NUMBER 68 | JULY 2022

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

CYBERSECURITY CHALLENGES IN THE METAVERSE

We would like to take advantage of the start of a new RADAR to reflect on cybersecurity and new technologies, in particular the metaverse. As we go deeper and deeper into what the metaverse is and what we want the metaverse to be, we understand that there are several technological challenges to make it a reality, as an environment where experiences and sensations are like in real life; these challenges are around extended reality; user experience; IOT | Robotics; Artificial Intelligence; Blockchain; Computer Vision; Edge Computing; Cloud; Network.

And in parallel to solving these challenges, different challenges related to cybersecurity and privacy need to be addressed. Here we introduce some of them:

User identity: some environments will seek to hide the identity of a person through an avatar; but this will involve ensuring moderation, even implementing a traceability mechanism where you can know who did each action; however, companies are also already thinking about implementing their environments in the metaverse as another place for interaction between employees and stakeholders (customers, students, talent...) so it will be necessary to show the identity and ensure its authenticity.

Privacy: we may think that the metaverse will follow similar privacy rules as our physical world. If a user visits certain sites and their data is logged, this data is sensitive and cannot be shared. The theft of this data will be a security incident, and there will be a right to be forgotten. Another area of privacy is “presence”. In the physical world we perceive people when they are close to us. In the metarverse, shapes must be designed to be able to perceive other avatars that observe us.

Information management and assurance: Just as in the real world, information about people and products will be stored in the metaverse. This information must be stored securely and immutably. Any information leak will represent a security incident just like in the real world.

All the methodologies we currently use to protect organisations’ infrastructures (whether cloud, IT, OT...) will be useful in the metaverse after an evolution. Hackers will try to enter different metaverses as if they were a black box, and once inside, white box and grey box techniques will be used. Cyber-surveillance will allow us to know if a brand is being used well within the metaverse and also to define how to respond to a security incident or a continuity plan, as many organisations will use these spaces as another environment.

There is undoubtedly much to be done and resolved on what is sure to be an exciting road to a new promised land.

María Pilar Torres Bruna

Cybersecurity Director at NTT Data Europe & Latam

CYBER NEWS

We begin our cyberchronicles by talking about the multiple vulnerabilities that are becoming known and allow cybercriminals to perform remote code execution and privilege escalation on the infrastructures and technologies used in OT (Operations Technology) systems and industrial control systems.

Attackers see these systems as an easier target for vulnerabilities since, unlike IT systems, OT systems put availability above security and other factors. This is due to the fact that they deal with assets designed for industrial operation, which in case of failure could lead to large losses in terms of production and therefore security is neglected.

> “Follina allows an attacker to perform remote code execution by exploiting a flaw in MSDT”.

It should also be noted that in terms of security regulations, OT has not been able to standardise, as different industrial sectors would require different standards and rules.

Since most OT systems still lack minimum security, attackers focus on using the most known threats in any system using hardware and software. Examples include non-existent or insufficient encryption, lack of network segmentation, default configurations, command injection, parameter manipulation or remote access policies, among others.

Given this lack of security, critical vulnerabilities affecting well-known OT systems have been identified, such as the vulnerabilities found by researchers Yuval Ardon and Roman Dvorkin of OTORIO, which affect one of the largest OT companies in the market, GE Digital.

Two high criticality vulnerabilities were found in their HMI/SCADA system of the Proficy CIMPLICITY product. One of them is the vulnerability with the “CVE-2022-23921” identifier, which has a CVSS score of 7.5. This vulnerability exploits improper privilege management and can lead to an attacker performing local privilege escalation and subsequent code execution.

The second vulnerability is “CVE-2022-21798” which has a CVSS score of 7.5. It exploits the clear text transmission of credentials over the CIMPLICITY network, which would allow an attacker to capture them and exploit them for any number of malicious uses within a company’s internal network.

According to a study by TrendMicro, 89% of companies that provide OT systems and companies that are clients of these products (electricity, oil, and gas companies, etc.) are falling victim to attacks that can lead to the loss of operations and even compromise the company’s entire internal network. This highlights the importance of starting to see cybersecurity as a primary element in any industrial process involving operations technologies or industrial control systems.

However, vulnerabilities are not only present in OT. As usual, Microsoft has been affected by a vulnerability identified by MITRE as CVE-2022-30190 or more commonly known as “Follina”, which lies in a bug in the Microsoft Support Diagnostic Tool (MSDT) and exploits functionalities of Microsoft Word such as URL calling. Any Windows operating system has been identified as vulnerable, both desktops and servers.

“Follina” allows an attacker to perform remote code execution by exploiting a flaw in MSDT. Exploitation of this vulnerability starts with the generation of a document (often a “Word” document) infected with malicious code. When sent to a victim via social engineering, the moment the victim opens the document, the malicious code is executed. Most interestingly, this vulnerability does not require macros to be enabled.

Although Microsoft has not yet released a patch to remedy this vulnerability, temporary solutions have already been offered to avoid falling victim to this vulnerability, such as the removal of a registry key.

The above are just some of the news from the last few weeks in the world of cybersecurity that show us that cybercriminals never sleep.

THIRD-PARTY LIBRARIES: A LATENT THREAT TO APPLICATIONS

By: NTT DATA

The use of third-party libraries and components is a necessity for organisations' projects as 90% of the programs integrate elements from external sources (Uchill, 2021)to meet the functional requirements.

