NIS DIRECTIVE

Privileged access management, key to compliance with the NIS directive

WALLIX | 2018

WALLIX
TRACE, AUDIT & TRUST

NIS DIRECTIVE

Privileged access management, key to compliance with the NIS directive

SUMMARY

The NIS (Network Infrastructure Security) directive was adopted by the European Parliament on July 6, 2016, giving Member States of the European Union until May 9, 2018 to incorporate the Directive into their national laws. Aiming to standardize the various local security practices in each Member State, it was passed to ensure that operators of essential services and digital service providers are better protected against cyberthreats. The NIS Directive sets out a comprehensive plan to attain a high common level of network and information system security across all Member States, addressing in particular the protection of Operators of Essential Services (OESs) and Digital Service Providers (DSPs). This white paper will shed light on the challenges and implications of the NIS Directive with regard to cybersecurity practices in European nations, and make a case for how a privileged access management solution easily helps them in their quest for compliance.

WALLIX
TRACE, AUDIT & TRUST

INTRODUCTION

What is the NIS directive?

In our digital era, most businesses and public organizations have computerized and automated the way they store and process data, particularly to achieve economies of scale and improve productivity and efficiency. The ubiquity of digitization in everyday life has driven up the market value of data and this of certain critical resources, such as operators of essential services (or OESs). These operators are prime targets of cyberattacks, threatening organizations and individuals with severe potential damage on several fronts –financial/economic, reputational or even existential (for example, when the integrity of healthcare data hosted by a service provider is compromised, or when a financial service operator runs on a defective information system).

Organizations must therefore take all necessary security measures to arm and protect themselves in order to survive cyberattacks unscathed. Keeping in mind that systems and data within the European Union are interconnected, a common baseline level of security must be defined for the various businesses and organizations in Member States. Enforcing a uniform level of security underpins the EU's overall stability, which in turn depends on the stability of each Member State.

The NIS (Network Infrastructure Security) Directive provides a common legal framework throughout all Member States on how to strengthen security, ensure the EU's stability against cyberthreats, and increase the cyber resilience of networks and information systems on critical infrastructures.

As part of the proposal to transpose this directive, the aim is to enhance security on the information systems used by digital service providers and operators, which are currently not subject to any specific regulations. However, the proposed bill excludes social networks and electronic communications.

Operators of essential services and digital service providers in France must therefore declare incidents that affect their networks and information systems, and where applicable, undergo tests that the ANSSI (French national digital security supervisory authority) may conduct. As such, these actors need to identify the risks that threaten the security of their information systems and take the appropriate measures to counter them.

Any failure to comply with the provisions of the directive may be sanctioned as follows:

- Obstruction of the ANSSI's attempts to conduct testing may be punishable by a fine of €100 000;
- Failure to declare incidents, punishable by a fine of €50 000;
- Absence of necessary security measures, a fine of €75 000.

Who does it affect?

To cater to most of the risks that the EU has to tackle on a daily basis, the NIS directive focuses on two strategic sectors:

- **Operators of Essential Services (OESs)**, whose activity is vital to national equilibrium not only in the countries involved, but which, by default, reverberates across the rest of the EU as well. They belong to various key industries, such as energy, banking, transport, healthcare, drinking water supply and distribution, digital infrastructures, financial market infrastructures, etc. Owing to their status, they need to apply the particular technical and organizational security measures described in the NIS directive in order to enhance protection on critical equipment, and manage risks that threaten the security of their networks. A decree will determine the list of essential services for each operator's industry.

- **Digital Service Providers**, which regulate the storage and movement of data over the Internet. These may refer to online marketplaces, online search engines or cloud computing services. Given the widespread use of the Internet in society today, section (3) of the directive confirms the prominent role of digital service providers in the stability of the EU, emphasizing the part they play in the "cross-border movement of goods, services and people".

Context and legal impact of the NIS directive with regard to the French Military Programming Act (LPM)

By Garance Mathias,
expert in data privacy and cybercrime law, Mathias Avocats

The French Military Programming Act adopted in 2013 (LPM) lends more weight to the security obligations surrounding the information systems of Operators of Vital Importance (OVIs) by placing on them the onus of notifying the ANSSI (French national digital security supervisory authority) of incidents that affect the operation or the security of their information systems. In France, there are approximately 150 OVIs in seven sectors, which include food, water management and energy.

