The State of Cloud Security in Europe | 2022

The Shift Towards Zero Trust

30 YEARS ANNIVERSARY
techconsult
TECHNOLOGY MARKET ANALYSTS

Table of contents

Foreword 2
How companies protect their cloud environments 3
The biggest concerns in relation to the cloud 4
Failure to secure the cloud means running the risk of becoming the victim of cyber criminals 5
The benefits of Zero Trust 7
What prevents companies from adopting Zero Trust? 8
Conclusion 9
Further Information 10

Foreword

Cloud environments are an essential part of every company today. The increase in remote working in particular makes it essential to migrate key workloads to the cloud and give users the option of accessing key business processes from anywhere.

But on the other hand, cyber criminals also know that companies are migrating key business data to the cloud. These cloud environments are outside the company's protective perimeter and constitute a significant risk if inadequately secured. Phishing in particular allows cyber criminals to obtain real login information for such cloud environments and wreak havoc in them.

So how can companies protect their cloud environments against cyber crime? What concerns do you have in relation to the cloud and have you already been the victim of a successful attack? Can a modern security approach like Zero Trust help to improve cloud security?

To answer these questions, we conducted a survey among 400 decision makers who were asked about the maturity level of their cloud security, the frequency of attacks on cloud environments and the opportunities and problems with a Zero Trust policy. The participants in this study came from companies with 500 or more employees, distributed across all industries in Germany, UK, France, Scandinavia, Italy, Spain and the Benelux states.

Copyright

Disclaimer

The reproduction of common names, utility marks, designations of the goods, etc. in this work, even without special labelling, do not justify the assumption that such names are to be considered free in the sense of the trademark and brand name legislation and may therefore be used by anyone. References made in this study to any specific commercial product, process or service, through brand names, brands, manufacturer designation, etc., do not in any way mean a preference by techconsult GmbH.

Other Information

This study uses gender-neutral language wherever possible. All terms, examples and information therein applies generally to all genders in the sense of equal treatment.

How companies protect their cloud environments

More and more workloads are being migrated to the cloud. However, cloud security must also be ensured here. Many companies do not, for the time being, consider ensuring protection of the cloud to be their responsibility. But this is a misconception, because the principle of shared responsibility applies for cloud environments. Cloud providers are responsible for the security of the cloud, i.e. for all of the infrastructure on which cloud services are provided. Conversely, companies are responsible for security in the cloud, meaning for data management or for permissions for access to the cloud, for example.

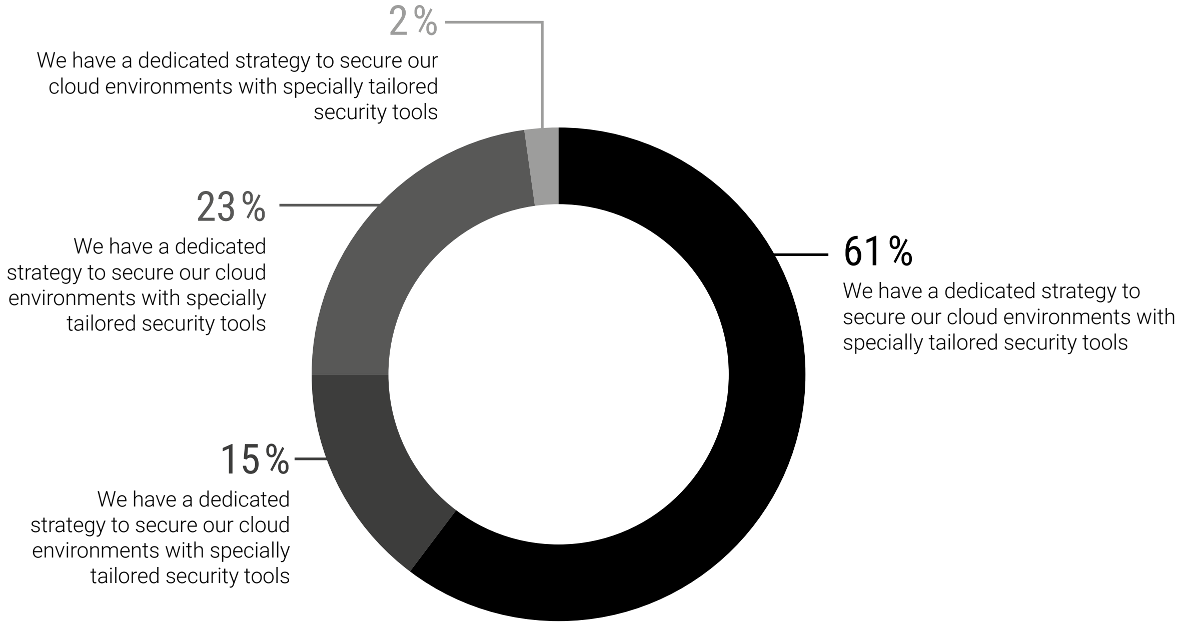
6 out of 10 companies currently say that they protect their cloud environments with specially designed security measures. Banks and insurance companies are the clear leaders when it comes to cloud security. Almost three quarters of financial service providers have already secured their cloud environments with a dedicated strategy and the remaining quarter are currently in the planning phase. The extremely strict rules and standards which financial service providers must comply with also come into play here. All other companies can take the financial service providers' security measures as a good example even without the corresponding legal regulations and take similar measures.

