NTT DATA

March 2025

Radar 100

cybersecurity numbers

A journey through time

Editorial by Maria Pilar Torres Bruna

Since December 2016, our magazine has been and continues to be a place to reflect on knowledge and ponder cybersecurity. Today, as we celebrate our 100th edition, we find ourselves at a significant milestone that invites reflection: what have we learned over these years, and how have the threats that concern us so much changed?

When we began this journey back in 2016, cyber threats were, for many, something distant, almost unrelated to the daily lives of businesses and common users.

There were organisations that did not have formalised cybersecurity policies, and security breaches were perceived as isolated incidents or exclusive to large tech companies. However, in 100 editions and 8 years of continuous work, we have witnessed a fascinating evolution.

The evolution of threats: From malware to sophisticated cyberattacks

Looking back, we can see how cyber threats have evolved from simple malware or virus attacks, like those that flooded the early issues of our magazine, to impressively sophisticated cyberattacks.

Today, threats include ransomware, advanced phishing, targeted zero-day attacks, and supply chain vulnerability exploitation, among others. However, what is most surprising when observing this evolution is that, at their core, the motivations and goals of attackers remain similar to those of 8 years ago: stealing sensitive data, disrupting operations, and, above all, exploiting human vulnerabilities.

The real change: How we receive threats

What has changed radically is the way we face these threats. In 2006, cyberattacks primarily arrived via email or malware downloaded from compromised websites.

Today, attack vectors are much more complex and diversified through social networks, mobile devices, the Internet of Things (IoT), and collaboration platforms.

Attackers are now everywhere: from online gaming platforms to corporate messaging systems. Phishing, for example, has evolved from simple deceptive emails to highly personalised (spear phishing) attacks targeting key individuals within an organisation.

Moreover, cybercrime has ceased to be a matter of "lone cybercriminals" and has become a highly organised and global industry.

Cyber mafias operate with a business structure, and ransomware attacks have gone from isolated incidents to large-scale extortion events, where victims not only suffer data loss but also face the pressure of paying large sums of money to avoid public exposure or prolonged service interruptions.

Are these threats still the same?

It is interesting to note that, although the tools and techniques used by attackers have advanced, many of the threats remain the same. Phishing, for example, continues to be one of the most effective attack methods, and human vulnerabilities remain the main issue. This reminds us that, beyond advanced technologies, user awareness and training remain one of the cornerstones of our defence.

Today's cyberattacks, while more complex and varied, feed on the same human errors: clicking on a malicious link, using weak passwords, or trusting too much in a public Wi-Fi network. Social engineering remains the attackers' favourite weapon, and increasingly, attackers understand that exploiting human trust is the most effective way to infiltrate corporate networks.

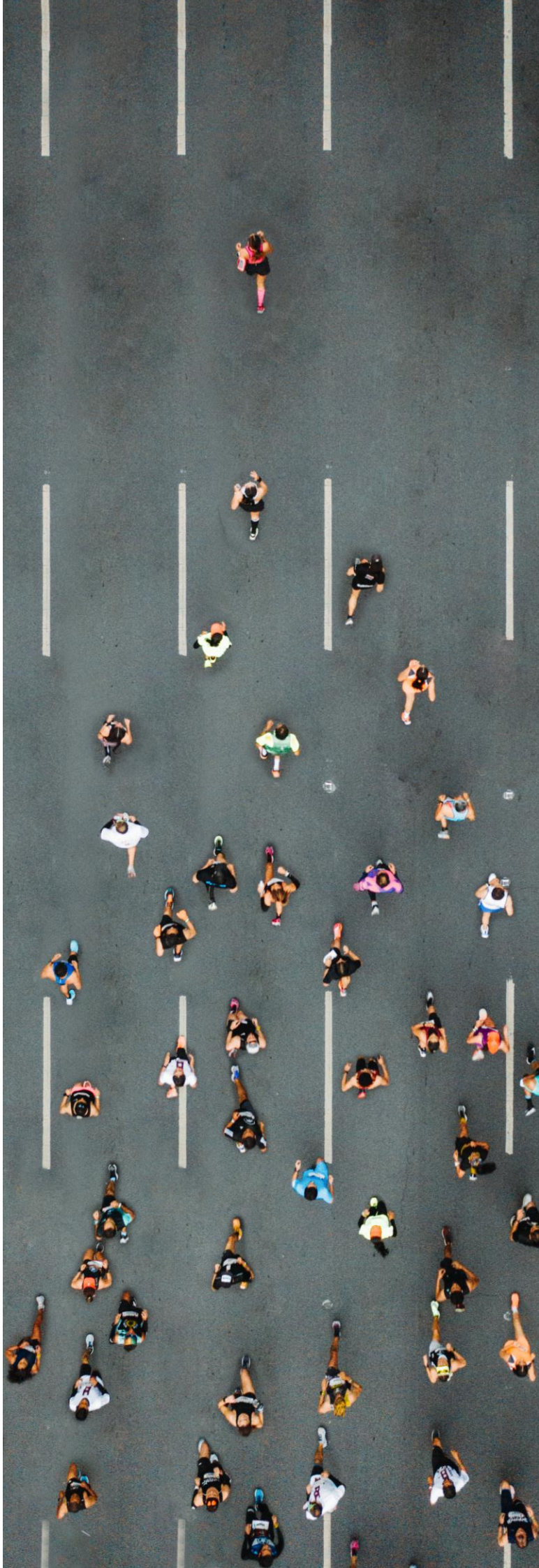
Looking to the future

Looking to the future, one of the big questions is how we should adapt to a landscape that, far from stabilising, seems to become more dynamic and challenging every day. AI-based attacks, deepfakes, voice cloning, massive data breaches, and threats related to quantum computing are beginning to emerge as new challenges on the horizon.

However, despite the growing sophistication of attackers, we must remember that threats are not unbeatable. The evolution of defence strategies, from Zero Trust to the integration of AI for threat detection and automated responses, promises to be the key to effectively facing them.

In short, as we reach our 100th edition, we celebrate the journey so far, but above all, we prepare for the challenges to come. Threats change, but what does not change is our mission to protect what matters most: our data, our infrastructures, and, above all, people.

Thank you for joining us on this journey. The future of cybersecurity is full of challenges, but together, we will continue to evolve, learn, and protect.



When the health sector becomes a patient

Cyber-chronicles by Héctor Palencia Sánchez

We begin our cyber chronicle by highlighting the recent cyberattack suffered by Ascension Health, one of the largest healthcare organisations in the United States.

On December 27, 2024, it was reported that data from 5.6 million patients was compromised, including sensitive health information. The incident originated when an employee inadvertently downloaded malware, allowing attackers to access internal systems and steal confidential data.

As a containment measure, Ascension diverted emergency care in some of its hospitals, temporarily affecting services to patients. This incident underscores the importance of ongoing staff training in cybersecurity protocols to prevent human errors that could lead to security breaches.

In the financial sector, the Japanese manufacturer Wacom, known for its graphic tablets, was the victim of a cyberattack on its online store. On January 8, 2025, customer payment information was compromised for those who made purchases during that period.

The company is investigating the incident and has contacted potentially affected customers, recommending that they review their bank statements, change passwords, and remain alert for possible phishing scams.

In the telecommunications sector, Telefónica suffered a cyberattack on January 9, 2025, in which a group of hackers extracted 2.3 GB of data from the company's internal incident management system.

Although some customer-related documents were affected, the company confirmed that residential customer data was not compromised. The attackers published the database on a forum, prompting Telefónica to take measures to block unauthorised access and reset compromised passwords.

In the government sector, a data breach affecting the Civil Guard and the Armed Forces of Spain was reported in January 2025. Emails and data of approximately 180,000 members of these institutions were leaked and put up for sale on a cybercrime portal, including nearly 20,000 personal email addresses.

Although the information theft likely occurred a year earlier, the incident recently came to light, raising concerns about data security in government entities.

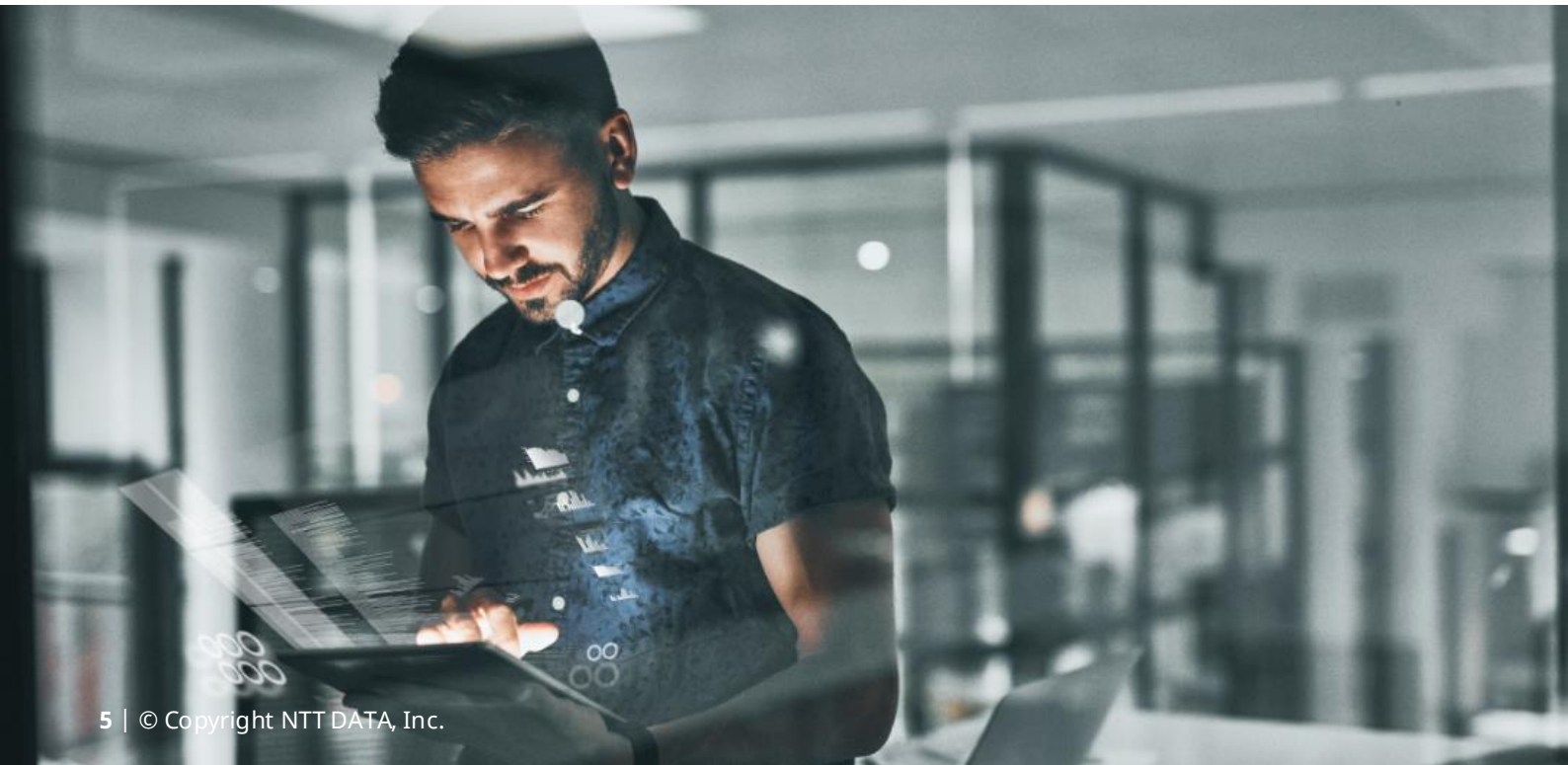
In the education sector, the Texas Tech University System reported on December 23, 2024, a data leak that compromised personal information of students and employees.

While specific details about the extent of the incident have not been disclosed, the university is working with cybersecurity experts to investigate and mitigate the impact.

In summary, three key conclusions can be drawn from the cybersecurity incidents analysed:

1. **Increase in ransomware attacks and data breaches:** Organisations from various sectors, such as healthcare, finance, and energy, have fallen victim to attacks that compromise sensitive information and affect the continuity of their operations. This increase in the frequency and sophistication of attacks highlights the need to strengthen security measures.
2. **Importance of training and awareness staff:** Several incidents originated from human errors, such as the inadvertent downloading of malware or the disclosure of credentials. Ongoing training in cybersecurity protocols and the promotion of a security culture are essential to mitigate these risks.
3. **The need for a quick and effective incident response:** the ability to efficiently detect, contain and mitigate cyber threats is crucial to minimising the impact of attacks. Implementing incident response plans and conducting regular drills can significantly improve organisational resilience.

These points underline the importance of a comprehensive cybersecurity strategy that covers both prevention and effective response to incidents.



2025, the International Year of Quantum

Quantum Space by María Gutiérrez

UNESCO has established 2025 as the International Year of Quantum Science and Technology, with this initiative it aims to "*increase public awareness of the importance of quantum science and its applications, as well as to raise awareness in society about the impact of this research on our daily lives and on the future of the planet*" in addition to celebrating and recognising the 100th anniversary of the first theoretical developments in quantum mechanics.

Although today we can already enjoy some applications of quantum technology (lasers, fiber optics, atomic clocks, microwaves, digital television, computers, etc.), what is coming is truly revolutionary, with an impact on sectors such as medicine, climate, energy, food security or water. This will allow us to have more powerful computers, more secure communications, materials with better properties or more accurate measurements, as well as possible explanations for many biological and physical phenomena.

It is true that this hardware is not yet fully available, but the market is already focusing its efforts on the development of the most diverse algorithms: optimisation algorithms, hybrid algorithms and quantum-inspired algorithms.

Companies are also preparing for the quantum transition by identifying cryptography that is not quantum-resistant, so it is crucial to start building capacity, training staff, and raising awareness about integrating quantum computing into our systems.

NTT DATA has a Quantum team focused on preparing clients for the quantum future, with services related to the post-quantum algorithms transition, advances in genomics, financial portfolio optimisation, logistics or cybersecurity. They are aligning technology with strategy for seamless adoption and competitive advantage, and doing so around these elements:

Hybrid Computing

The integration of quantum and classical computing makes it possible to subsequently emulate principles or behaviours of quantum physics. In doing so, you address current constraints while preparing for the full potential of quantum.

Methodology based on case studies

Our methodology consists in using technology knowledge to adapt it to our customers' needs and create valuable use cases.

Connection creation

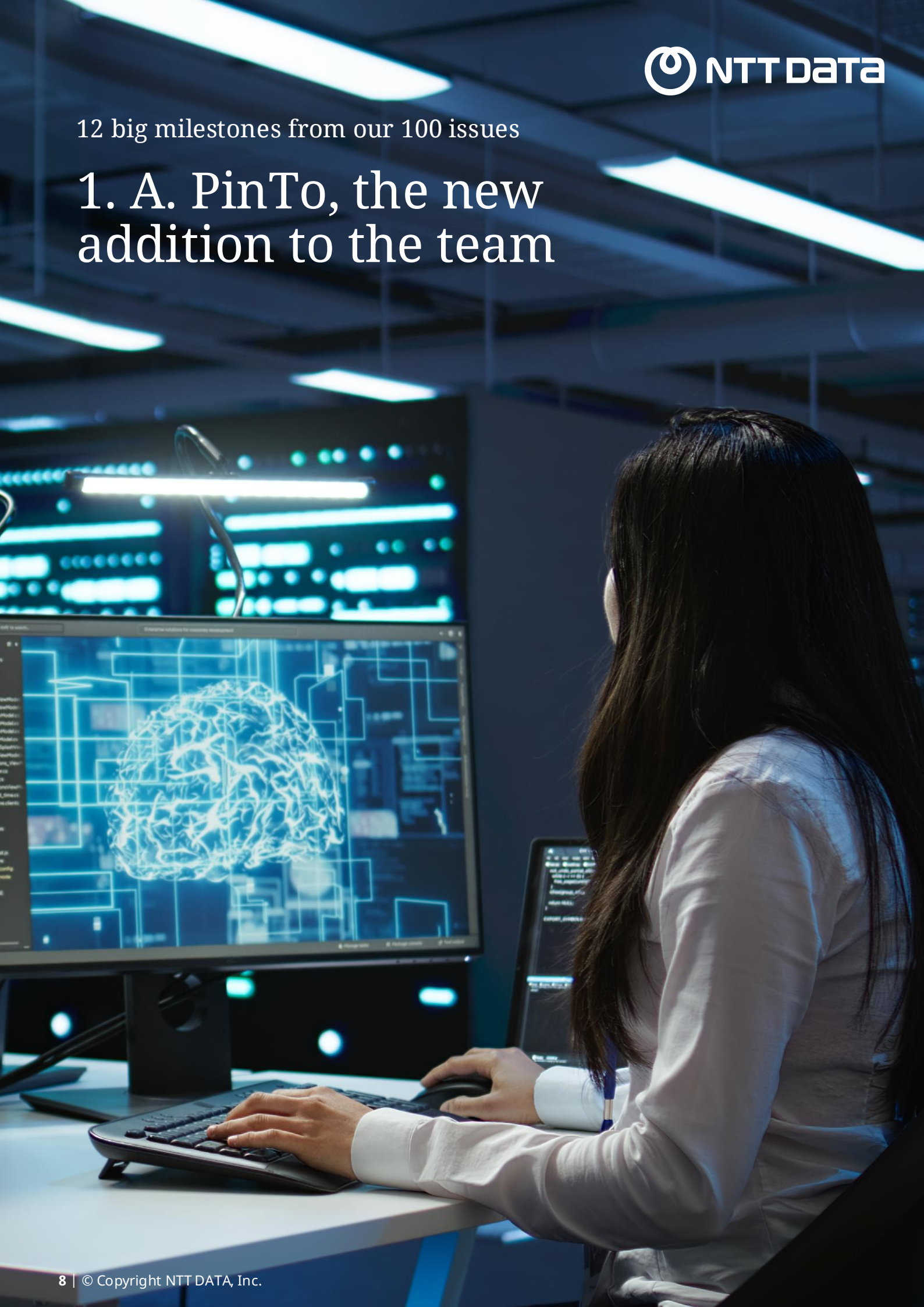
We create a network of contacts to ease cooperation, research and technology development, partnering with universities, manufacturers, and providers working in the field of quantum computing.

months,, quantum computing is barely taking its first steps, but it is evolving rapidly, with significant advances in hardware, algorithms, and applications. Organisations that work and explore to understand and leverage quantum computing at this early stage will gain a competitive advantage in their respective fields.

Over the next few months, we will tell you about the quantum initiatives and projects we are working on right now.

12 big milestones from our 100 issues

1. A. PinTo, the new addition to the team



 © Copyright NTT DATA, Inc.

Article May 2017

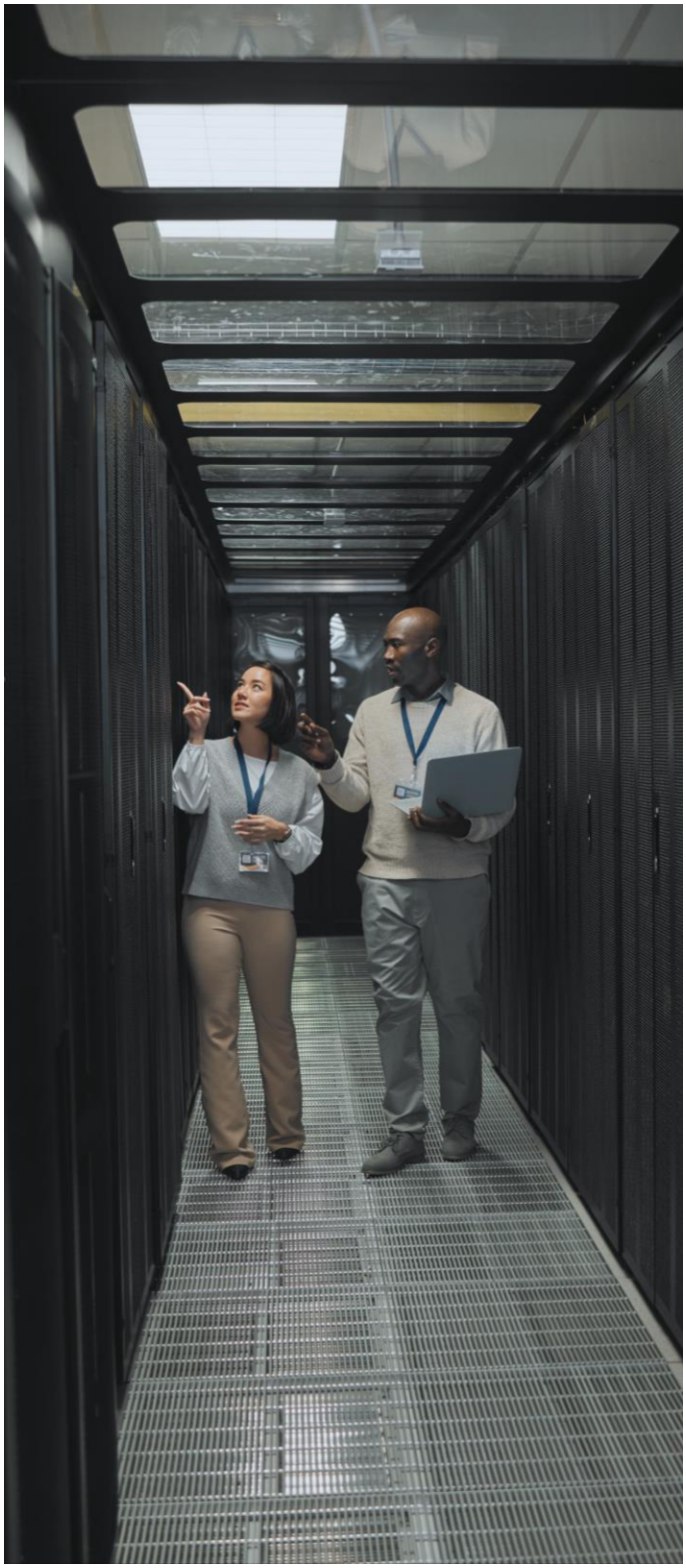
One of the most worrisome cyberthreats is what is known as APT (Advanced Persistent Threat). We can define it as the set of continuous actions and processes that, in a stealthy way, serve to carry out malicious activities. APTs are highly targeted threats that seek to illicitly obtain sensitive information, data of commercial value, financial data, etc. As the name suggests, they make use of the most advanced techniques and types of attacks to infiltrate a system and maintain access for long periods of time (weeks, months, or even years). The goal is to extract as much information as possible.