Directive 2016/1148 of July 6, 2016, known as the Directive on security of network and information systems, or NIS Directive, defines the measures to be implemented in order to ensure a high common level of security of network and information systems across the Union. The national strategy that each Member State should develop must cover at least the sectors concerning operators of essential services (OESs) and digital service providers (DSPs). The deadline for transposing this directive into local law is May 9, 2018.

In France, the ANSSI will coordinate efforts with the ENISA (European Union Agency for Network

and Information Security) to drive the process of transposition. The bill to transpose the directive was adopted on December 21, 2017 during the first Senate reading.

European institutions' definition of the term "OES" includes any business that plays a significant role in society and the economy, and which may expand in the following sectors: energy (electricity, oil and gas), transport (air, rail, water and road), banking (credit institutions), financial market infrastructures (trading venues and central counterparties), health (healthcare providers) or water (supply and distribution of drinking water). When determining whether an operator provides an essential service, three criteria must be met: the entity provides a service which is essential for the maintenance of critical societal and/or economic activities, provision of that service depends on network and information systems, and an incident would have significant disruptive effects on the provision of that service. Member States will assess these criteria, taking into account cross-sectoral factors, and where appropriate, sector-specific factors. Member States must identify such OESs by November 9, 2018. In particular, the NIS directive targets three types of digital service providers, defined as "any legal person that provides a digital service". These are, namely, online marketplaces, online search engines, and cloud computing services, which refer to *"a digital service that enables access to a scalable and elastic pool of shareable computing resources"*. The directive obliges each Member State to ensure that these economic actors take all appropriate technical and organizational measures as part of a risk management policy. Apart from the obligations imposed on DSPs and OESs, each Member State must also adopt a national network security strategy.

Member States should make sure that they have well-functioning computer security incident response teams (CSIRTs) as well, to guarantee effective and compatible capabilities to deal with incidents and risks, and ensure efficient cooperation at Union level. The directive's scope of application is therefore much broader than the coverage of the LPM. This means that the ANSSI is the legitimate authority that oversees the preparation of the transposition as an extension of the provisions of the LPM.

Significant challenges

For security to be reliable and sustainable, it should not simply start out with the adoption of one or several technologies, but rather, with the clear identification of requirements as well as a strategy that aims to satisfy them effectively. This is why the NIS directive covers a range of technical and organizational challenges to guarantee the implementation of exhaustive security mechanisms throughout the Union.

1. Organizational challenges

The first implication of transposing the directive is ensuring the standardization of security practices across the 28 Member States of the EU. This creates a challenge on several levels in terms of organization and communication.

1.1 Identification and cooperation

The identification and assignment of each member country's role in securing OESs and DSPs define the reach and scope of the NIS directive at national level, comprising the first step towards the standardization of security measures within the EU. Points (20), (22) and (24) help Member States to identify the OESs and DSPs under their responsibility, regardless of whether they are located in their own territory or in another Member State. They describe the sectors and sub-sectors that the directive targets, and distinguish services that are considered essential. Furthermore, point (24) defines the rules for sharing responsibility where an entity provides an essential service in two or more Member States.

At the same time, point (35) of the directive provides for close cooperation between the public and private sectors, i.e., between OESs and DSPs. Since their services are often interdependent, the NIS mandates the establishment of regular and informal cooperation mechanisms between both sectors. This cooperation is the foundation on which national entities will rely to communicate effectively in order to foster Member States' responsiveness and resilience against cyberattacks, while enabling the existence of a holistic security ecosystem within the Union.

1.2 Responsibilities and communication

The first challenge with regard to communication lies in the cooperation arrangements that the NIS directive encourages and aims to implement. To ensure the effectiveness of the directive, cooperation mechanisms on a larger scale — especially between Member States and the European Union — must also be adopted. Likewise, structuring communication processes and identifying responsibilities in the coordination and dissemination of best practices will become essential on a wider scale.

