NUMBER 80 | JULY 2023

NTT DATA
Trusted Global Innovator

Radar

Cybersecurity magazine

TALENT SHORTAGE AND HIGH TURNOVER: TODAY'S GROWING CONCERN

Organisations are increasingly reliant on technology, which is evolving at high speed, resulting in an exponential increase in increasingly sophisticated digital threats with attacks that are difficult to detect and defend against. As a result, there is now a global demand for cybersecurity professionals that far exceeds the available supply.

But, how big is this GAP?

Some studies reveal that worldwide there are 3.4 million security specialists (26% more than last year), for example, in Latin America there are 700,000 professionals. These studies further reveal that as the labour force grows, demand grows faster, while the gap between supply and demand widens on a larger scale than the availability of talent.

Searching for specialised and better qualified professionals

The critical competencies and experiences required can be summarised in the following key elements:

1. Relevant IT and cybersecurity work experience.
2. Knowledge of advanced cybersecurity.
3. Understanding of threats and vulnerabilities.
4. Problem-solving skills.
5. Capability to influence and articulate across the organisation.
6. Strategic thinking, responsiveness, and decisiveness.

So on the one hand we have technology and its evolution, which can always be learned, and on the other hand we have skills such as curiosity, problem solving and critical thinking, which are increasingly valued and considered essential for this speciality. With these conditions, the complexity and challenge of identifying talent for this speciality (function) increases consistently.

How can the talent gap be bridged?

In the face of the talent demand challenge, organizations must react by focusing on cybersecurity training. This involves, on one hand, upskilling actions or improving capabilities, and on the other hand, complementing with reskilling or acquiring new skills. Both strategies result in greater impact. We find that organisations with initiatives to build internal talent through rotational work assignments, mentoring programmes and encouraging employees from other specialisations to join the cybersecurity field are less vulnerable to a lack of skilled cybersecurity professionals.

Enrique Bernao

Cybersecurity Manager at NTT DATA Europe & Latam

CYBER NEWS

In this edition of RADAR we will discuss end-user security. It is no myth that humans are the weakest link in the chain. A recent attack on citizens was reported to be affecting traffic offenders. If you have traffic fines and are overdue for payment, you should be careful, as scammers are tricking the unwary through social engineering. Scammers take advantage of citizens' need to renew their driving licences by offering them supposed discounts for the payment of their fines, when in fact they are robbing them.

One of the victims of this scam mentions that he received an email stating that his driving licence was about to expire, and that he could access discounts on his offences. The victim accessed a link where a website "exactly like the official one" showed him his offence history and redirected him to an advisor via WhatsApp.

> "Discord, the instant messaging, and VoIP service most widely used by Gamers, Influencers and Streamers, is notifying its users that last May they suffered a hacking attack that resulted in the exfiltration of data from the platform"

In this WhatsApp conversation, a supposed advisor, who also had exact data such as: number of fines, amounts to be paid, dates, addresses and the payment document, asks the victim to make a deposit. The scammer informs him this deposit is done in order to access a supposed discount on the infringement fee.

The cybernetic police command was alerted through citizen complaints and within a few hours the website was taken down; however, there is no exact record of the people who were scammed. Although there is a fundamental human factor for this type of fraud to materialise, there are security controls that can be implemented by application owners to reduce the surface area of this type of attack on their end users. For example, site cloning detection, authentication for information consultation, usability monitoring, captcha, verified advisor accounts, among others.

On a global scale, Discord, the instant messaging, and VoIP service most widely used by Gamers, Influencers and Streamers, is notifying its users that last May they suffered a hacking attack that resulted in the exfiltration of data from the platform. The attack occurred after an outsourced support manager was compromised.

The attack reportedly exposed all support tickets assigned to the contributor. Among the exfiltrated data there were email addresses, exchanged messages, and supporting attachments. Discord's security team mentioned that once the incident was detected, the contributor's account was disabled and his equipment was subjected to strict anti-malware checks.

"Due to the nature of the incident, it is possible that your email address, the content of customer service messages and any attachments sent between you and Discord may have been exposed to third parties," was the message that dawned on hundreds of users as they authenticated on the platform. They also mentioned that they are working with their support provider to implement efficient measures to prevent similar attacks in the future and advised their users to be strictly vigilant against targeted phishing attacks.

Once again, company employees are victims of social engineering attacks aimed at gaining access to the systems they manage. Hence the importance of effective awareness campaigns that enable all employees, regardless of their area or technical expertise, to detect and report such attacks. It is also important that end-users of support services refrain from sharing confidential information and be very concise about the issues they raise.

