WHITE PAPER

Security management for IT administration in France and German speaking countries

Lead Analyst:

Wolfgang Schwab

teknowlogy Group, May 2020

Commissioned by

Systancia

the human face of the workplace

teknowlogy GROUP

CONTENTS

PREFACE

Systancia
the human face of the workplace

Bernard Debauche
Chief Product & Marketing

Making sure IT systems are secure and managing trusted access has become the top priority for every organization. Systancia has partnered with Teknowlogy to conduct a survey about the state and the maturity of the administration of IT systems with an emphasis on the market forces preventing organizations from remaining in a status quo. To help frame the scope and focus, the survey explores several key topics:

- **Compliance**. A common requirement for any organization regardless industry, regulatory compliance has recently reached a peak with GDPR, NIS and the assignment of “organization of vital importance” and “essential service operators” in different countries.
- **Digital**. The momentum to convert IT to a digital transformation within and between organizations has been immense. But with all the focus, networking and computing has yet to reach the level of capacity, enabling an all-pervasive IT (“anywhere any time any device”, “Internet of Things”) and the infinite reach of ecosystems.
- **Security**. At the core of IT is the ability to ensure a secure environment for participants to operate and interact. Challenges persist even with the most advanced cybersecurity measures and technology and not one day goes by without enterprises making the headline news because they have been victim of a cyberattack jeopardizing their business.
- **Disruption**. In the midst of our current environment, innovation arises, not always from where you expect, adding disruption to the already turbulent course of the business.

Let us embrace some of the challenges above and find better operational solutions from which we can meet increasingly demanding levels of requirements:

- Mandatory separation the admin from user computer access and admin network from the production network
- The need to let more and more service providers securely access IT assets from outside of the corporate network
- Expanding to deploy in cloud environments and the complex administration of new IT resources – while still maintaining traditional environments

- Protecting access via passwords is a growing problem. The need to know at any time who is behind the screen when they access critical IT assets
- Security adds a growing burden, sometimes at the expense of people's productivity or of the workplace experience

Enterprises must act to meet these new challenges and solution providers have to move to innovate to help bridge the gaps. It takes ingenuity to find new ways to address these new challenges and that has always been the mission of Systancia. That mission is to engage together with its partners to leverage desktop virtualization for more security, embed AI/ML for better fraud detection, provision hardware solutions to better secure access, and embrace techniques used by "bad actors" and hackers to strengthen security solutions for our customers. We embrace all means and apply for a good purpose: to provide the highest level of security … seamlessly.

Bernard Debauche

Chief Product & Marketing

b.debauche@systancia.com

INTRODUCTION

Security Management is challenging, especially for the group of IT administrators, as they need to be able to access most critical systems but in a safe and efficient way. Are concepts like privileged access control, virtual IT administrator workstations, or dedicated IT administrator networks already a reality in many user organizations or just a good concept waiting for implementation in the future?

This whitepaper is based on a survey of companies with more than 2.000 employees with activities in manufacturing, services or the public sector itself in France and the German speaking countries (Germany, Austria, and Switzerland).

The key questions which answers this whitepaper are:

- How do companies manage their compliance and monitoring needs regarding IT administration?
- What are their behaviors regarding Identity & Access Management for IT administrators?
- What resources do companies need for IT administration?
- To what extent are administration tasks automated?
- Do companies use outsourcing for IT administration?
- How do they manage security using external providers?

The answers make it easy for the interested reader to benchmark his or her own security management for IT administration against the peer group. This helps to identify investment needs and topics which are currently well established and do not require fundamental changes so far. Both kinds of information support an efficient resource planning in the IT security management space.

KEY FINDINGS

Voluntary compliance

Most companies are not required by law to comply with national authorities' recommendations but are willing to do so.

Dedicated workstations without truly isolated network

Companies mostly use dedicated workstations for IT administrator tasks but not always a separate administration network. Moreover data transfer is mainly managed through a router – not really the best solution!

High level of security in the authentication space

For administrators' authentication, all companies use usernames / passwords. 9 companies over 10 use at least a second method (token, fingerprint or iris scan).

Administrator access is secured through VPN, not ZTNA yet

IT administrators are often provided with a special dedicated VPN, which is important when working from home, however no respondent uses the highest level of access security which is ZTNA.

Virtual machines for administrators

Companies often provide dedicated virtual machines to their administrators to manage the security and stability of their workspaces, rarely a one-time virtual machine.

Automation and AI – a field of future investments

94% consider AI/ML techniques to detect malicious intent or fraud but only one third implement it. 1 in 2 companies has automated half of its administration routine tasks.

Outsourcing for IT administration

Half of the surveyed companies use outsourcing to manage their IT, using 2 to 4 external providers. Most of these companies provide their service providers with a special administration VPN network. To keep control on their security two thirds of companies grant their providers with a specific virtual machine.

COMPLIANCE AND MONITORING NEEDS

The need to comply with national authorities' recommendations regarding the security of the administration IT is first of all limited to companies in the critical infrastructure like telecoms, electricity & gas, water supply, banking, etc. and the public sector. When 97% of the surveyed companies express their need to comply with recommendations issued by the French ANSSI, the German BSI, the Swiss ISB or the Austrian Federal Ministry for Digitalization and Business Location, this is interesting as it means that many surveyed companies see a need to comply on a voluntary basis. This can be seen as very positive, because beyond the efforts made to secure their administration and IT operations, they really want to secure their IT as part of a global approach. In other words, **security is not only seen as an expensive necessity**, but as a necessary basis for a secure business process as such.