Due to its characteristics and the persistence of the intrusion, an APT could even be considered the worst hire a company can make.

What are they after?

This type of attack is usually focused on obtaining a considerable profit, usually causing significant damage to the victim. The most common reasons are usually:

- **Economic motivation:** The aim is to achieve an economic benefit through the theft of bank details, the falsification of invoices, blackmail, the sale of information, etc.
- **Information theft:** extraction of private or commercial information, about current and future projects, etc.
- **Unfair competition:** obtaining of information on business strategy, research of activities and new developments, system sabotage, etc. The aim is to achieve a competitive advantage either by getting ahead of the victim company or by harming it.
- **Reputational damage:** oftentimes the objective is to damage the reputation of a company, leaking internal information, compromising systems, etc.



 © Copyright NTT DATA, Inc.

How do they do it?

It is difficult to determine the *modus operandi*, as the main characteristic of this type of attack is that it is targeted, and therefore highly personalised. Despite this, we can group the set of techniques into a series of relatively common actions:

1. Recognition and scanning of the target

When deciding to attack a target, data collection is the first step. This search is carried out progressively, starting with techniques where there is no contact with the victim, using data from OSINT sources to collect relevant news, contacts, personal data, etc.

The target is passively researched for strategic information that can be used to make the attack effective. This includes the collection of usernames, email addresses or websites.

Once this initial passive reconnaissance has been completed, an investigation of the external infrastructure is carried out to discover potential entry points that can be exploited to gain initial access.

These actions are usually active, have a direct effect and can be detected. It includes actions such as port and IP scanning, identification of REST/API services, detection of vulnerabilities, etc.

Attackers will complete the organisation's map using scanning techniques where the victim is already touched, which may raise the first suspicions.

2. Gaining access / Initial intrusion

The previous phase will provide the attackers with the information they need to gain initial access. Now the goal is to infiltrate the network and establish an entry point into the systems from which to expand. To achieve this, attacks are executed against the vulnerabilities found by means of exploits, code injections or even social engineering actions against employees' emails.

At this point, it is easier to detect this type of threat, as it is usually acting from outside the network infrastructure.

3. Entry point establishment

Once access to the network and systems has been gained, the next critical step is to establish a stable entry point, known as a foothold or beachhead. In this way, the attacker can continue his intrusion into the network, looking for ways to advance until he reaches his target.

From this point, a connection is established to the attacker's command & control centre, normally used exclusively for each APT, so that the chances of detection are reduced.

4. Lateral movement

This is the longest phase of the attack, which can extend over several months or even years. The attacker has already gained access to the company's network/infrastructure and seeks further access to achieve his goal. Several actions are performed at this stage:

- **Persistence:** The first step, and fundamental point for the attacker, is persistence: to ensure his presence within the network. For this, it is common to use custom-designed malware to go unnoticed and maintain access.
- **Internal recognition:** Once the previous action is secured, we proceed to investigate new accesses, selecting the next jumps in the network that will be carried out to increase the range of action of the attackers.
- **Escalation of privileges:** After strengthening his position, the intruder continues the analysis by escalating privileges and stealing credentials in order to expand access to new systems within the network.

These three steps are repeated throughout the intrusion, allowing to achieve and advance towards the objective, whether it is extracting information, compromising systems, or any other.

5. Data extraction and fingerprint erasure

Finally, once the target information is accessed, it is extracted, thus completing the attack.

Then, the intruder usually erases the traces that he may have left, thus making it difficult to determine how he gained access to the information once his actions were discovered.

Another very common action, along with fingerprint erasure, is the installation of a common malware to distract IT teams and complicate the detection of the real attack.

Malware on demand

A business that has proliferated considerably in recent years, and that is provided mostly through developers that are offered on the Deep Web, is the generation of on-demand malware, custom-designed against a particular target.

In total, it is estimated that this type of activities, driven especially by ransomware, moved more than 1,000 million dollars (918.3 million euros) in 2016, according to Trend Micro's Annual Security Report.

These services are complemented by more traditional ones, such as DDoS, also on demand and for agreed periods of time, or the rental of zombie equipment from a botnet for use in various attacks such as massive malware distribution, bitcoin mining or key cracking.

Recommendations

As it has been observed, APTs are sophisticated cyber threats, of complex execution and usually have a great impact on the organisations that suffer from them. Although these attacks are usually very elaborate, they are not invisible and can be detected.

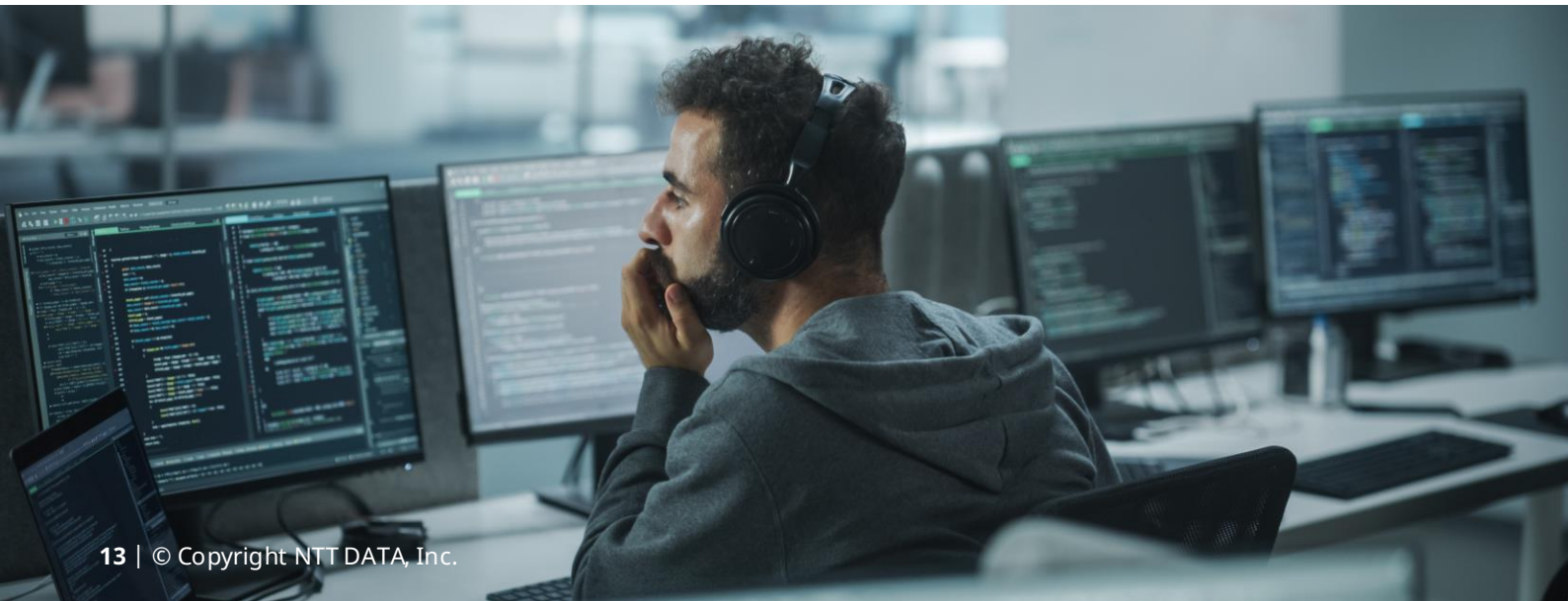
From a technical point of view, the control over the organisation's network and over incoming and outgoing connections acquires a special importance in the prevention of APTs. Are of particular interest in this context:

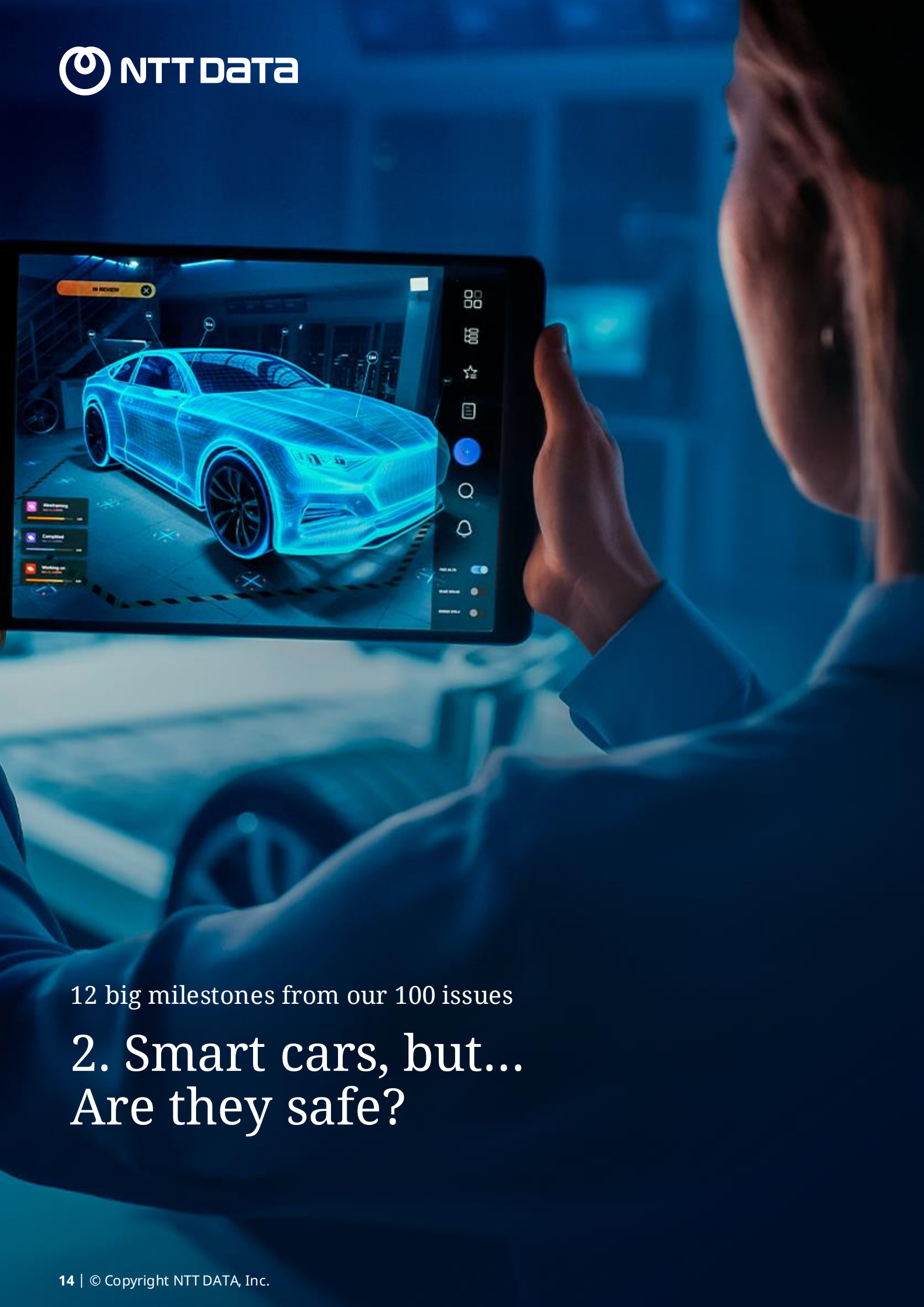
- The monitoring of network elements.
- The software update policies.
- The implementation of SIEM/IDS solutions to detect invalid logins, uncontrolled accesses, etc.

On the other hand, many times the weakest links in the security chain, and through which companies' networks are sometimes accessed, are the employees themselves, who are usually poorly prepared and aware of these issues.

Therefore, every organisation should promote preventive measures:

- Development of employee awareness campaigns to prevent the theft of credentials, infections, etc.
- Training about cybersecurity best practices.
- Creation of an incident response and employee care team.





12 big milestones from our 100 issues

2. Smart cars, but… Are they safe?

 © Copyright NTT DATA, Inc.

Article August 2017

New car models are increasingly becoming a simple showcase of technology and connectivity. While the driver experience has improved dramatically in recent years as a result, both the increasing reliance on computers and the entry of the Internet into our vehicles introduce new risks that the industry must address.

We live in an increasingly interconnected world, and proof of this is the advancement in the use of technology that the automotive sector has been experiencing in recent years. For example, it is already unusual to find cars that have a CD player and, instead, the presence of USB ports is more common through which it is possible to connect any device to the onboard computer and interact with it, install new applications, etc.

Other features presented by the new car models are the synchronisation with smartphones, the opening of doors via Bluetooth, the possibility of driving and parking autonomously or using them as a Wi-Fi access point.

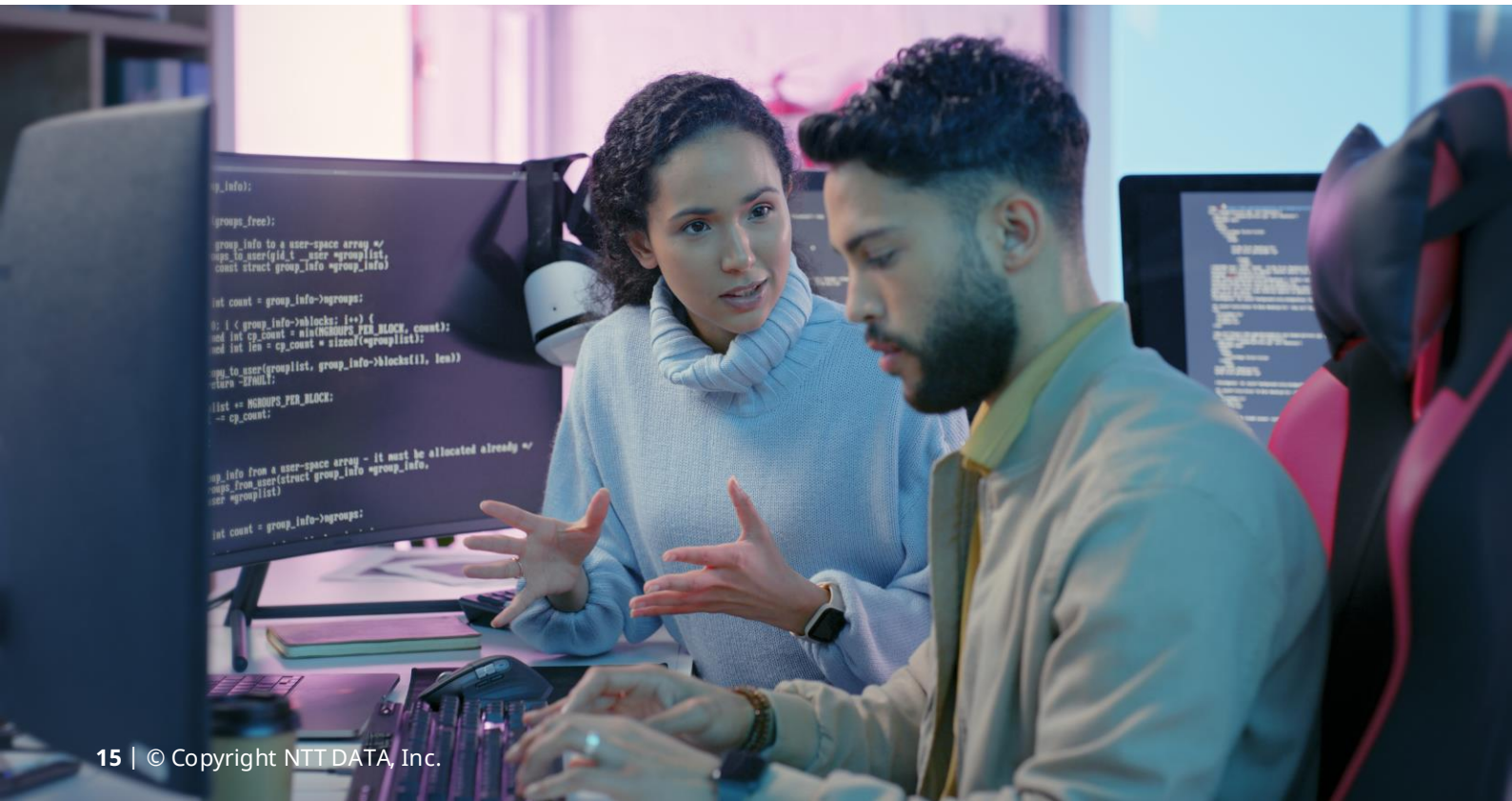
All this represents a significant improvement for the usability and convenience of users, but what risks does it entail?

Risks and threats

One of the factors to take into account is that the communication protocols used in vehicles were designed years ago with security requirements that are currently outdated.

An example is the CAN protocol (Controller Area Networking, for its acronym in English), developed in the 80s with bus topology and which is characterised by being able to transport frames of up to 64kb of data.

These frames include the priority identifier of the transported message, responsible for establishing the order of execution of the vehicle's actions.



 © Copyright NTT DATA, Inc.

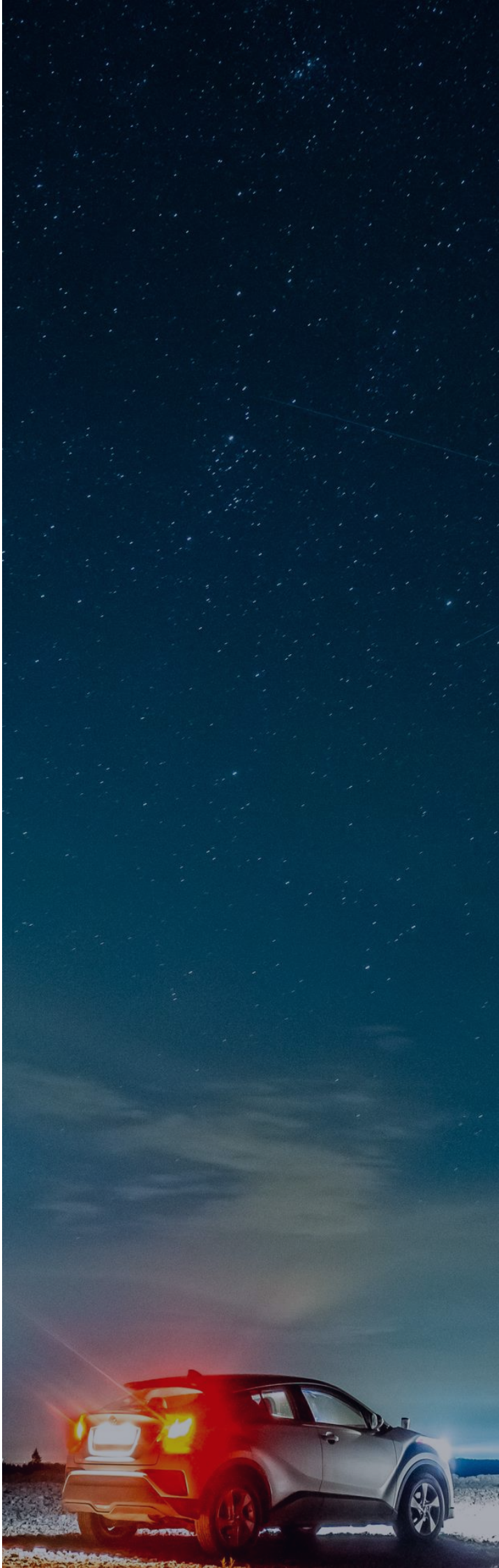
Among other things, the CAN protocol makes it possible to control the engine and interconnect the ECUs (Electrical Control Units), the central locking, the sunroof opening, the lights, the climate control or the control panel. Due to its topology, any device that connects to the bus will be able to send messages to the rest of the modules and have them listen to it.

It should be noted that this exchange of messages is not encrypted, so it is susceptible to being intercepted and manipulated, being able to cause a denial of service (DoS) in compromised vehicles.

Since this protocol is implemented in most car models, an attacker could use a microcontroller to inject frames through the OBD-II connector (*On Board Diagnostic*) and remotely modify the behaviour of the lights, warning lights or any other module of the vehicle, as demonstrated by Sheila Berta and Claudio Caracciolo at the 2016 Ekoparty conference. In addition, since the location of this connector is usually not known, it is more complicated for a driver to determine if he is being victimised by an attack or if it is a real vehicle failure.