Continuing with denial of service attacks, Microsoft suffered a denial of service attack in early June. Azure users had their access to the platform affected, in what is suspected to be a distributed denial of service (DDoS) attack. According to the monitoring site Downdetector, 77% of users had problems accessing the Azure website, while 18% experienced problems authenticating.

The incident led to a statement from Microsoft, in which they acknowledged the problem and promised to provide an update within the hour or as events unfolded. The website went offline after an individual identifying himself as Anonymous Suda claimed he was carrying out a DDoS attack. However, Microsoft, which is renowned for its robust protection against such attacks, argues that it has been able to mitigate the impact.

This type of attack on Azure infrastructure has been recurrent so far this year. For example, between January and February, Microsoft reported that the availability of its WAF service, Azure FrontDoor, was affected, causing all sites protected by it to be down, forcing companies to disable this protection and expose their services to the internet for more than 12 hours. These attacks on Microsoft's cloud demonstrate that no one is immune to cyber-attacks, so organisations must have proven defence-in-depth models, backup mechanisms and disaster recovery plans in place.

Finally, Progress Software Corporation, renowned for its IT software and services offerings, has alerted its customers to a worrying vulnerability in its MOVEit Transfer and MOVEit Cloud products. This vulnerability, which was catalogued as CVE-2023-34362, was discovered at the beginning of June and is said to affect hundreds of thousands of users of different companies around the world that use these services.

MOVEit Transfer is a cloud solution used to securely store and share files across computers, servers, departments and even supply chains. Its web-based functionality enables effective collaboration and automated transfer of sensitive data, all without the need for programming skills. Russian cybercriminal groups are said to have exploited a SQL injection in different instances of MOVEit and managed to exfiltrate information on its clients, including the BBC, British Airways and Boots. These criminals are reportedly claiming a reward for not disclosing the captured information.

In a series of statements, Progress Software Corporation says it is actively working on a fix for the vulnerability, and that it is committed to maintaining the confidentiality and privacy of its customers. Additional updates are expected in the coming days to address this issue and further strengthen the security of MOVEit products.

DATA SECURITY IN MULTI-CLOUD AND REAL-TIME ENVIRONMENTS

By: NTT DATA

The favourable results from the use of big data in terms of optimisation and efficiency in companies are unprecedented. The exponential growth of data generation has great challenges in terms of technologies that allow the processing of large amounts of data streams in the shortest possible time and in the most economical way.

In addition, the processing and use of real-time data is key for more accurate decision-making.

In this sense, we can cite at least four key milestones in the development and growth of the use of real-time data:

1) the number of devices available to capture data,
2) the internet of things (IoT),

3) cloud and

4) in-memory processing, which has become more accessible and popular in recent years.