97%

of the surveyed companies feel a need to comply with national authorities' recommendations regarding the security of the administration IT.

Do you feel the need to comply with national authorities' recommendations regarding the security of the administration IT?

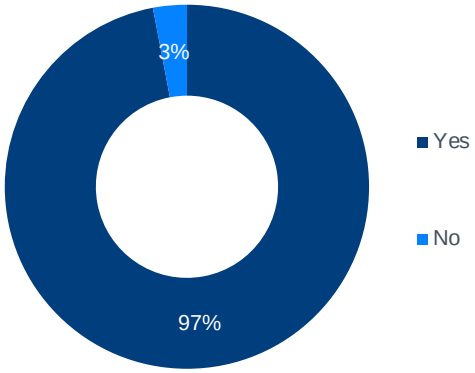


Fig. 1: Compliance with authorities' recommendations

IT ADMINISTRATORS WORKSTATIONS

While virtually all surveyed companies feel the need to comply with national authorities' recommendations despite not all of them are not obliged to do so, a quarter of these companies still do not provide their IT administrators with dedicated workstations for IT administrative tasks. To teknowlogy's knowledge, the market average is even much higher than a quarter, hence teknowlogy believes the surveyed companies are optimistic and show more aspiration than reality. Not providing a dedicated workstation for administrative tasks is a clear violation of the NIS directive, even if most of the surveyed companies do not fall into the class of critical infrastructure providers..

Do your IT administrators use a workstation dedicated only to their administrative tasks, as recommended by national authorities?

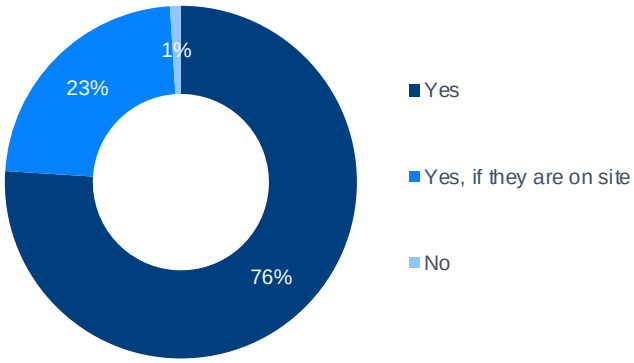


Fig. 2: Use of dedicated workstation

Only 1%

of the companies do not provide dedicated workstations for IT administration.

Almost a quarter of the surveyed companies provide their IT administrators with a dedicated workstation when they are on-site, which implies that while being at home, on vacation or traveling, they use a different kind of workstation for emergency actions. This is critical, given that in such most probably critical situation, the security of the workstation is not necessarily ensured.

Administrator workstations are a promising target for hackers as they need to have access to critical and sensitive systems. Therefore, administrator workstations need to be effectively secured. Beside standard tools like anti-virus / anti malware, personal firewalls, etc. the workspace as such has a big impact.

The highest level of security in this field shows a one-time virtual machine for each administrator, as for each new session a new and safe workspace environment is provided. Unfortunately, only 13% of the surveyed companies follow this concept.

At least one virtual machine dedicated to the administrator is provided by 29% of the surveyed companies, which is a good practice for occasional administrators.

58% of the surveyed companies at least use dedicated administrator devices. For internal administrators this might be an option, for extern administrators it's not.

How do you manage the stability of administrator workspaces: permanent administrators vs. occasional administrators?

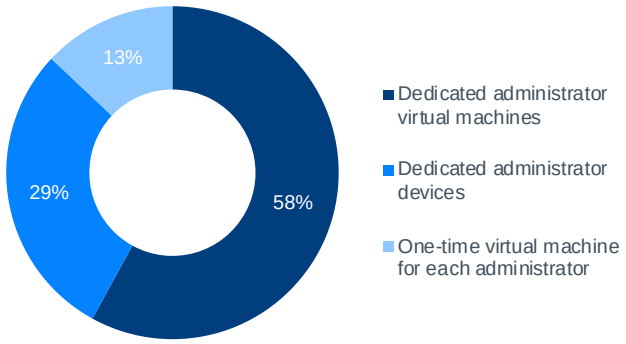


Fig. 3: Management of administrator workspace stability

Only 13%

of the companies provide a one-time dedicated virtual machine for each administrator.

SEPARATION OF ADMINISTRATIVE AND OFFICE NETWORK

It is best practice to separate the administrative network from the office network. 19% of the surveyed companies do not use a separate network for administration, which is surprising considering the high maturity of the sample. When looking more in detail, few companies follow exactly regulatory agencies' recommendations, as for example the French ANSSI advises that administration system should not be connected to internet.

Do you have an administration network separated from your office network?