Therefore, depending on the number of modules connected to the CAN bus that can be breached by an attacker and the functions they perform, the criticality of the attack will be more or less high.

For example, if the control panel is compromised, it could be modified and indicate that the engine has overheated or that it is missing oil, and thus have to stop the car.



The connectivity of the devices

Continuing with the issue of physical access, it should be noted that actions such as connecting a USB device, synchronising our smartphone or tablet to be able to interact with the vehicle, or customising it with hacking tools such as MZD-AIO-TI (MDZ All In One Tweaks Installer, an all-in-one that allows installing new applications to alter the Mazda factory software), carry risks: if the device we connect is infected with malware or contains malicious code, it is possible that the car may be compromised.

Jay Turla demonstrated it in a PoC (Proof of Concept), by connecting to a Mazda3 a USB stick containing a series of scripts that he executed remotely and whose result was displayed on the car's dashboard screen.

Being a PoC, the code only returned the type and version of the installed operating system, but it could be more critical orders that alter the operation of the vehicle or could pose a risk to public safety.

It has recently become known that the wave of attacks caused by the WannaCry ransomware has also affected the automotive sector.

Some Renault and Nissan plants in Japan, the United Kingdom, France, Romania and India had to stop production due to having their network compromised and fearing the possibility of products being infected. What could happen if such ransomware was running in a car?

It would be something similar to what happens in other computer equipment, the entire system would be encrypted, and it would ask for a ransom to be able to unlock it and resume driving.

To this day there have been no real cases of this and all the information about it is theoretical. However, due to the constant evolution of IoT and interconnectivity, it is not unreasonable to think that it could occur at any time.

On the other hand, as the Internet connection is spreading in this sector, other ways of attack appear other than the physical connection using microprocessors.

From the point of view of information security, equipping cars with systems that are increasingly less dependent on the human factor and delegating such delicate actions as controlling driving or the safety distance to them requires ensuring that they are properly secured.

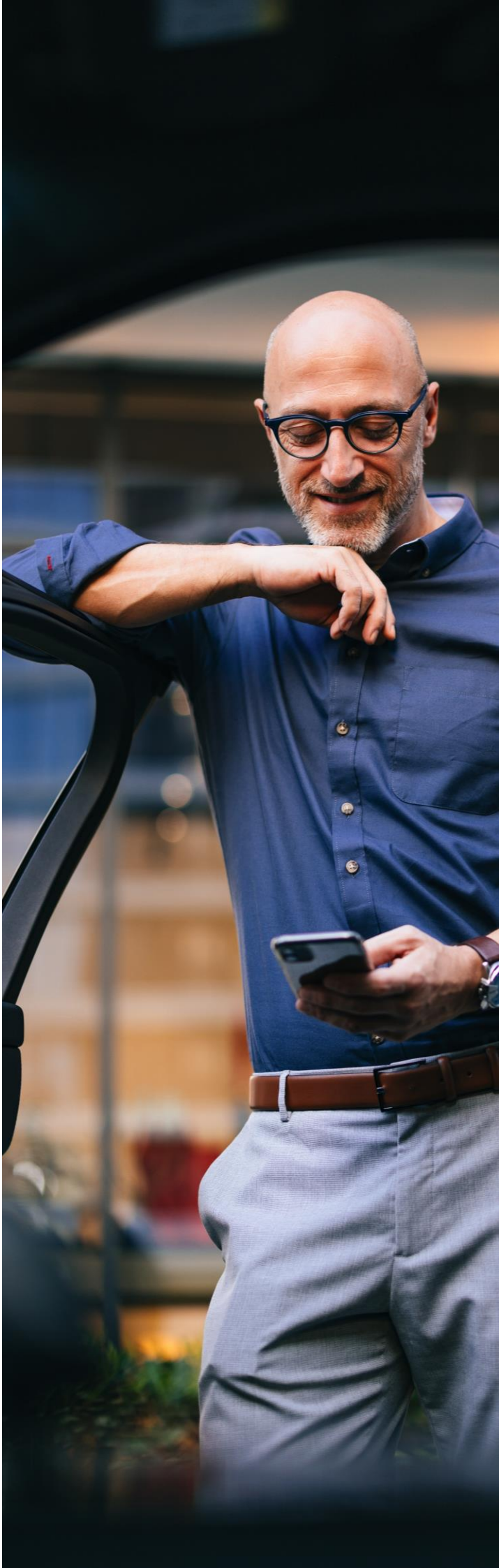
If not, a malicious user can take advantage of existing security breaches and take control of the vehicle remotely, even endangering the lives of its occupants.

Precisely this has been one of the main topics in several editions of Black Hat and DEF CON, the two most important cybersecurity conferences in the hacking world, in which Chris Valasek and Charlie Miller have presented their research in this area. Among their most famous contributions, it stands out that, in 2015, they were able to remotely control a Jeep Cherokee taking advantage of only that its multimedia system was exposed on the Internet.

Thanks to this, it was possible to hack it from any geographical location (in this case from the sofa at home) to gain control of the air conditioning system, the audio, the windshield wipers or even to lock the pedals and turn off the engine.

This vulnerability has already been corrected by the firm and according to the latest study by these researchers, published in 2016, it was necessary to have the laptop connected to the car's computer system to carry out the attack.

Another topic of interest are smartphones and mobile applications distributed by car brands to communicate with the vehicle and control it. Last year Troy Hunt demonstrated how it was possible to access a Nissan LEAF through the brand's mobile application, which allowed to act on the air conditioning system or collect information stored on the on-board computer about recent trips, consumption or state of charge.



To carry out this attack, it was enough to use an intermediate proxy that captured the requests that the mobile application sent to the server, in which the VIN (Vehicle Identification Number or VIN number) could be easily identified within the URL. This, added to the fact that it is very simple to know this number, implies that it was possible to get hold of any Nissan LEAF remotely.

In addition, Hunt proved that a brute-force attack could be carried out anonymously to list the VIN numbers of different cars of that brand and obtain data or remotely control those that successfully responded to the request. The application did not verify the user's identity or record session information.

Finally, we cannot forget about the weakest link in the chain: the human being. A few months ago, two hackers used social engineering techniques to trick a user who was waiting while refuelling at a Tesla gas station.

The bait was to offer free Wi-Fi and a free hamburger if a mobile app was downloaded. What the user did not know is that this application contained malware that, once installed, stole and sent the attackers their data, including the credentials that would allow them to access and start the vehicle.

For all this it is necessary to become aware of how important it is both the constant updating of the vehicle software and the incorporation of cybersecurity at the beginning of the life cycle and development of any product that contains electronic or computer components.

The best way to prevent security incidents is by applying the necessary measures at the time of creating and making use of the technology.

12 big milestones from our 100 issues

3. Machine Learning: teaching cybersecurity to our machines

 © Copyright NTT DATA, Inc.

Article April 2018

Technology is moving fast and, with it, the desire to have the knowledge and the ability to get ahead of users. Every day we use and are used by this technology that allows us to predict what the user wants through the statistical analysis of huge amounts of data such as locations, Internet searches or friend relationships. In this article we are going to talk about machine learning and how it can be applied to cybersecurity.

A simple example of machine learning can be found on most sales portals. When we are browsing products, the page itself is responsible for recommending others that might interest us and, generally, they match our tastes. These sites make use of machine learning to suggest items that the potential buyer may want to purchase and does so based on the data obtained from other users who are looking for the same thing. However, could this technology be applied to cybersecurity?

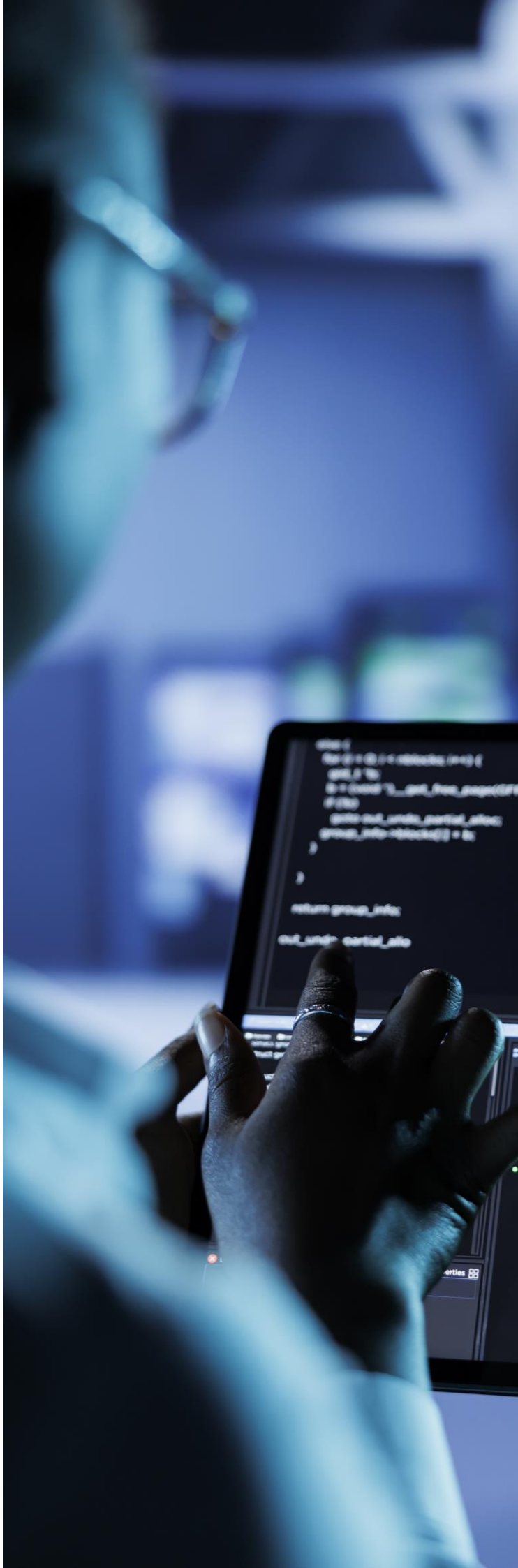
Before getting into the subject, it is necessary to define in more detail what machine learning consists of. As the name suggests, this technology tries to teach a machine to make decisions by itself using artificial intelligence. This means that the developer does not have to manually program what the machine has to do, but she is in charge of choosing what is right, being able to solve problems for which a static algorithm could not find a solution.

Let us say, for instance, we want our machine to learn how to distinguish traffic signs, more specifically a stop sign and a forbidden one. To do this, we are going to give you 20 different images of stops. If the machine returns that 17 of those images are stops and 3 of them are prohibited, we could say that it has an 85% success rate. But we need that percentage to increase, so this time we are going to pass 1,000 images, 10,000 or all the ones that are on Google Maps. In this way, as he receives more information, he improves his ability to detect each of the traffic signs that are provided.

We could divide machine learning into three groups according to how it works:

- **Supervised learning:** it uses information from tagged datasets for its training. Thus, by analysing data and learning to differentiate them, it is able to predict the label of a new unlabelled data. Therefore, this type of algorithms are used to classify and categorise.
- **Unsupervised learning:** unlike the previous one, the algorithm does not have labels in the data to orient itself, but it is itself that categorises the data based on the patterns it finds.
- **Reinforcement learning:** this technique is based on rewarding the algorithm when it gets its prediction right and punishing it when it fails. In this way, he learns by trial-and-error techniques to perform his task better. It is the most promising technique because it does not need large amounts of data to train the algorithm. It is currently being applied in autonomous driving systems.

Currently we have huge amounts of data, what we call big data, so we could use techniques of machine learning in any area of knowledge that we can think of.

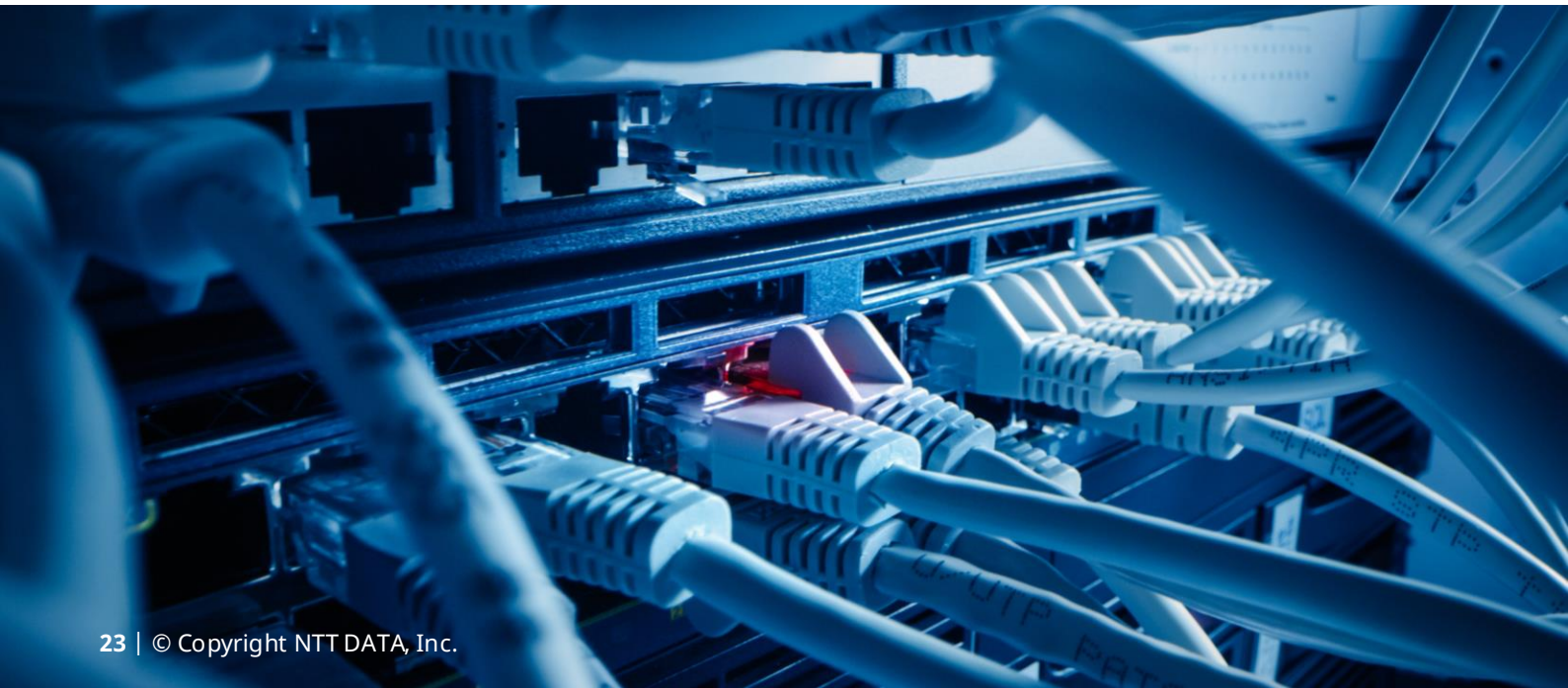


Applications in cybersecurity

Machine learning is being applied in various scientific areas due to its adaptability, scalability and ability to quickly adjust to unknown challenges. Using the machine learning as a support method for cybersecurity, it is possible to make the machine able to predict when it is going to be attacked and decide how it can defend itself, preventing different attacks and analysing the patterns and tools that criminals use. Machine learning is being used in cybersecurity, especially for:

- **Phishing and spam detection:** by analysing the patterns of sending email accounts, message structures and their content, the algorithm is able to learn what phishing or spam can be and isolate the messages from the user's mailbox, even blocking the sending addresses becoming possible.
- **Intrusion detection system (IDS):** the IDS monitors the network for suspicious activity. Traditional systems are based on rules and a series of expected behaviours on the Internet. Sophisticated attacks can easily bypass these defensive measures because they use unexpected new patterns. Machine learning is being applied to analyse millions of attacks and intrusion attempts so that the system on its own evaluates whether it is being attacked or not and tries to mitigate or completely block the problem.
- **Malware analysis:** it is used as a support to the forensic analyst when collecting information from the attacked system, facilitating the labelling of logs, organising the tests of modified files and analysing which code may be harmful.

However, it should be borne in mind that, in the same way that machine learning is being applied in attack mitigation, it is also being used by attackers to devise more sophisticated malware that is able to dodge the defensive measures of the target system on its own.

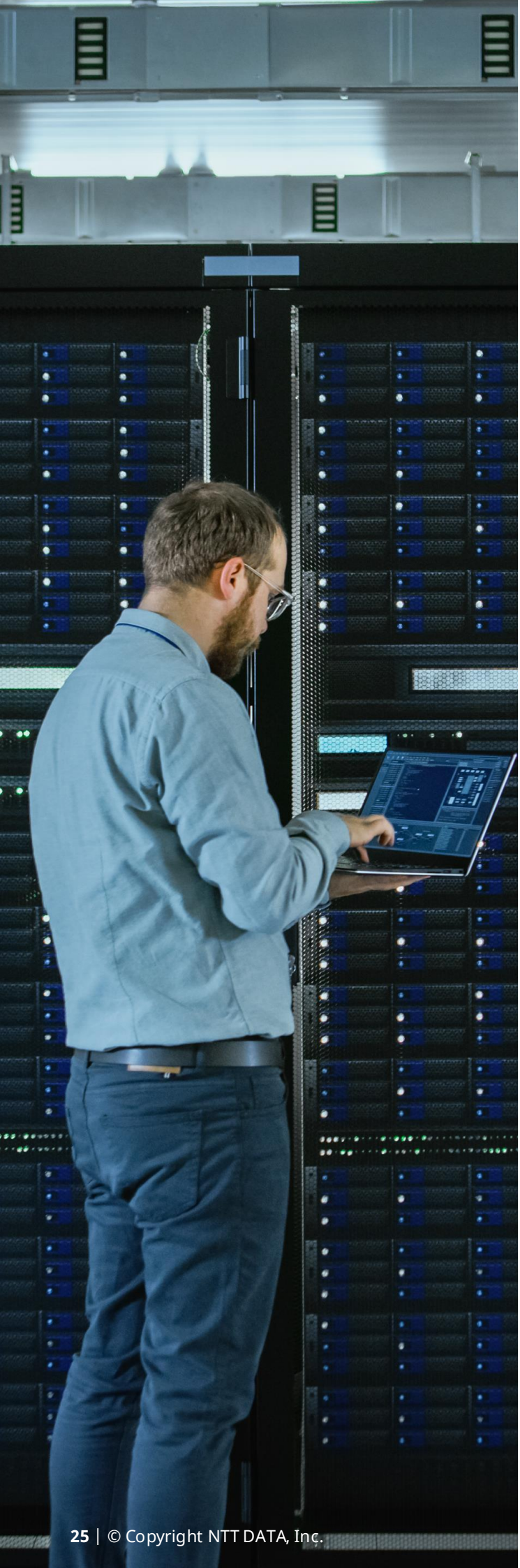


Applications in other areas

At present, machine learning is being used by many companies that need to deal with huge amounts of data to offer their users a more satisfying and personalised experience. The giants of technology and information have been improving for several years and betting on the machine learning, among these companies we can find a:

- **Amazon:** one of the largest sales portals in the world also owns one of most developed machine learning and artificial intelligence platforms. While we are shopping and browsing your website, you are suggesting items that we would be interested in purchasing based on the purchases and search patterns of other users. Amazon also applies this technology in its web services, AWS, and in its artificial intelligence, Alexa.
- **Google:** the search engine par excellence is one of the pioneers in the use of artificial intelligence and also one of those that use it the most. He uses his algorithms of machine learning in almost all its services to offer the user the results he is looking for (Google. com, YouTube, Google Now), the advertising that interests you (AdSense), the translation that most resembles natural language (Google Translate) or the self-management of the emails you receive (Gmail).
- **Salesforce:** it is the American company of cloud computing and big data with the greatest value in the world. They are the creators of Einstein, an artificial intelligence implemented in their cloud services, sales, marketing and applications, designed to improve many of their products with algorithms of machine learning.

These are just a couple of examples, but many other large companies such as Facebook, Tesla, Netflix, Microsoft, Apple, Intel, IBM or Alibaba are also using this technology.



Disadvantages to consider

As a counterpoint to all the above, we have to warn that not everything in the world of machine learning is favourable, because this technology has its disadvantages

This is an expensive technology, which requires a lot of computational resources. Generally, the most used computing is based on the cloud since it has the ability to adapt to our needs at any time, but the rentals of these large machines are not cheap. For this technology to be developed, it needs an immense number of samples and useful data so that the algorithm learns and can reduce its margin of error, offering fewer false positives and increasing the reliability of the system.

The machine learning it is yet another tool. It is important to know when and how to use a particular algorithm. There are simpler algorithms and more complex ones, and we will have to choose based on our specifications.

Conclusion

Machine learning is a booming area of knowledge and continuous expansion for a few years now. Large technological companies are applying it in their services and continuously improving it, since it has a flexibility that other static methods cannot offer.

It presents a promising future in the area of cybersecurity, since the ability to get ahead of the attacker is fundamental so that protected systems end up being compromised. But it is not a solution for everything, but one more tool for the analyst in his task to keep the systems safe.

