NUMBER 66 | MAY 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

THE IMPORTANCE OF BEING PREPARED

The current geopolitical context implies a high risk for organisations, companies, and citizens. We all see on a daily basis the cybersecurity implications of the conflict in Ukraine, where supporters of the Russian side are trying to weaken the countries that are applying the most sanctions against Russia, causing serious security incidents in public applications, and affecting different companies, especially those that have decided to leave the country. Similarly, there are other companies that have seen their technological assets attacked by pressure groups, with some of their systems being shut down for weeks, as for example after the speech made by Ukrainian President Vlodímir Zelenski in the Spanish Congress of Deputies, where he pointed to several Spanish companies that still do business with Russia.

This situation exposes many companies that are even less public, including small and medium-sized enterprises, which until not so long ago no one could have imagined being attacked by such targeted attacks. It is therefore clear that the level of cybersecurity attacks is affecting more and more companies and organisations, and those that are better prepared will be able to resist these attacks by preventing them from being carried out.

How prepared organisations are makes the difference between a security attack and a security incident. The main IBEX 35 companies suffer cyberattacks on a daily basis, which is not something new, although the number of cyberattacks and their accuracy have increased in recent times. However, what really makes the difference is the number of serious security incidents that these companies have during a year. And it is here that the best prepared companies can take the lead.

There are many factors that define the level of cybersecurity maturity of an organisation, but one that makes the difference is the degree of relevance of the CISO of that organisation. At NTT DATA we have seen in our experience accompanying different organisations, that the level of cybersecurity awareness of some is so low that it only allows the execution of tactical projects, preventing the creation of a solid protection framework.

It is clear that a good level of cybersecurity maturity usually involves the adaptation of the company to different security standards or frameworks that set out, in detail, the security controls and mechanisms that must be implemented. This has led more and more companies to obtain certifications such as ISO 27001 or ISO 22301, and perhaps, thanks to this, they have managed to reduce the number of security incidents even though the increase in attacks is evident.

Adapting to a framework implies the definition of a strategic framework for the organisation and the creation of all the mechanisms and controls necessary to apply it. This brings us to another critical point when talking about cybersecurity: the budget. It is clear that spending in this field has become important for those companies with a good level of cybersecurity maturity, where expenditure is between 5% and 12% of total IT expenditure and growing.

It is not only the cybersecurity budget that is important, but obviously how you invest it. And it is here, where companies that invest in key aspects (cybersecurity training and awareness, cybersecurity strategy for different technological aspects such as cloud environments or development projects, attack simulation and disaster recovery plan training, etc.) have been able to reduce the number of serious security incidents and their consequences.

José Manuel Moreno Guerra

Cybersecurity Director at NTT Data Europe & Latam

CYBER NEWS

Today we start our cyber-chronicle with our sights set, once again, on the war between Russia and Ukraine, as we already have a measure of the impact it has had in terms of cybersecurity.

The two sides involved in this war have seen cyber-attacks on each other. Russia has become the most cyber-attacked country in the world and has experienced attacks on the Central Bank of Russia, which has suffered a 28 GB data leak perpetrated by the Anonymous group, or leaks of information about secret service officers based in Moscow.

> “Simultaneous attacks with IPs located in Siberia affect Madrid’s commuter train network and the Spanish parliament”.

On the other side, in Ukraine, attacks against the country’s electricity infrastructure have been detected. This attack, in the end, did not achieve its first objective and could be stopped before causing damage. Of course, the rest of the countries and organisations supporting this side have seen the number of cyberattacks increase and, for example, in Spain, the number of cyberattacks against military systems has doubled since the beginning of the conflict.

Without leaving this warlike environment, one of the companies that have been attacked in recent weeks has been Iberdrola, whose data on 1.3 million users has been stolen. This attack originated from IP addresses located in Siberia and was launched simultaneously with attacks on the Madrid commuter train network and the Spanish parliament.

But it is not all about the war, as cybercriminals continue to look for new ways to obtain data and funding. In the last month, attacks in which cybercriminals have used SMS messages to communicate advantageous job offers to users and thus obtain their data or the use of WhatsApp posing as family members who have lost their mobile phones to gain the trust of the recipient and ask them for an urgent money transfer have been gaining notoriety.