Figure 1 summarizes the main steps in the organizational distribution described in the NIS directive and indicates the degree of responsibility as well as the operational framework assigned to each entity. As NIS requires Member States to be equipped with a security strategy at a national level, this is the first step to ensuring global implementation. Defining a national security strategy will encourage each member to determine an action plan by contemplating:

- Concrete measures that need to be adopted in order to meet the requirements of the directive.
- The significance and impact of a higher level of cybersecurity on their own countries as well as the potential repercussions within the EU and worldwide.
- The available time frame in which new laws and security measures derived from the directive are to be implemented.

Once a working plan has been defined for each Member State's national security strategy, it becomes simpler to address the second side of the directive's organizational aspect, i.e., the

definition of several key actors at national and European level, in particular:

- National competent authorities that contribute the necessary expertise to represent each industry impacted by the directive, overseeing the implementation, monitoring and standardization of security practices between the public and private sectors.
- A single point of contact defending the interests of the Member State in the Union and ambassador for the state-of-the-art security practices promoted by the EU.
- A computer security incident response team (CSIRT) responsible for risk and incident handling, consisting of one or several representatives.

These two or three entities (in cases where the single point of contact in the Member State differs from the CSIRT representative, as specified in Article 10) are expected to work closely together to see through the implementation and standardization of security practices at national level.

In order to set up a sound cybersecurity ecosystem bolstered by the involvement and trust of its members, in Articles 11 and 12 of the directive, the European Union requires the creation(1) of a cooperation group made up of representatives from each Member State, the Commission and the ENSIA (European Union Agency for Network and Information Security), and (2) a network of CSIRTs from each Member State that the ENSIA supports. Both of these cells are tasked with enabling Member States to exchange information with competent European authorities on the best security

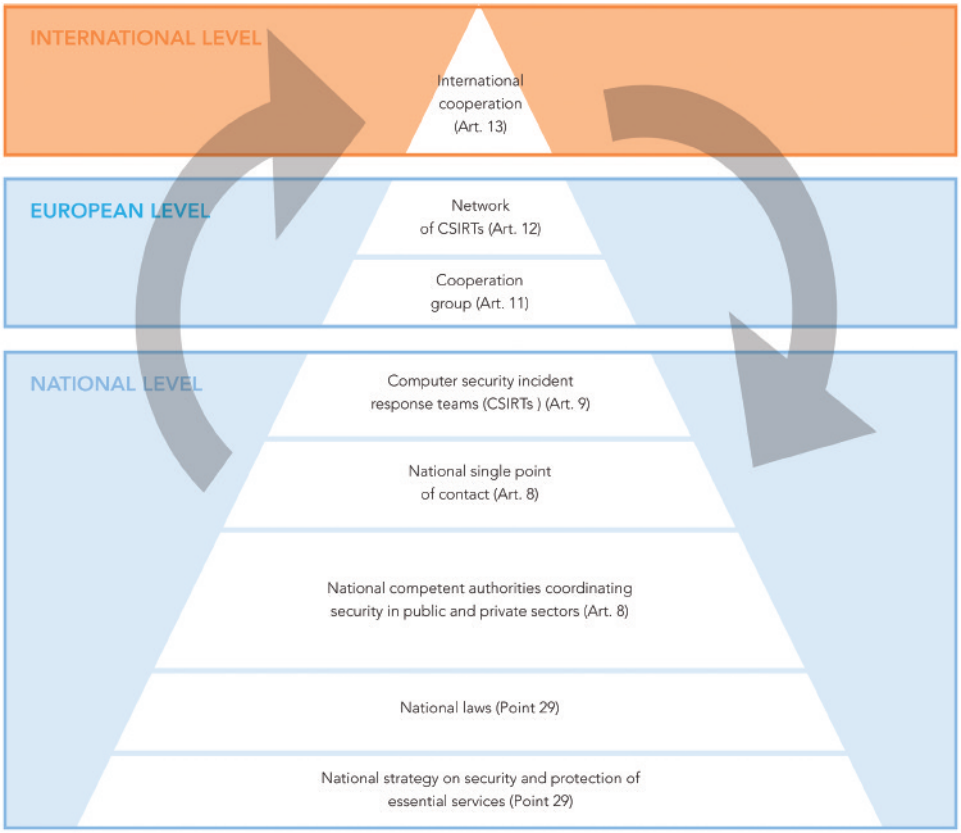

Figure 1: Organizational levels in the NIS directive

practices that need to be implemented to counter evolving cyberthreats. The network of CSIRTs must also facilitate swift communication of potential security incidents to improve the resilience of Member States and the agility of each actor in the implementation of new security practices.

