2020 CYBER ATTACK

In May 2020, computing centres across Europe were the victim of a cyber attack on HPC systems. UDE was also affected by this attack. As a result, the magnitUDE supercomputer had to be taken offline.

Following extensive inspection of the systems and enhancements to the security measures, magnitUDE has resumed – initially restricted – regular operation in September 2020.

Such attacks on computer systems are not uncommon. On the contrary, they are carried out in an increasingly professional manner and on a regular basis. The successful attacks on the universities in Maastricht, Gießen and Bochum in late 2019/early 2020 and the Düsseldorf University Hospital in September 2020 are just a few among many other examples.

This leaflet provides information on important protective measures.

INFORMATION ON IT SECURITY

uni-due.de/zim/en/it-security

www.uni-due.de/ciso

ZIM
Centre for Information and Media Services

HOTLINE

Mo-Fr 8-20.00 o'clock
Phone (DU): 0203-379-2221
Phone (E): 0201-183-4444

E-Mail: hotline.zim@uni-due.de

E-POINT

Mo-Fr 9-19.00 o'clock
Phone (DU): 0203-379-4242
Phone (E): 0201-183-4444

ADDRESS

Campus Duisburg
Forsthausweg 2

47048 Duisburg

Campus Essen
Schützenbahn 70

45127 Essen

uni-due.de/zim/en

UNIVERSITÄT
DUISBURG
ESSEN

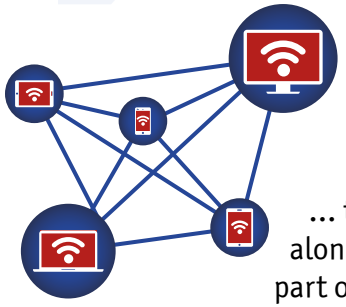
Open-Minded

ZIM
Centre for Information and Media Services

IT security

Information and protective measures in the context of the 2020 cyber attack

Did you know...



... that devices brought along by other users are also part of the campus network, e.g. if they use eduroam? Many of those users are not members of our university.

... that these devices may be infected with malware and pose a threat to your computer?

... that your computer can usually be accessed from the entire campus network and thus become a target of attacks?

What you can do...

... with regard to administration

If you do not administer your system yourself, please ask your system administrator to implement the measures below.

- Always keep your operating system and your applications up to date.
- Restrict the server services on your computer to the targets that are actually required using the local firewall.
- Entirely disable server services that you do not need. Full client systems do not normally require server services that are accessible from the network.

Auf Linux-Systemen
Serverdienste wie SSH, NFS, FTP oder Webserver

Auf Windows-Systemen
Dienste wie Remotedesktopverbindung Datei- und Druckerfreigabe

These services are frequently preinstalled or activated

... when using Secure Shell

- Set a strong password (at least 12 characters) or, preferably, select public key authentication.
- Protect your private key by means of a passphrase and only save the key on your own computer.