12 big milestones from our 100 issues

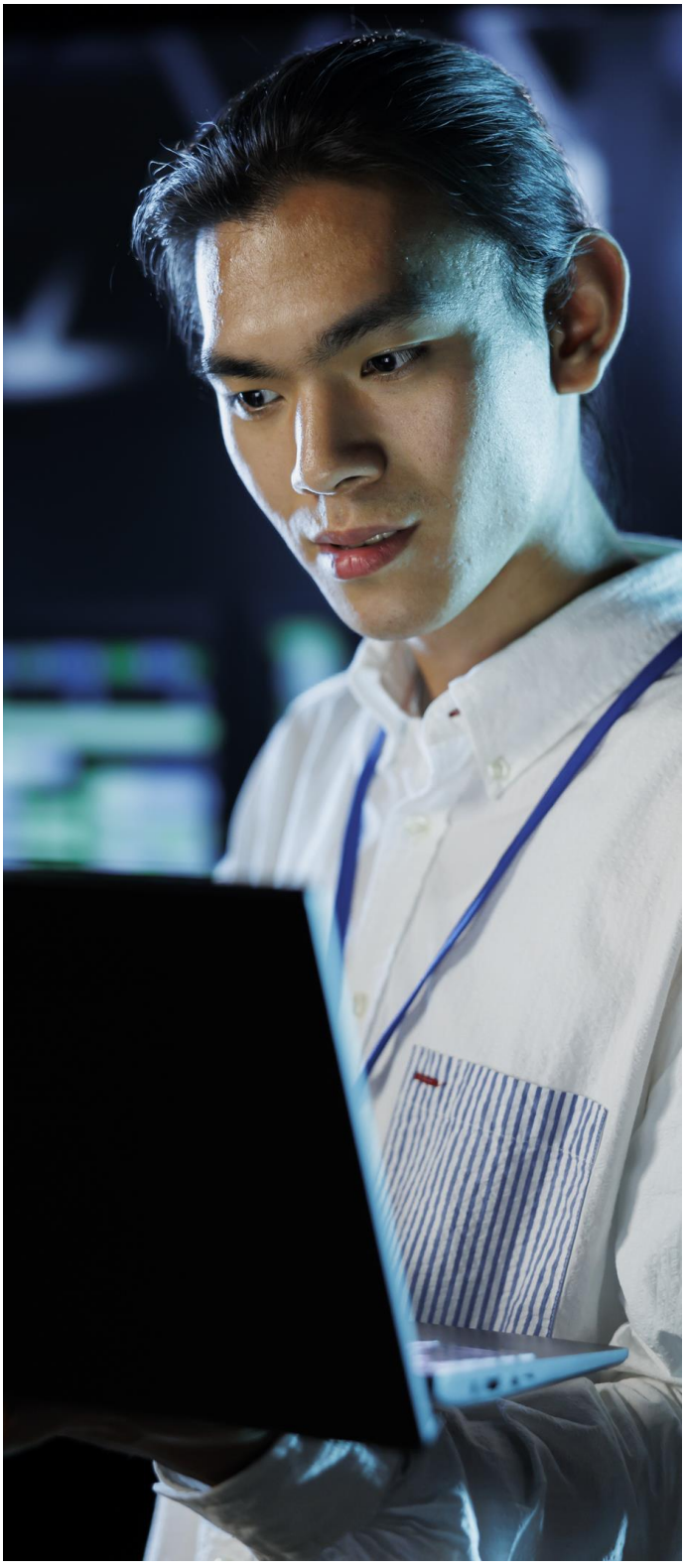
4. When you connect to the Internet, the Internet connects to you

 © Copyright NTT DATA, Inc.

Article April 2018

Perhaps the title sounds obvious, but this concept entails consequences that are worth paying attention to. Everyone understands the concept of the Internet and the opportunities offered by the interconnection of systems throughout the planet: a world at your fingertips. However, not so much attention is paid to the fact that the connection flows both ways, with what that entails. In this article we are going to see the different problems that being connected to the network can cause.

When we connect something to this large network to provide certain functionalities or services remotely, we have to be aware of the implications that this has and what things can be visible from the outside. When a device accesses the Internet through the router that gives us access, it is exposed to everything that happens on the network.



The bots

Not everything that moves around the Internet is the activity of physical people, much of it comes from robots (bots). If we analysed everything that reaches the router that gives us Internet access, we would see that there is a lot of activity from them. When it is opened to give Internet access to a device, in turn these bots will also try to connect to the device.

Among the bots, there are some that are innocuous (for example, those of search engines like Google, which index the Internet so that websites appear in our searches), and there are others with darker purposes. These malicious bots seek to gain access to the system in order to compromise it and have it under their control.

Once the system is compromised, the attackers behind that bot will be able to use it for an endless number of possible actions. Among them could be, for example, the mining of cryptocurrencies, the use as a reverse proxy (to carry out attacks and prevent it from being traced) or as part of a zombie computer army (for massive denial of service attacks).

Real case

A real case caused by bots was that of the zombie computer network (or botnet) called Mirai. For those who do not know her, she carried out one of the largest massive attacks known to date, which knocked out the Internet (or significantly affected) a large part of the main websites.

In this sense, he took advantage of the lack of security in Internet of Things (IoT) devices to control them.

Anything that connects to the Internet, no matter how simple it is, is exposed to these types of risks. One of the most compromised devices is IP cameras. There is such a volume of unprotected cameras that there are even websites that allow you to connect to them to see what's going on, such as: www.insecam.org.

Among the bots that do not have bad intentions are those that try to locate vulnerable devices (as the bots mentioned above do), but without that purpose of doing illegitimate activities.

For example, the aforementioned camera website only identifies and connects to those cameras. However, the objective of this type of websites is to demonstrate the problem of not taking security seriously when a device is accessible from the Internet.

Another page of this type is https://worldofvnc.net , which is based on VNC, a remote computer access system similar in functionality to the Windows remote desktop. This website tries to enter unprotected devices using this system and takes a screenshot of the screen it accesses. It has the same objective as the previous cameras page, to raise awareness about the risks of being exposed to the Internet but focusing on systems that use VNC.

They are not the only tools for that purpose. There is another one called Shodan (www.shodan.io), and known as "the Google of hackers", which analyses the different IPs by checking which ports and services are open and accessible from the Internet. This search engine allows us to know what we are exposing on the Internet in order to manage its security appropriately.

When you look at some of their results, it is worrying what you may find. There are computers, cameras, industrial control systems, refrigerators, etc. The growing trend of incorporating Internet access to more and more devices has made the vulnerable elements in that search engine grow. It seems that security on the Internet of Things is not a priority for manufacturers, and often not for their owners either.

In addition, the famous Google search engine can be used in order to detect vulnerable elements, since as we have indicated before, it indexes the Internet in order to perform searches. This technique is known as ”Google hacking" and takes advantage of certain searches to highlight the lack of protection in some element exposed to the Internet.

These search catalogues can be modified to focus the result more, being able to target specific organisations. If those tools that we have seen can find vulnerabilities in devices accessible from the Internet, malicious bots can too. Therefore, if a situation like the above is detected, the corresponding measures should be applied to prevent systems from being compromised (if they have not already been compromised).

Vulnerabilities

In the event that our vulnerable devices are located in the European Union, or have data of European citizens, the result can be much more serious. Not only will it involve the problem of one of our assets being compromised, but the corresponding fine for not complying with the new data protection regulation (GDPR) could have an even greater impact.

Apart from the Internet of Things, another type of devices that bots often find vulnerable are often components and machines in the cloud, which are used to provide services from the Internet without needing their own infrastructure, especially for small components.

However, many owners or users of these cloud computing services do not care about the security of their machines or what data is exposed to the Internet. In this case, the providers of these services provide some protection to help the machines not to be controlled by unauthorised agents. However, some of it depends on the service user, so only the measures of the provider are not enough.

In this type of elements, it is usually more frequent that there are leaks of information that is hung in those components. There have been several cases that have been in the news, such as the case of leakage of classified information from the US Army, in November 2017, through an Amazon cloud server that was not configured correctly. This shows that the elements or devices placed in the cloud have to be protected to prevent those bots from compromising or obtaining sensitive information.

Conclusion

Any element that is accessible through the Internet faces a set of risks that should not be underestimated. The important thing is to be aware that, if we connect something to the Internet, the Internet connects with that something, and with it, all the bots that patrol it. It does not matter if it is something temporary or something that we think is not important, the simple fact of being connected to the Internet is enough to keep security in mind. Everything that is accessible from the network should be checked in order to be able to rest easy and know that what connects with us will not bring unpleasant surprises.

12 big milestones from our 100 issues

5. Cybersecurity during elections: what could actually happen?

 © Copyright NTT DATA, Inc.

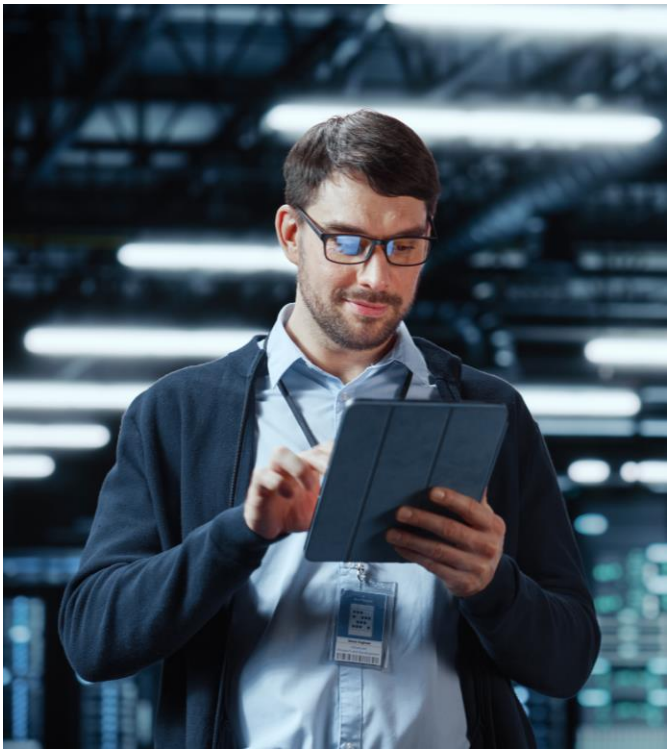
Article May 2019

To answer this question, we have to ask ourselves several questions: what can be attacked cybernetically and with what objectives, how and by whom it can be done. Finally, the most important thing we should ask ourselves is how we can protect ourselves. In this article we are going to answer these questions.

There are two reasons that have caused great uncertainty about cybersecurity in the upcoming April 2019 elections in Spain:

- There is a growing concern in society about cybersecurity in the daily use of information technologies. For example, my 12-year-old son is worried that there are hackers in the Fortnite game that can make him lose games, and even my 75-year-old father is worried about money being stolen when looking at his bank statement from the tablet.
- The open debate of a possible Russian interference in the 2016 US elections, as well as the vulnerabilities discovered in the voting software during them.

But what could happen if there was a cyber attack in the upcoming Spanish general elections?



What can be attacked cybernetically and for what purposes?

There are three main elements that are susceptible to attack:

1. Faced with an interest in influencing the electoral process, political parties are fundamental objectives. There are several known cases that have taken place during recent campaigns. For example, during the US elections Hillary Clinton's emails were hacked and before the French elections Emmanuel Macron's emails were leaked. The main objective is clear: to discredit politicians.
2. Citizens are another critical element in the electoral processes. In this case, the aim is to influence them at the time of voting. Western democracies are no strangers to influences that seek to unbalance them, mainly through propaganda campaigns and fake news.
3. Finally, government institutions are another key target in electoral processes. In this case, the objective is to weaken the democratic system in order to obtain geopolitical, economic and ideological benefits. and the computer systems that support the electronic processes are usually attacked, both for the vote and for the subsequent counting.

How can it be attacked?

The forms of attack are multiple and one of the greatest complexities we face in these cases is that they are targeted and specific attacks, they are not general attacks.

First of all, I would like to introduce the concept of a hybrid attack, which, in the field we are referring to, consists of combining conventional means such as media pressure and non-conventional ones, such as fake news. The latter are usually associated with social networks and new technologies.

Fake news is one of the main concerns, since it directly addresses citizens. To make the media or social networks sources of disinformation and speakers of fake news is a clear attack. In this sense, placing fake news in a widely known and trusted media has much more impact than using a platform that no one knows, even if it is only temporarily.

Another type of attack involves infecting electronic voting systems. Although in recent months there have been numerous news about vulnerabilities in this type of software, this type of infections do not yet apply in Spain, because electronic voting is not being implemented. However, it is worth mentioning anecdotally the case of an 11-year-old boy who was able to hack a replica of the US voting system and that was presented during the last edition of DEFCON, or that several researchers found security flaws in the Swiss electoral software before its use in the elections of this country.

On the other hand, it is possible to hack the electoral counting systems in Spain, although due to the electoral model of this country it would not achieve much more than generate confusion, because the telematic data always intersects with the manuals. Attacks can be carried out against central computer systems, communications or even counting devices in polling stations, but these would still be “minor evils”.

Finally, it is important to highlight the possible attacks on the information systems of the electoral parties and their websites. In these cases, the main objective would be to leak confidential information and use it in the “hybrid attack” format explained above.

All this highlights that it is not only the software used for counting votes that should be monitored and tested, but there are a large number of vulnerable factors and participants when it comes to affecting the election result. In that sense, those companies and organisations that may be close to the political scene or public communication should do exercises to try to minimise the risk of being participants in campaigns of interference in electoral processes.

Politicians and parties should always pay special attention to cybersecurity, but especially before an election, since it is the time of greatest risk of attempts to leak information. Nothing does more damage to a candidate's image than taking out his "dirty laundry" in the middle of an election campaign.

Who can attack?

There are mainly three different types of attackers:

1. Hacktivists can take advantage of this critical moment of elections to try to carry out actions that harm those who have governed and thus prevent them from being re-elected or, simply, to make themselves known.
2. Political parties and economic groups that seek to ”bring the ember to their sardine", as may have already happened in other electoral processes in several countries.
3. The experts with a lot of resources to be able to carry out focused and highly targeted attacks on their victims.

The latter group has the most likely and most dangerous profile, because their knowledge about technology makes the slightest deficiency in the systems generate the greatest catastrophes.

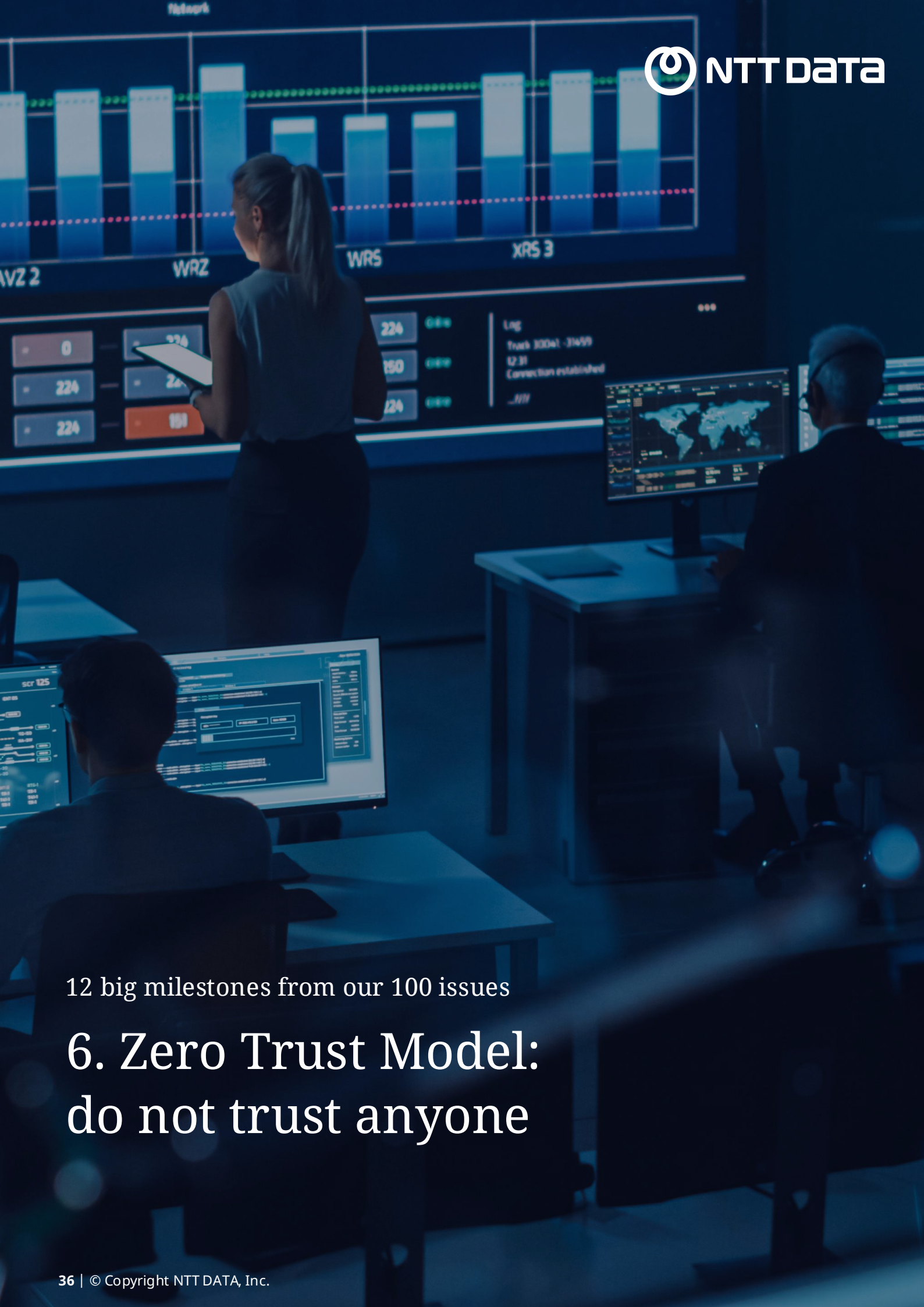
How can we protect ourselves?

First of all, it is important to note that, no matter how much you protect your home from being burglarised, it is always possible that it will end up happening. Of course, it is less likely to happen if you have alarms, bars and private guards, than if you leave the door open.

1. Many countries are in the process of improving their protection barriers and they are improving little by little. For example, it is worth highlighting the case of ENISA that, in its effort to protect the European elections, organised together with the European Parliament, the European Commission and the Member States a joint exercise to test its response and contingency plan in case of potential incidents that may affect the European elections. In addition, the Special Security Device (DEC) has been created in Spain, which has numerous government agencies involved, such as the National Centre for Infrastructure Protection and Cybersecurity (CNPIC), the National Police and the Civil Guard, among many others, to strengthen security during the electoral period.
2. Those responsible for electoral campaigns should avoid information leaks, mainly through the implementation of basic security measures and through the monitoring of social networks and the Internet.
3. ICT providers such as Telefónica, Google, Facebook, etc. could contribute by eliminating illegal or false content quickly and avoiding, as far as possible, the creation of false profiles, known as trolls.
4. The media should properly weigh whether it is better to give a scoop or make sure that the information is truthful. In this sense, it is important to emphasise that financing models through advertising do not favour this process, because it is more lucrative to give a news that attracts many visits than to verify the reliability of it.
5. App manufacturers would also have to get involved and, in fact, some are already doing so. For example, WhatsApp no longer allows you to spread news to all your contacts in a massive way.
6. Finally, citizens should also do our bit by using common sense and implementing basic security measures, for example, not forwarding the first thing that arrives to us or preventing malicious software from being installed on our devices that can then be used to attack other citizens.

Cybersecurity is the best foundation to sustain democracy, especially when both it and society are being digitally transformed. If we cannot rely on technology for the most critical aspects, it will cease to be used, and therefore we will not be able to benefit from its advantages.

 © Copyright NTT DATA, Inc.



12 big milestones from our 100 issues

6. Zero Trust Model: do not trust anyone

 © Copyright NTT DATA, Inc.