However, when it comes to the use of third parties, there is a problem that occupies the sixth place in the top 10 most common vulnerabilities proposed by OWASP (A06:2021 - Vulnerable and outdated components); this is that the systems and projects of the organisations generate security breaches if they do not have controls over their external components. This happens when:

- There is no clarity on the versions of third-party libraries or components.
- Regular vulnerability scans are not performed.
- Updated or remediated libraries are not tested for compatibility.
- Unreliable, vulnerable, and even outdated libraries and components are used.

Therefore, the lack of controls in third-party libraries makes it possible for threats to materialise in the source code that impair the functionality and availability of applications.

There are cases where the developers of popular libraries themselves misuse their power and corrupt their own products by adding malicious content.

Moreover, the exploitation of these vulnerabilities is known as supply chain attacks and can affect multiple internal components of organisations. This article therefore presents a brief description of dependency attacks and the most common secure practices to mitigate them, specifically the correct use of secure internal repositories for external components.

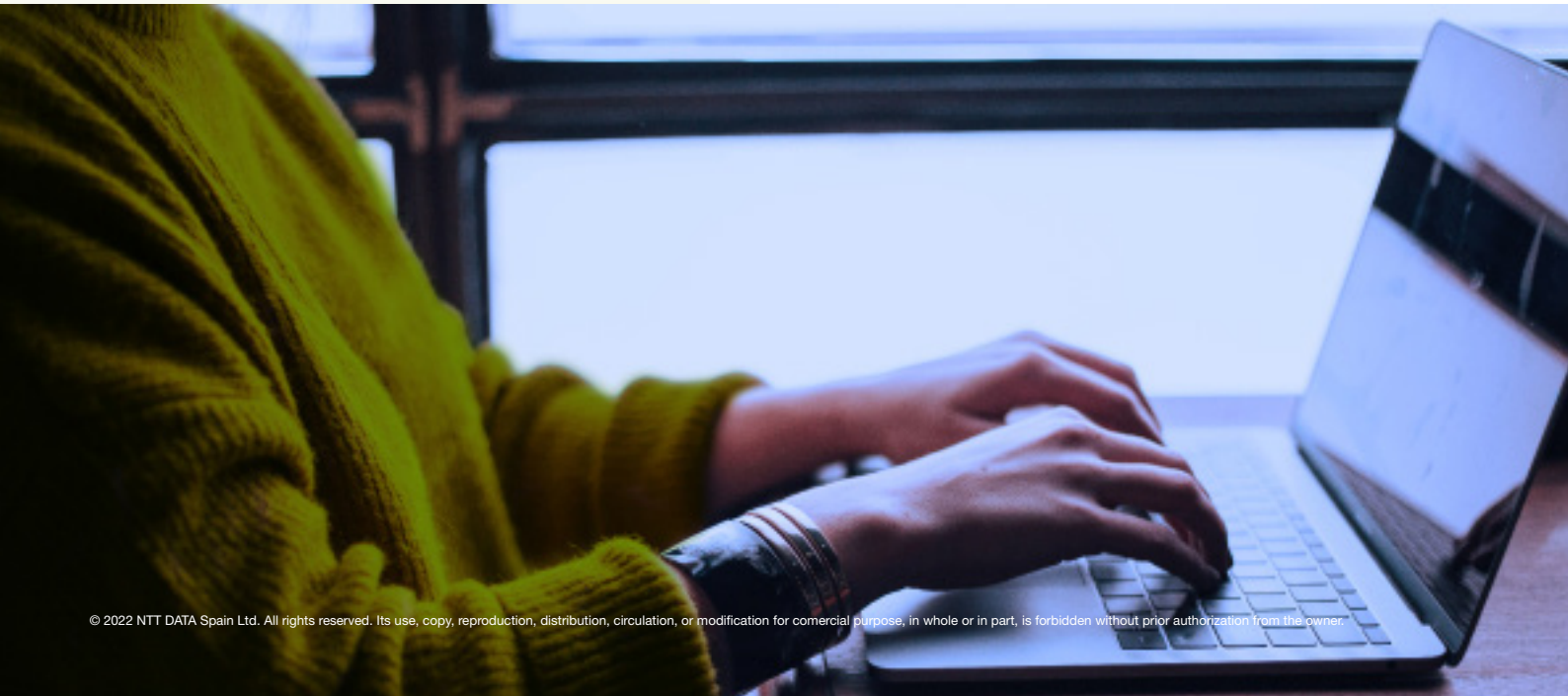
On libraries sabotaged by their own developers

It seems uncommon, but recently, prominent projects, such as those presented below, have been affected by unexpected updates that have harmed millions of users.

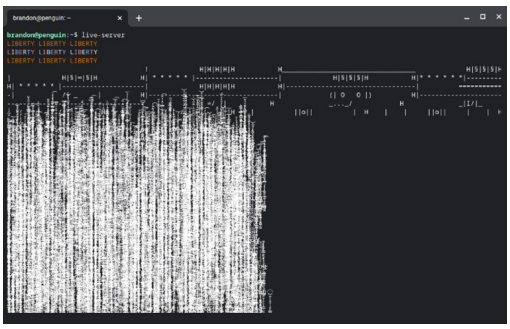
- Colors and Faker: Marak Squires, along with more than 30 collaborators, is known for developing libraries such as Colors, which allows the user to have colour and styles in their node.js console, and Faker, which generates massive amounts of fake data for testing and development environments.

  During January 8, 2022, these libraries underwent a change in one of their components that affected open source projects such as the Amazon Cloud Development Kit (aws-cdk).