15 percent of companies do not currently have any measures implemented, but are planning to at least introduce dedicated safeguards for cloud environments in the future. Exactly what these plans will look like and what their timescales will be is not yet known. Waiting for too long may make their cloud environments an attractive target for cyber criminals for a similarly long period.

23 percent of companies have safeguards for cloud environments within the context of the general IT security strategy. Here, we can assume that there is at least a certain basic degree of protection. However, without addressing the individual requirements of cloud security with explicit solutions, the security of cloud environments is not guaranteed.

How mature would you say your cloud security strategy is?

Base: 400 companies



The biggest concerns in relation to the cloud

Migrating workloads to the cloud isn't all up-side. Companies also feel exposed to various security risks. The survey participants were asked to select their three biggest concerns.

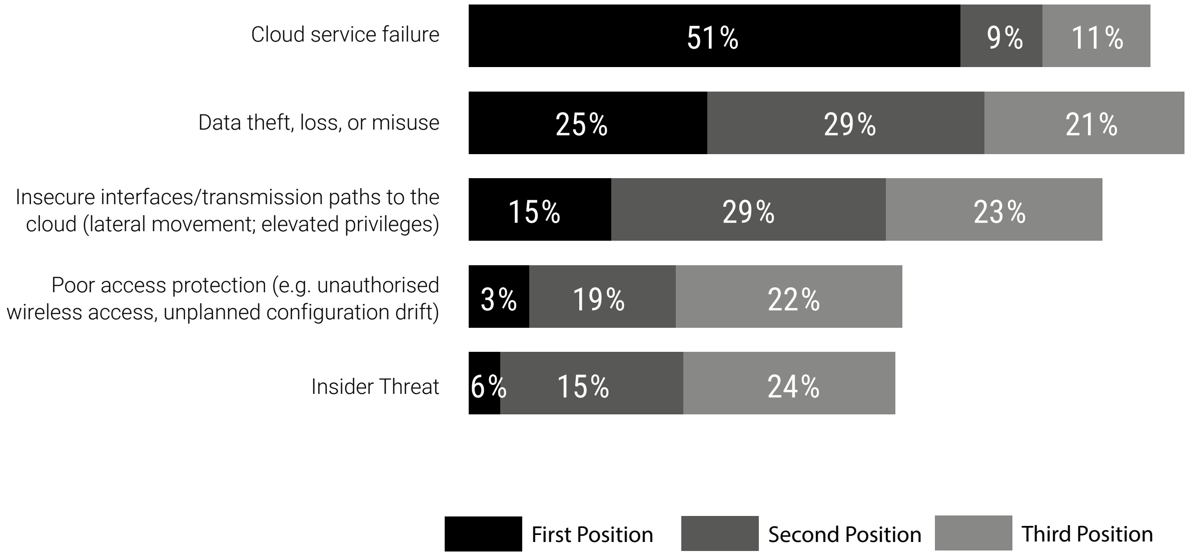
A general cloud service outage was most commonly chosen as first among the security risks. Little wonder, because a cloud service outage also means that a whole company could come to a standstill, depending on how many workloads take place in the cloud. The countries in which the survey was conducted also agree here: a cloud service outage was chosen as the biggest risk in all countries.