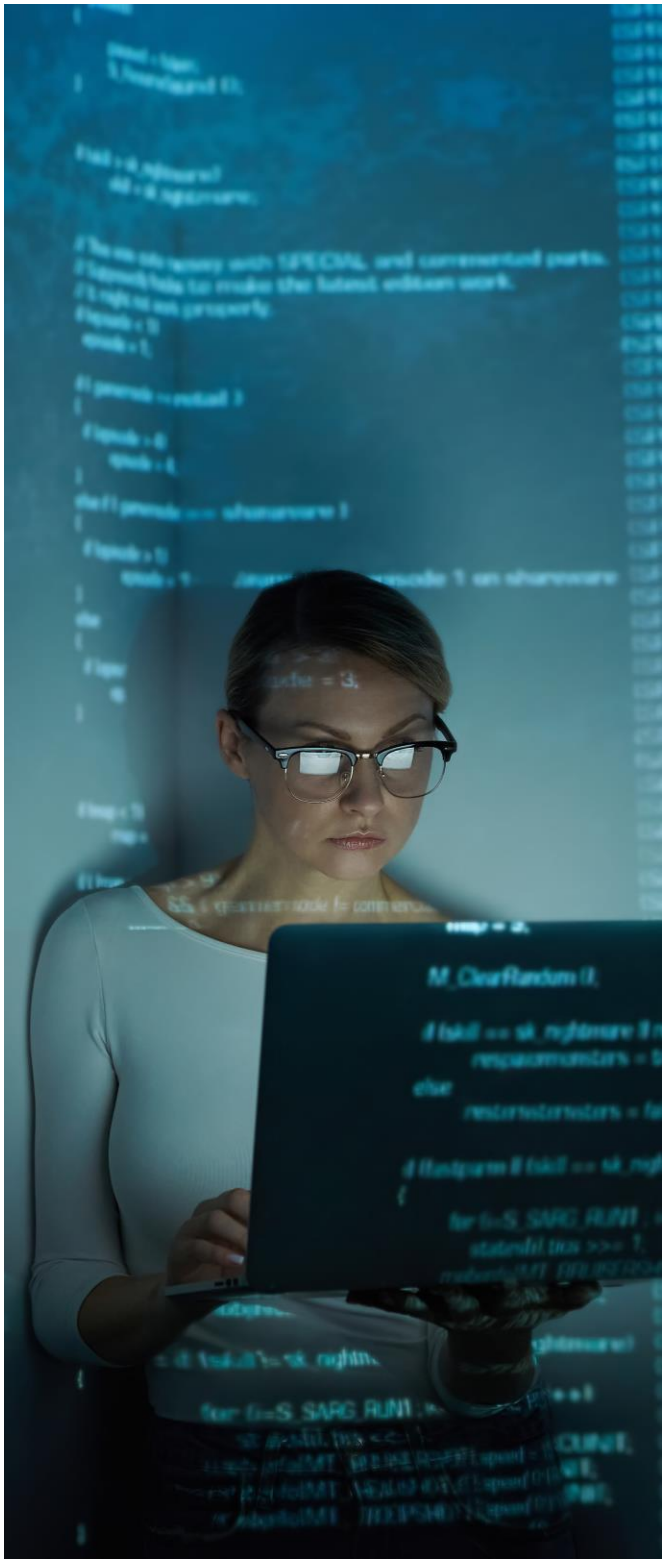
Article October 2019

One of the most prominent security events in recent months has been the case of the Capital One bank, which suffered a security breach exposing information of 106 million users. The CEO of Akamai commented in a news published at the end of July that this event highlighted the need for the Zero Trust Model, but what is Zero Trust? This article will focus on answering this question.

This concept is a new way of understanding the networks of organisations that rejects the idea of “castle and moat”, in which everything that is outside my network is not trusted and what is inside is. Nowadays, the physical perimeter of organisations is not the only digital perimeter of the company, the users and devices (managed computers) of an organisation can be outside the business network, and in the same way, other people's users or devices can be inside the network. Therefore, it cannot be assumed that everything that is inside the network is reliable. Security threats can arise internally, through a malware infection, for example, and endanger the entire organisation.

Thus, this model is based on ”never trust and always verify". This system prevents threats from moving laterally across a network, that is, attackers from making their way through a network to get to assets and data. This is achieved through minimum privilege strategies with exhaustive access control, micro segmentation of the networks and constant monitoring of their status.

John Kindervag presented the Zero Trust model in 2010, exposing micro networks, dedicated exclusively to monitoring. It is a new network element figure (Network Segmentation Gateways) that included security naturally to the model with functions of cryptography, monitoring, content filtering, firewall, intrusion detection and access control.



 © Copyright NTT DATA, Inc.

All this, centrally managed to control the infrastructure.

The theoretical model of Kindervag laid the foundations in this way of conceiving the network, gaining weight with the BeyondCorp initiative (https://www.beyondcorp.com) powered by Google after suffering an attack called Operation Aurora.

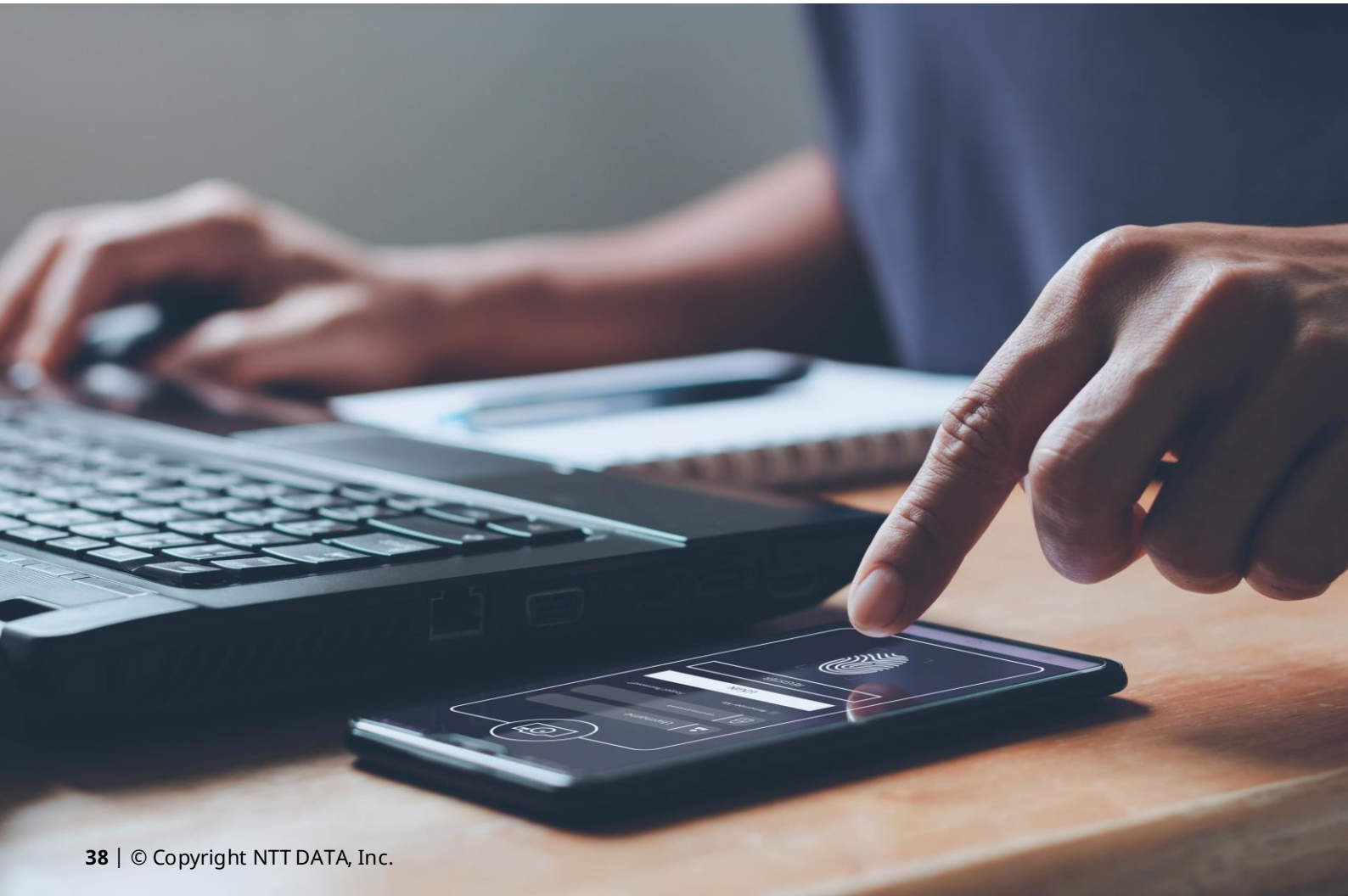
After the attack, Google conducted research to implement the Zero Trust model in its networks. The results of the initiative are published on its website. Some interesting ideas they mention are:

- Keep an updated inventory with all corporate devices where the identity is confirmed with a certificate generated by each of them and that is renewed periodically. Also maintain a control of all the changes that have been carried out in the managed corporate devices.

- All access must pass through an access control engine, regardless of its position in the network where it applies the corresponding access policies.

- Use an inference and trust engine that serves to control the degree of trust of a user and device over time based on their behaviour. This information is used to assign or modify permissions over time.

At this point, we found a set of interesting ideas that can help us increase the security of our networks.



If we want to carry them out in our organisations, there is no single strategy to follow, since it depends on the particular characteristics of each organisation, as well as the degree of non-trust that we want to reach.

It is clear that regardless of the chosen strategy, the basic idea to be considered is the strong segmentation of the network, where there will always be an access control in each segment, as well as the continuous monitoring, inventory and status of all network devices. It would also be desirable that an authentication of the device is required and, depending on this, access permissions are modified. To have clear and controlled the information flows that take place in the network, as well as the necessary connections between the different elements and to know their temporal behaviour (at what times they should have activity and at what times they should not).

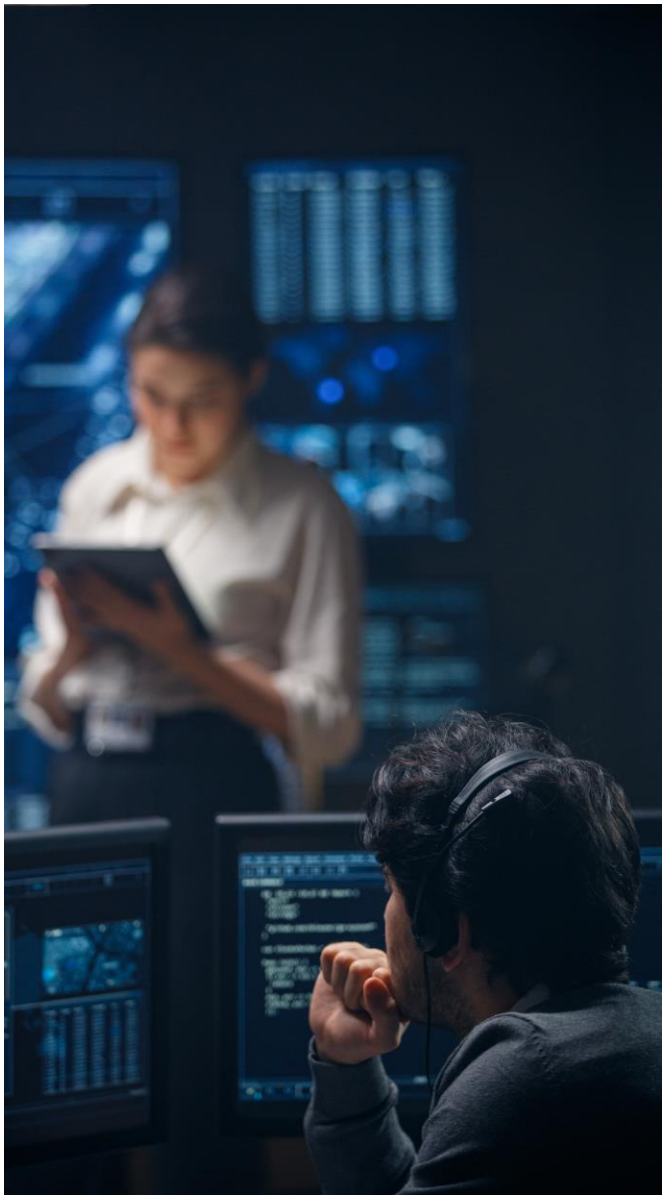
Additionally, a network dedicated to monitoring should be implemented that allows each network segment to be monitored, and force that the administration tasks of the same can only be carried out in certain physical sites (location-based authorisation).

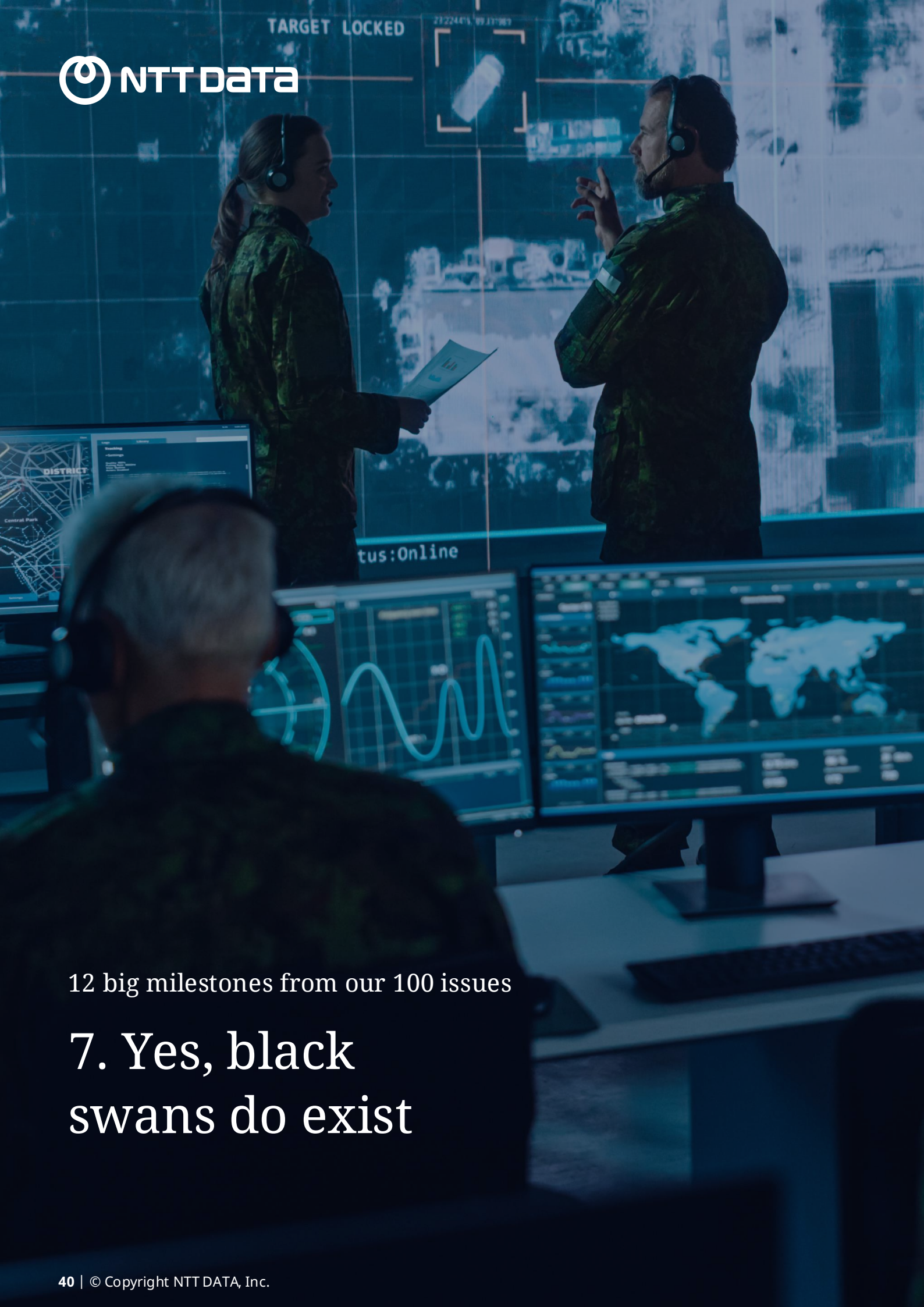
To limit the services available depending on the device in use will require the use of double factor to users and differentiate between devices since a device that is under complete control of the organisation should not have the same level of trust as an external one, regardless of the user who uses it.

One of the most interesting measures to be added would be that access control mechanisms could use behavioural information (the temporal evolution of trust), as the example of Google.

As we have seen, this model seeks to ensure that it is operated with the minimum privilege, thus avoiding access unless express permission and checking what is happening on the network. Control is also one of the key pillars, as we have already mentioned, it is necessary to have the inventory of devices updated and their status, as well as the expected behaviour of them.

Finally, it is important to note that this model can be implemented completely or partially, in a part of the network or in its entirety, depending on the risk appetite of the organisation. Regardless of the decision made regarding the use of this model, the Zero Trust Model must be taken into account in the digital world, where the danger is not only found outside the network.





12 big milestones from our 100 issues

7. Yes, black swans do exist

Article April 2020

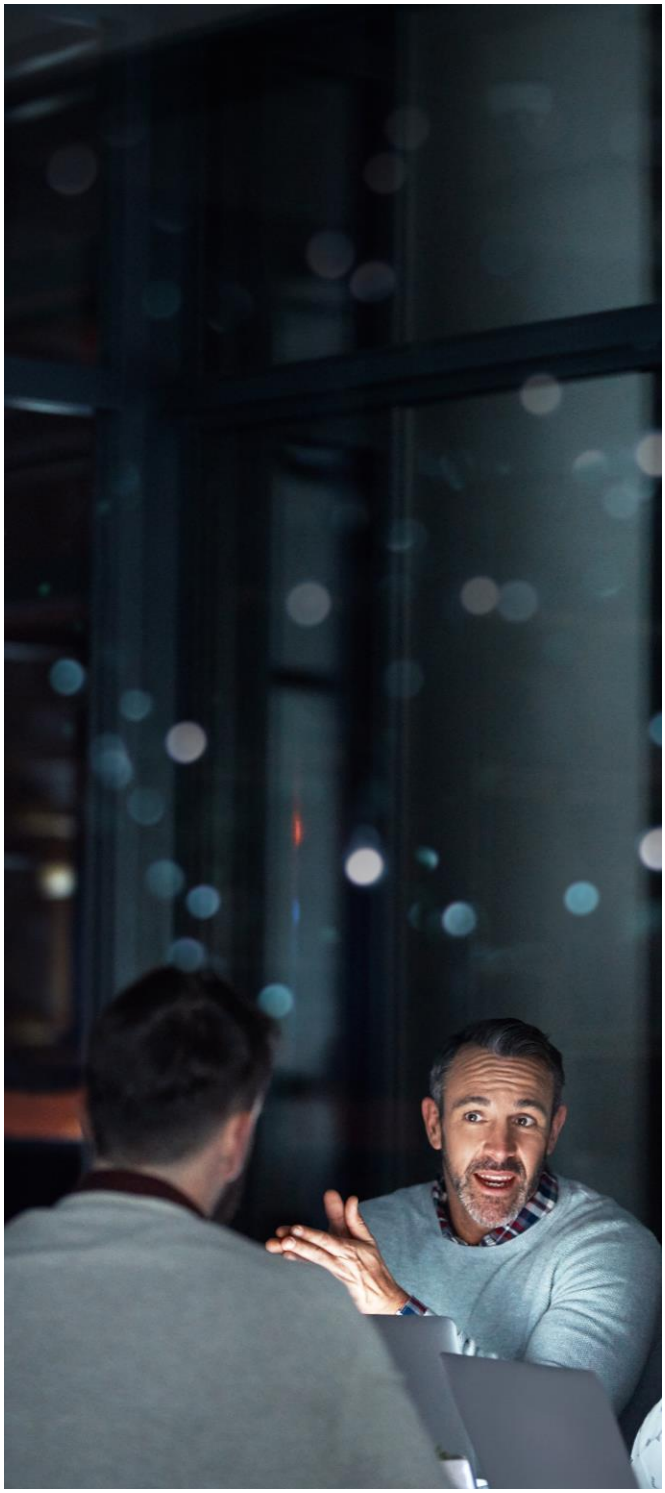
In recent decades we have experienced unusual events that we would never have thought could have such a great impact on the economy and society. These events are contemplated with a very low probability of occurrence but, when they happen, their impact is enormous. These facts are called black swans. For example, we all remember that September 11th. No one thought that two planes could crash into the Twin Towers. Now, a pandemic puts the world economy in check and one of the many questions that arise these days is whether we are technologically prepared to face it. In this article we will develop the measures that we have to take into account to be able to carry out our activity safely from home.

The world is living a new situation in which our way of working, of carrying out our daily life, has been drastically modified. Companies have been forced to promote teleworking massively and adapt to operating remotely. Faced with this new situation, workers have had to change our work routines and habits, but that does not mean we should let our guard down. Cybercriminals take advantage of any loophole to have an opportunity to attack.

The companies

Companies that have not been forced to close and continue with their activity have had to activate their business continuity plans to be able, as far as possible, to continue offering services, at least the minimum. Others have had to implement teleworking solutions in a short time to offer this possibility to their employees.

These plans are based on a first phase in a Business Impact Analysis (BIA). These analyses establish the critical services of each organisation, as well as the personnel, necessary material and the impact that a service interruption can cause on both tangible assets (people) and intangible assets (reputation). Based on the results of this analysis, strategies to be followed for the disruption scenarios that arise will be defined.



 © Copyright NTT DATA, Inc.

After what happened in recent weeks and after the declaration of the State of Alarm by the Government, in many continuity plans it will have been seen that the data contained in each BIA are not completely correct and adequate. Therefore, when this situation is over, they will have to carry out a complete review and an update, realistically. This will be an exercise of lessons learned to be able to establish guidelines and actions for future occasions.

One of the facts that will change the mentality when faced with these analyses will be that one of the scenarios that is contemplated for this type of pandemic cases is the unavailability of personnel. Therefore, it should be reinforced so that the direct impacts, such as the lack of personnel who have become infected, and the indirect ones, such as not being able to leave home or having the possibility of offering massive telework to both critical and non-critical personnel, are mitigated.

The employees

Faced with the current pandemic, teleworking has been established as a measure to avoid contagions and continue with the operation of companies as much as possible.