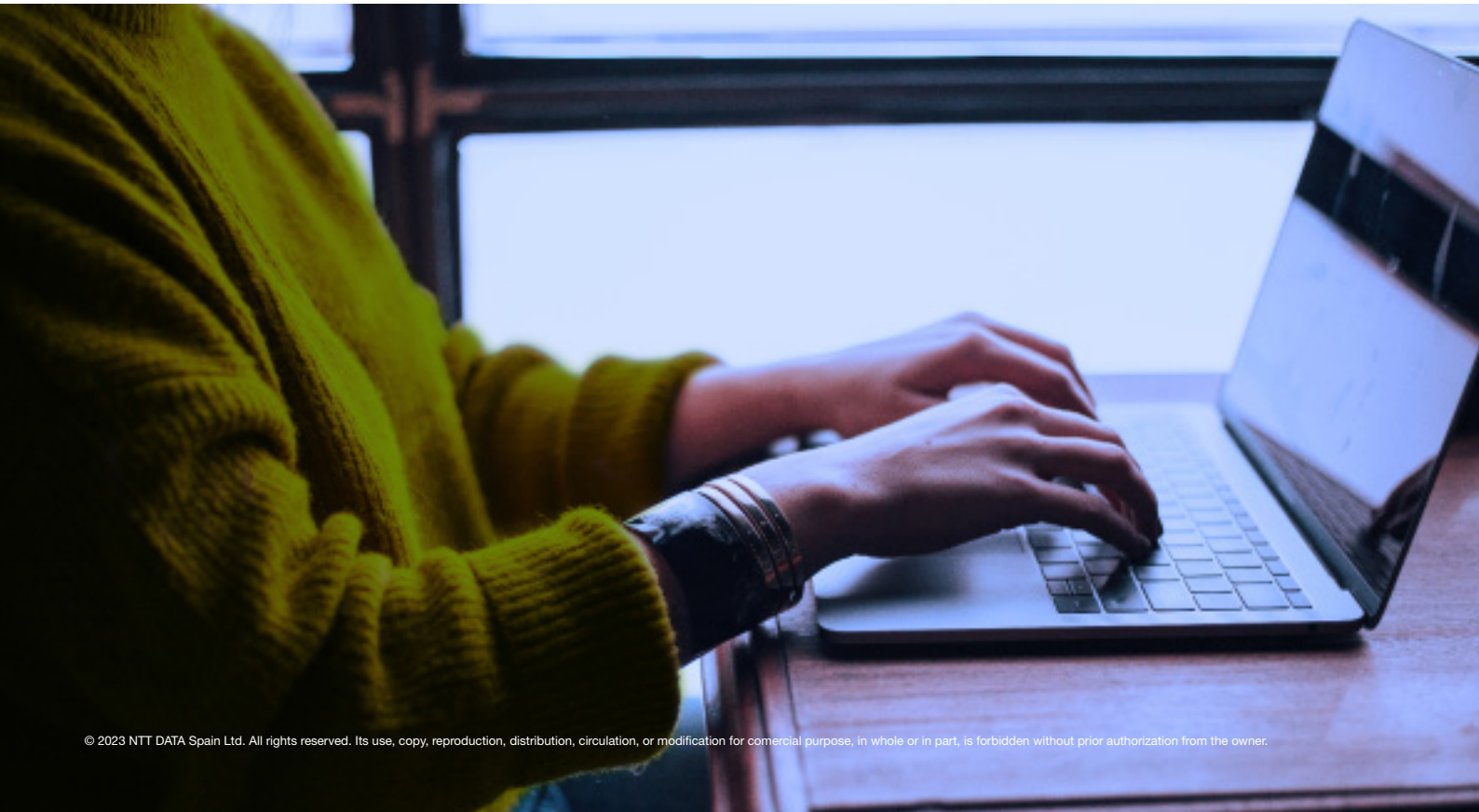
The implementation of all these tools and processes have one major challenge in common: end-to-end data security.

Following the conceptualisation of Data Security developed by DAMA-DMBOK , it includes the planning, development and implementation of security policies and procedures to provide adequate authentication, authorisation, access and auditing of data and information assets.

The objective of data security practices is to protect information assets in alignment with privacy and confidentiality standards, contractual agreements, and business requirements.

Despite the imperative of implementing such measures, Confluent , in its 2022 report, shows that only 27% of the companies interviewed have security tools in place to deal with real-time data processing, with the biggest challenge being the implementation of security and compliance in multi-cloud environments.

Some of the fundamental aspects to be taken into account in the implementation of security measures in real-time and multi-cloud data processing are:



- Real-time threat identification: It is essential to have monitoring and data analysis tools to detect and prevent potential threats in real time. There are currently a number of developments that apply AI to processes to carry out these practices.
- Segmentation and security in accesses: identify and generate accesses according to the associated permissions, with appropriate authentication, to avoid the risk of unauthorised accesses, guaranteeing that those with valid authorisation have access to the data.
- Protection of data in transit: organisations must ensure high levels of security around data in transit by implementing solutions to ensure data integrity.
- Rapid response to security incidents: It is important to have contingency and security incident response plans in place to ensure a rapid and effective response in the event of a security incident.
- Continuous updating: keeping security systems and tools up to date is key to ensuring that new security threats can be identified and prevented in real time.
- Network segmentation: Network segmentation is used to divide a network into smaller segments and control the flow of data between them. This helps prevent attackers from moving laterally in the network and gaining access to sensitive data.
- Integration of security tools: In a multi-cloud environment, it may be necessary to integrate multiple security tools from different vendors to ensure complete protection. This can be a challenge in terms of compatibility and tool configuration.
- Regulatory compliance: carry out a regulatory compliance plan, according to the rules applicable in each country, especially taking into account those relating to international data transfers. This has a high degree of complexity when considering multi-cloud environments, as data and applications may be distributed across multiple cloud service providers with different security policies and protection tools, which need to be unified.

One of the most disruptive trends in data security, which has gained prominence in recent times, is the adoption of artificial intelligence and machine learning-based technologies to improve threat detection and real-time security incident response, some of which have been mentioned in our RADAR from March.

In terms of security approaches, Zero Trust challenges the traditional implicit trust model and assumes that all interactions, both internal and external, must be constantly verified and authenticated to reduce security risks.

Today's Zero Trust security model has been extended and its principles have been implemented in many ways, including Zero Trust architecture, Zero Trust Network Access (ZTNA), Zero Trust Secure Web Gateway (SWG) and micro-segmentation. Zero Trust security is also sometimes referred to as perimeter-less security.