In second place were worries about data theft, loss and misuse. In total, three quarters of all respondents put risks relating to data in one of the top three spots. Data is a particularly attractive target for cyber criminals, especially in companies for which data processing is a key part of their business activity – and critical business data reaching the wrong hands can be fatal for a company.

Insecure interfaces or transmission paths to the cloud round out the top 3 biggest security problems in relation to cloud environments. Increasing numbers of companies are making use of cloud solutions in order to handle their business processes, particularly owing to the increase in remote working. Cyber criminals can obtain a user's real login details by means of social engineering or man-in-the-middle attacks. Such a compromised user can rapidly become a serious problem. Once attackers have gained access to the network, they can also acquire additional privileges and spread evermore widely and deeply through the network. Often they can even do this without ever being discovered, because their movements in the network looks like normal network traffic to traditional security tools.

What do you think are the top security risks related to cloud environments?

Base: 400 companies



Failure to secure the cloud means running the risk of becoming the victim of cyber criminals

The frequency of attacks on cloud infrastructure is proof that cyber criminals really are focusing their attacks on cloud environments and that protective measures are necessary. One third of the companies surveyed said that at least one attack on cloud environments was successful. 12 percent of companies had even suffered multiple successful attacks. 42 percent of companies were able to detect attacks but managed to stop them.

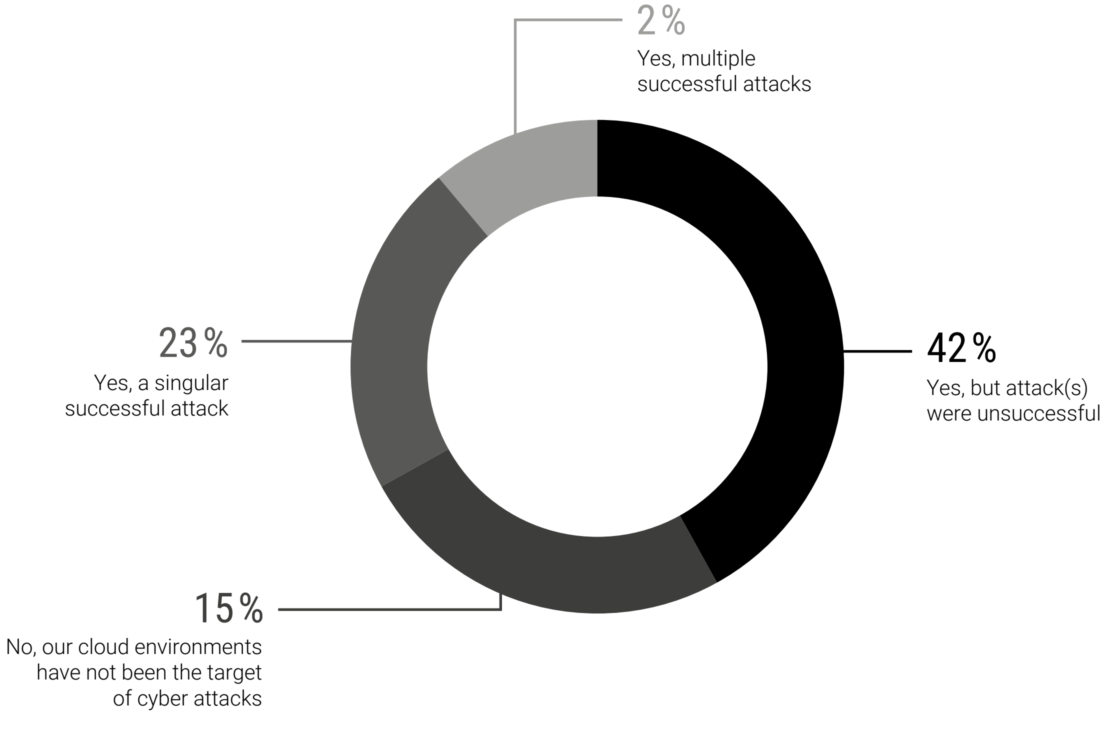
The regional differences with regard to successful cyber attacks in the companies surveyed are noteworthy. While almost a quarter of respondents in Germany, Italy and Spain were victims of cyber crime at least once, other regions are beset by cyber attacks significantly more frequently. 38 percent of companies surveyed in the UK and 40 percent in France were victims of cyber attacks on cloud environments. And the picture is even worse for companies in the Nordic region and Benelux. Here, half of the companies had actually been victims of a successful cyber attack at least once.