An extra layer of cooperation can be added to this arrangement if the Union wishes to benefit from cooperation with third countries or international organizations in certain activities of the cooperation group.

What these layers of cooperation and compliance represent to Member States is an excellent opportunity for support in the application of best security practices and their efforts to achieve compliance with the NIS directive. However, they also presumably entail major (re)organization and (re)structuring of security processes at a national level, including the identification of trusted actors and agents who will be ambassadors of their countries at both European and international levels, pushing for state-of-the-art rules governing security.

2. Security challenges

In addition to the organizational requirements to be implemented, Member States must rely on competent authorities or their CSIRTs to ensure that they comply with specific security rules pertaining to their OESs and DSPs.

2.1 Operators of essential services

In Chapter IV, the NIS directive sets out the security measures to be adopted in order to ensure that OESs are protected and compliant. They are required, in particular, to ensure the definition and implementation of appropriate technical and organizational measures proportionate to the risks that they encounter. This involves awareness and knowledge of the dangers and the way they evolve as new technologies and user habits surface. Under the directive, OESs are encouraged to maintain awareness by conducting regular cybersecurity risk assessments. At a macro level, the organizational layout set out in the NIS facilitates the process of raising risk awareness (Figure 1). This diagram should serve as an example of a structure to improve the understanding and anticipation of more minor risks. Using the diagram as a guide, OESs must therefore define a security policy as well as a reliable organizational structure to guarantee that they comply with the security measures they wish to implement.

OESs must also take the necessary preventive measures in anticipation of potential security incidents. While this means equipping themselves with technical solutions tailored to their needs, it also creates a huge challenge - ensuring that all parties are well aware of the consequences of their actions so that the risk of negligence is kept low and stakeholders are informed of the best security practices and the role they play in securing OESs.

Lastly, and in the event they find themselves involved in a security incident, the NIS directive requires OESs to notify the competent authorities or the CSIRT as soon as possible, in general within 24 to

72 hours after discovery of the incident. OESs are therefore expected to provide all information necessary for assessing the impact of a security incident both on national and international levels. They must be able to indicate the magnitude and impact of the incident by informing the CSIRT of the number of users affected, as well as the duration and geographical spread of the incident. Such essential information would allow the CSIRT or competent authorities to pursue their incident management role by holding meetings with the CSIRT network or cooperation group, and by determining the potential cross-border impact of the incident (in which case, they will also need to notify affected stakeholders, such as certain Member States or the general public, for example).

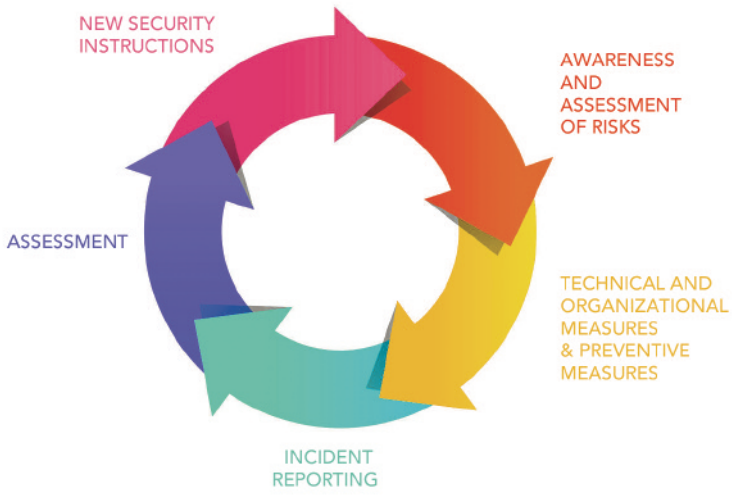

Figure 2: Cycle of security requirements for OESs in NIS

To ensure their compliance with the NIS directive, OESs in Member States must therefore be in a position to meet a cycle of security requirements (Figure 2), relying on their knowledge and the assessment of the risks that they face to:

- Show that a reliable and consistent security policy has been implemented, by providing supporting audit reports, for example.
- Provide all information necessary for managing security incidents handled by the CSIRT or competent authorities (affected users, duration and spread of the incident, etc).
- Patch potential vulnerabilities and oversee the update of their security policy.