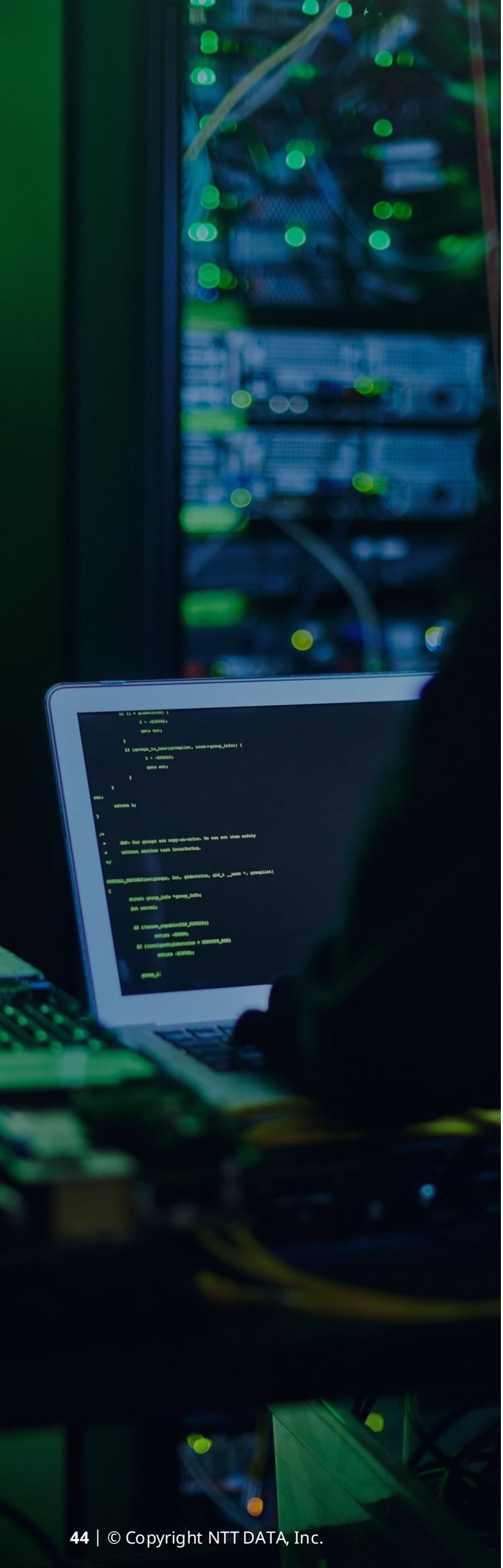
Workers who do not belong to the sectors/ services that are allowed to go to their usual job, have the responsibility to stay at home telecommuting to help slow down the contagion curve.

This obligation to carry out work activity from home is being exploited by cybercriminals. Now, more than ever, we need to be alert to any signs of malicious activity. That's why we want to share some recommendations to follow during the telecommuting working day:

It uses only corporate equipment. These devices have a security maintenance that guarantees the adequate security of the systems.

- Connect to your home Wi-Fi, but first change your network password to a robust one with a length of more than eight characters with uppercase, lowercase, numbers and special characters. The default passwords of the routers may have been leaked.
- Perform a patch and antivirus update review of your computer.
- Pay attention to the emails you receive and do not open any attachments about Covid-19.
- Do not access unknown or unsafe websites. Remember to check the protocol that establishes the communication and that it is HTTP Secure.
- When communicating with your co-workers, always use the corporate applications that have been provided to you.
- Do not install any software that is not allowed by your organisation or use peer-to-peer download tools on the corporate computer. These actions can compromise the security and privacy of your computer.
- Once the working day is over, turn off the computer and do not use it for recreational activities at home or viewing content.

Additionally, the National Cryptological Centre has made available to users a recommendations guide for teleworking in which a series of guidelines are taken into account to ensure the security of the tools and solutions used. You can download it here.



The cybercriminals

During this health crisis, the National Police has warned of the discovery of cyber attacks directed against health systems to completely break the hospitals' computer system.

The method that has been discovered is a ransomware-type attack called NetWalker. The modus operandi of this attack is the sending of emails with a clear theme, information about Covid-19, with health and hospital workers being its main target. As we have mentioned in previous articles, this type of attack hijacks the systems of its victims and asks for a ransom to recover them, usually in Bitcoins. The National Police has alerted the entire population of these mass emails so that they maintain caution in the face of this threat, which takes advantage of the enormous amount of information circulating these days on the Internet to sneak into our systems.

In addition to the distribution of ransomware, the massive publication of fake news is also common these days. More than 200 hoaxes and false news have been registered that are only intended to instil fear and panic. Therefore, we recommend that you always check all information with the official media and do not spread hoaxes. In addition, faced with this situation, the Civil Guard has opened a citizen communication channel to receive information about online frauds and scams in order to collaborate and report.

Conclusions

We live in a difficult situation having to be confined to our homes, but that does not mean that we should lower our guard in terms of cybersecurity. We workers must get used to this situation and perform the same actions that we would do being in offices or in clients. At the same time, companies must protect their employees and also have certain scenarios contemplated that sometimes, perhaps because they seem implausible, occupy a secondary role in risk analyses. Because black swans exist, although between all of us we can overcome them.

12 big milestones from our 100 issues

8. The digitalisation of the utilities sector and cybersecurity

 © Copyright NTT DATA, Inc.

Article November 2020

We are in the midst of the era of digitalisation, a frantic race not to be left behind. However, as we have seen, the faster progress is made, we also leave mistakes that take their toll on us in the long term. In this article we are going to visualise how the utilities sector has managed to advance in the digital career but has also been a victim of the problems that not taking cybersecurity into account in its processes can lead to.

Let's start from the basis that digitalisation is providing companies and the entire utility sector with a great improvement in their services, since infrastructures are modernised, improving efficiency and reliability, something that in one way or another has a satisfactory and positive impact on the consumer. However, we keep seeing an increase in cyber attacks in a sector that, let's not forget, is part of our critical infrastructure network (energy, water, gas, etc.) and as can be seen in the numerous studies carried out by organisations such as the CCI (National Centre for Industrial Cybersecurity) here in Spain, or ENISA (European Union Agency for Cybersecurity) itself, cybersecurity is an aspect that is not being taken into account, when in fact it should be prioritised and updated on a continuous basis.

The need to obtain, analyse, process and store data is a toll to pay that companies currently see as unavoidable in order not to miss the train of the future of technology in the short and medium term. Let's not lose sight of the fact that the vast majority of companies in the utilities sector have a business whose scope is not limited only to IT infrastructures, but to a large extent to the industrial sector (OT).

This combination of IT and OT infrastructures, and the convergence between the two, means that these types of companies have to face comprehensive cybersecurity strategies that cover the needs of two very different worlds and that serve as a shield against possible attacks that affect their service.

We have only to imagine if for a long period of time there was no electricity, water, or gas. Not only the consumer himself would be affected, but the interdependencies or cascading effects that this would have on other sectors such as, for example, transport or the nuclear sector or even on other countries that consume these resources.

If we know the dangers and the damages that a cyber attack can cause, why do we not take cybersecurity into account?

 © Copyright NTT DATA, Inc.

Are we ready for the next decade?

The irruption of new technologies (Cloud, Big Data, etc.), hyperconnectivity and the psychosis for collecting data for processing and improving efficiency in processes, has made all system infrastructures a vulnerable target to possible attacks. As mentioned above, companies in the utilities sector are exposed to the risks of both the IT world and the OT world.

There has been a lot of talk about how to deal with cybersecurity in the IT field, but especially significant, both for its importance and for its consequences, is the case of Industrial Control Systems (ICS), the core of any automated process in the OT field (generation plants, substations, water supply and sanitation infrastructure, etc.).

Although current systems are designed, implemented and operated taking cybersecurity into account as an initial requirement (or at least they should be), the biggest challenge facing us in the industrial world is that posed by legacy systems, whose security measures were not designed to face current cyber threats. One, but the most, of the main problems proposed by these operating systems (OT), lies in the life cycles of the same.

Unlike IT systems, OT systems have a life cycle that is not uncommon to exceed 25 years. This is because they are systems designed to last over time, due to their complexity and the need to offer maximum availability of the process to be controlled. Therefore, the need arises to ”secure“ already operational systems and ”add" security to systems that were designed and installed without taking into account the control measures for current threats and for which a replacement would not be a viable option, due to its complexity and the necessary investment.

Given that a great gateway of threats for SCI is given by its openness and convergence with the IT world, we must not forget that the heart of the automated system is the controller and the instrumentation that provides it with signals. Taking protection measures aimed at the system core should be mandatory (equipment bastioning, access control, configuration and change control, authentication, etc.). Combining this type of tools and measures with change management and configuration solutions in critical components within industrial environments, gives the strategy great visibility over the system assets, so that in the event of anomaly detection, be able to take the appropriate actions to not lose control of the process.

 © Copyright NTT DATA, Inc.

As we have seen in the various attacks produced, cybercriminals launch their attacks with different objectives, ranging from the collection of a sum of money, usually in bitcoins for the hijacking of data or services; the theft of sensitive customer information, the damage to the public image of the company and causing its shares to fall; service interruptions to cause the malfunction of critical infrastructures and cause human losses. Therefore, companies must face these cybercriminals and be well prepared for the challenges that come in the coming years and face the particularities that this sector offers, so they should take into account the following points:

- Increase the corporate culture in cybersecurity throughout the company by involving all the staff to feel part of that cybersecurity culture and be prepared for possible incidents.
- Train and raise awareness among employees as the center of cybersecurity and thus reduce the risks that may lead to causing an internal threat.
- Have policies and procedures that clearly define and guide professionals, always following the standards and regulations that affect the sector. Managing to define a good industrial cybersecurity strategy that minimises existing threats.
- These procedures must also be updated and adapted to innovative solutions such as IIoT (Industrial Internet of Things), in which the clearly defined layers of the Purdue model, which have been helping to bastion operational environments for 20 years, are abandoned in favor of cloud-based solutions that are changing the way industrial control networks, the heart of the sector, are implemented.
- Define and carry out a specific cybersecurity plan and strategy in both the IT and OT fields that addresses the needs of two clearly differentiated worlds that are currently converging as a result of the hyperconnectivity of systems.
- Establish and identify the assets and components of the OT system to perform a monitoring using Deep Packet Inspection (DPI) technology.
- Carry out security plans with the necessary measures to prevent, detect and respond to any type of incident, performing a correct and rapid management and communication of incidents to the appropriate authorities.
- Be up-to-date on new regulations, threats, studies, contingency measures that institutions and organisations may present.
- Collaborate with these organisations and institutions, participating in the different existing knowledge forums where information and good practices are shared.
- Ensure that the opportunities offered by new technologies will have data protection and integrity.
- Maintain a process of annual audits to maintain an updated, robust system, along with a thorough analysis of risks and the necessary measures to mitigate them.

These aspects should be agreed by the organisation given the great impact they cause and that is why it is necessary to find an equality between the new cybersecurity measures implemented and the response that is achieved to the incidents.

In addition, not only organisations in these sectors must be prepared, but we must also think about the different agents that are within the value chain of the sector, since we must all be focused and have cybersecurity in mind. For example, manufacturers must take into account privacy and security by default from the design.

Therefore, all the members should be clear that to face the following years where technology will offer great advantages, but more sophisticated attacks will also occur, each party involved should:

- **Operators**: to improve their ability to recover from any type of incidents.
- **Manufacturers**: provide secure equipment and that security patches are distributed when vulnerabilities are detected.
- **Cybersecurity solution providers**: to provide technology and solutions for early warning of cyber attacks in addition to network monitoring.
- **Cybersecurity services companies**: assist and collaborate in the application and implementation of policies and standards.
- **Cloud providers**: acquire the responsibility of hosting applications that interact with components of the control systems, with all the guarantees of confidentiality, availability and integrity.

Conclusions

The utilities sector is of vital importance within the economy and society, ensuring its resilience and ability to adapt and service continuity to any type of threat or cybersecurity incident.

For the profound transformation with digitalisation and connectivity that the IoT world will entail along with 5G, it will be necessary to ensure a proper functioning of existing infrastructures, and as we have mentioned, it will be necessary to take into account cybersecurity, along with privacy and security by default from the design and throughout the entire supply chain, as well as its lifecycle.

Therefore, the definition and monitoring of clear standards is essential, along with a governance framework within organisations that provides security to users, manufacturers and operators. With all of them we will manage to promote a cybersecurity culture that will allow us to face the threats that come from abroad, either by defining policies and training our employees with greater knowledge to be able to react and think about responses to possible incidents.

12 big milestones from our 100 issues

9. Industrialising security work in the software development life cycle

 © Copyright NTT DATA, Inc.

Article February 2021

For years, when it comes to software development, companies have paid more attention to quantity and operation than to quality and security. Currently, with the increase in cyber attacks, this trend is changing and more and more security controls are being integrated into the software development lifecycle.

The race towards digitalisation is causing organisations the need to generate a large volume of software. This has led to a tendency to industrialise the construction, testing, deployment and operations processes, which translates into cost savings, time, and improved software quality, thanks to the integration of automatic tools throughout its entire life cycle. The expansion of this model also has repercussions in the field of software security, which must be integrated in parallel and form part of these automatic processes.

But how can we properly include security in its life cycle? How can we know if the security controls adopted are sufficient?, How do we automate the control tasks? There are methodologies to check the level of security maturity on the SDLC of an organisation, OpenSAMM is an example.

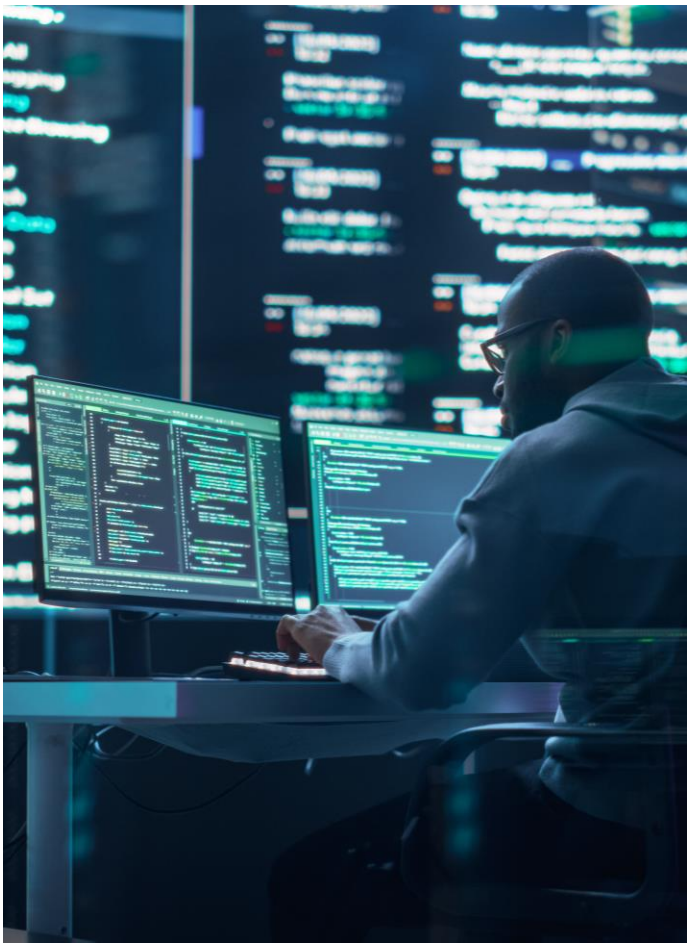
Before going deeper, we must understand what the concept of software development life cycle consists of (which we will hereinafter call SDLC) and how its industrialisation and automation of processes leads to what we know as DevOps.

The SDLC (Security Development Life Cycle) is the methodology adopted by a company that defines, organises and orchestrates all the processes and tasks involved from the moment the need to create a software is born until it is deployed in production. When security is integrated into all these processes and tasks, what is known as Secure SDLC (or SSDLC) is achieved.

Within the SSDLC, tasks and processes are grouped into clearly differentiated phases by their typology, making it easier to define the limits of responsibility and security compliance to allow the passage of the software to the next phase.

For anyone who has been involved in development projects in any way, the following phases of an SSDLC will be familiar:

1. Requirements.
2. Design.
3. Implementation - development.
4. Testing and verification.
5. Deployment.
6. Operation.



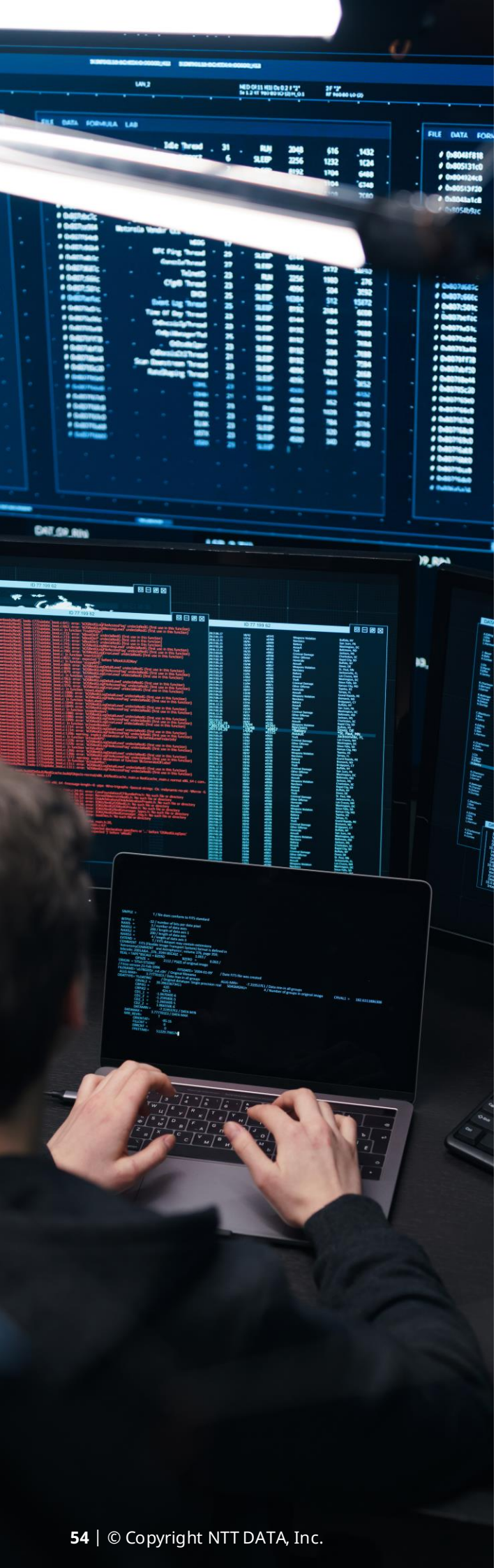
 © Copyright NTT DATA, Inc.

Below, we list a series of tasks that are recommended to be performed when looking to increase the security maturity level of an SDLC to convert it into a Secure SDLC:

1. During the requirements taking there should always be a security architect role that knows how to establish the security needs according to the business requirements of the software, as well as the baseline of requirements that it must meet. It is always a good practice to rely on standards such as OWASP ASVS, OWASP WSTG, PCI DSS (if applicable), etc., in order to cover all security domains.

2. Designing and modelling the software according to the requirements is an important task that is gaining increasing weight from the security point of view. It is in this phase that the analysis of attack surfaces and threat modelling is carried out. The importance of these tasks lies in the discovery of potential vulnerabilities at early stages of the software lifecycle, even before the development itself begins. Detecting possible security deficiencies at the beginning allows you to improve your security, reduce vulnerabilities in the future and, consequently, reduce development costs to mitigate them.

3. The execution of security scans on the source code during the implementation/ development stage allows vulnerabilities to be discovered while it is being developed. Having SAST and SCA tools in CI/CD systems makes it possible for developers to detect vulnerabilities while they are developing, both in the code and in the dependencies. At this stage it becomes very interesting to have the role of Security Champion, a figure who will belong to the development team, but who will have basic security knowledge, which will make him able to translate the terms of the security team to the development team.



4. When the software is already functional and begins to be deployed in integration or testing environments, the testing and verification phase begins. Here the tests are usually executed by both automatic and manual tools (the latter executed by ethical hackers), trying to reproduce the behaviour of malicious users. These tests are complementary to the tests on the source code, since they are able to discover weaknesses in the software that would be difficult to find by analysing the code, such as privilege escalation or session management.

5. Finally, and after having successfully passed the security tests in the previous phases, the software is deployed in productive environments. These environments are the real ones, where the released version is made available to end users and, therefore, is accessible to possible malicious users. Therefore, in this phase of the SSDLC, testing tests (automatic and manual, mainly the latter) will continue to be carried out as in the previous point, but in this case with certain limitations, since we do not want to cause the unavailability of the software: test windows will be defined, denial of service tests will be avoided, etc.

6. In the last phase, the software is already deployed and has to be kept operational and protected during the time that the version in question is in production. To this end, there are tools and probes for detecting attacks and protecting the software in real time. An example of this type of tools are the IAST, responsible for monitoring, detecting and even in some cases, stopping the attack. In this phase it is recommended to register and monitor the events of the perimeter security elements (firewalls, IPS, IDS, agents, etc.) to detect anomalous operations caused by an attacker.

Whether the execution of the above tasks will have a successful impact on the security of the software will depend to a large extent on the orchestration between each of the phases. As if it were an orchestra conductor, the security team should be the one in charge of establishing a management and administration system for the vulnerabilities detected in each phase, as well as tracking them according to their criticality and the moment they were discovered (the higher this is, the greater the penalties).