Additionally, larger companies were victims of successful attacks less frequently (20 percent) than companies with fewer than 5000 employees (37 percent). This would suggest that security measures in large companies are significantly more developed than is the case in smaller companies.

Also interesting to note: companies not yet actively protecting their cloud environments were victims of successful cyber attacks significantly more often, when compared to companies that protect their cloud environments either with the help of a specific cloud security strategy or in a rudimentary manner as part of the IT security strategy. 59 percent of companies with no specific cloud security measures conceded that they had been the victim of a successful cyber attack at least once. Among companies with dedicated cloud security, this was true for only 31 percent. It is therefore clear: companies that secure their cloud environments with specific measures have a lower risk than those that give no consideration to cloud security.

Have your cloud environments been the target of a cyber attack?

Base: 400 companies



A Zero Trust policy can help companies improve their IT security and protect the cloud environments in the process. In this security concept, no device, user or service inside or outside the network is trusted. Comprehensive measures for authentication of all users and services are used for this and all network traffic must be verified. This helps companies reduce the risk to their networks in relation to external and internal threats. By contrast, traditional security concepts focus on external threats and consider internal users and services to be generally trustworthy.

So far, a little more than a quarter of companies are using a Zero Trust model. Once again, institutions in the financial and insurance sector are leading the way here. More than 40 percent of financial service providers already use a Zero Trust policy. Another 40 percent are already in the implementation phase. Companies in the retail sector (20 percent) and public administrations (21 percent) are clearly lagging behind. Zero Trust is still in its infancy here, but it will grow in the future. This can be seen by the fact that almost 46 percent of retail companies and 33 percent of public administrations are already in the process of implementing a Zero Trust security model. There are only a few regional differences. The degree of application is between 21 percent and 28 percent across all regions.

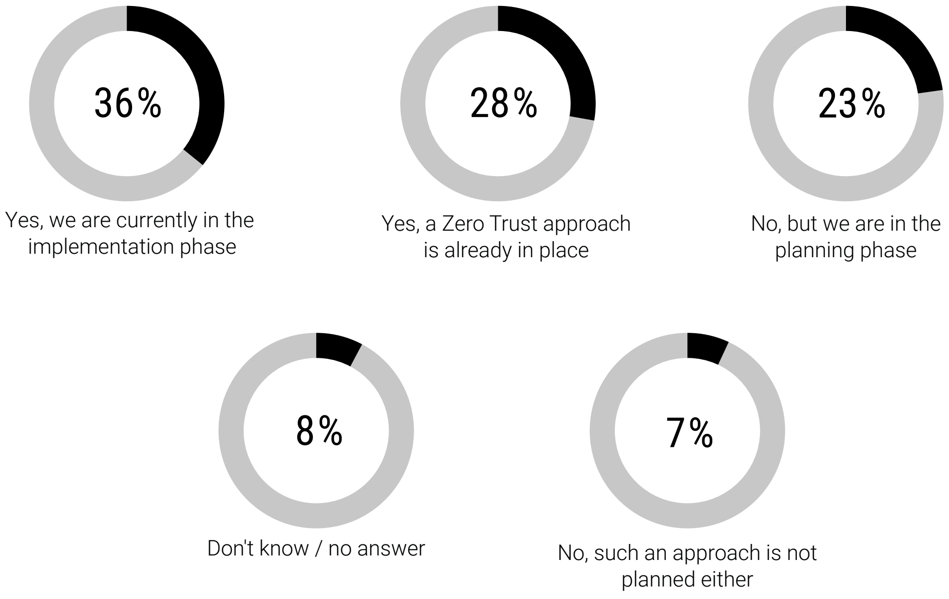
More than a third of companies are currently in the process of implementing a Zero Trust approach, and a further fifth are at least in the planning stage without having started concrete implementation steps. This clearly indicates that Zero Trust is considered to be the security concept of the future in the minds of most companies.

Companies that also have a dedicated strategy for protecting cloud environments are ahead of the pack with Zero Trust security. 38 percent of these companies are already using a Zero Trust security model, a further 38 percent are currently in the process of introducing Zero Trust and 15 percent are currently in the planning phase. This means that, provided that they all follow through, the number of companies using Zero Trust will be more than 90 percent in the near future.

