

Establish trust through security



Security & data protection

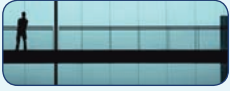
Physical security:



Hetzner datacenters are spaciouly distributed and not recognisable as such from the outside. The street addresses are only disclosed on request.



Entrances and server rooms are **monitored by camera**.



Access is permitted only to authorised contractual partners with scheduled appointments and who bring proof of identity. Authorised representatives require written confirmation from the contracting party.



Access to the server rooms is only possible when accompanied by an employee.



Colocation rack clients have their own key (optional) for the separate colocation rooms as well as an access code for the secure rack.



The **uninterrupted power supply** is guaranteed by a 15 minute battery capacity and emergency diesel-generated power.



Climate control is effected by a raised floor system.



A modern **fire detection system** is directly connected to the fire alarm centre of the local fire department. If the system experiences a failure the security company is automatically informed.

Network security:



Multiple redundant connections to the largest German internet exchange point, DE-CIX, ensure smooth data transfer.



All existing upstreams and peerings are integrated in the backbone via state-of-the-art routers from Juniper Networks in order to boost the network's capacity.

System security:



Security updates are continuously performed on managed servers.

There is a central back-up server to save backed-up data.

The RAID-1 hard disk system reduces the likelihood of data loss.

Other optional features such as the Flexi-Pack guarantee the highest availability.

Qualified experts are available through our "24/7 Standby Service" to give individual support.

Data protection:

Personal information is saved and used exclusively for the preparation of invoices and for contact purposes.

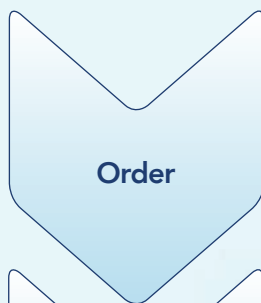
All employees are contractually obliged not to disclose internal business information to third parties.

Information is solely relayed to respective registrars for the registration of domains and for the preparation of invoices to service partners concerned (e.g. banks).

In all cases it is necessary to forward information according to the regulations of the Federal Data Protection Act (BDSG). The amount of information is kept to a minimum.

Security & data protection

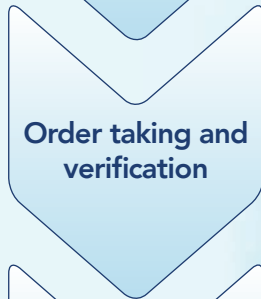
Safer order process and service orders for products e.g. root server:



Order



Clients order their desired Root Server online at www.hetzner.de through a secure connection.



Order taking and verification



At the Hetzner head office the order is verified and recorded through a validity check.



Installation and start-up



Notification is sent to the computer centre to install and start up the server. If needs be, individual configuration and setting up of the requested server is done through subsequent checks server tests.



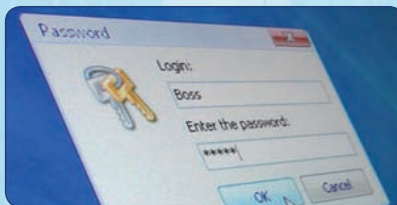
Preparation



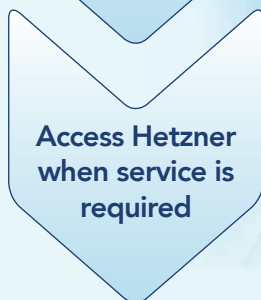
Information is sent to the client via the email address provided on ordering. Clients receive the necessary passwords for server access and the administrations interface, with the request to change these promptly.



Password change



From this point Hetzner Online no longer has password access and can therefore carry out no maintenance on the server without the client's acceptance.



Access Hetzner when service is required



If requiring service the client has various options to request support:

- A request via the password-protected administrations interface
- A request by fax signed by the contract holder
- A telephonic request by means of password authentication