NUMBER 74 | JANUARY 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

NEW YEAR, NEW FOCUS ON CYBERSECURITY

We have completed a year, 2022, in which we have seen a normalisation of the teleworking situation, and we have moved towards hybrid models that are more likely to remain in place over time. This moves IT professionals towards maintaining the infrastructures created both for online work and for providing services to our customers without being physically present anywhere, but at the same time being aware that physical meetings are going to happen again. So, although the year is changing, the minds of cybersecurity professionals are still focused on achieving greater security maturity in very particular areas:

- **Cloud security:** the cloud has been and will continue to be the focus of security areas this year; their objective is to adopt security models in the cloud and to set out on this path in a solvent manner. Although the road may be long, it is necessary to have a well-defined strategy for this adoption and to move steadily towards it.
- **Security focused on the human factor:** Organisations have already shown clear signs that they understand that most attacks could have been prevented by a human being. Therefore, efforts to promote cyber security behaviours, beyond the protection achieved by tools, will be key this year.
- **Definition of a correct cybersecurity framework:** given the existence of a large number of security frameworks (ISO27001, NIST, FFIEC, IAC62443 and several others), each organisation will focus on defining its own framework, clearly based on these, but taking the best of each one oriented to the organisation. In addition, we are gradually seeing an evolution from qualitative risk measurement to quantitative risk measurement, using methodologies such as FAIR.

For those of you who feel this is not enough, this year we welcome will see the evolution of certain technologies, which if they continue to grow as expected will require new visions to protect them. In particular, the metaverse, a technology that has come on leaps and bounds and is now in the midst of finding use cases for businesses to start adopting. As soon as companies are convinced that business can be done, our lives and those of our customers will burst into this new dimension and with it the need to secure privacy and identity.

And telcos continue to advance with 5G, a technology that will allow us to become hyperconnected, and with it, new models of interaction with many companies, such as communications, retail, or banking. Likewise, we will need a security framework that gives us confidence.

All these challenges for cybersecurity professionals will come to us in 2023, and we are already delighted to be working on solving them.

Miguel Ángel Thomas

Top Executive Principal Head of Cybersecurity at NTT DATA Europe & Latam

CYBER NEWS

We begin this cyber chronicle by recalling the best known cyber-attacks of 2022, such as those perpetrated by the LAPSUS$ hacker group, who attacked the multinationals NVIDIA, SAMSUNG and the Argentinean company Mercado Libre; the different attacks suffered by health entities in Colombia, as well as the cyber war that broke out after Russia's invasion of Ukraine, where Mikhail Fedorov announced the launch of a cyber-army.

This news alerted the CISOs of many companies around the world, who invested significant time and resources to protect their companies' information.

> "WhatsApp suffers security breach and the phone numbers of 360 million people in 108 countries have been exposed".

However, some of these efforts were not enough to counter the cybercriminals who every day generate new ways of acting and who seem to be always one step ahead.

In the last month of the year, a cyber-attack has knocked out the New York Opera House.

The cyber-attack in the middle of the pre-Christmas season, considered its peak season, prevents the Metropolitan Opera House from selling tickets and paying its employees.

Meanwhile, all Vatican websites were down on Wednesday afternoon following an alleged cyber-attack. The director of the Holy See's press service, Matteo Bruni, told AFP that there had been anomalous access attempts and that technical investigations were ongoing.

Uber suffered yet another data breach that leaked employee email addresses, corporate reports and IT asset information stolen from a third-party vendor in a cybersecurity incident.

The leaked data includes numerous files that claim to be source code associated with mobile device management (MDM) platforms used by Uber and Uber Eats and third-party vendor services.

WhatsApp has also been breached just as the year drew to a close, exposing the phone numbers of around 360 million people in a total of 108 countries. The phone numbers of 360 million users of this instant messaging application are said to be for sale on the darknet.

In other news, a group from Iran called Nemesis Kitten has claimed to be the author of a previously unknown custom malware called Drokbk, which uses GitHub as a means of leaking data from an infected computer or executing commands.

We start a new year expected to be full of cyber security news not only related to 0-days of multiple cloud platforms, but also to the evolution of attacks related to ransomware and its different mutations. Moreover, attacks on satellites, which according to what happened with VIASAT in February 2022, show the capabilities and evolution of persistent attacks.

On the other hand, it is predicted that email platforms will be a key target for obtaining information from large companies in different sectors, including government entities, due to the different geopolitical situations that arise worldwide. Information extraction and destructive attacks on industrial infrastructures will be a major focus for the world’s leading hacker groups.