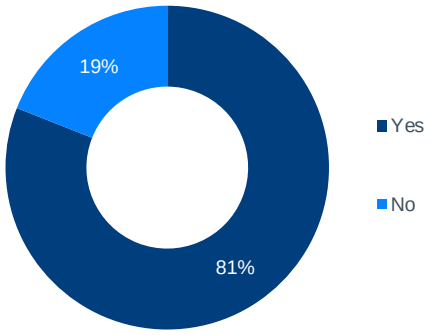


Fig. 4: Use of separate network

But if there is a separation between both networks, it is essential that such a separation is not undermined by a possible data exchange via layer 3 routing, which is done by 84% of the companies. Only 16% of companies transfer data through USB stick, which at least ensures a true separation. This is surprising, because, if a company takes the effort to have a network separation, the use of a secure data exchange system should be a given.

Another best practice is not to open any session from a network to another but to transfer data on an unidirectional mode, which requires a secured data transfer platform. **All in all, administration network should be not just separated but fully isolated**, which means that absolutely no data could be transferred to it except through a dedicated secured gateway.

How do you manage data transfer between your administration network and your office network?

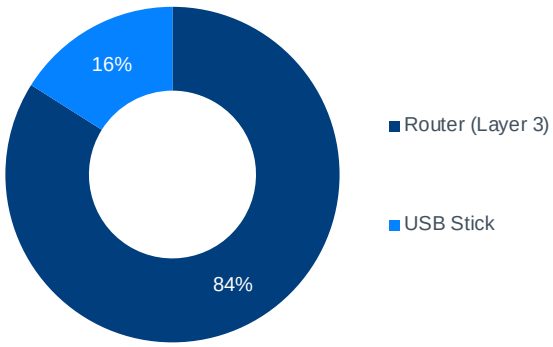


Fig. 5: Management of data transfer

Only 16%

of the companies truly isolate their administration network from the office network.

IDENTITY & ACCESS FOR IT ADMINISTRATORS

Authentication is extremely important not only for IT users but also for IT administrator roles. It is interesting, that all surveyed companies use username / password as a first authentication method. In addition, almost two thirds of the surveyed companies use a second authentication method, i.e. either token / smart card or fingerprint scans. Iris scans in only used by less than a quarter of the surveyed companies, most probably because there are no really secure mobile iris scanners widely available today.

The usage of a secondary authentication method is significantly higher in German speaking countries than in France, e.g. Token / smartcards usage in German speaking countries 76%, in France only 50%.

What are your preferred authentication methods?

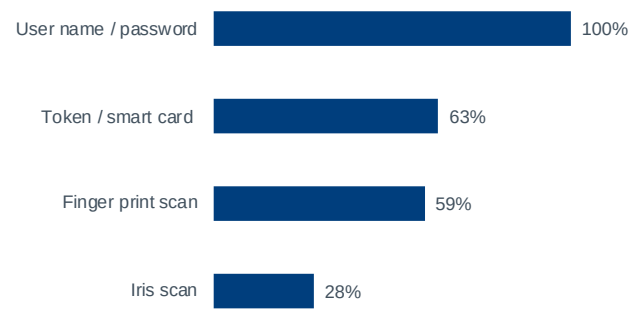


Fig. 6: Preferred authentication methods

VPN FOR IT ADMINISTRATORS

IT administration is partly subject to outsourcing (see section “Outsourcing of IT administration tasks”) and even internal IT administrators need access from outside the companies premise in case of on-call duty or in case of an emergency. **To secure such external access to critical systems, special security means should be in place and be used**. VPN solutions are the means of choice.

Positive is the fact that all surveyed companies use VPN solutions for external access, but almost one third are using general VPN solutions, i.e. for administration and standard user purposes. This can be problematic from a security point of view and is not exactly following the recommendations of ANSSI, BSI, etc.

However, if all companies use VPN and mostly use dedicated VPN for administration, **no company of the sample uses more advanced solutions such as the Zero trust network access (ZTNA)**, which is more granular.

82%

of companies in German speaking countries use special admin VPN solutions, while only 60% of the French companies do so.

How do you manage the security of your administrators' access when they are on the move?