Another of the big blows executed by cybercriminals has been that against the game development company Sky Mavis. The company suffered a $620 million theft of its Axie Infinity game, which was allegedly committed by the North Korean groups Lazaros Group and APT38. These groups were able to infiltrate as part of the Ethereum-based blockchain system that the game uses for its rewards. This attack was the largest in the cryptocurrency sector in terms of the amount stolen and, according to the company itself, it will take several years to recover the value stolen.

Another of the attacks that have had some notoriety in recent days has been the one that has taken place at the Spanish Football Federation, where the email accounts and text and audio conversations of the federation’s executives have been accessed. The stolen information has been offered to the media and, in this way, the organisation has become aware of the attack against its information systems.

SECURITY IN DOCKER TECHNOLOGIES

By: NTT DATA

Docker is a container system that provides a simple way to package and isolate software. It simplifies the installation of complex applications by providing a complete file system with everything needed in a single package.

The idea behind Docker is to make it easy for programmers to create and deploy applications built from components, while giving them the ability to use other people's components.

Docker provides an isolated environment that allows to avoid interactions between programs, making each program independent of the underlying operating system.

There are many benefits to using Docker for your business, but what about the disadvantages? Here are some ways to evaluate whether Docker will be beneficial to your business.

What are the advantages of using Docker?

Docker provides a level of abstraction between the underlying system and the application. This means it is easy to package applications from any environment and deploy them anywhere.

There is no need to worry about how your application will integrate with the current operating system. Docker's containerised approach also ensures that your applications are isolated from each other, avoiding conflicts or dependencies.

It is also worth noting that Docker is made for developers by developers: its creators are programmers and understand what programmers need in an environment.

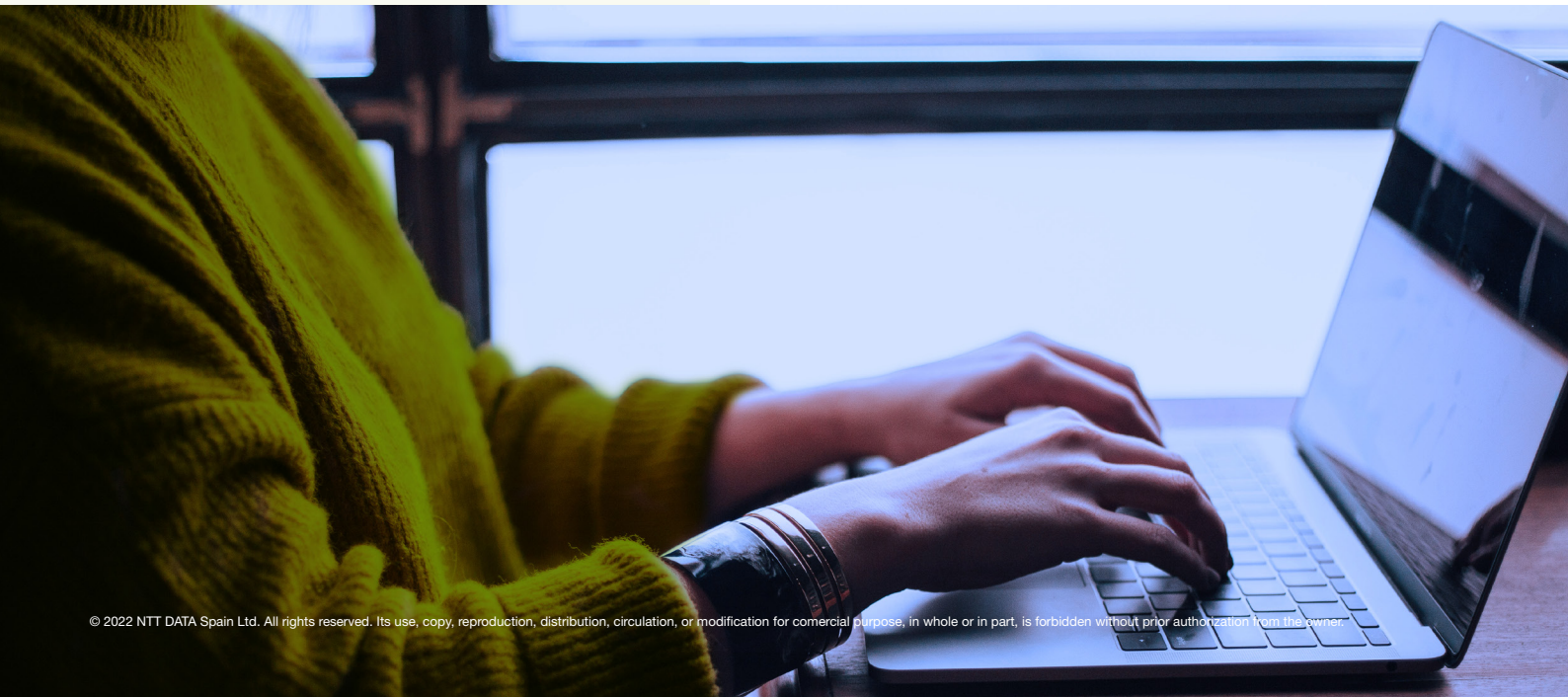
Docker is an open source software developed to offer an alternative to virtual machines. The main advantage of the software is the portability of the containers, which run on any computer, regardless of the operating system.