CYBERSECURITY IN OPERATIONAL TECHNOLOGIES (OT) FRAMED WITHIN THE ENTERPRISE ARCHITECTURE

By: NTT DATA

One of the great challenges facing cyber security architects is to be able to frame in a converged enterprise architecture the different layers of services that support their own and particular business requirements, as well as to articulate two networks that conceptually have great differences but that together must harmonise in order for information to flow and be used securely.

When designing a security architecture for an OT environment, it is recommended to separate the OT network from the corporate network.

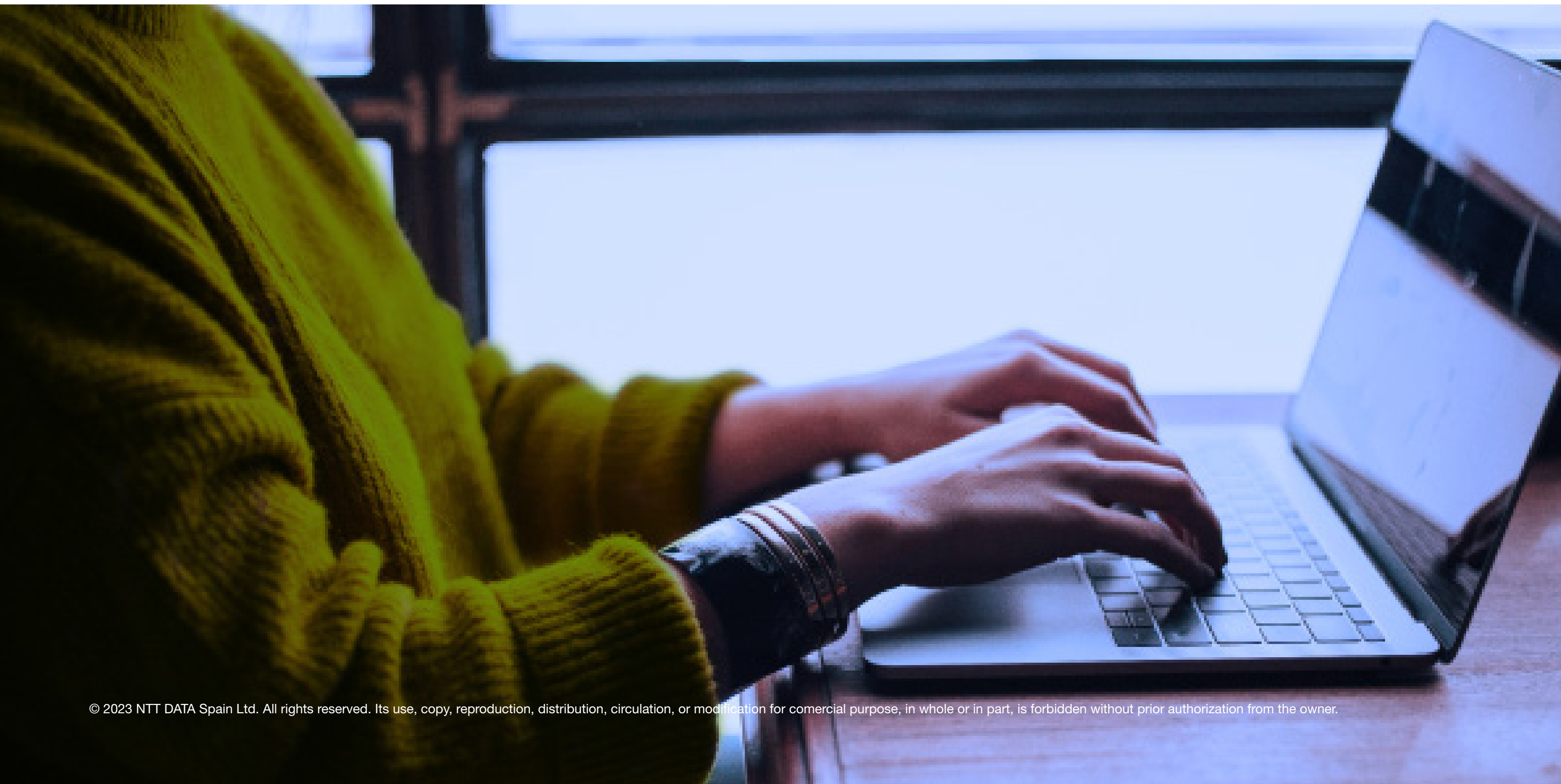
The network traffic and policies on these two networks are different, as services such as email and remote access among others will normally be allowed on the IT network but not on the OT network.