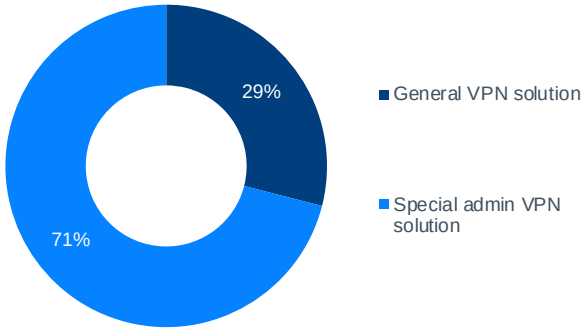
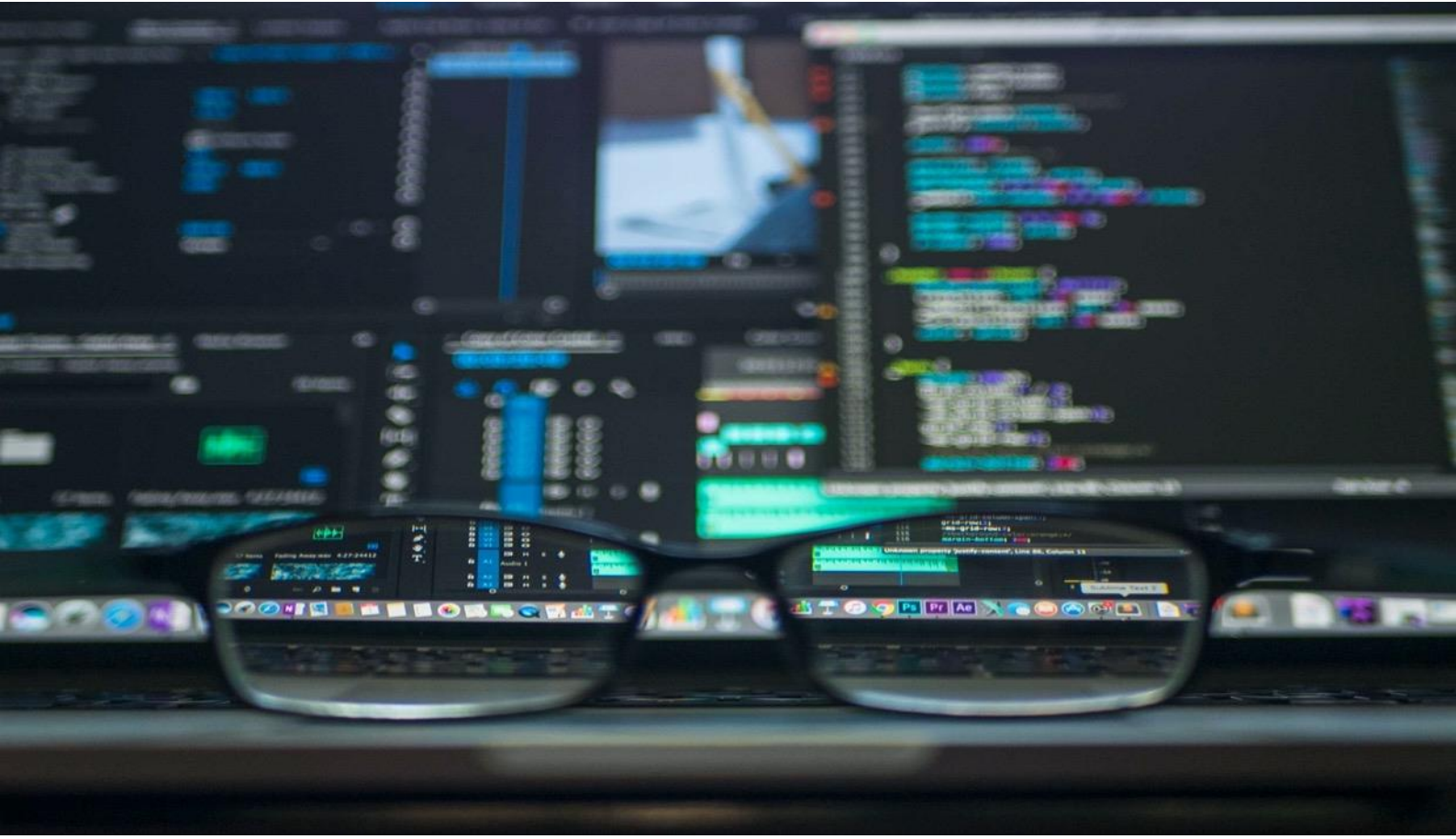


Fig. 7: Management of administrators access security



IT RESOURCES AND AUTOMATION

With a rising adoption of cloud computing the need to administrate cloud infrastructures and SaaS solutions is also increasing. In addition, administration tools are increasingly provided as cloud solutions. Taking this into consideration, the share of internal IT resources is high. This can be put into perspective by the fact that public sector organizations are part of the survey, as their cloud use is still very low.

Are your IT resources for administration internal (datacenter or private cloud) or external (XaaS)?

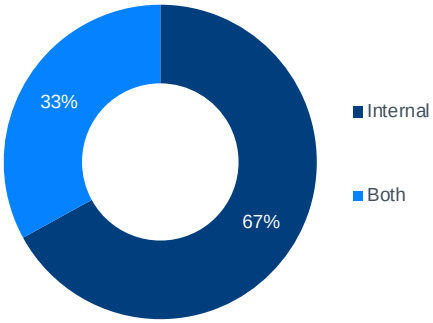


Fig. 8: IT resources for administration

EFFORT TO ADMINISTRATE NEW RESSOURCES

IT infrastructures are usually pretty dynamic, i.e. resources come and go over time. This means that **administrators must deploy or remove new infrastructures and applications on a regular basis**. The amount of time used for such tasks is a good indicator for the automation and the tooling around such tasks.

For over two thirds of the surveyed companies it takes two to three person-days to deploy a new resource, i.e. a new application or new infrastructure, in average. For ¼ of the surveyed companies it takes more than 3 person-days. Indeed, a major share of the loads and costs of a new resource consists in injecting and rotating passwords for it. Hence, accelerating this process enables companies to reduce significantly their time to market.

For standard infrastructure elements there is room for improvement in respect to faster deployment, for applications it depends heavily on the application, the needed customization and the number of users associated with it.

What are the loads and costs of administering a new resource (application, infrastructure)?