Docker uses containers that include only the software and resources needed to run the application. The container can be moved to another server with an operating system without interrupting the functionality of the container.

What are the disadvantages of using Docker?

There are many advantages to using Docker, but there are also disadvantages to this technology. It can be difficult to set up and use Docker, as it requires knowledge of the underlying operating system.

It is also important to note that Docker can only be used on Linux-based systems. Although Docker was designed for Linux-based systems, it will not work for containerisation on Windows machines or on Macintosh.



What is Docker technology composed of?

Each container consists of an encapsulated system that behaves as an independent machine and can be isolated from other containers. By using a set of technologies, it is possible:

- For the application to have a view of the OS resources (namespaces).
- To limit and measure the resources that are available in the OS (cgroups).
- To have a fictitious view of a system for the container, creating its own root and home (chroot) execution environment.

How can we protect the host environment running Docker?

The Docker security assessment allows you to verify the security controls present and configured when deploying Docker in an organisation's environment. It should be used to assess the security stance of the deployment and help identify areas for improvement.

In order to secure a working environment with Docker, the first step is to analyse the Linux Kernel of the host operating system (OS). Remember that there is not a complete OS in each of the containers. There are several open source tools to analyse the Kernel, such as Lynis or OpenVAS, capable of providing a complete report of failures and recommendations to be made to secure the system.

The next recommendation to further isolate the Docker environment by adding an extra layer of security is to install it on a virtual machine, rather than on the host system itself.

By default, Docker requires administrator (root) privileges to create and manage the different containers. A malicious script can exploit this attack vector to perform privilege escalation on a Linux host.

To prevent this attack vector, capabilities such as setgid and setuid can be discarded to prevent other programs or processes from changing their User Identifier (UID) or Group Identifier (GID) to a different one. This can be achieved when running the docker run command by adding the --cap-drop SETGID and --cap-drop SETUID parameters.

Another recommended option is to create your own user to manage Docker operations, instead of using an administrator or root user. This is as simple as creating a user (groupadd) and adding it to the docker group (usermod).

It is also recommended to manage containers with Namespaces. This is a namespace that can prevent containers from running as privileged users by mapping between the uid and gid of the host system and the container. This option will be enabled by the subuid and subgid functionalities.

Finally, to avoid denials of service due to excessive consumption of container resources, it is recommended to manage Docker using cgroups.

Given that a productive environment can have more than one container, it is possible to allocate host resources to containers through cgroups.

These control groups allow defining hierarchies in which processes are grouped so that an administrator can define in great detail how resources such as cpu, I/O or memory are allocated.

TRENDS

WE REMAIN ALERT FOR CYBERATTACKS DUE TO THE WAR

The Internet is a double-edged sword. Thanks to its use, society can access practically all existing information by clicking on a screen; however, progressive digitalisation has also made us more vulnerable to the risks hidden on the Internet; to a cybercrime that is increasingly organised and prepared. This became clear during the first months of the pandemic, when many workers began to type from their living rooms, increasing the exposure of companies and administrations.

Now, with the war in Ukraine, all experts expect cyberattacks to pick up internationally, although for the time being they remain focused on the two warring countries.

This has become evident with the recent attacks against large companies and public administration in Spain, such as the incidents suffered in recent months by the SEPE, the Ministry of Labour and Iberdrola.