In the beginning, the coexistence of traffic from OT devices over IT infrastructure was common, but in the use of the corporate network, OT communication protocols are exposed to cyber-attacks or bottlenecks.

The use of separate networks allows greater flexibility to address security and performance requirements in both environments.

In implementing new trends such as digital transformation, the cost of installing OT or maintaining the infrastructure often means that a connection is required between OT and other proprietary or third-party IT networks.

This connection represents an additional risk for which, in many cases, vendors suggest solutions that do not take cybersecurity into account and do not consider controls for these connections, only concentrating on the flow of information and the owner of such infrastructure, when implementing in this way is exposed and can generate manifest vulnerabilities (e.g. connecting IT and OT network segments via a PC or server with two network cards) that exploited by experienced attackers sacrifices the security of the IT and OT environments.



In this regard, two aspects that are of great relevance for designing secure OT architectures are described in Figure 1:

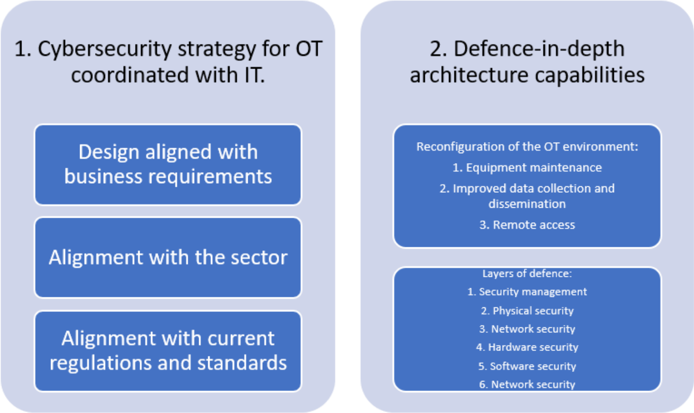

1. Cybersecurity strategy for OT coordinated with IT.
Design aligned with business requirements
Alignment with the sector
Alignment with current regulations and standards
2. Defence-in-depth architecture capabilities
Reconfiguration of the OT environment:
1. Equipment maintenance
2. Improved data collection and dissemination
3. Remote access
Layers of defence:
1. Security management
2. Physical security
3. Network security
4. Hardware security
5. Software security
6. Network security

Figure 1. Aspects relevant to the construction of secure OT architectures

OT and IT integration is increasingly necessary and evolving as organisations adapt to current requirements, as well as to the upcoming environment, sector, industry type and global changes in cyber-security related aspects.

The use of the principles of a defence-in-depth architecture requires the implementation of the aforementioned layers of defence. This implies a security environment that involves and is aligned with people, processes, and technology, resulting in a strengthened security system, where attackers have greater difficulty in penetrating the environment undetected.

Another aspect of great relevance for improving the design of a cyber security architecture in OT is the Zero Trust Architecture (ZTA).

ZTA focuses on the protection of resources based on authorisation decisions based on an evaluation of requests, rather than implicit authorisation.

Traditionally, network users are granted permissions to the different resources of the organisation because they are considered trustworthy; therefore, protection devices do not mitigate the risks to these users, leaving the environment of the users that are part of it unprotected.

In addition, with the increasing prevalence of distributed computing, wireless and mobile communications, along with cloud and hybrid cloud environments, traditional network perimeters and boundaries are becoming less defined. For these situations, organisations could consider incorporating zero trust principles into their security architecture.

In order to migrate the architecture to a zero-trust environment, aspects such as the organisation's level of maturity and technical capacity must be taken into account, along with the investments in money and time that this implies. As well as operational efficiency, i.e., the responsiveness and requirements of implementing ZTA (Figure 2).

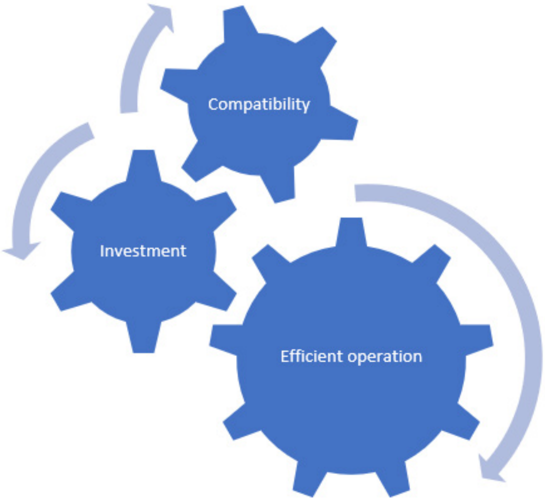


Figure 2. Challenges of ZTA implementation

Another aspect to be studied is the delay that would be generated in communications by the response of multiple OT devices sending credentials. For the correct functioning of the ZTA, redundancy provisions must be made according to the process being monitored and controlled. A bottleneck in the OT network is undesirable because safety functions (security of people in OT) are also managed on it.