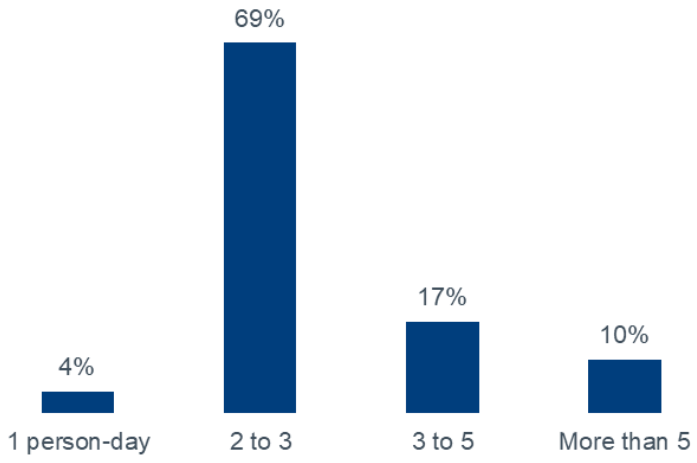


Fig. 9: Loads and costs of administering a new resource

For 1/4

it takes more than 3 person-days to administer a new resource.

AGILITY OF THE IT

The agility in IT is constantly growing as the agility in the business is growing. **Shorter time to market needs faster reactions in the whole organization and therefore in IT**. This leads to higher frequency of changes in IT and to a higher workload for IT administrators.

For almost half of the surveyed companies, this is not the case as they have changes in their information systems only once a month. 17% even less. Only 5% of the companies report changes on a daily basis.

Since administering a new resource requires several day person-days and occurs often once a week, agility of Privileged Access Management is essential.

How often is the information system changed, decommissioned or a resource added?

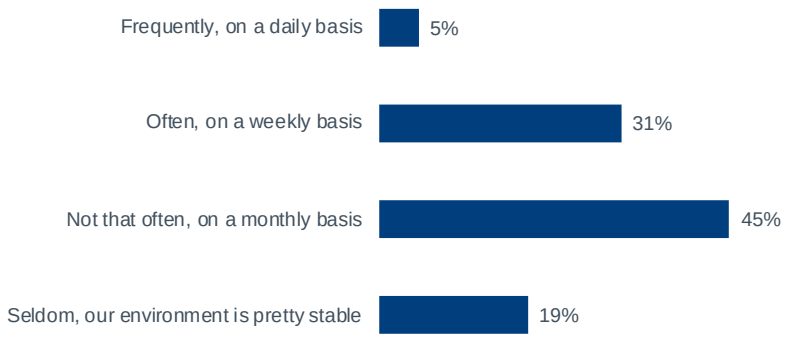


Fig. 10: Frequency of information system changes

24%

of surveyed companies in German speaking countries report a stable environment, while only 14% of French companies do so.

TOOLING FOR ADMINISTRATION AND SECURITY

Do you have a mapping of all your IT resources and a repository for authorizing access to all resources?

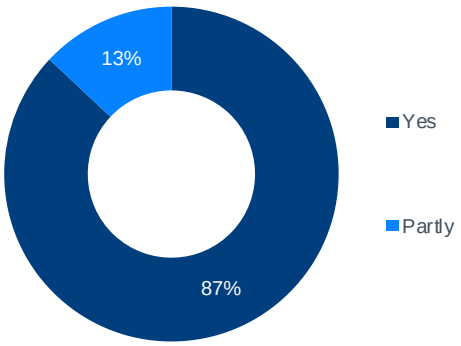


Fig. 11: Mapping of IT resources and access repository

Having an overview of IT resources and a repository for authorizing access to all resources is basically a very good idea, at least at a certain level of size of the infrastructure and a certain number of applications. All surveyed companies have at least some of this information at hand and a surprisingly high number of companies, i.e. 87%, have a complete mapping of IT resources and authorization to access all resources.

One of the top hype topics in IT currently is artificial intelligence, mostly in the meaning of machine learning. After a longer training cycle, **such systems can support IT or security departments in recognizing malicious intents of users but also of IT administrators, as well as fraud**.

Are you willing to invest in AI/ML techniques to detect malicious intent or fraud?

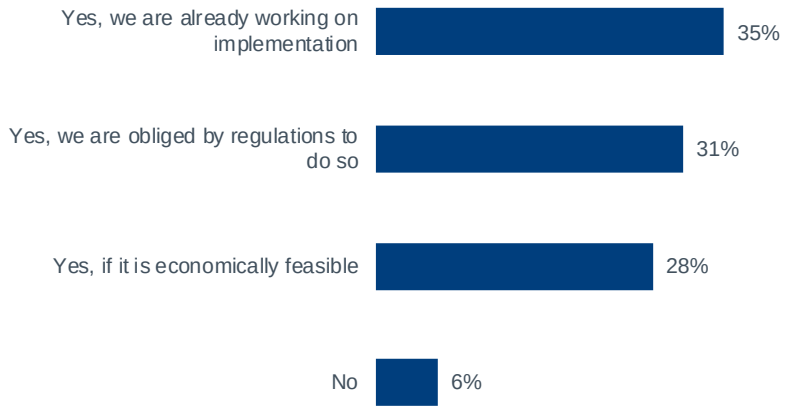


Fig. 12: Use of AI/ML techniques for security

2/3

of the surveyed companies are not implementing AI/ML for fraud detection.

The survey results show very clearly that the **marketing around AI/ML and the claims of the security providers to include AI/ML in their tools have worked perfectly**. 31% of the surveyed companies think they are obliged by regulations to invest in such tools. In fact, no one is currently obliged to do so. 35% report that they currently work on an implementation. This is hard to believe, as most tools are limited in the use of AI or ML. 28% will invest in such solutions, if it is economically feasible, an approach which is reasonable. Only 6% are currently not willing to invest in such new solutions, probably waiting for further maturity of the solutions.