The first two institutions were affected, precisely, by the attack that can do most damage to the proper functioning of a company: ransomware, capable of paralysing equipment and stealing internal information and which generates billions of euros in losses every year.

How would the conflict affect Spain?

A set of measures has recently been approved to tackle the crisis caused by the war between Russia and Ukraine, known as the War Response Plan, which in its fourth point establishes an allocation of more than one billion euros for the New National Cybersecurity Plan.

In addition to the economic amount, the creation of a Cybersecurity Operations Centre for the General State Administration and its public bodies was confirmed, as well as the strengthening of the security of the new electronic communications networks to be established with the expansion of 5G.

VULNERABILITIES

SIEMENS

CVE-2022-22965
Date: 19/04/2022

Description. Several Siemens systems have been affected by the recent discovery of the Spring4Shell vulnerability. This security flaw has a direct impact on all systems using the Spring MVC and Spring WebFlux framework in JDK9+. Through its exploitation, it could allow an unauthenticated remote attacker to execute code on the systems. In this case, exploitation of this vulnerability requires an endpoint with DataBinder enabled and depends on the application's servlet container.

Link: https://cert-portal.siemens.com/productcert/pdf/ssa-254054.pdf

Affected Products.

- Operation Scheduler, versions prior to 2.0.4;
- SiPass integrated V2.80, all versions;
- SiPass integrated V2.85, all versions;
- Siveillance Identity V1.5, all versions;
- Siveillance Identity V1.6, all versions.

Solution: Update to the latest versions of the systems.

Sophos

CVE-2022-0492
Date: 03/03/2022

Description. Shophos has published a vulnerability of critical severity in its firewall software. Exploitation of the vulnerability would allow an attacker to bypass the authentication system in the user portal and administration interface and then remotely execute arbitrary code on the systems.

The company has issued a statement indicating that the vulnerability is being actively exploited against specific organisations, primarily in South Asia.

Link: https://www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce

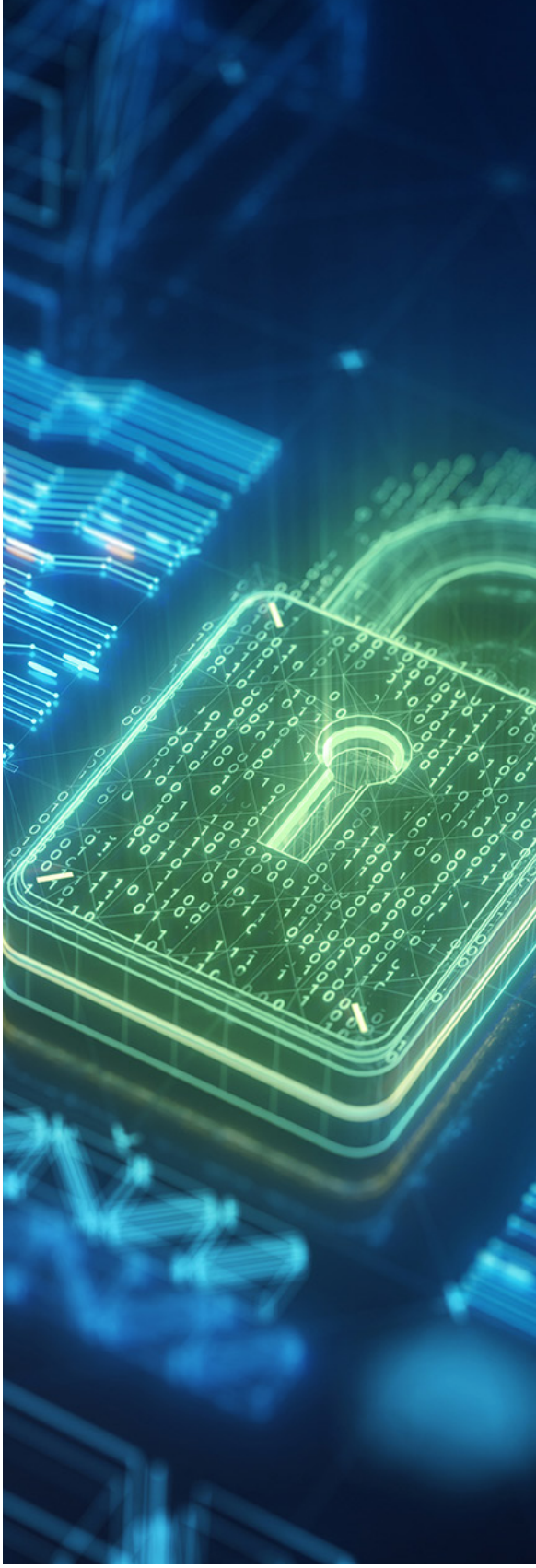
Affected Products.