Finally, the last aspect is the logging of identities that in many cases are not personal but attributable to a set of people who share profiles on a productive shift that affects the ZTA philosophy.

Several of the principles outlined above can help in conjunction with other technologies to increase cybersecurity in an ever-changing OT environment.

WHAT SECURITY RISKS CAN THE METAVERSE HIDE?

By: NTT DATA

The metaverse is said to be the next phase of the internet, a new virtual reality, the social network of tomorrow, among others. Virtual reality, augmented reality, social networks, video games are the bases that can form part of the metaverse, but only when they collaborate with each other. The metaverse aimed at individuals would be to walk down the street looking at augmented reality advertisements, checking their social networks, and then getting home to play a virtual reality game, without at any point noticing the transition of platforms or interruption of their experience.

The metaverse is coming in ways both predictable and unexpected. Like all trends, there will be a change in usage and consumption habits, a period of adaptability for users of this new technology. Likewise, the security risks will be much higher than we might have first imagined.

The number of companies exploring the possibilities of the metaverse is growing and, as a result, major cybersecurity firms are studying the impact this virtual world can have. Metaverse, like other IT networks, has privacy and data security risks. However, it is necessary to develop an individual strategy considering the characteristics of this technology.

For example, Metaverse user data resides on different servers around the world. It is necessary to discuss how to protect users when they either perform a transaction or share information through a conversation.

They assume that security will primarily be compromised in IoT devices such as smart glasses and virtual reality headsets, risks related to identity theft, payment fraud and online security. While the metaverse will empower virtual identities, allowing individuals to perform many tasks that were previously limited to the traditional physical world, it will also put more pressure on authentication processes.

Data Protection

Data privacy has always been a focus when it comes to cybersecurity. In this case the metaverse is faced with handling sensitive data for the users who will be living the experience.

Now, it is necessary to define which entity will be in charge of processing and protecting that data, and more importantly, in the case of an actual attack, who will be responsible for the leakage of that data?

User-targeted attacks are not the only focus for the metaverse to worry about, building a real-time user communication experience involves being prepared for attacks concentrated in its own domain, such as infiltrating private sections by brute-force password cracking, flooding the service with a DDoS attack, or identity theft within the experience. Before marvelling at all the services, entertainment and environments that break with the familiar and are made possible by this new technology, the metaverse must assure its users of security, first and foremost.

While new technologies such as the metaverse will always be presented as a new environment with more distant limits compared to those already established, it is necessary to build on the pillars of cybersecurity, an environment without limits of creation but with high security flaws is nothing more than a warning to stay away from, for the safety of the users.

The privacy and data protection of users must continue to be safeguarded, and the metaverse cannot be an exception. The technologies involved will collect much more data, including highly sensitive data such as biometric data.

Companies must ensure that privacy is built into the very design of the metaverse. Care must be taken to ensure that the right processes are in place that will link essential data, thus understanding who will be responsible for collecting, processing and, above all, protecting it.

Quantum computing as a threat to current public key encryption standards

Nowadays, most communication protocols are based on three essential cryptographic functionalities for secure and efficient data transmission: public key encryption, digital signatures, and key exchange.

To ensure that these functionalities meet the objective of altering the information so that it cannot be manipulated or stolen, a series of asymmetric ciphers have been defined, such as RSA, ECC and DSA. These base their computation on mathematical problems such as factoring the product of two large prime numbers, the encryption of elliptic curves or the calculation of a discrete logarithm, which are difficult or intractable for conventional computers.

However, with increasing research into the capabilities of quantum computers, such mathematical problems can be solved in a matter of hours. Quantum computing is focusing on using aspects of quantum mechanics, such as quantum entanglement or quantum superposition, to perform computations at speeds inconceivable to classical computers.

Thus, ciphers such as RSA, elliptic curve and other encryption techniques could, in theory, be broken by these speed increases in a matter of hours, making popular asymmetric encryption algorithms susceptible to quantum attacks.

Faced with this threat, the National Institute of Standards and Technology (NIST) opened on 20 December 2016 the call for applications for Post-Quantum Public Key Cryptographic Algorithms. As of 5 July 2022, the institute announced the selection of four candidate algorithms that represent the first approach to post-quantum cryptography standards and are based on finding mathematical problems that are computationally difficult for both conventional and quantum computers.