Do you have a Security Operations Center (SOC) in place?

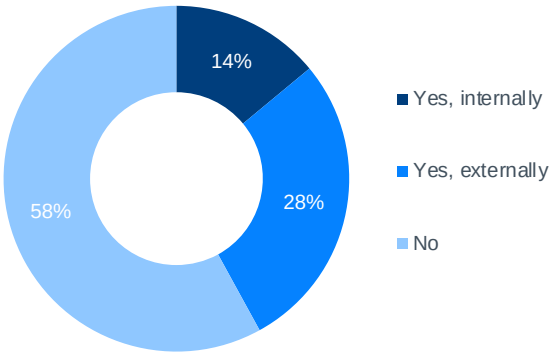


Fig. 13: Use of SOC

62%

of the surveyed companies in France have no SOC in place vs. 54% of companies in German speaking countries.

The identification of cyber security threats is a very specific task, needing special tools and even more important special knowledge. Setting up such a task force internally is only feasible for very large companies, while the use of an external service should be the norm for any company of a reasonable size.

Nevertheless, 58% of the surveyed companies do not own or use a SOC at all. This is all the more worrying since in this study only companies with more than 2.000 employees were surveyed, which at the same time seem to be willing to follow the guidelines of ANSSI, BSI, etc. A lot of companies are building their SOC and it is important that Privileged Access Management solutions sends all relevant data for fraud detection to the SOC.

Equally important for a safe IT administration is the automation of routine tasks. This is important due to 2 factors:

- Routine tasks take a huge amount of time. Time which could be used more productively by IT administrators.
- Routine tasks are boring and therefore error prone.

How much are your system administration routine tasks automated?

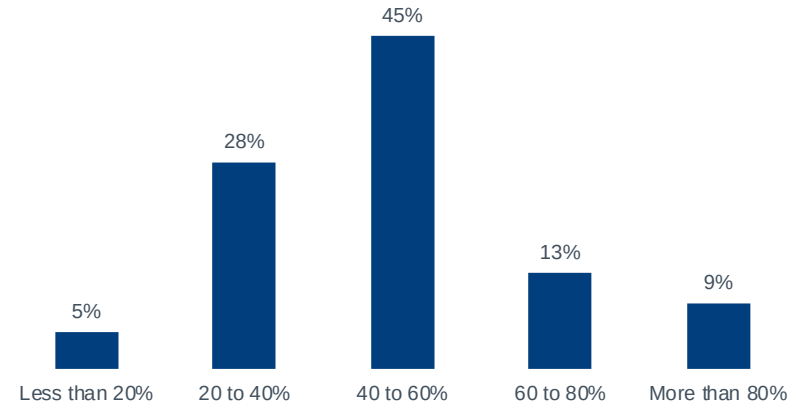


Fig. 14: Automation of administration routine tasks

Best practice is therefore to automate as many routine tasks as possible. The surveyed companies are mostly on a good way to do so. Only 5% of the companies have still automated less than 20% of their routine tasks, while a little over two thirds of the companies already have more than 40% of their routine tasks automated. Given the size of the surveyed companies and **the high number of repetitions of such routine tasks, this is a first step, but rate of automation of routine tasks can still be considered low**.

OUTSOURCING OF IT ADMINISTRATION TASKS

Outsourcing of IT administration tasks is pretty common throughout the industries. This includes classical IT administration tasks as well as security administration, not only SOC services.

In this survey 55% of the surveyed companies said they use outsourcing or managed services to manage their IT. **In order to make sure such services are performed in a safe way, some measures are necessary**, such as ensuring . the security of the service providers' workstations.

Do you use outsourcing or managed services to manage your IT?

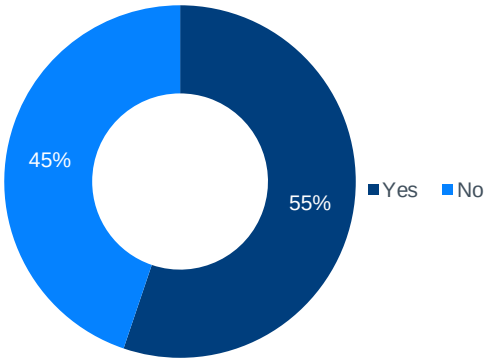


Fig. 15: Use of outsourcing to manage IT

More than half of the surveyed companies outsource administration tasks to 2 external providers or more.

EXTERNAL SERVICE PROVIDERS

For outsourcing and managed services there is no direct need for a dual vendor strategy to avoid vendor lock-ins, but over the last decade **the trend goes definitively to smaller service contracts and more specific tenders**. Therefore, it is clear that only a minority of surveyed companies use only one service provider.

How many external service providers are involved in your IT?