2.2. Digital service providers

Along with the requirements of risk identification and the organizational and technical measures to be implemented, in line with the security imperatives set out for OESs, digital service providers must show proof (Article 16, paragraph 1) of the following:

- the security of systems and facilities
- incident handling

- business continuity management
- monitoring, auditing and testing of implemented security practices
- compliance with international standards.

Accordingly, they must make it possible to develop and comply with a security policy while raising stakeholders' awareness of healthy cybersecurity habits to adopt in order to improve prevention capabilities. The implementation of adapted technologies is an additional factor in guaranteeing effective incident management and the protection of their data and facilities. Compliance with the directive also consists of integrating an ecosystem of solutions to ensure the security of resources and services, preventing and detecting threats in order to facilitate incident management within the shortest time frames, commissioning the mandatory audits to fix vulnerabilities, and adhering to current and future international standards.

This ecosystem must empower digital service providers to contain the impact of incidents on their activity, guarantee resilience and gauge the spread of such incidents when they arise. Article 15 of the directive requires providers to be able to accurately evaluate the impact of incidents as soon as they obtain sufficient information allowing them to respond. Figure 3 shows the details that need to be indicated and places emphasis on DSPs' ability to assess the magnitude of the impact of potential incidents not only on their activity, but across the sector, both nationally and internationally. For example, if a security incident impacts the continuity of essential services that the provider offers, and which an OES uses, the OES must be notified and briefed on the incident.

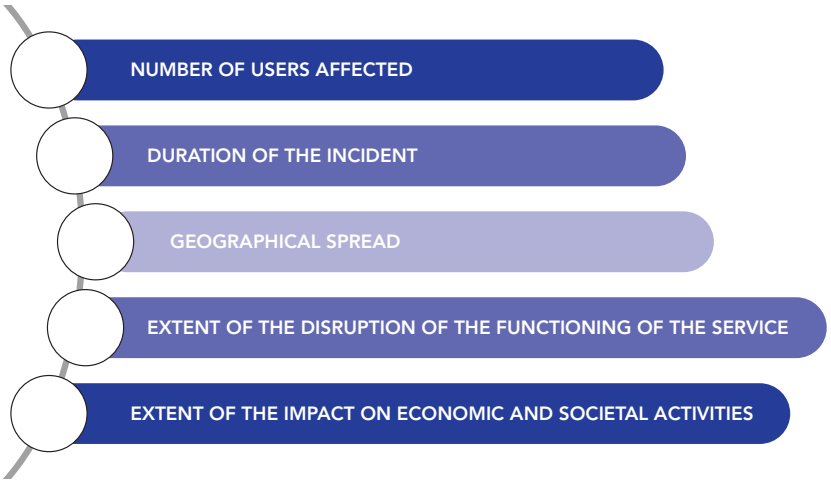

Figure 3: Security challenges for digital service providers

How privileged access management facilitates compliance with the NIS directive

Privileged Access Management (or PAM) is part of the solution to effectively meet the organizational

and technical challenges that the NIS directive has brought to light. It does so by shielding confidential and strategic data from cyberattacks by monitoring access to target systems and actions performed by privileged users who hold elevated administration privileges. Due to their privilege, such users can therefore pose a major threat to OESs and essential service providers as they may have one or several levels of access — granted either legitimately, negligently or by way of an attack allowing them to escalate their privileges — to sensitive digital data. As negligent or malicious privileged users could easily steal data, compromise its integrity or even erase it, causing serious security incidents in their wake, there is an urgent need to:

- Secure confidential data by monitoring access to the most critical resources.
- Gain full visibility over actions performed by privileged users by identifying who has access to what, when, how and why.

This aspect is a key step towards compliance with the NIS directive as it requires implementing and monitoring state-of-the-art security practices, particularly by obliging OESs and DSPs to define a stable and scalable security policy, and enforcing advanced prevention, detection, response and compliance measures.