For general encryption, CRYSTALS-Kyber has been selected. On the other hand, for digital signature functionality NIST has selected CRYSTALS-Dilithium, FALCON and SPHINCS+.

The main advantage of these new algorithms is that they use mathematical problems related to lattices, which are computationally more difficult to solve for both traditional and quantum computers. This will henceforth be known as lattice-based cryptography and will be the first step towards mitigating quantum attacks on public-key ciphers.

VULNERABILITIES

Fortinet

CVE-2022-42475
Date: 12/12/2022

Description. Fortinet issued a security advisory on Monday reporting a 0-day vulnerability categorised as critical affecting FortiOS SSL-VPN, which has been assigned the identifier CVE-2022-42475. It also acknowledges that it is aware of the actual exploitation of the vulnerability in at least one instance. This vulnerability can lead to a type of buffer overflow called heap overflow, which can result in remote execution of arbitrary code (ACE) by an unauthenticated attacker using specially crafted requests.

Link: https://olympecyberdefense.fr/vpn-ssl-fortigate/

https://www.fortiguard.com/psirt/FG-IR-22-398

Affected Products: Esta vulnerabilidad afecta a los siguientes productos de Fortinet:

FortiOS:

- Versions from 7.2.0 to 7.2.2.
- Versions from 7.0.0 to 7.0.8.
- Versions from 6.4.0 to 6.4.10.
- Versions from 6.2.0 to 6.2.11.

FortiOS-6K7K:

- Versions from 7.0.0 to 7.0.7.
- Versions from 6.4.0 to 6.4.9.
- Versions from 6.2.0 to 6.2.11.
- versions from 6.0.0 to 6.0.14.

Solution: Update to the latest version of the software. In cases where updating is not possible, the following is recommended:

- Disable the VPN-SSL function if it is not essential.
- Monitor the logs and check for unauthorised access.
- Restrict connections from particular IPs by configuring access rules.

Citrix

CVE-2022-27518
Date: 13/12/2022

Description. A new 0-day vulnerability of critical severity has been reported, the exploitation of which could allow an unauthenticated remote attacker to execute arbitrary code on vulnerable devices. This is due to not maintaining full control over the resources during their lifecycle. Several attacks exploiting this vulnerability have been reported, so it is recommended that devices be updated as soon as possible.

Link: https://support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518
https://www.citrix.com/blogs/2022/12/13/critical-security-update-now-available-for-citrix-adc-citrix-gateway/
https://media.defense.gov/2022/Dec/13/2003131586/-1/-1/0/CSA-APT5-CITRIXADC-V1.PDF

Affected Products: Citrix ADC and Citrix Gateway, versions:

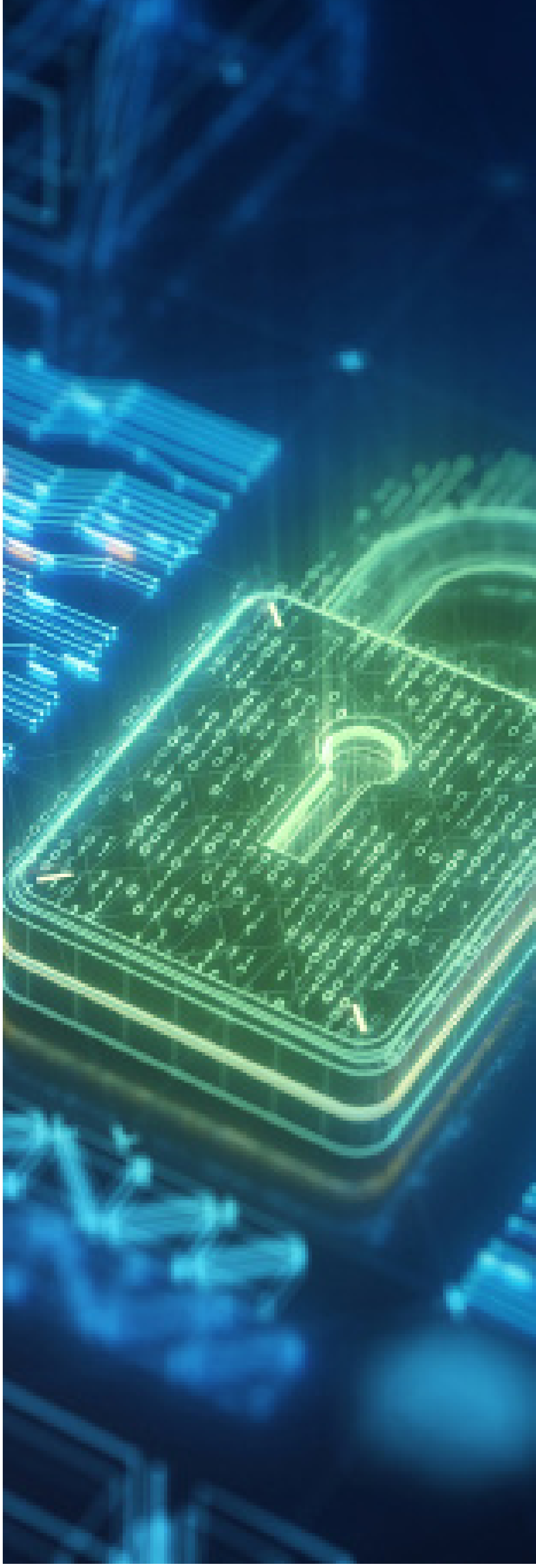
- prior to 12.1 and EOL;
- 13.0 prior to 13.0-58.32
- 12.1 prior to 12.1-65.25

