of events
8.16 Monitoring activities	12.4.3 Operator and administrator logging
FOCUS ON AND PROTECTION OF INFORMATION ASSETS IS PRIORITISED	
5.9 Inventory of information and other associated assets	8.1.1 Inventory of assets
5.10 Acceptable use of information and other associated assets	8.1.3 Acceptable use of assets

Hopefully, this evolution will bring organisations a renewed vision of the importance of cybersecurity in digital transformation and, therefore, in business development.

ZERO TRUST, THE KEY TO SECURITY IN CLOUD ENVIRONMENTS

A couple of years ago, in this very magazine, we talked about Zero Trust as the new security paradigm to face cyber-threats and challenges. In fact, it is still one of the most important topics in cybersecurity today, as adoption in many organisations is not yet complete..

Zero Trust extends the “distrust” from the external perimeter to the internal network, which establishes a new paradigm for the “freedoms” that users, applications and devices that interact on the internal network have. There is no single solution for implementing Zero Trust, so complementary options need to be considered to protect information assets along with the hardware, software and communication devices that store, process, or transmit them..

The model applies the principle of least privilege, which ensures that only data and resources that are actually required are accessed. This model not only verifies the device, but also verifies the identity.

How to address Zero Trust?

We can apply the Zero Trust model to both existing and new architectures. The first step for organisations is to conduct an assessment of their initial state, with the aim of identifying security gaps that could allow risks to materialise for potential attackers. At this point, we can ask ourselves the following questions:

1. What is my organisational context?

We need to know all the assets (workstations, IoT devices, routers, modems, etc.), users and business processes.

2. Which are the focus assets to secure?

Once the organisational context is known, it is easier to determine the areas that require the most work. To do this, we will identify and classify the critical resources that contain sensitive and/or confidential information in order to carry out more rigorous controls on them.

3. What controls do I currently have?

An identification of the existing controls of the prioritised assets must be carried out and their effectiveness must be determined.

4. Which users and devices access the information and how?

Employees, third parties, RPAs/bots, as well as users with identified privileged access and the detail of the information flow they use to access information.

5. What are the different solutions and the strategy to be followed?

Based on knowledge of the risk environment, we can identify solutions to counteract the security breaches found. Technical measures, ranging from a strong perimeter security to the implementation of a secure architecture that includes the business, data, application, infrastructure, and cybersecurity domains. In addition, the implementation and/or improvement of policies and processes that support these controls. Finally, awareness and supervision measures related to the people who are key to maintaining trust.

6. How to monitor and control it all?

The implementation of a Zero Trust policy must maintain permanent monitoring and evaluation schemes to ensure that the different security aspects are being controlled.

Zero Trust represents the future of network security; in fact, it has become a fundamental lever for business development. It is therefore essential for organisations to identify their initial level of maturity, identify the best practices that can be implemented and visualise the challenges, in order to avoid mistakes and ensure that this path develops in the most fluid and beneficial way.

VULNERABILITIES

SCHNEIDER ELECTRIC

CVE-2022-22805;-22806;-22783;-0715;-24323;-24322

Date: 09/03/2022

Description. Schneider Electric has published six vulnerabilities: two critical, two high and two medium severities. Of the two critical vulnerabilities, one allowed an attacker to remotely execute code on SmartConnect devices when a TLS packet is mishandled during reassembly. The vulnerability CVE-2022-22806 allows, via a malformed connection, to gain access to one of these devices without authentication.

Link: https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-067-02

https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2022-067-01

Affected Products.