However, it is worth noting that all technological security implementations will be successful as long as the people working in the companies are trained in security and practice security on a daily basis. That is why security awareness, literacy and education is the essential pillar, especially in data driven companies aiming at the democratisation of data.

In conclusion, the implementation of data security processes and tools is imperative and should be taken into account from the beginning in the data strategy of any organisation, and should be one of its main objectives, since it not only responds to business needs in terms of the ability to make good decisions, but its non-compliance entails legal and economic consequences for companies.

“ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FROM NIST RMF AND NIST AI 100 APPROACH ”

By: NTT DATA

Nowadays we find that Artificial Intelligence (AI) has rapidly transformed our world through the automation of tasks, agility in processing large amounts of information, etc. Due to the great progress of this, several tools have emerged that incorporate AI within their functionalities, offering increasingly advanced software.

This, in turn, brings with it a number of risks and threats that we may not have been aware of before or that we are currently viewing in a different way. The issue of risk management in the implementation of AI is an essential issue, given its increasing prevalence in various activities. In addition, the adoption of AI systems can exacerbate certain risks within an organisation, especially with regard to information security and privacy.

This is why the debate on this issue is becoming increasingly relevant.

Some of these risks include discrimination, job loss and data privacy, as well as the lack of transparency and explainability of algorithms. Ethical and social challenges related to AI have also been explored, including algorithmic bias, the criticality of some personal data and cyber security.

While AI can process large amounts of data in seconds, it can also significantly increase the risk of privacy breaches, for example.

It is important to mention that to address and respond to the challenges and complexity of AI risk management there are frameworks, such as NIST RMF and NIST AI 100, that can be of great help to organisations in managing the risks associated with AI.

These frameworks not only provide guidance for the identification and assessment of risks, but also provide a structured approach to implementing security measures and to monitoring and responding to risks.

With the growing importance of AI in our world, effective risk management is essential to protect privacy and data security, as well as to ensure trust in AI technology.

By applying appropriate security frameworks in the implementation of AI, organisations can minimise the associated risks and maximise the benefits that AI can offer. This is why risk management, from a GRC (Governance, Risk and Compliance) approach, has become essential for AI to be developed and used safely and responsibly in processes within an organisation.

The NIST RMF and NIST AI 100 are complementary frameworks that together can help organisations assess and manage the risks associated with implementing artificial intelligence. The NIST RMF consists of six phases: categorisation, selection of controls, implementation of controls, evaluation, authorisation, and continuous monitoring. By following this framework, organisations can assess the risks associated with information systems and take steps to minimise those risks.

On the other hand, the NIST AI 100 is an AI-specific framework that can be applied to the RMF to provide additional guidelines for risk assessment and risk management in AI implementation. This framework is composed of five key areas: governance, AI lifecycle, explainability, privacy and security. By combining both frameworks, organisations can have a more complete understanding of the risks associated with AI implementation and take steps to mitigate those risks more effectively.

While the use of both frameworks cannot completely eliminate the risks associated with AI, they can help organisations to effectively assess and manage these risks. In this way, it is possible to reduce the likelihood of occurrence of behaviour that is identified as risky, such as security breaches.

To ensure proper management of the risks associated with AI, the NIST AI 100 recommends a series of 5 key steps:

The first step is risk identification, which involves identifying the potential risks associated with AI implementation. In this phase, both security and privacy risks should be considered, as well as other risks that may be specific to the organisation’s environment.

The second step is risk assessment, which involves carrying out a detailed evaluation of the identified risks to determine the impact and

likelihood of their occurrence. This assessment should be based on a detailed risk analysis and should take into account both technical and business aspects.

Once the risks have been assessed, the third step is risk mitigation, which involves implementing mitigation measures to reduce the identified risks to an acceptable level. These measures may include additional security controls, risk management procedures, security policies and practices, among others.

The fourth step is verification and validation, which involves verifying that the implemented mitigation measures are working properly and that the risks have been mitigated to an acceptable level. This may include penetration testing, security testing, vulnerability scanning, among others.

Finally, the fifth step is monitoring and continuous improvement, which involves establishing a monitoring and continuous improvement process to ensure that mitigation measures remain effective over time and that they are kept up to date in response to changes in the organisation's environment.

By incorporating a Governance, Risk and Compliance (GRC) approach, a comprehensive strategy for Artificial Intelligence (AI) management can be developed. This approach to GRC involves critical aspects such as risk identification, the design and implementation of clear policies and standards, the careful selection of suppliers, the implementation of security controls and adequate training for employees. This last factor is essential to foster a culture of compliance within the organisation.