Key challenges of the NIS directive	Added value of our privileged access management (PAM)
Defining a security policy (technical and organizational security measures)	PAM can help OESs and DSPs define a comprehensive security policy by factoring in the most critical elements of their security: stronger access privileges and monitoring of actions performed during sessions. Moreover, before the integration of a PAM solution, each user's permissions and authorizations, and their access to internal and external resources, must be mapped out. Creating a list of these elements makes it easier to identify the resources that need protection, and defining the technical and organizational measures to be implemented in order to strengthen the security of essential services.
Implementing preventive measures and strengthening security on information systems	A privileged access management solution can play a significant role in the implementation of preventive measures and other measures to strengthen security through its three key modules: - Password management, aligned with various security policies to guarantee the confidentiality and proper use of passwords and SSH keys, particularly by using a password safe, regularly and automatically changing passwords or managing service accounts. - Session management, for better risk prevention and control over access and activity (by setting up approval workflows for certain sessions) presented within a context and in real time. Automatic alerts in real time can also be implemented to automatically suspend or shut down a session opened with fraudulent credentials. - A web administration console that offers full, centralized visibility and control over every user's privileged access and roles on every target server and resource. Last but not least, the auto-discovery module in privileged accounts, often associated with PAM solutions, allows administrators to identify all privileged accounts, especially suspicious and unprotected user accounts, so that vulnerabilities can be fixed and threats can be prevented more easily.

Key challenges of the NIS directive	Added value of our privileged access management (PAM)
Reporting incidents within the shortest time frames	The session management module, at the core of every PAM solution, provides the necessary visibility to enable meeting the requirements described in the directive with regard to security incident reporting. Since user actions and command lines are recorded on video, the competent authorities and CSIRT can count on PAM to provide them with useful information relating to incident reporting within the given deadlines. For example, if a privileged user runs a bogus or suspicious command with an OES or service provider, PAM traceability tools can warn administrators of the incident in real time and immediately shut down the session. These tools can also show the exact duration of the session, the types of actions performed, as well as when and how they occurred. When PAM interfaces with a SIEM solution, it can also supply the solution's reports with user session logs and provide more exhaustive information that would be useful for incident reporting. Likewise, a PAM solution can show the number of users affected by an incident or its geographical spread and magnitude if the incident took place inside the network, and can therefore aid in the assessment of an incident's full impact.
Monitoring, auditing and testing of implemented security practices	The session management module on a PAM solution enables full traceability of sessions by recording command lines in real time, and also allows administrators to review all actions performed or revisit a specific event that occurred during the session. It provides the logs needed to build audit reports and monitor implemented security practices.
Compliance with international standards	Regardless of the industry targeted, privileged access management is a key element to compliance with many international laws and standards (NIST, HIPAA or PCI-DSS in the USA; GDPR in Europe; LPM or HDS in France, etc.). There is also a full chapter on the topic in the ISO 27001 standard (A.9) and indirect reference is made to it in many other sections of the ISO.

Conclusion

To protect essential services and increase the European Union's stability against cyberthreats, the NIS directive requires OESs and DSPs in each Member State to comply with baseline security practices. However, the standardization of practices that the directive aims to achieve creates a large set of organizational and technical challenges, both nationally and internationally. Privileged access management (PAM) helps OESs and DSPs in Member States to overcome these challenges by guiding them on how to define a security policy and by enhancing prevention, detection and incident reporting practices. Combining access control and session traceability with easy deployment and integration, PAM is a powerful link in the digital trust chain that plays a significant role in meeting the security challenges in line with the directive's state of the art.

WALLIX
TRACE, AUDIT & TRUST

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties: WALLIX Bastion. The WALLIX bastion accompanies more than 100 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 100,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

Twitter: @wallixcom
More information on: www.wallix.com

OFFICES & LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)
http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.co.uk
Email: ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG,UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND
http://www.wallix.de
Email: deinfo@wallix.co
Landsberger Str. 398
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)
http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781-569-6634

WALLIX RUSSIA & CIS
http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC
(Bizsecure Asia Pacific Pte Ltd)
Email: contact@bizsecure-apac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA
SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré 7ème Tranche Cocody
06 BP 2517 Abidjan 06
CÔTE D'IVOIRE
Tél. : (+225) 22 50 81 90

www.wallix.com