In comparison, just a little less than every eighth company without specific cloud protection is using a Zero Trust security approach. However, this number is expected to increase dramatically in the future. Because concrete implementation of a Zero Trust policy or general planning for use are proceeding apace, even at companies which still don’t use Zero Trust at all. According to their own statements, more than three quarters of these companies will build on Zero Trust in the future.

Have you already implemented a Zero Trust approach in your company or are you planning to use a corresponding model in the future?

Base: 400 companies



The benefits of Zero Trust

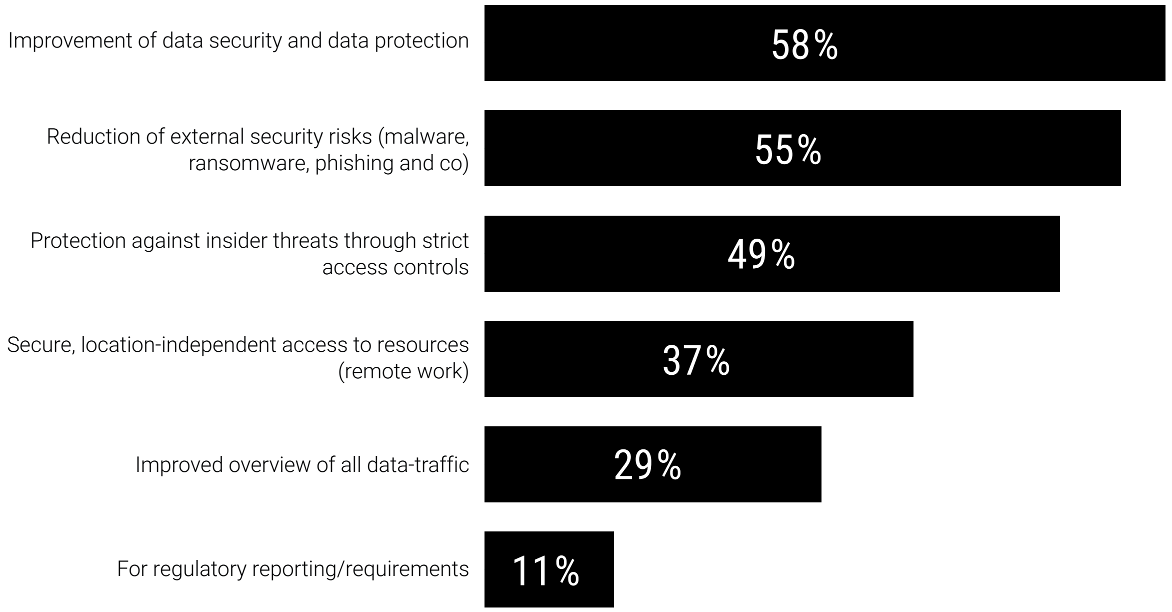
Data protection and the reduction of external and internal risks – these are the three main benefits that companies see for themselves within the context of Zero Trust. Traditional security concepts are not fully effective, particularly in light of the increasing use of cloud computing.

Six out of ten companies consider the improvement of data security and data protection to be a primary reason for the use of Zero Trust. In the Zero Trust model, for example, all data traffic is analysed and any unnoticed infiltrations – which would remain unnoticed using traditional approaches – can therefore be detected. In traditional approaches, devices would be classified as trustworthy and could do as much damage as they wanted within company networks. With the Zero Trust model this would be prevented from the outset, thus minimising the risk of sensitive company data falling into the wrong hands.

This is followed by the reduction of external security risks such as malware, ransomware or even phishing at 55 percent. The increasing number of successful phishing attacks is one reason why traditional security measures are losing the fight against modern cyber threats. Because cyber criminals can bypass email security checks, for example, with real login data from employees and can then spread through the network. The Zero Trust approach, on the other hand, assumes that a sender which has previously been authenticated can be compromised at any time and verifies it again each time. “Unnatural” activities in the network would therefore be detected immediately and the user would be quarantined accordingly. Protection against internal threats through strict access controls (49 percent) completes the top 3.

What are the main reasons for using a Zero Trust model?

Base: 343 companies



What prevents companies from adopting Zero Trust?

Companies which have so far remained sceptical about a Zero Trust approach primarily consider the high investment costs to be problematic. Almost a third of the companies in question gave this as one of the main reasons for not introducing a Zero Trust security model. But Zero Trust is not a single product to be installed, but rather a strategic approach in which the entire organisation must be analysed with the appropriate security measures taken. Investments in Zero Trust are therefore strategic in nature but absolutely pay off, because security incidents and the loss of sensitive data cost significantly more – both monetarily and in reputational impact.