Adopting the GRC approach not only enables more efficient risk management, but also helps companies to ensure compliance with regulatory requirements that may arise. This is achieved through the implementation of appropriate security policies and practices, which in turn contributes to the security and effectiveness of the organisation's AI implementation.

In summary, the combination of the NIST AI 100 framework, NIST RMF and the GRC approach can be an effective strategy to mitigate the risks associated with the implementation and use of artificial intelligence in enterprises. The security, privacy and reliability of artificial intelligence systems are crucial to an organisation's success, from a holistic and well-planned approach to ensure a secure and responsible environment.

TRENDS

The use of facial biometrics during the onboarding process as a key factor for acquiring more customers

The constant technological evolution offers endless business opportunities for companies willing to embark on the journey of digital transformation. And when it comes to delivering high-value, customer-focused experiences, digital onboarding makes a significant contribution.

But before we delve further into the importance of digital onboarding, it is necessary to understand what digital onboarding is. A brief description could be a set of instructions or interactions that a user must follow in order to obtain a certain product and/or service.

The great challenge of digital onboarding

This definition of a set of instructions and interactions has become one of the main challenges for organisations in the coming years. While users demonstrate their preference for using digital channels, the reality is that around 70% of users abandon product and service acquisition processes because of a complicated and tedious experience during the onboarding process (Financial Brands, 2022).

Reasons for abandoning the acquisition process

It is no secret that a user's first interaction with your product and/or service is critical, and a bad experience can impact new customer acquisition or retention of existing customers. Here are the 3 main reasons why users drop out of the process:

1. Long processes: Indicates that the process exceeds the time expected by the user.
2. It does not add value to them: It did not generate enough attention for them to initiate and/or complete the onboarding process.
3. Too many requirements: The process is either too demanding or too complex to carry out.

Large companies addressing this challenge

In response to the main reasons for abandonment, biometric facial identification offers a seamless and secure user experience that improves conversion rates during the onboarding process. Also, given that this type of solutions are probabilistic (at a certain level of % they confirm the identity of the users) and in order to ensure continuous improvement, it is important to develop certain capabilities such as:

- Secure and scalable development and integration model.
- Analytical model through the steps the user goes through.
- Preventive model for impersonation cases

Positive results can already be seen in the United States and Europe, with an average reduction of 20% in the drop-out rate. However, in the case of Latin America, the adoption of biometric facial identification solutions is still lower.

Finally, companies planning to increase their attraction rates and retain customers through innovation and transformation of their digital channels should not overlook the critical role of defining and managing their onboarding processes. The incorporation of biometric facial identification solutions enhances the security of customer information and helps deliver a frictionless experience every time a user interacts with the brand.

VULNERABILITIES

Android

CVE-2023-21127;-21126;-21128;-21129;-21131;-21139;-21105;-21136;-21137;-21143
Date: 05/06/2023

Description. Multiple vulnerabilities have been discovered in Google's Android operating system, the most serious of which could allow remote code execution. Android is an operating system developed by Google for mobile devices, including but not limited to smartphones, tablets, and watches. Successful exploitation of the most serious of these vulnerabilities could allow privilege escalation. Depending on the privileges associated with the exploited component, an attacker could install programs; view, change or delete data; or create new accounts with full rights.

Link: https://source.android.com/docs/security/bulletin/2023-06-01?hl=es-419
https://www.securityweek.com/androids-june-2023-security-update-patches-exploited-arm-gpu-vulnerability/

Affected Products: This vulnerability affects the following Android AOSP versions:

- Version 11
- Version 12
- Version 12L
- Version 13

Solution: The main workaround for this vulnerability is to update to the latest versions of Android.

Fortinet Fortigate

CVE-2023-27997
Date: 11/06/2023

Description. Fortinet issued an update recently, following the discovery of a bility that could allow remote unauthenticated code execution on devices. The CVE-2023-27997, is a heap-based buffer overflow error. This bug, when exploited, can allow unauthenticated users to remotely lock devices and potentially execute code.

At present, it remains uncertain whether this vulnerability has been actively exploited by attackers. However, the rapid discovery and response serves as a testament to the importance of continuous vigilance in cyber security.