- EcoStruxure™ Control Expert, V15.0 SP1 and prior
- EcoStruxure™ Process Expert, V2021 and prior
- Smart-UPS Family:
  - SMT Series: ID=18: UPS 09.8 and prior; ID=1040: UPS 01.2 and prior; ID=1031: UPS 03. and prior,
  - SMC Series: ID=1005: UPS 14.1 and prior; ID=1007: UPS 11.0 and prior; ID=1041: UPS 01.1 and prior,
  - SCL Series: ID=1030: UPS 02.5 and prior; ID=1036: UPS 02.5 and prior,
  - SMX Series: ID=20: UPS 10.2 and prior; ID=23: UPS 07.0 and prior,
  - SRT Series: ID=1010/1019/1025: UPS 08.3 and prior; ID=1024: UPS 01.0 and prior; ID=1020: UPS 10.4 and prior; ID=1021: UPS 12.2 and prior;
  - ID=1001/1013: UPS 05.1 and prior; ID=1002/1014: UPSa05.2 and prior
- SmartConnect Family:
  - SMT Series: ID=1015: UPS 04.5 and prior,
  - SMC Series: ID=1018: UPS 04.2 and prior,
  - SMTL Series: ID=1026: UPS 02.9 and prior,
  - SCL Series: ID=1029: UPS 02.5 and prior; ID=1030: UPS 02.5 and prior; ID=1036: UPS 02.5 and prior; ID=1037: UPS 03.1 and prior.
  - SMX Series: ID=1031: UPS 03.1 and prior,
- Ritto Wiser™ Door, and prior

Solution: Upgrading to the latest version provided by the provider.

Cisco

CVE-2022-0492

Date: 03/03/2022

Description. A critical vulnerability has been detected in Linux devices, which directly affects the computer kernel. The security flaw allows a user to use the "release_agent" functionality of the "cgroups v1" component, located in the computer's kernel, to escalate privileges.

Link: https://access.redhat.com/security/cve/cve-2022-0492

https://unit42.paloaltonetworks.com/cve-2022-0492-cgroups/

Affected Products.

- Affects all devices using Linux

Solution: Updating the Linux kernel to the latest available versions.

PATCHES

Microsoft ●

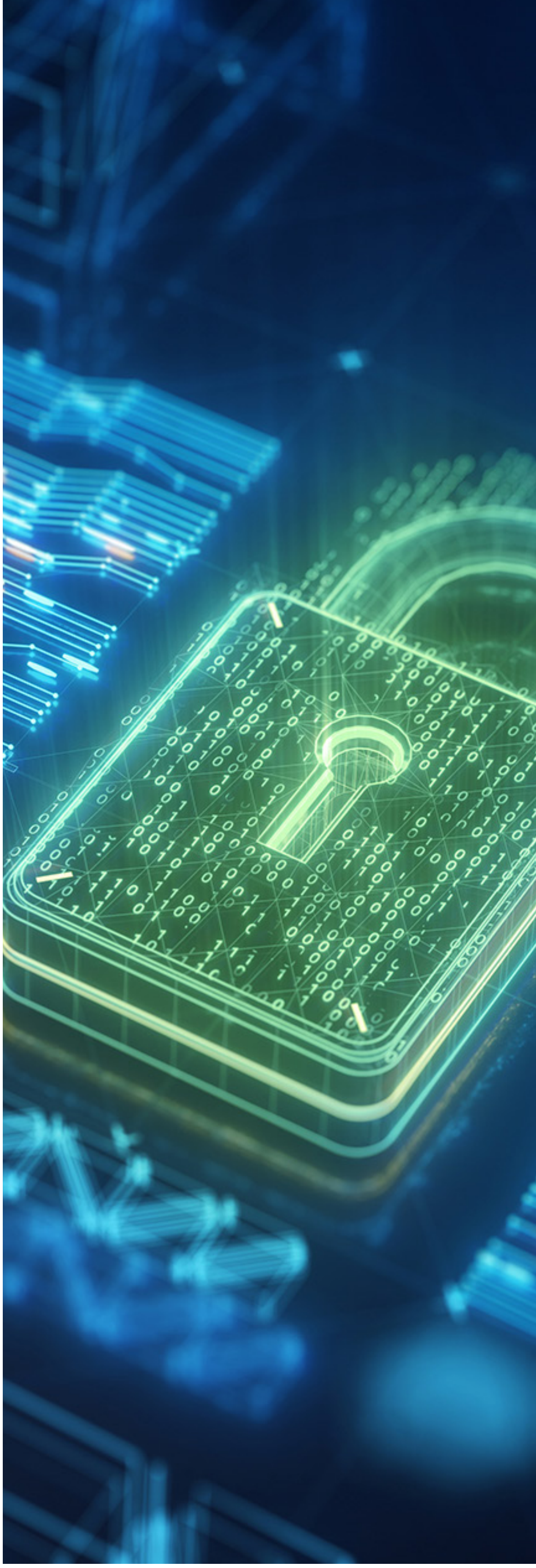
Date: 08-02-2022

Description. Microsoft has released the security bulletin for March, in which it indicates the need to apply the new security update patch. It fixes seventy-one vulnerabilities, three of which are critical and the remaining sixty-eight are of high severity.In addition, Microsoft also reportedly fixed three 0 Day vulnerabilities, one of which affected the remote desktop protocol.