  Marak made a commit under the name "Add new module to the US flag" where a file was modified by including three lines that printed the text "LIBERTY LIBERTY LIBERTY LIBERTY" followed by a sequence

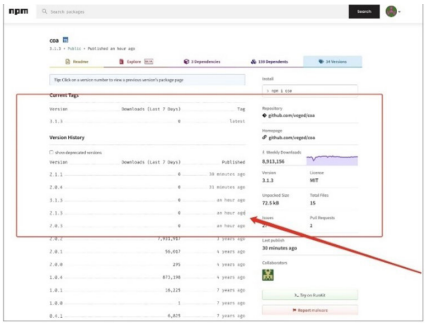


of non-ASCII characters, as can be seen in the following image:



These characters led to an infinite cycle that ran in the consoles of the applications that made use of Colors and Faker. After the incident, Colors returned to its stable version and Faker was adopted by the community.

- COA and RC: After 4 years without any updates, on 4 November 2021, the COA (Command Option Argument) library, known to be a command line option parser, and RC, which allows easy loading of configurations into applications, were altered with new versions visible in the image below:



These versions contained the compile.js, compile.bat, sdd.dll files, which appeared to act as malware, very similar to the Danabot Trojan, made to steal passwords on Windows. When loaded, Danabot steals passwords in browsers and applications, captures stored credit card information and even takes screenshots of active windows (Sharma, 2021).

- UA-Parser-JS: Organisations such as Google, Amazon, Facebook, IBM, and Microsoft were affected by the hijacking of one of the most popular libraries in the developer community: UA-Parser-JS. This library is used to analyse the user agent of a browser to identify the browser, the engine, the operating system, the CPU of a visitor.

  Lead developer Faisal Salman announced on 22 October 2021, via a thread in the library's repository, that the attack occurred because his login credentials to his NPM (Node Package Manager) account were breached. This led to the attackers uploading malicious code to the repository, which installed crypto miners and Trojans that stole passwords on Linux and Windows devices.

How can these security breaches be quickly remedied?

The following are the most secure and common practices to prevent new developments from being affected by attacks such as those mentioned above.

- Defining assessment criteria and using trusted sources: as proposed by the Software Assurance Maturity Model (SAMM) in the security requirements section, this is necessary: "Identify specific security activities and technical evaluation criteria to be considered when contracting third party services" In the case of using free access projects, it is possible to obtain the components from official sites with digital signatures to confirm the integrity of these.
- Creating a test environment: before putting third-party libraries into use, it is possible to isolate them in a test environment to validate their correct functioning and to discard untrusted components.
- Encouraging the use of internal repositories: the idea of these repositories is that they store all kinds of external libraries in a secure way. These repositories help control direct downloads and automatic updates of external components and thus help mitigate risks. This is achieved because, in the event that malicious changes exist in open source libraries, the application that makes use of them will not be affected immediately. As additional management over these repositories, their access control can be managed by assigning the least number of privileges to avoid internal risks.
- Documenting: it is suggested to properly manage the configurations of the dependencies and document each of them. Also, generating an inventory of the versions of each component and constantly monitoring them.

Conclusion

It is clear that the use of external libraries provides tools to support and improve new developments. Their management is considered a very relevant part during the secure development process, and, for this reason, it is necessary to know the threats and possible vulnerabilities when working with them.

As has been presented, attacks on this type of dependencies not only occur by external agents, but also by the creators themselves, who can introduce changes that put the system at risk. Therefore, the process of integrating these elements into internal projects must be carried out with planning and caution; promoting the use of secure internal repositories, creating test environments, defining evaluation criteria, and documenting procedures.

METRICS AND INDICATORS AFTER THE IMPLEMENTATION OF ZERO TRUST IN THE CLOUD

By: NTT DATA Europe & Latam

Although previous editions of RADAR have dealt extensively with the subject and we recommend that you read them, it is worth recalling the NIST (National Institute of Standards and Technology) 800-207 publication which defines the principles, bases, and guidelines to be followed for the implementation of this methodology. This publication describes the need to change the traditional approach (Defence in depth) to one in which identity and data protection are at the centre of priorities.

This publication describes the need to change the traditional approach (Defence in depth) to one in which identity and data protection are at the centre of priorities.

Under Zero Trust architecture there is no implicit trust based on user or device location, asset ownership, authentication, or authorisation. Instead, security measures focus on protecting resources (assets, services, accounts) regardless of their location in the network under the fundamental premise of the imminent existence of security breaches. Security threats can materialise at any time and gain ground by overcoming the technological obstacles that have been designed (when they exist).

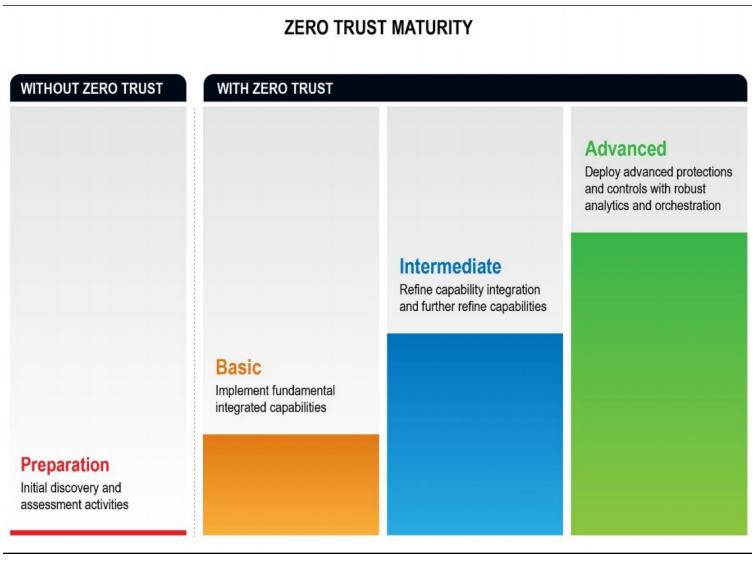
Once the attacker has overcome a barrier, they will continue to look for ways to go deeper, learning, modifying their methods, while erasing the traces to make it difficult for the investigator to detect and block the attack.