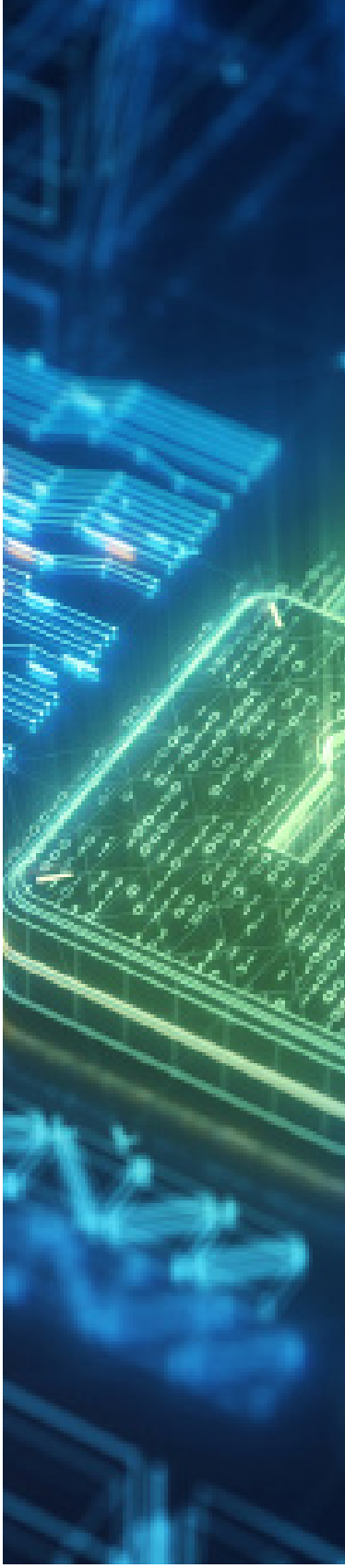
Link: https://securityonline.info/cve-2023-27997-fortinet-fortigate-pre-auth-rce-vulnerability/
https://www.bleepingcomputer.com/news/security/fortinet-fixes-critical-rce-flaw-in-fortigate-ssl-vpn-devices-patch-now/

Affected Products: The affected products correspond to all previous versions of FortiOS:

- 6.0.17
- 6.2.15
- 6.4.13
- 7.0.12
- 7.2.5

Solutions: Update products to the latest versions as previously mentioned.

PATCHES



Microsoft

Date: 02-06-2023

Description. The company that owns MoveIT Transfer and MoveIT Cloud software (Progress Software) has released a patch fix for a critical vulnerability known as CVE-2023-34362. This vulnerability is of the SQL injection type and would allow third parties to take control of the control panel of this software on a server. Once access is gained, data could be stolen or installed as webshells (backdoors) and modifications could be made to the compromised server. It is known that this vulnerability has been exploited since the end of May, and it is also known that the attackers who are exploiting this vulnerability are creating backdoors on the compromised servers with the name "human2.aspx".

Link:
https://www.incibe.es/incibe-cert/alerta-temprana/vulnerabilidades/cve-2023-34362
https://news.sophos.com/es-es/2023/06/07/informacion-sobre-la-vulnerabilidad-cve-2023-34362-de-moveit-transfer-y-moveit-cloud/

Affected products: The affected products are:
- Move IT Transfer
- Move IT Cloud

All versions prior to 13.0.6 are found to be vulnerable.

Update: It is recommended to update the relevant products to the latest available version (15.0.1).

Samsung

Date: 06-06-2023

Description. Samsung has published its security bulletin to reveal more information about the June 2023 security patch. It includes 53 fixes from Google for security vulnerabilities found in Android smartphones and tablets. Three of them are marked as critical, while 50 are marked as very important. The update also includes 11 fixes for security flaws found on Samsung devices. The South Korean firm has explained three of these 11 vulnerabilities (SVE or Samsung Vulnerabilities and Exposures). The remaining vulnerabilities will not be disclosed until all Galaxy phones and tablets receive the June 2023 or later security patches.

Link: https://www.sammobile.com/news/samsung-june-2023-patch-detailed/
https://www.dealntech.com/samsung-june-2023-security-update-galaxy/

Affected products: Android versions 11, 12 and 13 prior to this update.

Update: For the correction of these vulnerabilities an update to the latest security patch of June 2023 is required.

EVENTS

Cyber Security Training at SANSFIRE

10 - 15 July 2023 |

Learn how to combat the world's latest cyber threats with up-to-date training from real-world professionals. Connect with other professionals in the cyber community at one of our biggest events in 2023. Join us in Washington, DC, or live online for SANSFIRE 2023 (10 July - 15 July, EDT).

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

Cyber Security Training at SANS Cloud Security

17 - 22 July 2023 |

Learn real-world cybersecurity skills from top industry experts during SANS Cloud Security San Francisco (17-22 July). Join us in San Francisco, CA or live online to experience interactive training with hands-on labs, practice your skills during one of our NetWars Tournaments and network with other professionals in real time. Choose your course and register now!