- Sophos Firewall, version 1.5 MR3 (18.5.3) and earlier.

Solution: The patch that fixes this vulnerability is automatically installed on devices that have this option enabled.

In addition, Sophos recommends disabling online access to the user and administrative portals completely.

PATCHES



Microsoft

Date: 12-04-2022

Description. Microsoft has recently released security updates that address quite significant vulnerabilities. Specifically, one of them, which consisted of an elevation of privileges in the Windows Common Log File system driver, had already been addressed in previous updates. This security flaw is reportedly being used by some APT groups, according to the NSA.

In addition, in this same package, ten critical vulnerabilities have been fixed, one of which has received a score of 9.8 out of 10 and which would allow a remote attacker to execute code with elevated privileges on vulnerable systems.

Link: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24521
https://msrc.microsoft.com/update-guide/releaseNote/2022-Apr

Affected Products:
Systems with Windows Operating System.

Solution: Install the relevant updates.

GitLab

Date: 31-03-2022

Description. Security updates have been published in different products of the company GitLab that correct a total of 17 vulnerabilities of which 1 is critical and 2 are of high severity. An attacker could access credentials, exploit a Cross-Site Scripting (XSS) vulnerability, access the log token and environment variables, or cause a denial of service, among others.

Link: https://about.gitlab.com/releases/2022/03/31/critical-security-release-gitlab-14-9-2-released/

Affected Products:
All versions of:

- GitLab CE/EE,
- GitLab Omnibus,
- GitLab Charts,
- GitLab Pages.

Solution: Install the latest versions of each tool.

EVENTS

Tactial Edge 2022

11 and 12 May |

Tactical Edge's annual event covers a multitude of important cybersecurity topics, from the importance of cybersecurity awareness to new technology solutions using Artificial Intelligence and Machine Learning.

Link: https://www.ibm.com/events/think/

IBM Think 2022

10 and 11 May |

How are we responding to today's complex global challenges? Leaders recognise that technology innovation, applied to business transformation expertise, is inspiring game-changing solutions. From AI and automation to hybrid cloud and cybersecurity, see how we are applying technology and expertise to shape a brighter future.

Link: https://www.ibm.com/events/think/

Barcelona Cybersecurity Congress 2022

10 to 12 May |

Interact with the most experienced professionals in the industry and build a network of contacts with your peers to find solutions to your cybersecurity problems. The BCC format emphasises the sharing of relevant knowledge, encourages interaction between participants and produces a dynamic environment conducive to the generation of new ideas.

Link: https://www.barcelonacybersecuritycongress.com/

ASLAN 2022

18 and 19 May |

ASLAN2022 will offer a complete overview of advances in IT innovation and cybersecurity from leading manufacturers and specialised technology partners, the experiences of CIOs/CTOs/CISOs who are leading digitalisation projects in key sectors such as healthcare, industry, and transport, and all the latest news on the opportunities offered by European recovery funds to develop the full potential of technologies such as 5G and Artificial Intelligence.

Link: https://aslan.es/congreso2022/

RESOURCES

Spring Shell

Collection of information and tools on the critical vulnerability CVE-2022-22965, found in Spring Core Framework and commonly referred to as SpringShell or Spring4Shell.

Link: https://github.com/NCSC-NL/spring4shell

API security

Collection of tools, documentation, and resources on API security, especially focused on the Open Source community.