Citrix ADC 12.1-FIPS, versions prior to 12.1-55.291.

Citrix ADC 12.1-NDcPP, versions prior to 12.1-55.291.

Solutions: Apply appropiate security patches.

PATCHES



VMware

Date: 08-12-2022

Description. A new update has been released that addresses a total of nine vulnerabilities in several VMware products. Specifically, two of the above mentioned vulnerabilities are of critical severity and their exploitation could allow command execution. One would allow commands to be injected via the REST API and the other would apply to an attacker with local privileges who could execute code on the host.

Link:
https://www.vmware.com/security/advisories/VMSA-2022-0030.html
https://www.vmware.com/security/advisories/VMSA-2022-0031.html
https://www.vmware.com/security/advisories/VMSA-2022-0032.html
https://www.vmware.com/security/advisories/VMSA-2022-0033.html

Affected products:
ESXi, Center Server, Cloud Foundation, vRealize Network Insight (vRNI), Workspace ONE Access, Identity Manager (vIDM), Workstation Pro / Player, y Fusion Pro / Fusion.

Update: Install the corresponding updates.

Siemens

Date: 14-12-2022

Description. Siemens has released new security updates that fix 139 vulnerabilities in a large number of its products. Exploitation of the critical vulnerabilities could allow denials of service, authentication bypass, arbitrary code execution, integer overflow or out-of-bounds writing.

Link: https://support.industry.siemens.com/cs/start?lc=es-ES

Affected products:
All versions of:
- Simcenter STAR-CCM+;
- Polarion ALM;
- JT2Go;
- different models of SIPROTEC 5 listed in SSA-552874 and SSA-223771;
- PLM Help Server 4.2.

SICAM PAS/PQS, versions:
- prior to 7.0;
- 7.0 and above up to 8.06.

Teamcenter Visualisation, versions listed in SSA-700053 and SSA-360681.
Parasolid, versions listed in SSA-588101
- SIMATIC WinCC, different versions and models listed in SSA-547714.
- APOGEE PXC Series, versions prior to 3.5.5; 2.8.20.

TALON TC Series, versions prior to 3.5.5.
SIMATIC, RUGGEDCOM, SCALANCE and SIPLUS, various versions and models listed in SSA-413565, SSA-412672, SSA-382653, SSA-363821 and SSA-333517.
ICE Calibre, versions 2022.4 and higher.
Mcenter, versions 5.2.1.0 and higher.
Mendix:
- Email Connector, versions prior to 2.0.0;
- Workflow Commons, versions prior to 2.4.0.

Update: Update to new versions of the affected products.

EVENTS

International Conference on Cybersecurity, Cyberwar and Cyberthreats ICCCC

9 - 10 of january 2023 |

The International Conference on Cybersecurity, Cyberwarfare and Cyberthreats aims to bring together leading academic scientists, researchers, and research scholars to exchange and share their experiences and research results on all aspects of Cybersecurity, Cyberwarfare and Cyberthreats. It also provides a premier interdisciplinary platform for researchers, practitioners, and educators to present and discuss the latest innovations, trends, and concerns, as well as practical challenges encountered and solutions adopted in the fields of Cybersecurity, Cyberwarfare and Cyberthreats.

Link: https://waset.org/cybersecurity-cyberwar-and-cyberthreats-conference-in-january-2023-in-bali

SANS Security East 2023

16 - 21 of january 2023 |

Where you can gain real-world cybersecurity knowledge from top industry experts during SANS Security East, experience interactive training with hands-on labs, practice skills during NetWars tournaments and network with your peers in real time.