One point of interest in task orchestration is the establishment of security checkpoints. We have talked about how to analyse the security in each phase; however, we have not commented anything about the establishment of penalties if the test results are not successful, avoiding moving to the next phase if the software has a high number of critical vulnerabilities or they have not been solved for a long time. These checkpoints are called Security Gates and function as thresholds or limitations that prevent vulnerable software from moving to the next phase in its lifecycle and may even be deployed in a productive environment.

In order to establish these thresholds, theoretical models are defined using formulas, such as:

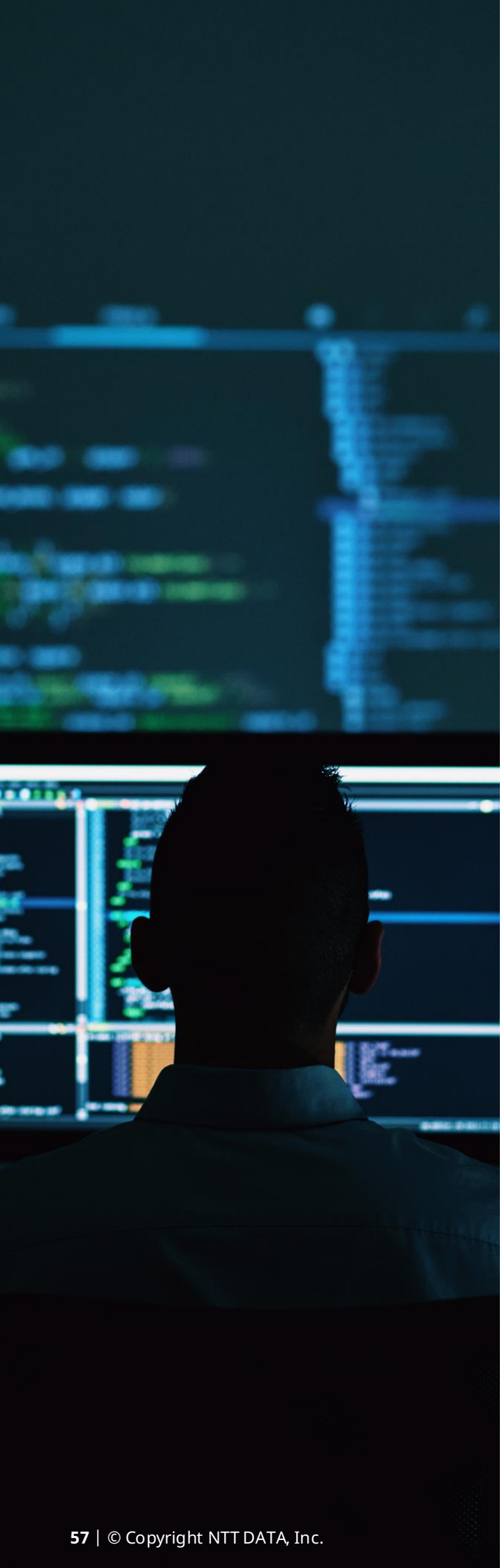
$$health = 100\ x \frac{\log_{10}\left((4\ x\ CVN + 3\ x\ HVN + 2\ x\ MVN + LVN) + 1\right)}{\log_{10}(nº\ of\ lines)}$$

The above formula represents the health obtained by weighting the results of a SAST analysis, where:

- **CVN (Critical Vulnerability Number):** is the number of critical vulnerabilities found.
- **HVN (High Vulnerability Number):** is the number of high vulnerabilities found.
- **MVN (Medium Vulnerability Number):** this is the number of average vulnerabilities found.
- **LVN (Low Vulnerability Number):** is the number of low vulnerabilities found.
- The number of lines corresponds to the total number of lines of code that have been analysed.
- The factors 4, 3, 2 represent the weighting assigned to each type of vulnerability according to its criticality, assigning greater weight to critical vulnerabilities.

It is noticeable in view that theoretical models are very complex and difficult to measure when automating tasks, that's why the volume of vulnerabilities and their criticalities are usually taken as a reference.

For example, if after a SAST analysis, the source code presents a critical vulnerability, the software will not be able to proceed to the testing and validation phase. This is much simpler than developing a script that performs the logarithmic operation of the model and makes a decision.



At this point, we have managed to establish an SSDLC in our organisation with a maturity level that will depend on how many of the security processes exposed above have been covered.

These processes should be maintained and improved over time to avoid obsolescence and maintain/improve the level of security maturity acquired.

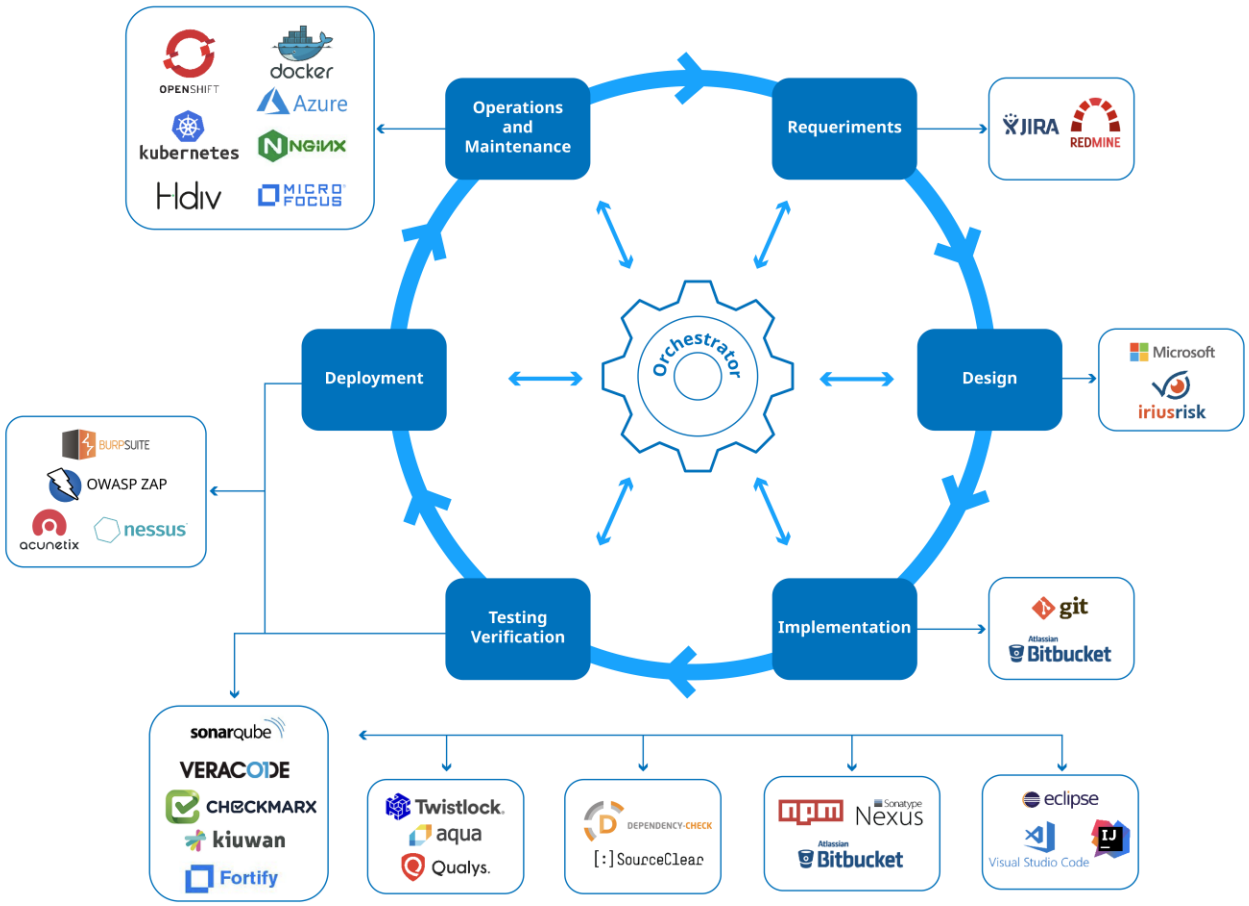
As we introduced at the beginning, companies are tending to the industrialisation of processes. When the SSLDC processes are automated we get a SecDevOps (or DevSecOps). There are numerous discussion forums about where to place the syllable 'Sec' in the word 'DevOps', in this case, we have chosen to put it at the beginning, since we think that security should be from the beginning of development, from taking requirements and design to the maintenance and operations phases in final or productive environments.

Automation is achieved by inserting tools that perform the tasks and processes defined in the methodology of our SSDLC. The basic piece of this gear of tools will be the orchestrator, which will launch the tools.

Complying with the methodology, the orchestrator will mark the flow of phases, in such a way that, if the results obtained by any of the tools are not successful, the execution of tools will be stopped. In these failed cases, where the defined Security Gate has not been exceeded, an alert should be generated, both for those responsible for the security team, and for the Security Champions of the development teams. This will ensure that detected occurrences are reviewed and, if necessary, registered as a vulnerability in the vulnerability management system.

An example of a widely used orchestrator is the Jenkins tool, of which there are numerous plugins for integration with security tools that automate tests in the SSDLC. In this case, Jenkins allows to define processes called 'Pipelines', where the flow, the order and the execution instructions of the tools are configured in case of success or failure.

Below, we can see examples of tools that are usually used in SecDevOps environments for the automation of tasks in the SSDLC:



We have appreciated the upward trend of companies towards integrating security into their SDLC. Likewise, we have detected in our clients a high awareness of adopting good security practices from the early stages of software development. However, the investment in security is still small compared to that used in the developments and, in many cases, insufficient.

Beyond the need to continue improving security in the SDLC, the real challenge is announced with the migration of organisations to Cloud environments, where the OnPremise model is abandoned, and security tools will be integrated as one more service within the Cloud that we have.

In this new model, the security and development teams will have to be closer than ever since the line between environments, configurations, development, implementations, will be less and less appreciable and the SecDevOps model is charged as a new paradigm.

12 big milestones from our 100 issues

10. Privacy, widespread disinterest

 © Copyright NTT DATA, Inc.

Article August 2022

With the evolution of technology, new services are available to people, which allow from making purchases via voice from our homes to carrying out a complete monitoring of our health parameters on the smartphone.

For the development and improvement of these services and methods of interaction with technology, it is necessary to collect data on the use that people make of them, which has allowed optimising the processes and adapting them to the needs of consumers.

In addition to the purely technical purpose of data collection, new opportunities arise, based on the collection of data for use in commercial purposes, that is, its sale to third parties to identify the tastes and preferences of users in order to build a profile that ad companies will use to focus their content towards a more specific audience, thus achieving a greater impact on their ads.

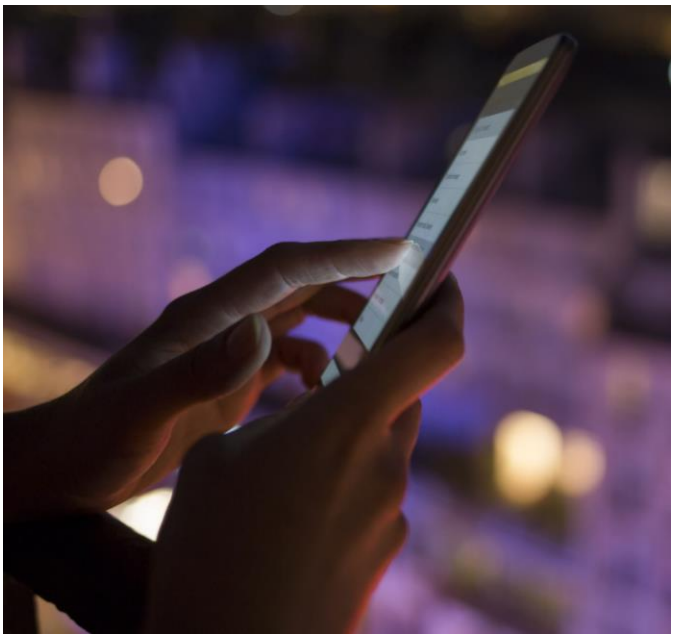
At the same time, new information collection mechanisms are being created, which make it possible to extract data from previously inaccessible areas, as they do not have a digital support.

Generally, the form of communication to users about what data is being collected and how it is processed is done through a privacy policy, which must be read and accepted by said users before they can use any service that processes and collects data.

The use made of this information has led to various privacy problems, both from a more commercial point of view, and from a governmental level, in which ideally, data about citizens are used to increase their security. As explained below, the treatment of people's information is far from being in an ideal scenario, since various practices have come to light that make us question to what extent the privacy of users is being respected, acting in the supposed benefit of optimising applications and services or maintaining the security of citizens.

Origins and evolution

A few years ago, privacy was something almost unknown to many people, the same ones who made use of new technologies to make their day-to-day life easier, making a phone call, sending an email, surfing the internet or using an instant messaging application.



The problems around privacy began to appear in 2013, when a former employee of the Central Intelligence Agency (CIA) and the National Security Agency (NSA) named Edward Snowden revealed information indicating the use of massive espionage programs by the NSA, such as PRISM and XKEYSCORE.

This worldwide scandal revealed how citizens from all over the world had been secretly being spied on. Snowden wanted to make this information public so that people would be aware that their privacy had been compromised without their consent. Additionally, he revealed his identity and decided not to hide anonymously from leaks, since according to him he had done nothing wrong.

It has been a few years since Snowden showed the world how vulnerable privacy is, because users do not have as much as they think. In this new case, the protagonist is an Israeli company called NSO Group, which has developed an espionage software known as Pegasus.

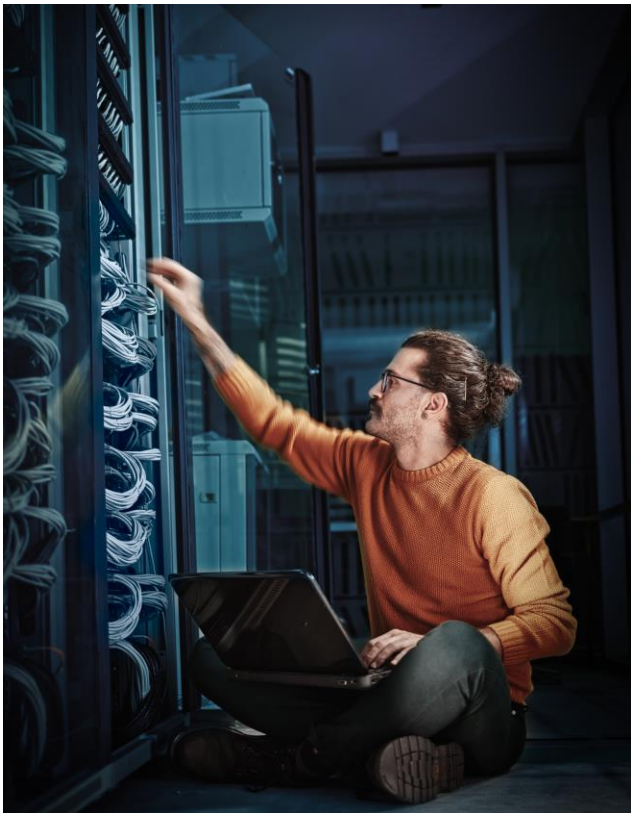
This software allows you to infect and control a device almost without the need for user interaction, giving the software total control to extract information on demand, such as listening to calls, viewing exchanged messages or geolocating the device.

In both cases, the ”justification" for the creation of this type of intrusive espionage software is none other than to prevent terrorism or serious crime. This only causes concern in those who ask themselves: To what extent is this intrusive behaviour allowed and how much does it endanger the privacy of users?

As a result of this issue, and from a commercial point of view, there have been several outstanding cases in which some companies violated the privacy of users, carrying out a processing of user data that has been considered abusive, or was not included in their privacy policies.

One of the recent cases in terms of user privacy affected three of the largest technology companies: With the rise of the market for intelligent personal assistants, the processing of their users' voice data became increasingly common. Although in most cases the data processing is carried out by automated means, according to the NY Times it was discovered that the three companies had employees who listened to some of the users' voice messages, without having previously informed them about the possibility that their voice recordings could be listened to and processed by people.

All the companies stated that this processing was done in such a way that the recordings remained anonymous, but some reports pointed out the possibility that the recordings could include the user's name, user identifiers or the device that was used. After these facts, all companies duly inform about the human review of voice recordings, giving the possibility to the users of their intelligent assistants to decide whether their voice samples can be analysed by people or not.



Use of current data and trends

On a daily basis, we carry out numerous interactions with different technological devices, such as a computer, mobile phone or voice assistant, and surely, we do not stop to think about the amount of information we provide by simply using these.

It is common that during an internet browsing the configuration of cookies is requested to continue displaying the content. This request usually comes intrusively with a message that prevents the viewing of the content, and which requires that you pay attention to it by selecting one of the available options. At a first glance the most highlighted option will be to "Accept all cookies" and continue viewing the desired content, perhaps it is the fastest option, but what if instead of accepting everything the configuration is reviewed? Surprise!, on numerous occasions more information is being provided than would a priori be necessary.

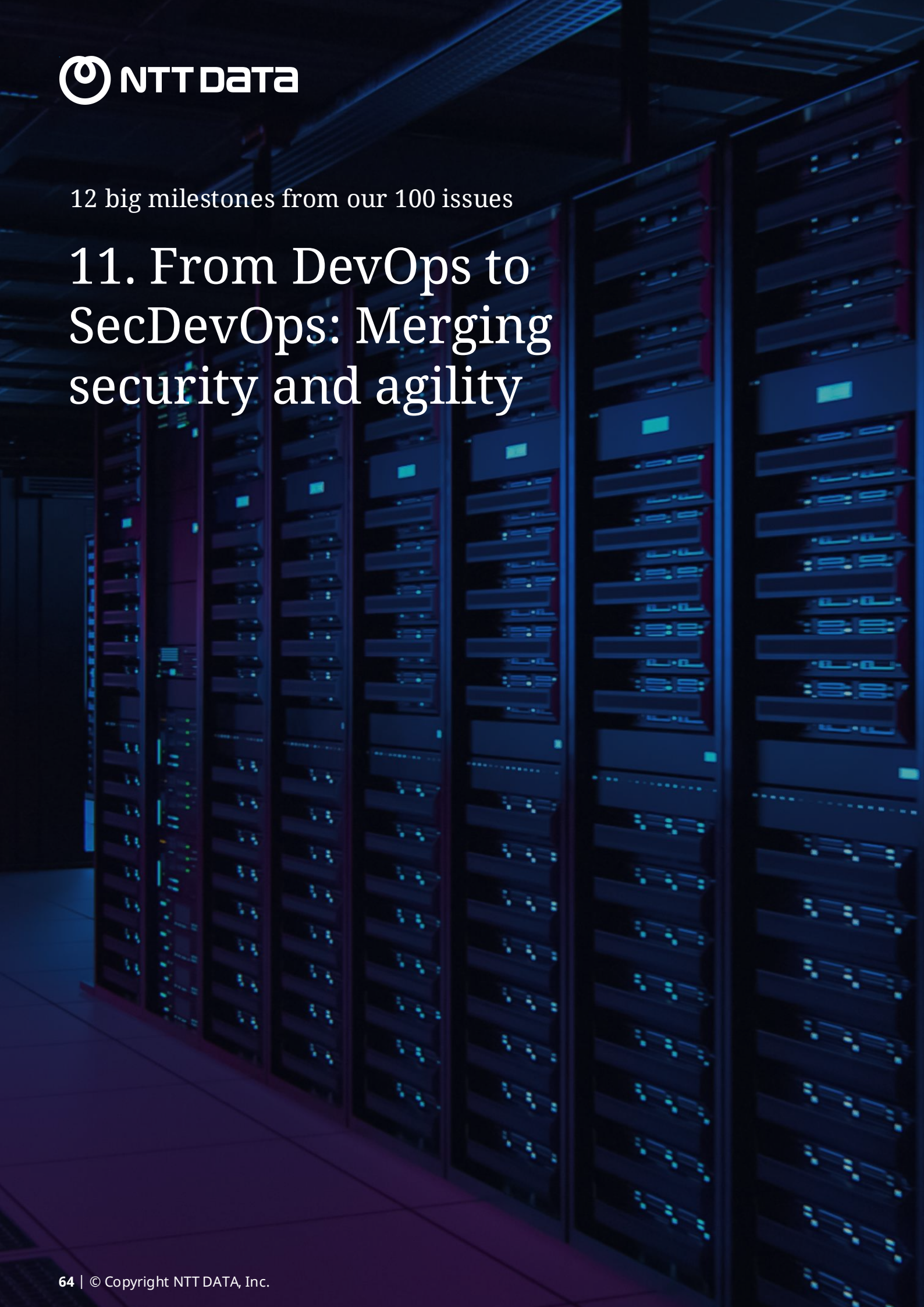
On the other hand, many users have a wearable, such as a smart watch, which is monitoring the heart rate, sleep quality, counting steps, sharing the location or even the messages that arrive from the mobile device. All this information is handled by the manufacturer of this product, which has the power to decide what to do with it, whether to sell it, share it or bet on privacy and that it is not known by third parties, this type of information will depend on the privacy policy that each one has.

In recent years, thanks in part to the exposure of some practices, such as those mentioned above, initiatives have emerged to provide users with greater protection against abusive collection of their data. For example, the Application Marketplaces (first in the iOS App Store and later in the Android Play Store), incorporate a note about the data that will be collected from the user when using an application that he downloads from the Marketplace, giving a more appropriate view that summarises part of the application's privacy policy, which otherwise the user would not normally read to check how his data will be used.