LInk: https://www.sans.org/cyber-security-training-events/cloud-security-san-fran-2023/

Splunk Conf

17 - 20 July 2023 |

It is not your typical cybersecurity conference, but if you are a Splunk user and you are in the cybersecurity field, this is an event you should attend. At Splunk Conf, you will be able to learn from Splunk experts, peers and Splunk partners about how they are tackling real-world security challenges. You will be able to learn with hands-on sessions on Splunk security products and learn best practices to strengthen your security posture and improve your skills.

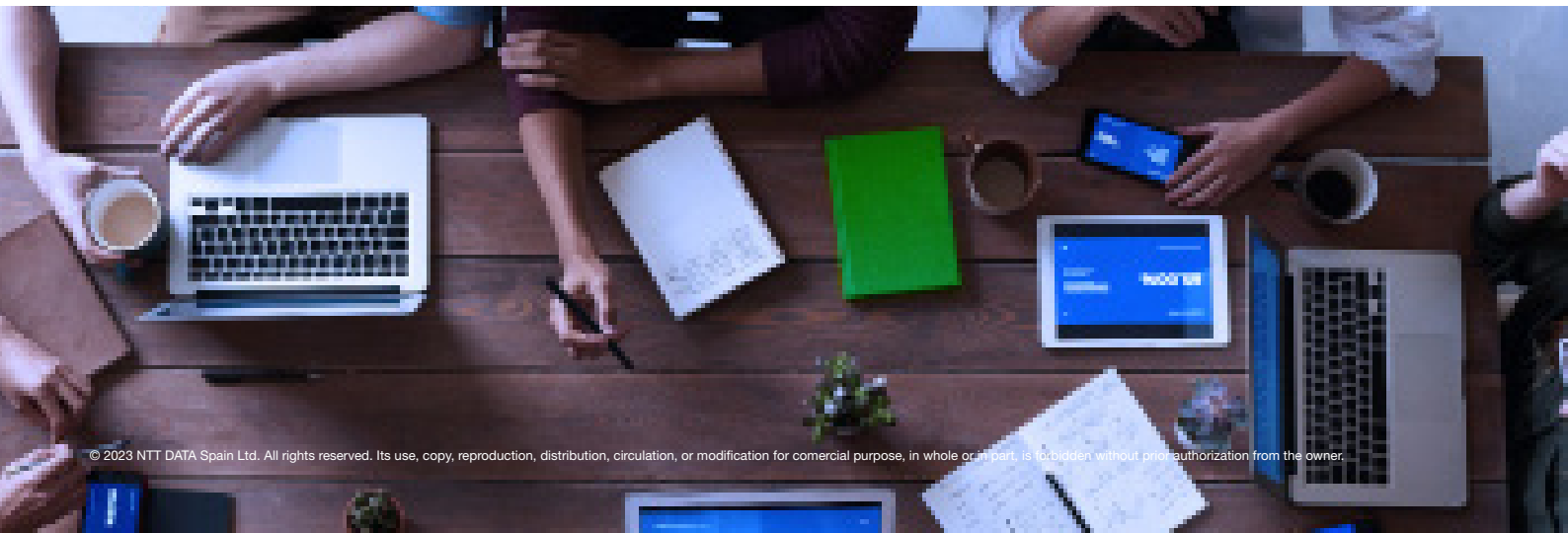
Link: https://conf.splunk.com/

Black Hat USA 2023

5 - 10 August 2023 |

The Black Hat Briefings are a series of highly technical information security conferences that bring together thought leaders from all facets of the infosec world, ranging from the corporate and government sectors to academia, including underground researchers. The environment is strictly vendor-neutral and focuses on the exchange of practical ideas and timely and applicable knowledge. Black Hat remains the biggest and best event of its kind, unique in its ability to define the information security landscape of tomorrow.

Link: https://www.blackhat.com/upcoming.html



RESOURCES

Google unveils new cybersecurity features for ChromeOS

Google LLC has announced a set of new features for ChromeOS aimed at helping businesses protect corporate data and employee devices from hackers. The features were unveiled at the annual RSA conference in Las Vegas.

Link: https://cloud.google.com/blog/products/chrome-enterprise/protect-business-data-chromeos-data-controls-and-new-security-integrations

Understanding Zero Trust's two maturity models

CSA Zero Trust and Industry Insights Blog Post by John Kindervag comparing and contrasting the new version of the CISA Zero Trust maturity model and Forrester's 2017 maturity model that he developed in 2016 while working for Forrester.