Link: https://www.sans.org/cyber-security-training-events/security-east-2023/

Cybersecurity Standardisation Conference 2023

16 - 21 of january 2023 |

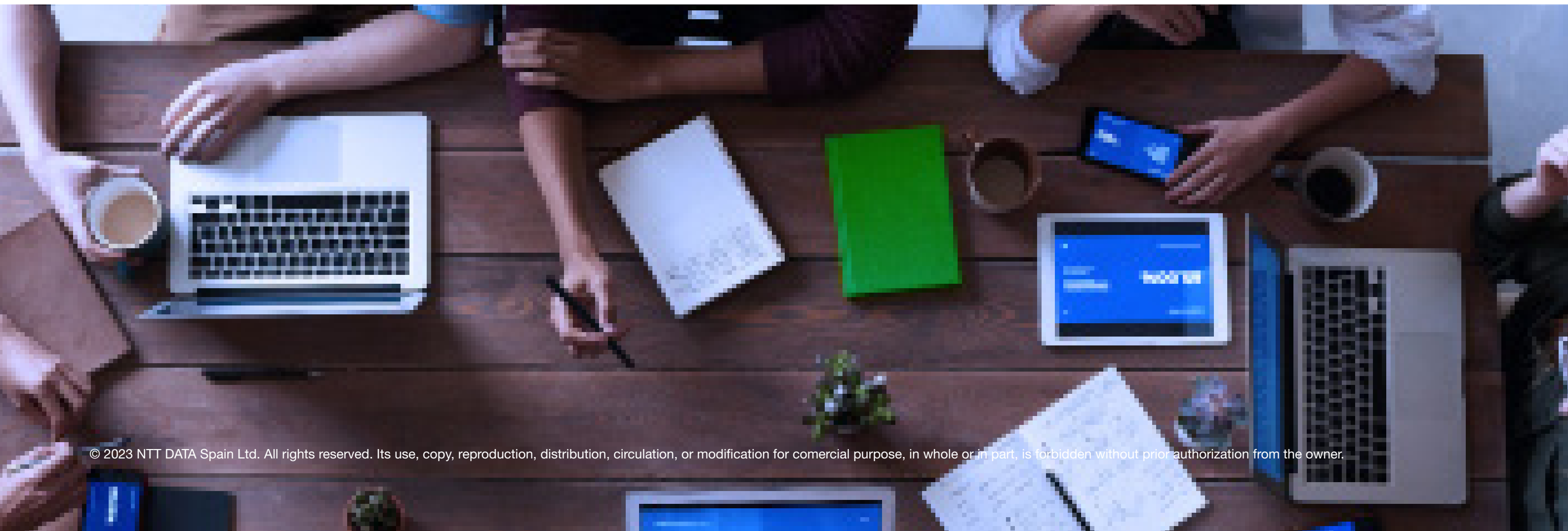
Where you can gain real-world cybersecurity knowledge from top industry experts during SANS Security East, experience interactive training with hands-on labs, practice skills during NetWars tournaments and network with your peers in real time.

Link:https://www.enisa.europa.eu/events/cybersecurity_standardisation_2023

International Data Protection Day

28 of january 2023 |

Additionally, on 28 January 2023, the International Data Protection Day will be celebrated worldwide, whose objective is to raise awareness and promote good practices related to the use of data protection, rights, and obligations of users; therefore, we recommend that you pay attention to the webinars, talks, courses, workshops, etc. that will be presented on this day.



RESOURCES

Zero Trust as a Security Philosophy

This paper looks at what Zero Trust means for your organisation, both from a vendor and technology solution perspective, and provides recommendations for developing a strategy and supporting architecture that supports the organisation and its workflows, aligning IT with business goals and outcomes.

Link: https://cloudsecurityalliance.org/artifacts/zero-trust-security-philosophy/

INCIBE's "Your help in Cybersecurity" Service

Its main objective is to raise awareness and sensitise citizens, minors, and companies on the safe and responsible use of the Internet and technology. It also addresses the importance of taking precautions in their digital life, as the current situation, caused by the pandemic, has increased what is called the 'risk surface', i.e., the greater the use of technology, the greater the space for cybercrime and cyberthreats to appear.

Link: https://www.incibe.es/sala-prensa/notas-prensa/el-servicio-tu-ayuda-ciberseguridad-incibe-protagonista-nueva-campana

What is email spoofing and how can it be identified?