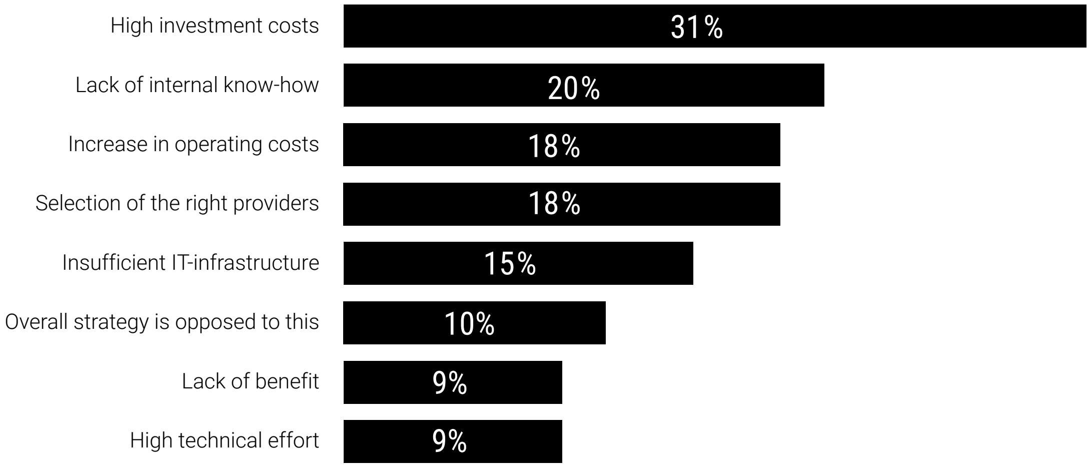
This is followed by a lack of know-how within the company (20 percent) for the implementation of Zero Trust. Since Zero Trust is not a traditional security concept in which a stand-alone solution is simply purchased, but rather a multidimensional framework of various technologies, it is necessary to integrate Zero Trust throughout the company and to transform existing processes and structures.

A Zero Trust approach cannot succeed without the necessary know-how and the inclusion of all relevant parameters such as security policies, identity management, classification of data or without breaking down silos. Here, providers specialising in Zero Trust can support companies with company-wide implementation.

However, 18 percent of companies say that they have problems choosing the right provider. Companies should therefore consider in advance exactly what the aim of Zero Trust should be and how providers can help with achieving this goal. Questions concerning user-friendliness, deployment models, industry-specific knowledge or the technology partners should be taken into account in the considerations.

What are the main reasons for not implementing a Zero Trust approach?

Base: 55 companies, multiple answers possible



Conclusion

While companies benefit from the many advantages of cloud solutions on the one hand, cyber criminals see great potential for infiltrating company networks through insecure cloud environments and their access channels. Almost a third of the companies in the countries surveyed in this study had actually been the victim of at least one targeted attack on their cloud environments. In order to effectively protect themselves against such attacks, companies therefore need to secure cloud environments with a dedicated cloud security strategy and implement modern approaches within the company.

Zero Trust is one such approach. In this approach, every device and every user is fundamentally viewed as a potential source of danger and must be authenticated again each time. Companies implementing this approach, which goes far beyond traditional security solutions, minimise possible points of attack for cyber criminals and reduce the total potential impact of any successful attacks.

However, the introduction of Zero Trust is not a simple undertaking. It is a holistic, company-wide strategy which analyses and transforms all the processes and structures rather than just being a stand-alone security tool. Successful implementation of Zero Trust therefore means tackling the transformation process together with an experienced partner. This is the only way to guarantee maximum protection.

Further Information

Imprint

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

Mail:	**info@techconsult.de**
Phone:	+49 561 8109 0
Fax:	+49 561 8109 101
Web:	**www.techconsult.de**

Contact

Raphael Napieralski
Analyst

E-Mail:	**raphael.napieralski@techconsult.de**
Tel.:	+49 561 8109 0

About techconsult

As a research and analyst company, techconsult has been the partner for providers and consumers of digital technologies and services for 30 years. techconsult GmbH is led by executive partner and founder Peter Burghardt at the Kassel location with a branch office in Munich.