In this order of ideas, the controls, accesses, and actions carried out must be evaluated, checked, and monitored permanently in order to be able to prevent, detect and contain those security threats even within the trusted perimeters.

Maturity models

The evolution in the implementation of Zero Trust in cloud environments implies a thorough knowledge of the methodology on which organisations must base their work. For this, the NIST 800.207 publication, the Open Group guidelines, the NSA documentation, or the recommendations issued by the different cloud providers can be taken as a reference framework. Some of them incorporate maturity models in which, according to specific criteria, they measure not only the progress in the implementation of controls but also the degree of automation and optimisation of each one of them. In the following graphs you can see at a very high level the maturity model proposed by CISA (Cybersecurity and Infrastructure Security Agency) and DISA/NSA (Defence Information Systems Agency and National Security Agency, respectively.

	Identity	Device	Network / Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
	Visibility and Analytics	*Automation and Orchestration*	*Governance*		
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
	Visibility and Analytics	*Automation and Orchestration*	*Governance*		
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted
	Visibility and Analytics	*Automation and Orchestration*	*Governance*		



Generally, organisations carry out the implementation of controls based on variables such as:

- Mitigation plan for higher cybersecurity risks to the organisation
- Control implementation costs such as the acquisition of security solutions, licensing, qualified personnel or training, deployment time and effort
- Those already included in the budgets of the Cybersecurity Plan
- Results of security audits resulting from a vulnerability management plan

These aspects affect the prioritisation that organisations may give to the implementation of certain controls, which leads to a scenario in which the level of maturity is more advanced in one aspect than in another. One of the cases that is most observed in organisations is the strengths in issues related to identity management or network management. However, advances in those that have to do with data classification and protection, or the management of devices and applications are moving at a slower pace.

The main reason can be found in the variables described above and has to do with the typically used "Defence in Depth" model. In this model, personnel, and the market in general, have strengthened and entrenched their knowledge of networks and identities, so technologies and deployment times tend to be more manageable for administrators and implementers, and somewhat more economical.

The second reason has to do with cybersecurity audits whose results generally list a significant number of weaknesses related to AAA (Authentication, Authorisation and Accounting). Not surprisingly, 3 of the top 10 security risks listed in the OWASP Cloud TOP 10 are related to these issues.

The third reason is due to the complexity still involved in constructing policies focused on device control and the classification and protection of data. In the first case, the design of controls today must consider models such as Bring your Own Device "BYOD" or Choose Your Own Device "CYOD" which means: Supporting technologies such as iOS, Android, Microsoft, and others that may emerge; allowing connections from any point from which the legitimate connection occurs and in the same sense being able to block connections considered atypical.

It is important to talk about those techniques that have made it possible to advance towards an optimal level of maturity in which analytics, automation and orchestration capabilities allow the work of cybersecurity analysts to focus on making decisions based on previously processed and refined information. This limits the possibility of incurring risks either by not being able to analyse threat data from multiple information systems, by performing actions without sufficiently enriched information or by the limited ability to reconfigure solutions with the IOCs (Indicators of Compromise) detected. Among these techniques are some of the following:

- Machine Learning (ML): For prediction of security threats based on statistical information, analysis of anomalous events, risk assessment before a vulnerability can be exploited by an attacker.
- Artificial Intelligence (AI): They allow for improved attack prediction capabilities using self-learning by emulating human analytics processes through the use of algorithms, which in turn allow for improved learning models.
- Threat intelligence: It consists of the analysis of information from numerous sources in order to determine, based on context, indicators, experience, and reporting, when a threat occurs, how to avoid and how to mitigate it.
- User and Entity Behavioural Analysis (UEBA): By combining AI techniques, ML, and analyst research, it allows determining the typical behaviours of legitimate users in order to generate alerts in case of deviations in actions that could pose a threat.
- Extended Detection and Response (XDR): Technology that seeks to respond to each stage of the cybersecurity incident management process.

The implementation of the above controls will allow us to define action plans tailored to the organisation's needs and restrictions, with gradual deliveries and with the possibility of being able to measure the progress of the adoption of the Zero Trust Methodology. One of the subsequent challenges would be: How can we measure progress?

Measurement and indicators of the level of adoption:

In the 63rd edition of our RADAR magazine, we talked about the importance of cybersecurity indicators for measuring business objectives, for monitoring specific problems or for showing the evolution of the measures implemented on each of the fronts (risk management, incidents, access, etc.). On this occasion, we will emphasise the use or construction of dashboards that allow us to assess the maturity of the implementation of controls in the cloud under the Zero Trust strategy. These dashboards can help determine the impact of measures within the overall cybersecurity score considering aspects such as network, data, computing, infrastructure, and identity assurance, among others. They also provide the organisation with the visibility needed to uncover weaknesses and strengths in order to adjust team priorities and build action plans.