Link: https://cloudsecurityalliance.org/artifacts/understanding-the-two-maturity-models-of-zero-trust/

CM Machine-readable package (JSON/YAML/OSCAL)

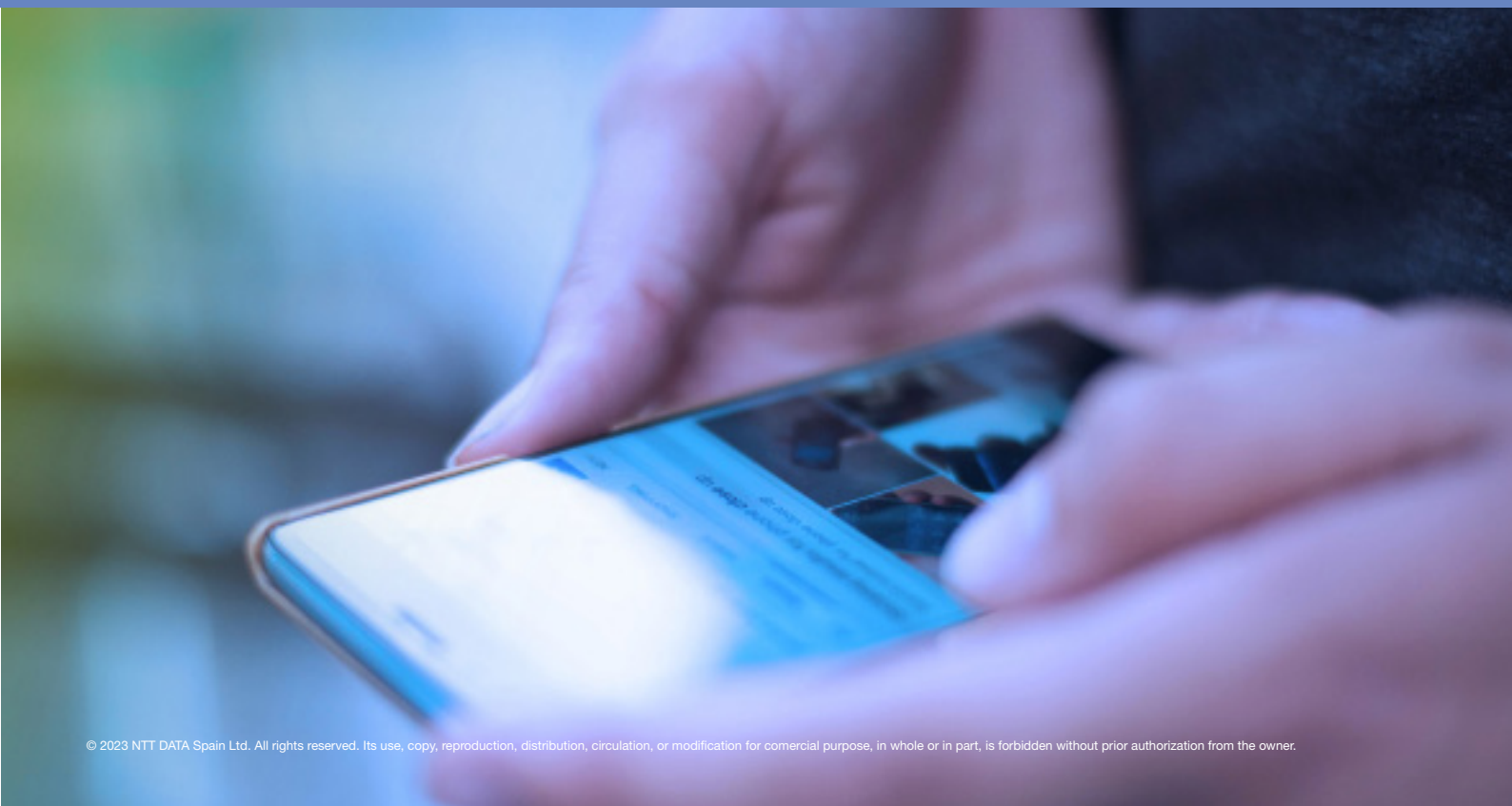
CSA provides in a machine-readable format the CCM Controls, the CAIQ Security Questionnaire, the Implementation Guidelines (both JSON/YAML and OSCAL) and the Correspondences (JSON/YAML) to support organisations wishing to promote CCM automation.

Link: https://cloudsecurityalliance.org/artifacts/ccm-machine-readable-bundle-json-yaml-oscal/

Google Palm2

PaLM 2 is the new version of Google's language model. This is the model that Google Bard will use from now on, and if Google claimed that PaLM was three times superior to GPT-3, it is to be expected that this new version will be able to compete directly with GPT-4.

Link: https://www.adslzone.net/noticias/seguridad/adios-malware-unidad-ssd-ia-evita-infecciones-ransomware/




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