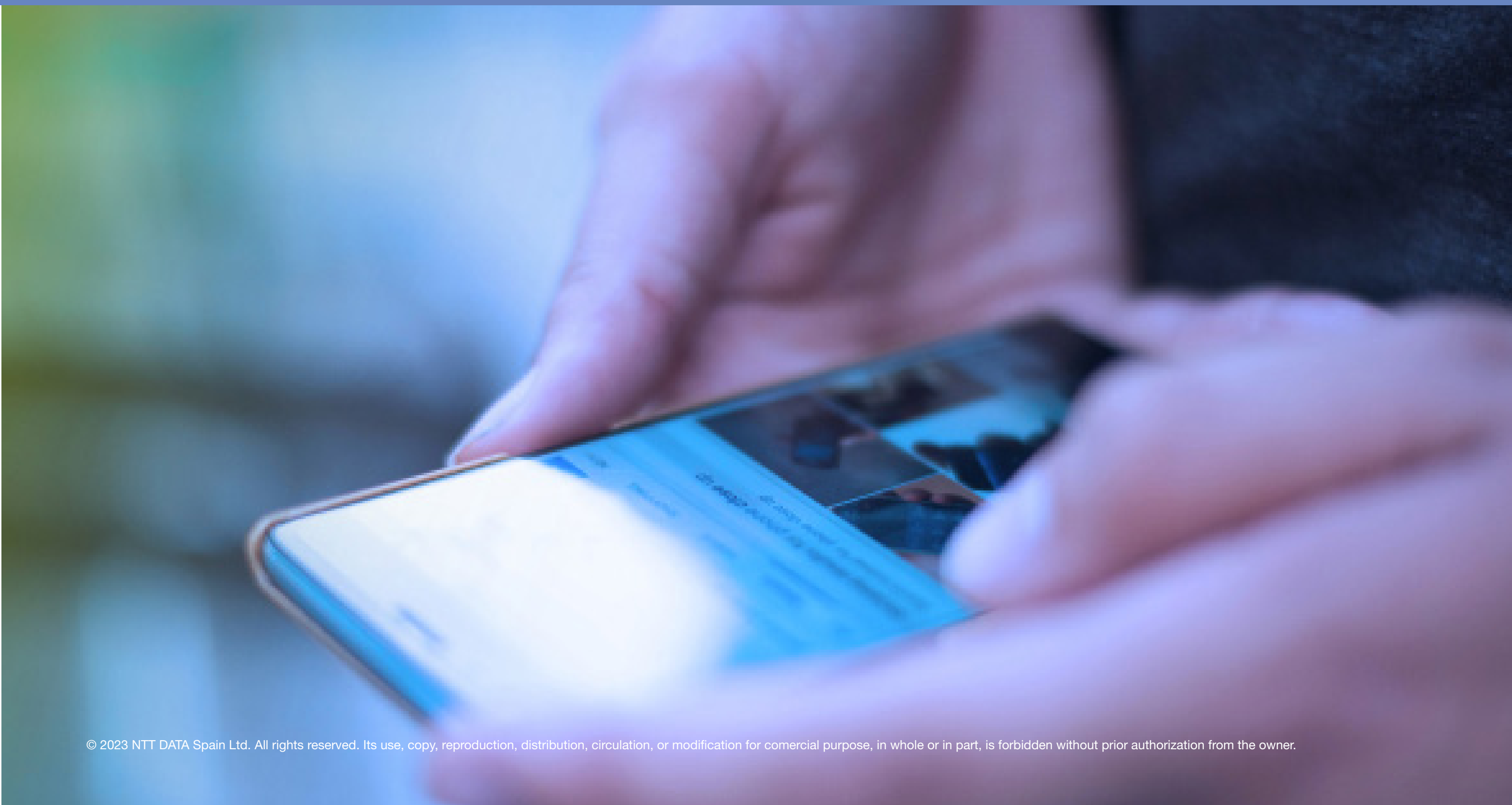
Incibe's cybersecurity bulletin gathers information, through a true story, about Fortnite, a multiplayer online multiplayer armed combat 'everyone vs. everyone' video game, with different game modes (with and without building possibilities, creative and cooperative), which is aimed at users over 13 years of age.

Link: https://www.incibe.es/sala-prensa/notas-prensa/el-email-spoofing-y-se-puede-identificar

A Visual Summary of SANS Pen Test HackFest Summit 2022

Ashton Rodenhiser of Mind's Eye Creative created graphic recordings of the presentations at the SANS Pen Test HackFest Summit. If you missed a talk or want to see the Summit through a visual lens you can do so at the following link:

Link: https://www.sans.org/blog/a-visual-summary-of-sans-pen-test-hackfest-summit-2022/



NTT DATA
Trusted Global Innovator

powered by the
cybersecurity NTT DATA team

nttdata.com