According to the type of dashboard (operational, tactical, or strategic), indicators can be proposed starting from the presentation of the maturity score for each of the domains such as data, identity, networks, applications, and devices. In order to obtain the necessary information for the construction of the indicators, it is necessary to be able to extract this data, which is key to determine the security posture, the level of maturity acquired and that which remains for the fulfilment of our objectives. This information is generally provided by the cloud provider itself, some data is embedded in default features, others require specific licensing, others need to leverage the use of specialised tools for obtaining security posture data (previously mentioned CASB, CWPP, CSPM, SASE solutions). In the event that we cannot access information on the evolution of Zero Trust implementation with any of the above methods, we can make use of office artifacts

in which, by means of specific questions, we can inquire about the degree of implementation in each of the areas. At NTT DATA we have artifacts that help our clients to easily determine the level of maturity in each of the areas, using maturity assessment frameworks such as CISA, DISA/NSA or even those of each of the cloud providers themselves.

As the level of maturity in cloud technology adoption advances and standards become more demanding in order to comply with the Zero Trust strategy, it is necessary to rely on tools that enable the collection of progress information on each of the fronts. This should be done either by using cloud-native tools or through specialised third-party solutions that collect the information.

The following indicators are common to the different Cloud providers and should be incorporated into the relevant information in the implementation of the Zero Trust strategy:

- Global security posture assessment
- Security posture score by area
- Status of progress in implementation by each of the areas

The specific maturity assessment for each of the domains should be assessed according to the chosen framework within the organisation's chosen Zero Trust strategy or by building a hybrid model that takes the best of each methodology and adapts it according to the specific needs of the business in alignment with the strategic technology plan. If we rely on CISA for example, we will have to consider the maturity model that takes conventional "Traditional Stage" company schemes as a starting point and goes through "Advanced Stage" and "Optimisation Stage" in later stages. As mentioned above, and with several points of similarity to other methodologies, the transition from one stage to another will depend on the implementation of more sophisticated controls and technologies.

As an example, we will use as a reference the area related to Identity Management, where we highlight that in order to move from one stage to another we will have to move from non-existent or manual processes to others with a high degree of automation. In this section we will describe the main controls that will help the organisation improve its capabilities, as well as some possible metrics for determining progress.

Authentication

Escalation: The initial stage is based on the use of strong passwords and should move towards the use of strategies such as "Passwordless" supported by Multifactor Authentication (MFA), One Time Passwords (OTP) and random token generation systems. At the optimal level, the automatic generation or adjustment of context-sensitive rules using AI, ML, ML.

Potential Indicators: MFA implementation status, MFA implementation for privileged users, Identities excluded from policy, False positive and false negative rate in detecting attacks on authentication systems.

Identity providers: The organisation should move from the use of non-centralised systems to cloud-based and specialised systems that also allow federation with other third-party authentication systems used by customers, providers, or partners.

Potential Indicators: Percentage of local vs federated users, increase of federated identities, federation related incidents.

Risk management: In initial maturity stages, creation of rules that determine login conditions considering geolocation, risk behaviours, blacklists, among others. In advanced and optimal stages, the rules should analyse the full context of the authentication using AI Artificial Intelligence, and Machine Learning ML.

Potential Indicators: Variation in risky logins, false positive or false negative rate, management of users at risk.

Visibility and analytics capabilities: Through this component, security and monitoring teams can verify as many login-related details as possible, including locations, devices, permissions, and history to determine the validity of user access. With user behaviour analysis "UEBA" the optimal level is scaled by reducing the error rate in the estimation of granted and revoked accesses.

Potential Indicators: Integration and enrichment of data systems with other information systems (SIEM, Human Resources, Blacklists), degree of Implementation of UEBA Capabilities, false positive and false negative rate in event detection.

Automation and orchestration: While organisations adopting automation and orchestration models already have advanced levels of maturity, the evolution in this area is the ability to automate the deployment of identities throughout their lifecycle using robotics. At the optimal level, not only the identities are generated through code, but also the access policies and controls for monitoring the activities performed.

Potential Indicators: Identity implementation times via automation, number of managed identities, incidents related to identity creation, policies and controls adjusted, degree of intervention by analysts.

Governance: Progress in identity governance should aim at the least possible human intervention in functions ranging from the creation of identities to the revocation of identities or adjustments to such permissions. Automation flows using RPA's, AI, ML or UEBA robots perform the permit review and generate policy adjustments based on the level of risk.

Potential Indicators: Time taken to set up identities via automation, number of staff required to set up and remove users, incidents related to the creation of identities.

The maturity level assessment in the example above can be carried out for each of the other related domains in the Zero Trust Model: Devices, Networks, Applications and Data. At NTT DATA we have methodologies, artifacts and solutions that can help the organisation not only to obtain global or specific maturity metrics but also in the design, implementation and optimisation of controls that facilitate the achievement of strategic objectives in this regard. Whatever the cloud provider, technologies chosen or degree of implementation, we can help organisations get a quick diagnosis and generate short, medium, and long-term action plans on the challenge of securely adopting cloud-based technologies.

TRENDS

Cyber exercises as a tool to increase business continuity and resilience

Drills are part of our history and our life. I am sure our readers remember some of them from school, in some countries fire drills are very common and in others earthquake drills are very common. The time it took to leave the building and reach the meeting point was measured there. They would make us run to get better scores every year.