Link: https://github.com/arainho/awesome-api-security

Top 10 risks in CI/CD environments

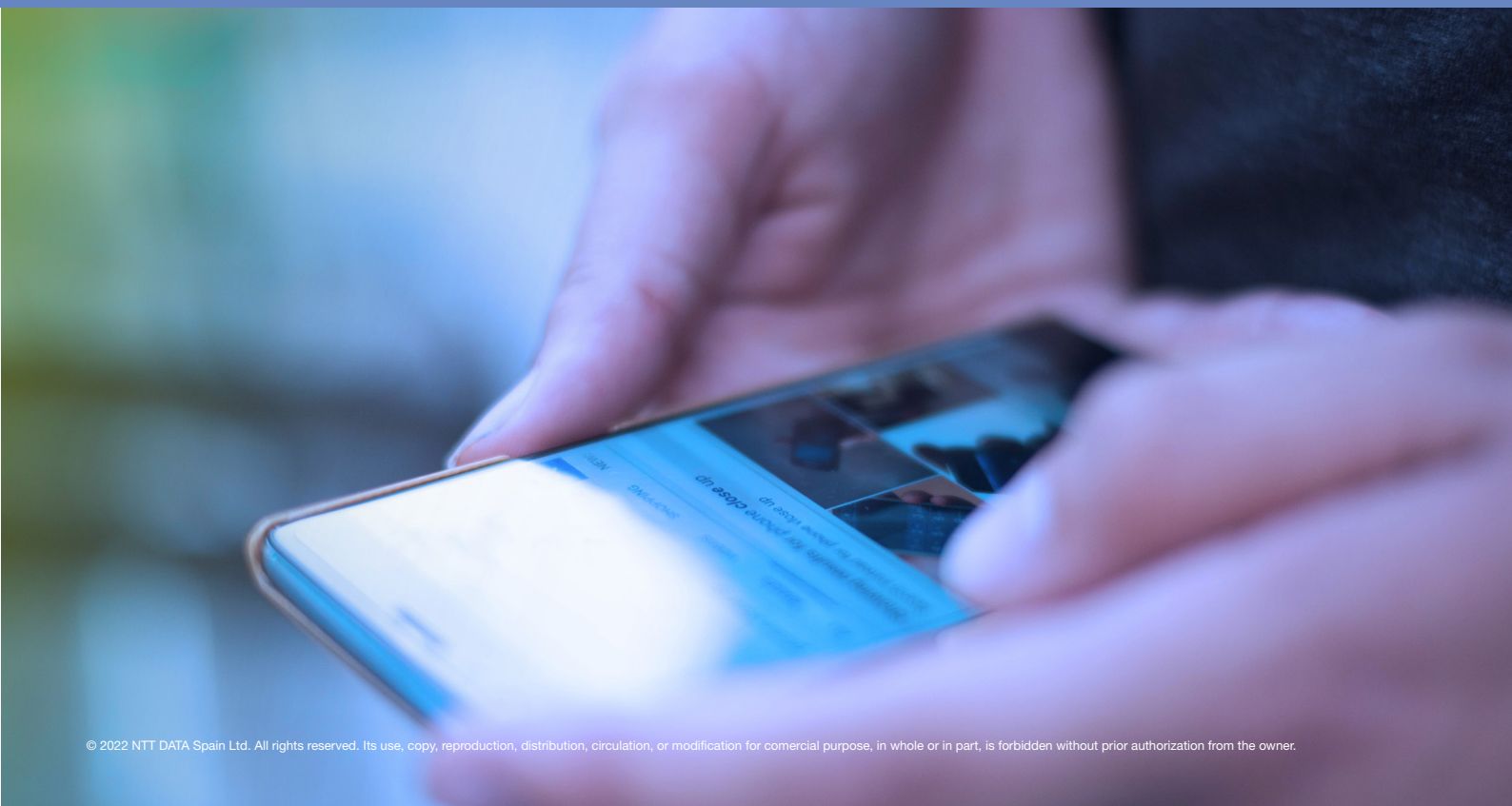
Detailed explanation of the main risks that can be found in CI/CD (Continuous Integration / Continuous Deployment) environments, which could have a major impact on the Confidentiality, Integrity and Availability of organisations' information or services.

Link: https://www.cidersecurity.io/top-10-cicd-security-risks/

Introduction to PCI DSS version 4.0

Introduction to the new version 4.0 of the PCI DSS (Payment Card Industry Data Security Standard), which was published in the first quarter of 2022.

Link: https://www.youtube.com/watch?v=o10vhgde1xU




NTT DATA
Trusted Global Innovator
powered by the
cybersecurity NTT DATA team
nttdata.com