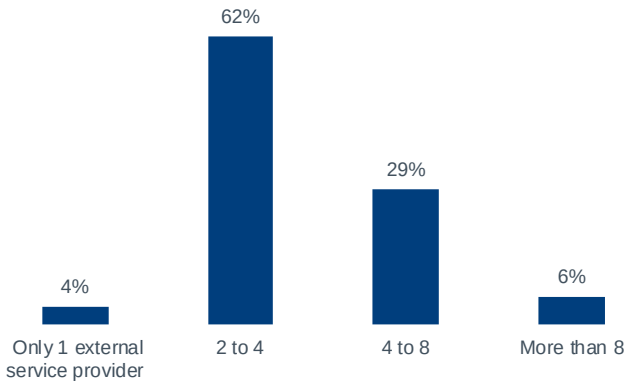


Fig. 16: Number of external providers

36%

of the surveyed companies in German speaking countries have 4 to 8 service providers involved, while only 21% of French companies use this many providers.

The vast majority uses 2 to 4 service providers, one third even more. **Obviously, with the number of used service providers the need for security measures and the risks due to complexity rise as well**. Provider management on all layers is increasing and requires specific in-house knowledge.

One measure could be a special admin VPN solution for controlling the access of service providers to the companies' network. But only 71% of the companies are using this option. The others use their standard VPN solution.

How do you control the access of your service providers?

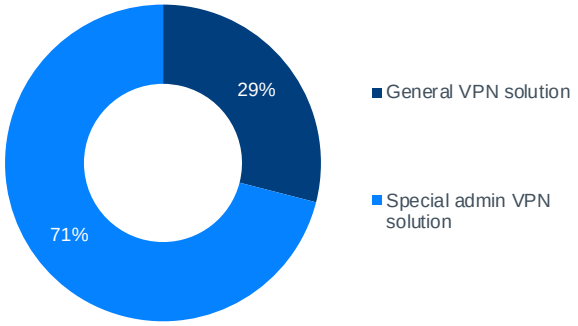


Fig. 17: Control of providers' access

88%

of the surveyed companies in German speaking countries have set up special admin VPN solutions, while only 71% of French companies have done so.

SECURITY OF SERVICE PROVIDERS WORKSTATIONS

The use of outsourcing or managed services requires trust in the selected service provider. On the other side, control is better than trust. This is why 64% of the surveyed companies provide a specific virtual machine to their service providers to perform their services.

Do you have control over the security of providers' workstations?

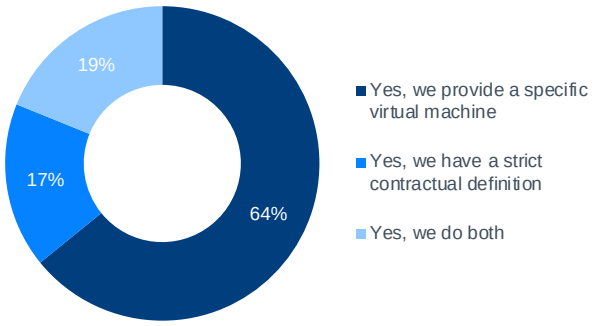


Fig. 18: Control of providers' workstations security

17% are confident that a strict contractual definition is sufficient to ensure the security of the providers workstation and 19% have a specific virtual machine and a strict contract in place.

76%

of the surveyed companies in German speaking countries provide a specific virtual machine, while only 54% of French companies do so.

CONCLUSIONS

The companies surveyed for this whitepaper can be considered to be security aware in many aspects of securing IT administration. However, looking in more detail they still have a way to go to reach the highest security level.

Even if most of them are not affected by the NIS direction of the EU, which is only mandatory for providers of critical infrastructure and the public sector, the vast majority wish to comply with the recommendations of their national authorities'. **As far as a concrete implementation is concerned, there is a certain gap between desire and reality**, e.g. 81% of the surveyed companies have a dedicated administration network in place but only 16% truly isolate it, allowing no data transfer from their office network except through a USB key or a dedicated secured platform.

When it comes to identity & access management for IT administrators, most of the surveyed companies use special admin VPN solution. That is all well and good, but only a few of these companies use one-time virtual machines for each administrator to manage the stability of administrator workspaces. There is a clear gap in perception. Moreover, **no company of the sample uses more advanced solutions** such as the Zero trust network access (ZTNA), which is more granular.

IT administration is also getting increasingly complex as 1 surveyed company over 3 uses IT resources in the Cloud and needs to change its IT systems every week, which consumes time and money. In addition, the vast majority of the surveyed companies are using outsourcing and managed services for IT administration, dealing with 2 to 4 service providers, sometimes even more.

Hence, teknowlogy believes that companies will need to be increasingly agile and secured at the same time regarding their IT administration. And this means going to the upper level of best practices for IT administration security.

METHODOLOGY

The results of this study are based on 100 telephone interviews with senior IT leaders in organizations of more than 2,000 employees based in France and DACH region (Germany, Austria, Switzerland).

All participants are involved in investment decisions related to cybersecurity of their organization, including CIOs, CISOs, Infrastructure managers/directors, etc.

The field research was undertaken during the first quarter of 2020, and included participants from the major industry sectors: manufacturing (including automotive, aerospace & defense, pharmaceuticals, food & beverage, etc.); services (including banking, telecoms, utilities, retail, etc.); and public sector (including central government, defense, health & social services, etc.). A breakdown of the study sample can be found below.