In recent years, disaster recovery plan drills or tests have become more standardised and we are now seeing a greater movement towards so-called “cyber drills”.

A cyber exercise allows an organisation to assess its behaviour in the face of a cyber-attack, and more specifically: (1) assess how its protection, detection and response mechanisms are in place; and (2) assess its procedures and the response of its people.

After carrying out the cyber exercise, the results should be analysed and points for improvement should be obtained. Taking these points into account, the organisation should clarify steps, define procedures or complement them with technology so that the response in a real situation is correct.

There are different types of cyber exercises:

- Exercises which include a controlled entry attack on the organisation and where the main objective is to know the response and reaction of the blue team and the SOC, and how the information flows from there.
- Mixed exercises, where serious damage to the organisation is simulated and it is observed how communication is carried out and what kind of information is included.
- Table top exercises, where the organisation’s infrastructure does not have to be touched and the aim is to measure how information flows from the most technical teams to the C-level itself.

In a real attack on an organisation, an important aspect is information, inwards, towards our employees and outwards: partners, stakeholders, clients and the general public. The cyber-exercises allow you to understand how communication would take place at the time and then assess how it can be improved.

A good cyber drill requires the same thing that was needed for more traditional fire or earthquake drills: getting into the role and actually acting as if the scenario was real. This is a key point in order to get to the bottom of the situation and move towards a better score year after year.

.

VULNERABILITIES

Microsoft

CVE-2022-30190
Date: 30/05/2022

Description. A new 0-day vulnerability has been published in the Microsoft Windows Support Diagnostic Tool (MSDT), which is widely used by other company software and can be exploited. The failure is caused by a misconfiguration in the input validation when processing the URL within the diagnostic tool. An unauthenticated remote attacker could gain control of the affected system by using the corresponding exploit.The vulnerability was detected by identifying a document developed through the Word word processor, which was intended to exploit the security flaw. In addition, Microsoft has reported that groups are actively exploiting this vulnerability.

Link:

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-30190

https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Affected Products.

- Microsoft Office 2013. 2016, 2019 and 2021

Solution: The manufacturer has issued a security update and a guide to protect systems from exploitation of the vulnerability. This guide can be found at the following link: https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

Zoom

CVE-2022-25235, CVE-2022-25236, CVE-2022-22784, CVE-2022-22786, CVE-2022-22787 y CVE-2022-22785.
Date: 25/05/2022

Description. Google's security research team has published information about several security vulnerabilities that would allow remote code execution on the Zoom platform without any user interaction. In this way, a remote user could execute malicious code via chat messages, without the need for the victim to reply to these messages.

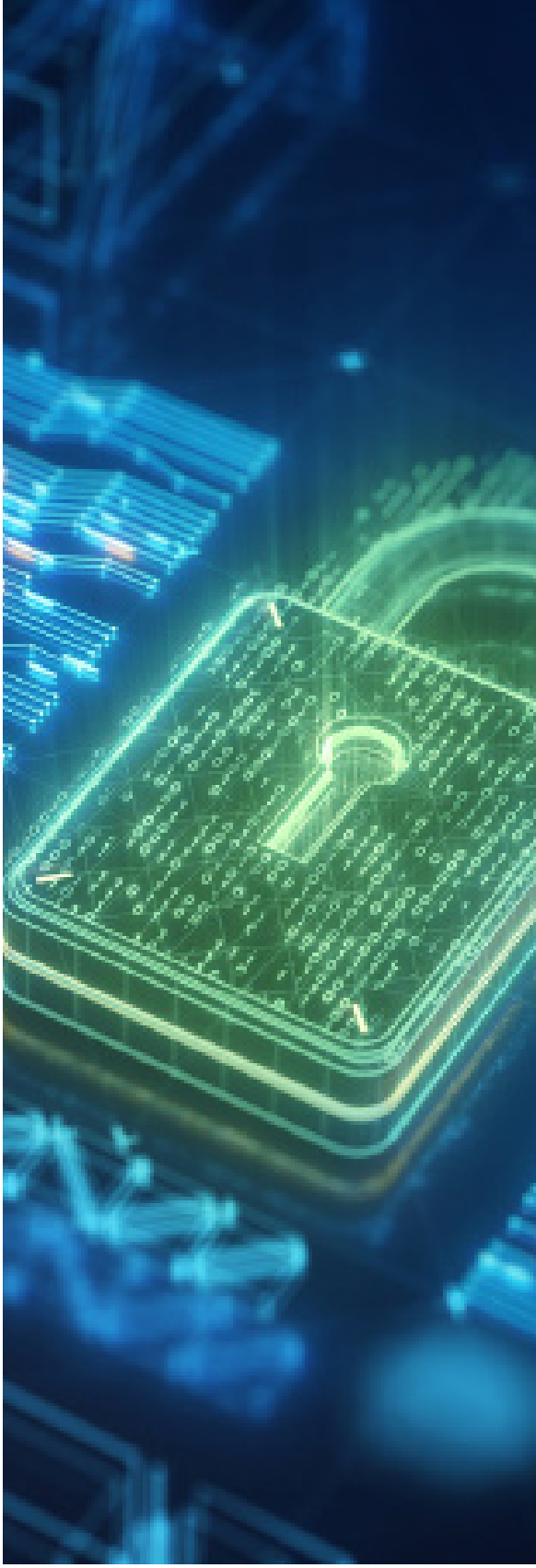
Link: https://bugs.chromium.org/p/project-zero/issues/detail?id=2254

Affected Products.