Link: https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar

Affected Products:
See the complete list of products in the reference link.

Solution: Applying the patch available through the Windows Update Centre.



Adobe ●

Date: 09-03-2022

Description. Similar to Microsoft, Adobe has released a patch that fixes three high-severity vulnerabilities in the Adobe Photoshop, Illustrator and After Effects applications. These vulnerabilities allowed an attacker to execute arbitrary code on the system and leak data stored in memory.

Link: https://helpx.adobe.com/security/products/photoshop/apsb22-14.html
https://helpx.adobe.com/security/products/illustrator/apsb22-15.html
https://helpx.adobe.com/security/products/after_effects/apsb22-17.html

Affected Products:
Photoshop, Illustrator, After Effects.

Solution: Updating to the latest available version of these products.

EVENTS

IAPP Global Privacy Summit

April 12-13, 2022 |

The world's leading privacy and data protection conference focuses on the latest developments in privacy and data protection and international privacy policy and strategy. The Summit features world-class expert speakers and regulators and offers unparalleled training and networking opportunities.

Link: https://iapp.org/conference/global-privacy-summit/

AI in RegTech Summit

April 21-22, 2022|

Focused on regulatory compliance for the financial services industry, this conference brings together a mix of academic and industry professionals who will explore the business value of AI, including use cases for risk management and data security.

Link: https://www.re-work.co/events/ai-in-regtech-summit-newyork-2022?ref=infosec-conferences.com

Silicon Valley Cyber Security Summit

April 27 , 2022 |

The Fifth Annual Silicon Valley Cyber Security Summit will be held in person but will also be live-streamed. It connects senior executives responsible for protecting their companies' critical infrastructures with innovative solution providers and renowned information security experts.

Link: https://cybersecuritysummit.com/summit/siliconvalley22/

Third-Party & Supply Chain Cyber Security Summit

April 28-29 , 2022 |

The 5th Annual Third Party and Supply Chain Cyber Security Summit is a conference where best case studies will be shared on end-to-end cybersecurity implementation practices when working with third parties, to ensure a truly resilient and secure supply chain network.

Link: https://sccybersecurity.com/

RESOURCES

Guide to Cyber-attacks

The Internet Security Office (Oficina de Seguridad del Internauta, OSI) provides users with the "Guide to Cyber-attacks". It lists the types and characteristics of cyber-attacks of which we can become victims while surfing the Internet. In addition, the guide helps us to learn the most popular security terms such as phishing, dumpster, spoofing or cryptojacking, among others.

Link: https://www.osi.es/es/guia-ciberataques

Tips and tactics to protect yourself from Ransomware

The National Institute of Standards and Technology (NIST) has published an infographic offering a series of simple tips and tactics to help organisations protect themselves against ransomware attacks and recover from them should they occur.

Link: https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Ransomware_Tips_and_Tactics_Infographic.pdf