Likewise, the system that manages the permissions of the most popular mobile operating systems has been improving to give more precise control over which device options an application can or cannot use. Users are given the possibility to select more privacy-friendly options, for example, when sharing the location data of their device with certain applications, it is allowed to give an approximate location, instead of providing an exact location.

Along with the native improvements of operating systems, applications have emerged with the idea of protecting the privacy of users, compared to traditional applications from different fields. For example, in the case of messaging applications, while Facebook Messenger collects and associates users with data such as financial information, location, contacts, search histories, user content (photos, videos, etc.) or contact information (name, email, physical address, etc.), other applications such as Signal do not collect this type of information to link it to each user and use it for commercial purposes.

Consumers' perception of privacy has been evolving, giving it more and more weight when choosing one service or another, although much work remains to be done to move from a more sales pitch to a real control that allows users to decide with whom their data can be shared and for what purpose.



12 big milestones from our 100 issues

11. From DevOps to SecDevOps: Merging security and agility

 © Copyright NTT DATA, Inc.

Article December 2023

DevOps: Development + Operations. Merge the own software development processes with those pertaining to the integration and deployment of said developments. It sounds difficult, and, in fact, it is. If we add cybersecurity to the equation, it gets complicated. From that moment we started talking about DevSecOps, or even SecDevOps, depending on how present security is in the entire process.

The synergies between cybersecurity and DevOps

Initially DevOps arises from the need to build and deliver software continuously and automatically as quickly as possible. A team of developers finishes implementing a new functionality in a web application, and it is interesting that this functionality is tested, integrated and deployed as soon as possible in productive environments with the aim of making it available to the end user as soon as possible.

The key concepts here are "collaboration" and "accelerate". We need to collaborate to achieve the agility in software delivery to which we aspire. This presents a number of challenges, mostly the change of mentality and that the need for communication between departments is sometimes shown to be not easy. An operations role cannot be put in the mind of a developer and vice versa. However, the change does not have to be immediate either and processes/technologies can be incorporated little by little.

The concern of companies around cybersecurity has been increasing in recent years, as both the number of attacks and the severity of the consequences have been growing.

It became clear that it was necessary to develop software paying special attention to its security.

We have a scenario in which we need to build and deliver software in an agile way (DevOps), but at the same time guaranteeing its robustness against cyber attacks (Sec). This is how DevSecOps was born. Again, this presents its challenges, since now it is not only a collaboration between Devs and Ops, but also the cybersecurity team are integrated.

In addition, the inclusion of security tools and processes at the end can have an impact on how quickly a development goes out to a productive environment. This is because the fact of including the necessary analyses to verify the security of such development can slow down the overall process, especially if it is necessary to include a filtering of false positives. However, we must decide what is important: that the developments go out as quickly as possible to productive environments regardless of the vulnerabilities they may contain, or that, despite a lower speed in this deployment, our developments have a sufficient degree of security.

From theory to practice: tools to make development safe

Nowadays there is a wide range of tools that help us to provide security to the developments included in a DevSecOps environment. Depending on the type of task they carry out and the time they are executed, we can differentiate the following types:

- **SAST: Static Application Security Testing**. In this classification we find those tools that analyse the source code of the developments in search of possible defects that may cause security vulnerabilities. Examples of SAST technologies are: Veracode, Fortify or Coverity.
- **SCA: Software Composition Analysis**. This type of software is responsible for detecting if there are known security vulnerabilities in the external dependencies used in the developments. Examples of SCA tools are: Snyk, Black Duck or XRay.
- **DAST: Dynamic Application Security Testing.** Similar to SAST, but with the difference that instead of analysing the source code of the developments, it analyses the behaviour of these once deployed. It performs automatic tests in search of behaviours that could be security flaws, such as information leaks or unavailability of services. Examples of DAST tools are Burp Suite, Nessus or Acunetix.
- **RASP: Runtime application self-protection**. Similar to the WAF (Web Application Firewall) technology. It is responsible for detecting and blocking possible attack attempts on deployed applications. Unlike WAFs, which work at the network level, rasps are executed at the application level. They have certain information about the functionality and internal infrastructure of the applications they protect and, therefore, are more accurate when detecting possible attacks. Examples of rasps are: Imperva, Hdiv and OpenRASP.

DevSecOps vs SecDevOps

Nowadays, both terms are used interchangeably as synonyms and the difference is quite diffuse. However, there are some nuances that set them apart.

- DevSecOps is a DevOps environment to which security additions have been included: SAST/SCA tools to analyse the code and dependencies, perhaps a RASP to monitor and protect the developments already deployed ... In short, security exists in the DevOps environment as a necessary addition, but without affecting each and every one of the processes that are executed.
- SecDevOps is a DevOps environment in which security is prioritised, and a conscious focus is placed on each of the existing processes being carried out taking it into account. Developers have SAST analysis tools available in their IDEs; there is a regularly updated security test battery that is executed every time code is uploaded to the repositories; complete SAST, SCA, DAST and/or IAST analyses are executed with security gates that prevent vulnerable developments from being deployed, and the deployed developments are monitored and protected using RASP and/or SIEM tools.

While in DevSecOps security is contemplated and taken into account, in SecDevOps it is prioritised and the element that has to cover the rest is considered.

As a final note, our goal is to build software, not only in an agile way, but also with the greatest possible security guarantees. Therefore, we should always aim to have a SecDevOps environment. However, it is most likely that trying to move directly from a DevOps environment to a SecDevOps one will be counterproductive, since all the users involved will be overwhelmed with such a volume of new tools and processes. The best strategy will be to gradually implement these tools and, at the same time, train users in the use of them.

12 big milestones from our 100 issues

12. Awareness: the cybersecurity doomsayers

 © Copyright NTT DATA, Inc.

Article June 2024

The human factor remains one of the most critical and, at times, vulnerable aspects in cybersecurity. The actions and decisions of individuals can significantly affect an organization's security posture, either strengthening it or compromising it. That is why awareness and training are cornerstones in defence against increasingly sophisticated cyber threats.

Cybersecurity training professionals have the task of educating clients about cyber risks and empowering them to protect their data and systems. This work involves a delicate balance: on one hand, it is vital to highlight the seriousness of threats and the potential consequences of suffering a cyber-attack; on the other hand, exaggerating or overly emphasizing these dangers can instill fear and mistrust among users.

Due to this dividing fine line, those of us dedicated to this task often face a curious label: the "doomsayers" of cybersecurity. Highlighting the inherent risks in the digital world and the catastrophic consequence of a successful attack puts us in an uncomfortable position, seen by some as bearers of bad news or alarmists. This perception, though common, is a simplification of a crucial and multifaceted job.

In all our training activities, participants confront the reality of cyber threats directly, experiencing firsthand how easy it can be to fall into a trap.

Through practical exercises and interactive demonstrations, the sophistication and variety of techniques used by cybercriminals to deceive victims and compromise information security are illustrated. Ultimately, cybersecurity trainers are educators, not prophets of doom.

However, on numerous occasions, users have expressed their concern about the anxiety and fear they experience when participating in some training activities. Just when they believe they have learned to defend against a specific threat, a new vulnerability or attack technique emerges for which they are not prepared. This concern has been so common that, jokingly, we have even toyed with the idea of distributing valerian root tea at the end of such sessions.

It is understandable that employees may experience some anxiety when facing cybercrime. Just a year ago, we were still recommending looking for spelling errors in emails to identify social engineering attacks. Today, scammers draft their fraudulent messages with enviable grammar thanks to artificial intelligence.

 © Copyright NTT DATA, Inc.

This perception reflects the ever-changing and evolving nature of the cybersecurity landscape, where cybercriminals constantly develop new strategies, and the feeling of constantly being one step behind can generate frustration among users.

To avoid this discouragement, it is important to focus on adopting secure online habits and behaviours, learn about preventive measures, and understand the benefits of good digital hygiene. Additionally, cybersecurity education should not be a one-time event but a continuous process. As a link (not weak, but essential) in the cybersecurity chain, it is our obligation to stay informed about the latest threats and security best practices.

We are familiar with preventive measures to protect our homes while on vacation, but are we aware of the risks associated with connecting to public hotel Wi-Fi networks without any precautions?

Both types of risks are real and persistent, so we must assume the role of defenders of our own security and that of our organizations. Cybersecurity is a collective effort, and every contribution is essential.

Our goal is to educate proactively, and we understand that cybersecurity can be intimidating, but we will always guide you safely through the vast cyberspace.

We are committed to providing the support and knowledge necessary for people to feel safe and confident in their ability to face any challenge.

More than doomsayers, think of us as those friends who always remind you to bring an umbrella even on a sunny day. Trust us, someday it will rain, and you will thank us for the advice.

Vulnerabilities

Critical vulnerability in Apple products

Date: January 27, 2025
CVE: CVE-2025-24154

SSQ: 9.8

CRITICAL

Description

The CVE-2025-24154 vulnerability is due to an out-of-bounds writing issue that affects several of the versions of the Apple macOS, iOS, iPadOS and visionOS operating systems.

This type of vulnerability occurs when a program writes data outside the limits of the allocated memory, allowing an attacker to cause unexpected system termination or memory corruption of the *kernel*.

This represents a significant risk, since the corruption of the memory of the *kernel* it can be used to execute malicious code with elevated privileges.

Solution

Apple has addressed this vulnerability by improving out-of-bounds input validation.

Users are advised to update their devices to the corrected versions to mitigate this issue.

- macOS Ventura 13.7.4
- macOS Sonoma 14.7.4
- macOS Sequoia 15.3.1
- Vision 2.3.1
- iOS 18.3.1
- iPadOS 18.3.1

Affected products

This vulnerability affects the following versions of Apple:

- macOS Ventura 13.7.3
- macOS Sonoma 14.7.3
- macOS Sequoia 15.3
- Vision 2.3
- iOS 18.3
- iPadOS 18.3

References

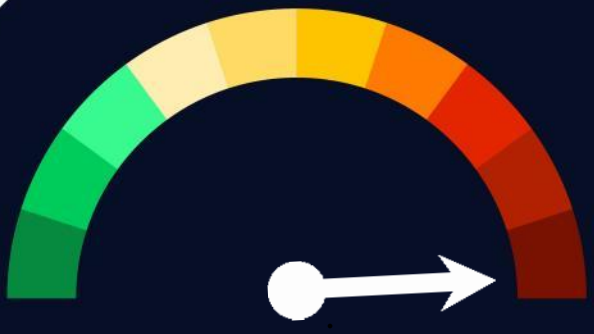
- nvd.nist.gov
- apple.com (iOS and iPadOS)
- apple.com (macOS Ventura)
- apple.com (macOS Sonoma)
- apple.com (macOS Sequoia)
- apple.com (VISIONS)

TLP:WHITE

Vulnerabilities

Critical vulnerabilities in Microsoft products

Date: February 4, 2025
CVE: CVE-2025-21396 and 1 more



SSC: 9.9

HIGH

Description

Microsoft has published two new warnings about critical vulnerabilities in its products:

- Critical authentication bypass vulnerability (CVE-2025-21396) with a CVSS Score of 9.8 that could allow attackers to falsify credentials and gain unauthorised access to Microsoft accounts. It affects authentication mechanisms that rely on insufficient or faulty validation methods.

- Critical elevation of privilege vulnerability (CVE-2025-21415) with a CVSS Score of 9.9, which affects the Azure AI Face service and allows attackers to bypass authentication mechanisms through phishing.

Solution

According to Microsoft, the vulnerability has not been publicly disclosed and there are no known ways to exploit it.

The vulnerabilities were discovered as part of an initiative by Microsoft to add transparency to the security update process by disclosing vulnerabilities, even if they have already been fixed on the server and no user action is required in these cases.

Microsoft offers more details of both vulnerabilities in its security bulletins:

- CVE-2025-21396
- CVE-2025-21415

Affected products

These vulnerabilities affect the following services:

- Microsoft Account
- Azure AI Face

References

- cybersecuritynews.com
- thehackernews.com

TLP:WHITE

February security bulletin from Android

Date: February 3, 2025
CVE: CVE-2024-53104 and 47 more

Critical

Description

The February 2025 Android security bulletin addresses a total of 48 vulnerabilities, including two critical ones. One of them is a *zero-day* in the *kernel* of Android (CVE-2024-53104), while the other is a memory corruption bug in Qualcomm's WLAN component (CVE-2024-45569). It is known that the first one has been exploited, posing a risk to users.

This bulletin fixes critical and high severity vulnerabilities involving the operating system and various components, and that could cause from privilege escalation, remote code execution and memory corruption, to system crash and unauthorised access to sensitive information.

Affected products

The components affected by these vulnerabilities are:

- Framework
- Platform
- System
- Kernel
- Third-Party Components:
  - Arm
  - Imagination Technologies
  - MediaTek
  - UNISOC
  - Qualcomm

In addition, devices with Android 10 and later versions have also been affected.

Solution

The manufacturer has published the corresponding security patches and it is recommended to update the affected products to the latest published version to protect against these vulnerabilities.

References

- android.com
- incibe.es
- csirtcv.gva.es

 © Copyright NTT DATA, Inc.

TLP:WHITE

Cisco Identity Services Engine (ISE) Security Bulletin

Date: February 6, 2025
CVE: CVE-2024-20124 and 1 more

Critical

Description

The Cisco Security bulletin, released on February 6, 2025, addresses multiple critical vulnerabilities in the Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC).

These vulnerabilities could allow an authenticated remote attacker to execute commands arbitrarily with permissions of root on the affected device.

In addition, it could allow an unauthorised attacker to access sensitive information, modify the configuration of the nodes and restart them.

Affected products

The versions of the affected products that are vulnerable are as follows:

- Cisco ISE: All Cisco ISE software versions.
- Cisco ISE-PIC: All software versions of ISE-PIC.

As you can see, the vulnerability affects all versions of these products.

Solution

Cisco has released updates that address these vulnerabilities. Therefore, users are strongly advised to upgrade their systems to the more recent versions of the software.

References

- incibe.es
- cisco.com

TLP:WHITE

Events

Mobile World Congress (MWC) 2025
3 - 6 March

From March 3rd to 6th, Barcelona will host the Mobile World Congress, the most influential event in the world in the field of mobile connectivity. Organised by the GSMA, the MWC25 will bring together business leaders, innovators and experts to discuss and showcase the latest trends and advances in mobile technology, including prominent topics such as artificial intelligence and 5G.

For three days, the event will focus on exploring the main trends in cybersecurity strategies, tools and standards. The agenda will be composed of educational and interactive sessions designed to promote the generation of knowledge, strategic planning and the exchange of experiences between experts in the sector.

Link

RootedCON 2025
6 - 8 March

A new edition of the RootedCON security congress will take place in Madrid from March 6 to 8, a fundamental meeting point for professionals in the sector, companies and organisations in which to share and discuss the latest advances in cybersecurity and technology. The congress will feature different talks conducted by industry experts, as well as additional bootcamps on specialised topics, such as Hardware Hacking or OSINT.

Link

National League of Challenges in Cyberspace (Ciberliga) - Final Phase
10th - 14th March

The *Guardia Civil* (Civil Guard) organises the VI edition of the National League of Challenges in Cyberspace, a competition that seeks to raise awareness among students about the safe and responsible use of new technologies. The final phase will be held from March 10 to 14, 2025 at the University Centre of the *Guardia Civil* in Aranjuez, Madrid, where participants will face "cyber-challenges" that simulate real incidents.

Link

Microsoft AI Tour
27 March

On March 27, Madrid will be one of the stops of the Microsoft AI Tour, a free event aimed at executives that explores how artificial intelligence can boost business growth and create lasting value. The *tour* it offers valuable content about security and is adapted to the specific needs of the attendees, providing an in-depth insight into the applications of AI in the business world

Link

Resources

INCIBE publishes the Android Security Bulletin

The February 2025 Android Security Bulletin addresses multiple critical and high vulnerabilities affecting versions 12, 12L, 13, 14 and 15 of the Android operating system. These vulnerabilities can lead to serious problems such as privilege escalation, remote code execution, memory corruption, and unauthorised access to sensitive information. Users of Android devices are advised to verify and apply the security patches provided by the manufacturers to mitigate these risks

Link

Third-party Risk: The Main Cybersecurity Concern for Companies in 2025

The Cybersecurity magazine highlights that the risk of third parties has become the main cybersecurity concern for companies in 2025. This risk arises from the vulnerabilities and threats associated with the integration of external services and providers. Third-party risk management (TPRM) is crucial to prevent security breaches that can compromise sensitive data and business operations. Cyber intelligence is used to complement TPRM, providing information and context for informed decision making.

Link

Microsoft Security Update

Microsoft has released the security updates corresponding to February 2025, correcting 64 vulnerabilities. Among them, 4 are critical, 57 important, 1 moderate and 2 low. Critical vulnerabilities include remote code execution and elevation of privilege issues. Users are advised to apply the security updates to protect their systems against possible exploits.

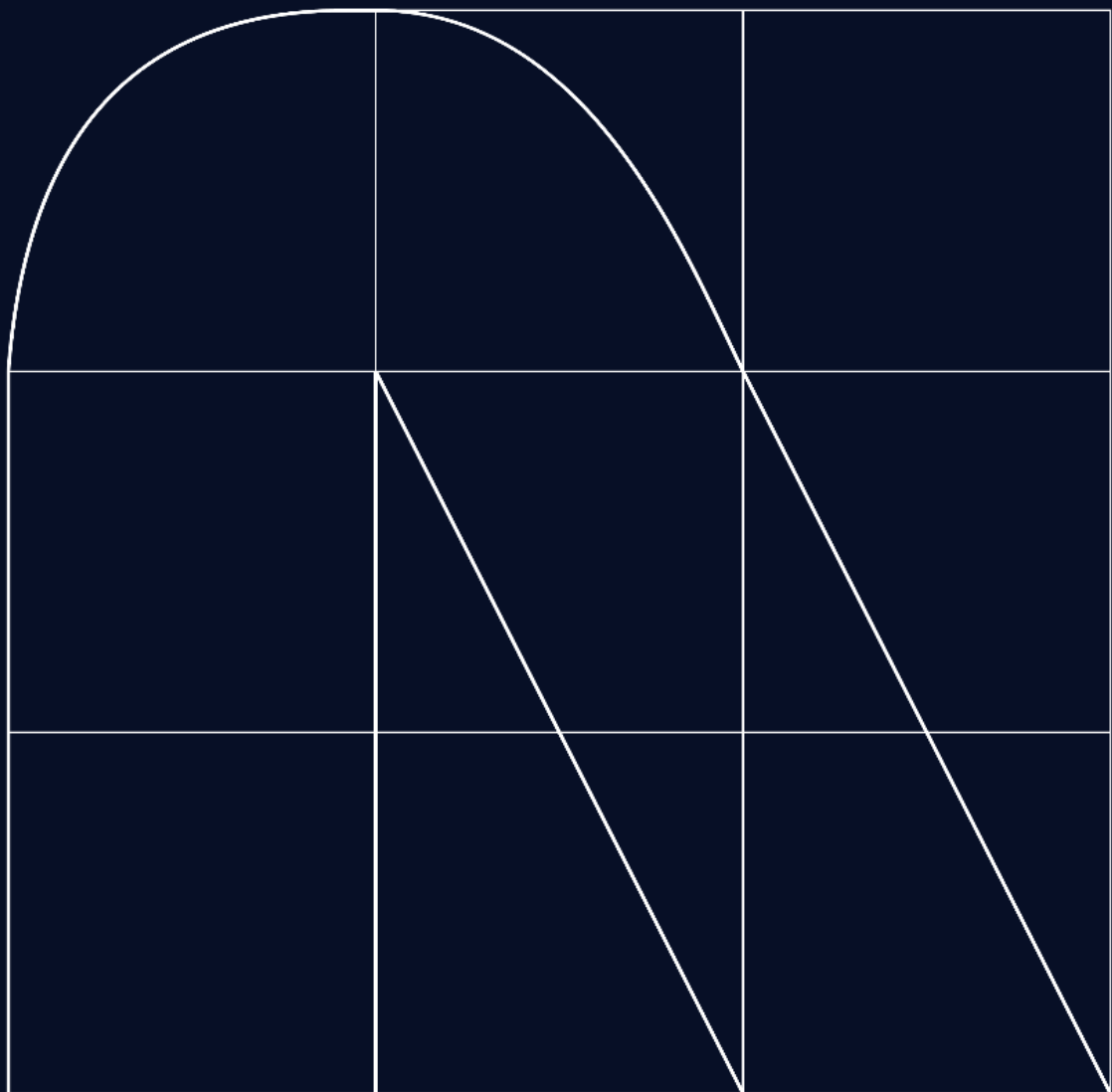
Link

AI and Cybersecurity: Keys for SMEs in 2025

This article highlights how artificial intelligence (AI) has become an essential tool to improve cybersecurity in small and medium-sized enterprises (*SMEs*) in 2025. AI helps to detect and respond to threats more efficiently, automating processes and improving the accuracy in identifying vulnerabilities. In addition, specific use cases and emerging trends are discussed that the *SMEs* they should consider to protect against increasingly sophisticated cyber attacks.

Link

Subscribe to RADAR



Powered by the cybersecurity NTT DATA team

es.nttdata.com