- Zoom versions prior to 5.10.4

Solution: Update to version 5.10.4 or later versions of the software.

PATCHES



GitLab

Date: 01-06-2022

Description. GitLab has updated the passwords of some users, after fixing a critical vulnerability that would allow them to take control of their accounts. In the affected versions, an encrypted password was set when the account was logged in using an OmniAuth provider. These passwords have been reset for users who might be affected.Two additional vulnerabilities have also been identified through which an attacker could inject HTML into the notes and execute XSS.

Link: https://about.gitlab.com/releases/2022/06/01/critical-security-release-gitlab-15-0-1-released/

Affected Products:
GitLab Community Edition (CE) and Enterprise Edition (EE) versions prior to 14.7.7, 14.8.5 and 14.9.2

Solution: Apply the necessary updates and patches provided by the manufacturer.

Confluence

Date: 02-06-2022

Description. Atalassian has released new versions of its software to fix the vulnerability with identifier CVE-2022-26134, which allowed remote code execution without authentication on Confluence Server and Data Center. As this is such a critical vulnerability, it is recommended that the software be updated immediately or, failing that, the corresponding files marked by the manufacturer on its website be modified as a mitigation measure.

Link: https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html

Affected Products: Versions 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4, 7.18.1 and prior

Solution: Update to versions 7.4.17, 7.13.7, 7.14.3, 7.15.2, 7.16.4, 7.17.4 or 7.18.1

EVENTS

CYBERSECURITY FINANCIAL & GOVERNMENT

7 July 2022 |

Fintechs, Banks, Governments, Cybersecurity Organisations and Technology Companies will gather at the region's leading Cybersecurity Conference to continue the dialogue on hyperconnectivity; how cybercrime continues to gain ground and what actions to take in 2022 to ensure business continuity in the digital realm.

Link: Cyber Security 2022 (cybersecuritylatam2022.com)

INTERNATIONAL CONFERENCE ON CYBER SECURITY

13 -17 July 2022 |

It is the world's leading cybersecurity event, taking place over three days and bringing together more than 60 distinguished speakers from government, the private sector and academia. This is a unique opportunity for global leaders in cyber threat analysis, operations, research and law enforcement to coordinate and share their efforts to create a safer world.

Link: Home - International Conference on Cyber Security 2021 (fordham.edu)

INDUSTRIAL CONFERENCE ON DATA MINING (ICDM) 2022

19 - 22 July 2022 |

The ICDM Data Mining Industry Conference is held annually. Researchers from around the world will present theoretical and application-oriented topics in data mining. Professionals can present and discuss their ongoing projects in the industry sessions.

Link: Home - International Conference on Cyber Security 2021 (fordham.edu)

CLOUDCON 2022

25 July 2022 |

Unique for being one of the few cloud-centric events worldwide. After spending two days with your fellow security professionals, you will be better equipped to make an immediate impact on the security of your company or organisation.

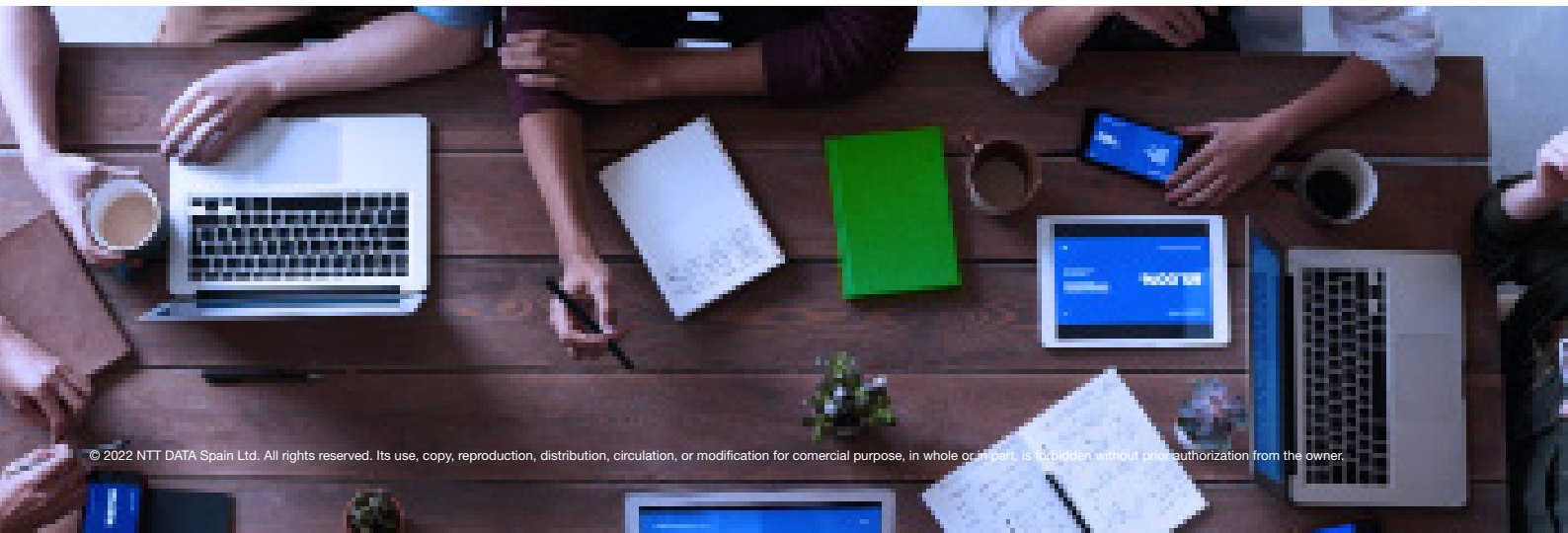
Link: https://cloudcon.us/

MAY CONTAIN HACKERS

22 - 26 2022 |

The event is organised by and for volunteers from all facets of the global hacker community. Knowledge sharing, technological advancement, experimentation, connecting with fellow hackers and hacking are some of the core values of this event. MCH2022 is the successor to a series of similar events held every four years since 1989. These are GHP, HEU, HIP, HAL, WTH, HAR, OHM and SHA.