Introduction to Cybersecurity Risk Management - Ransomware

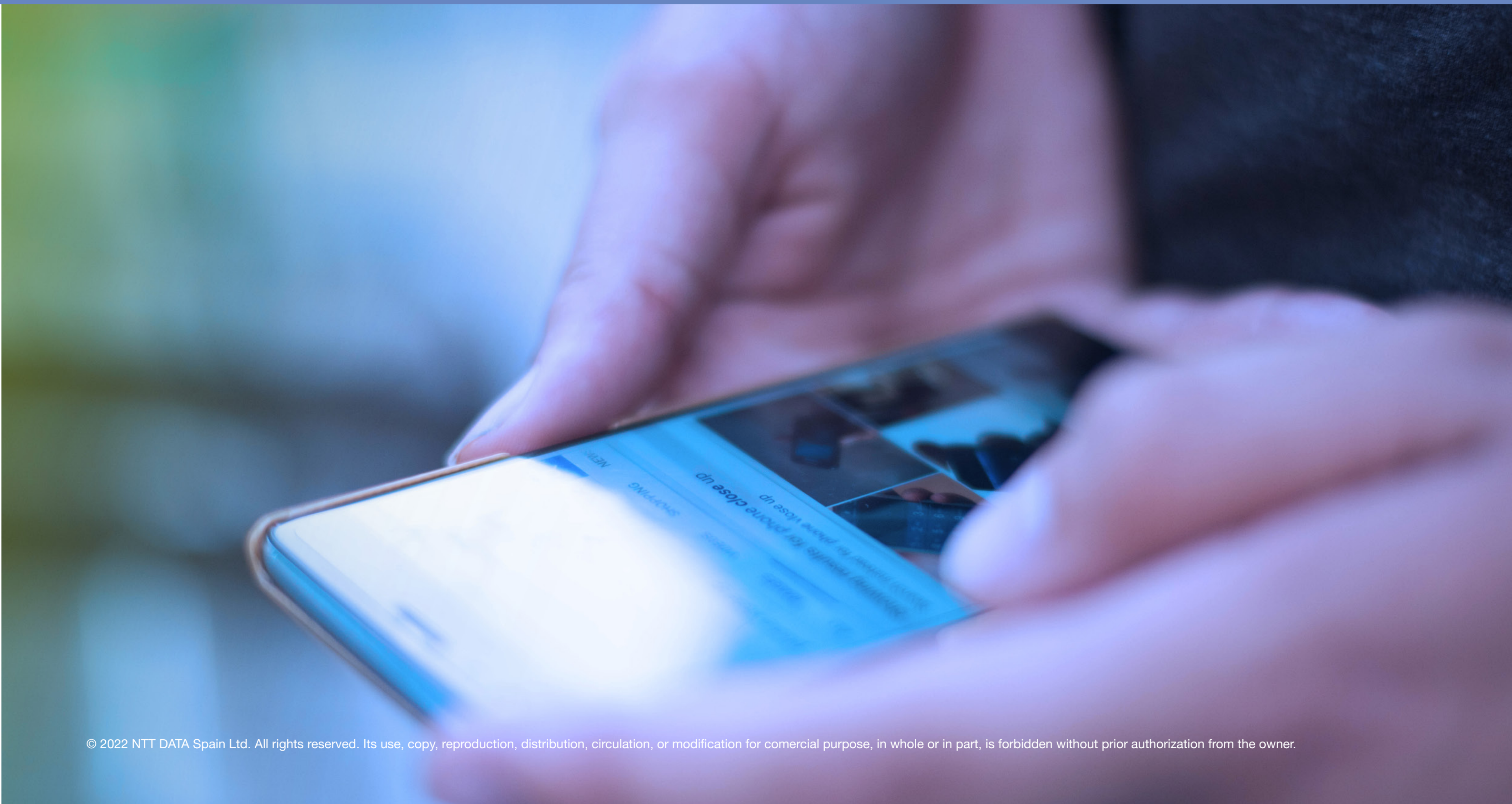
In the face of the growing threat of ransomware, this "quick start guide" can help organisations use the standards and technology for ransomware risk management from the National Institute of Standards and Technology (NIST).

Enlace: https://csrc.nist.gov/csrc/media/Publications/white-paper/2022/02/24/getting-started-with-cybersecurity-risk-management-ransomware/final/documents/quick-start-guide--ransomware.pdf

ISO 27002:2022

On 15 February 2022, eight years after the last version, the new update of this standard, which provides controls for information security, cybersecurity, and privacy protection, has been published. Recall that ISO 27002:2022 is not only a complementary standard for organisations that have implemented ISO 27001, but also a standard that helps to put in place the most effective best practices and controls to prevent attacks or breaches of the privacy of the organisation's customers or stakeholders.

Link: https://www.iso.org/standard/75652.html



NTT DATA

Trusted Global Innovator

powered by the
cybersecurity NTT DATA team

nttdata.com