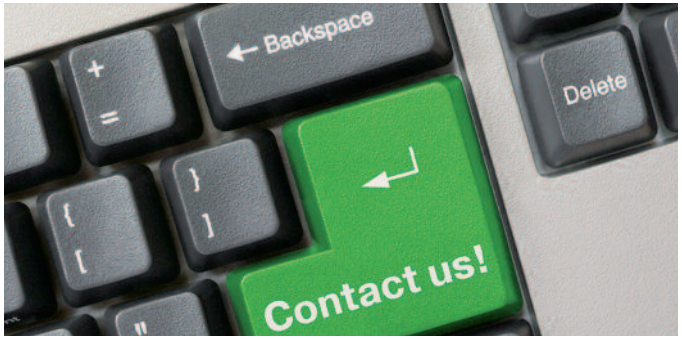
Recommendations

- Pay attention to potential providers' general terms and conditions.
- Choose a certified provider. *
- Check if the certified scope of the service meets your requirements.
- Make sure that the provider has implemented ISMS appropriately.
- Require the provider to ensure highest possible quality and security standards
- Clarify availability and failure compensation with respect to your business model.
- Become aware of the liability regimes in cases of loss of information and privacy breaches
- Ensure that an appropriate place of jurisdiction is stipulated in all contracts.
- In case of doubt, change the provider.

Do not hesitate to contact us and make an appointment for confidential awareness talks.



* for further information please see www.bsi.bund.de

Your points of contact in economic security

initiative wirtschaftsschutz

Protecting values in a concerted effort

For additional information and your local contacts' communication data, please visit the website

www.wirtschaftsschutz.info

Imprint

Publisher: BfV (German federal domestic intelligence service) for the community of the domestic intelligence services of the Federation and the federal states

Pictures: © vchalup - Fotolia.com
© LfV Niedersachsen
© Designed by pinnacleanimates / Freepik
© ccvision

DOI: July 2018

Domestic intelligence service

Federal Republic of Germany
Federal States

Economic Security

What small and medium-sized enterprises should know and pay attention to

Cloud Computing

Cloud Computing

means providing IT infrastructure service, such as storage space, performance and application software, via the Internet.

This opens up the opportunity especially for small and medium-sized enterprises to take advantage of highly available IT infrastructure in a cost-effective and flexible way, using minimal resources. The spectrum ranges from pure off-site data storage to the mapping of complete business processes.

If sensitive business data is involved, particular attention has to be paid to the fundamental objectives of information security:

Confidentiality

Integrity

Availability

Risk factors

- insufficient encryption of vitally important data
- lack of the provider's reliability
- inefficient security concept
- lack of transparency and control mechanisms on the part of the provider
- poorly performing Internet connection
- complex contracts
- ignorance or non-observance of rules on the protection of data
- country-specific statutory provisions valid where the cloud provider is based

Recommended action

Your decision on the nature and scope of using the cloud should be based on a company-specific structure and security analysis. The outcome is decisive for choosing the cloud model and the suitable provider.

- Define information and processes that are not permitted to be outsourced due to their vulnerability.
- Encrypt sensitive data before outsourcing.
- Regulate the scope of access rights and the level of logging in a binding manner.
- Operate an Information Security Management System (ISMS) and optimise it on a continual basis.
- Adapt your contingency plans accordingly.
- Insure the residual risk.

There is no cloud just other people's computers.

Be aware of the fact that your data in the cloud is stored beyond your direct reach.