Link: May Contain Hackers 2022 (mch2022.org)



RESOURCES

GITHUB

GitHub has just released version 3.5 of its Enterprise Server (GHES 3.5). This new release brings more than 60 new features to the platform, with advanced security and compliance practices to enable enterprises to take full advantage of DevSecOps.

Link: GitHub: Where the world builds software

CLOUD SECURITY ALLIANCE

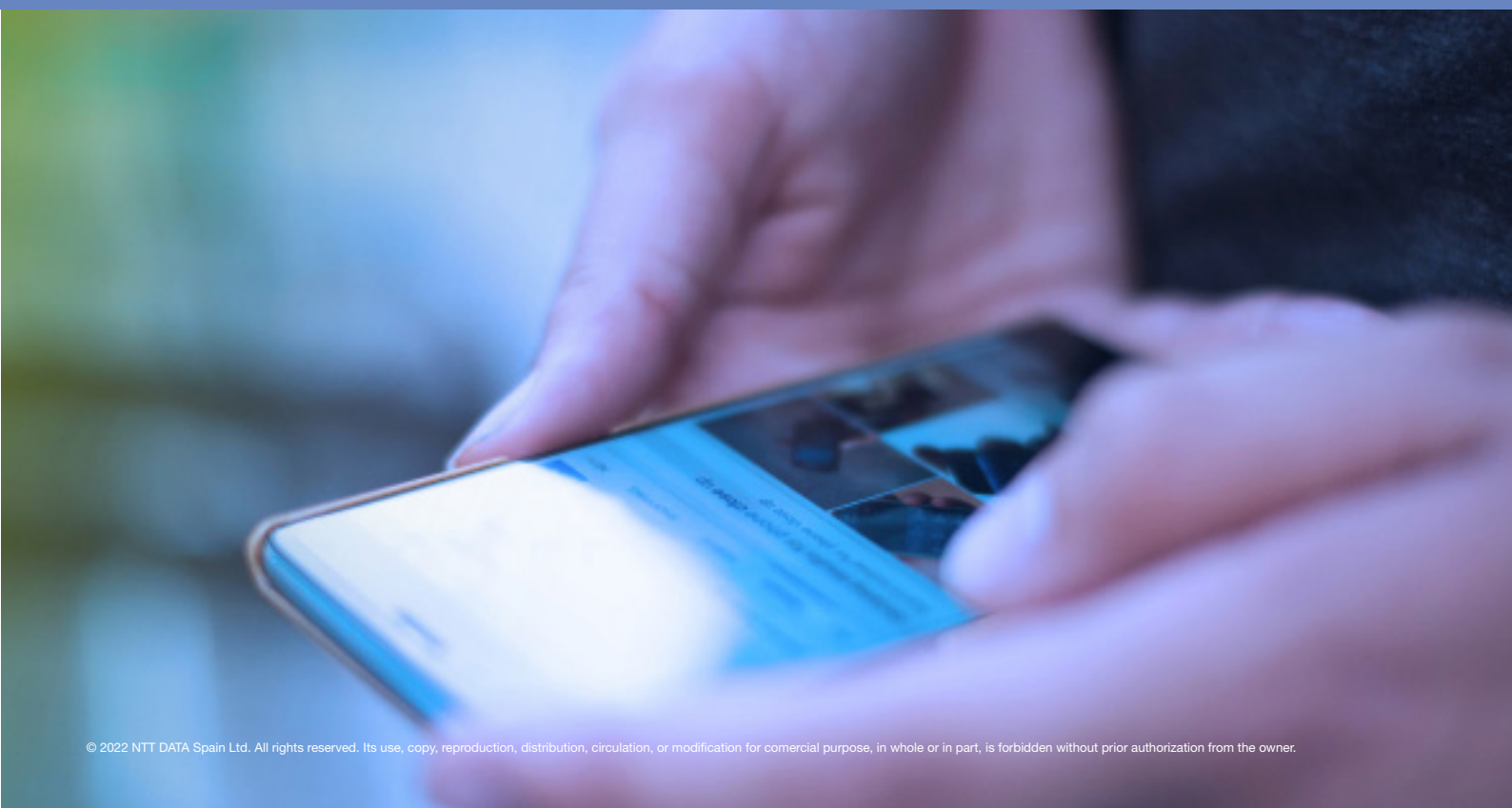
The Cloud Security Alliance (CSA), the world's leading organisation dedicated to defining standards, certifications and best practices to help ensure a secure cloud computing environment, has published software-as-a-service (SaaS) governance best practices for cloud customers.

Link: SaaS Governance Best Practices for Cloud Customers

CLOUD SECURITY ALLIANCE

Cloud Security Alliance discusses the importance of building business-critical applications with application security testing via its blog channel. The article focuses on how application security testing can eliminate blind spots when working with contractors and external developers.

Link: Security Testing for Critical Applications: Part 2




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