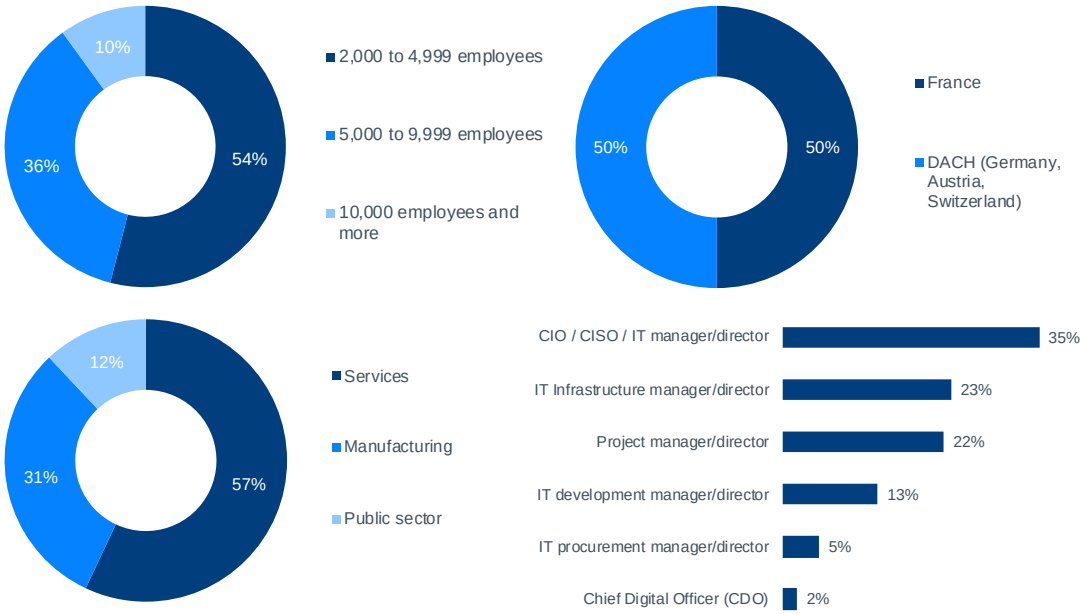


Fig. 19: Survey sample

Appendix

DISCLAIMER, USAGE RIGHTS, INDEPENDENCE AND DATA PROTECTION

The creation and distribution of this study was supported by Systancia.

For more information, please visit http://www.sitsi.com.

Disclaimer

Usage rights

Independence and data protection

This study was produced by Pierre Audoin Consultants (PAC) - a teknowlogy Group company. The ordering party had no influence over the analysis of the data and the production of the study.

The participants in the study were assured that the information they provided would be treated confidentially. No statement enables conclusions to be drawn about individual companies, and no individual survey data was passed to the ordering party or other third parties. All participants in the study were selected at random. There is no connection between the production of the study and any commercial relationship between the respondents and the ordering party of this study.

LIST OF FIGURES

ABOUT SYSTANCIA

Systancia is a European provider of secure access solutions for a better Workplace Experience - betterWE.

Our vision is that behind every workplace, there is a person who deserves to be empowered and trusted. We want to give a human face to the work environment, by placing technology where it should be: at the service of the people. That is why we invest the ingenuity of all our teams in meeting the human challenge of the digital workplace.

Our mission is to provide workforces with the most efficient and secure access to all their applications. To that end, we deliver an Access Platform which secures the users in their digital workplace, and the only Access Platform which spans the end-to-end chain of trust, with: access management (IAM) services to manage people's identities and entitlements; virtual access (VDI) services to provide end users with a remote experience to their applications and desktops; privileged access (PAM) services to assure compliance in securing administration access to the IT systems; and remote access (ZTNA) services to enable people outside of the corporate network to securely access enterprise applications and resources, whether on-premise or in the cloud.

We provide these secure access solutions alone or combined, as software products or as cloud services or in hybrid deployment models, leaving you the freedom to deploy them at your speed and at your convenience. We are the only independent software vendor in the market to blend virtualization, cybersecurity and AI/ML technologies to build unique solutions to increasingly complex business challenges.

That is why hundreds of mid to large public and private organizations trust Systancia's secure access solutions, in a variety of projects such as teleworking, user experience, access surveillance, workforce on-boarding, migration to cloud, for business agility and enablement, legal and regulatory compliance, modernization and innovation.

Systancia
the human face of the workplace

Contact:

Systancia

3 rue Paul-Henri Spaak
68390 Sausheim, France

+33 (0)389 335 820
www.systancia.com

ABOUT TEKNOWLOGY GROUP

teknowlogy Group is the leading independent European research and consulting firm in the fields of digital transformation, software, and IT services. It brings together the expertise of two research and advisory firms, each with a strong history and local presence in the fragmented markets of Europe: CXP and PAC (Pierre Audoin Consultants).

We are a content-based company with strong consulting DNA. We are the preferred partner for European user companies to define IT strategy, govern teams and projects, and de-risk technology choices that drive successful business transformation.

We have a second-to-none understanding of market trends and IT users' expectations. We help software vendors and IT services companies better shape, execute and promote their own strategy in coherence with market needs and in anticipation of tomorrow's expectations.

Capitalizing on more than 40 years of experience, we operate with a network of 140 experts.

For more information, please visit www.teknowlogy.com and follow us on Twitter or LinkedIn.

Contact:

teknowlogy Group

1 boulevard des Bouvets
92000 Nanterre, France

+33 (0)153 050 550
www.sitsi.com