# Cyberangriff 2020

Im Mai 2020 wurden europaweit Rechenzentren Opfer eines Cyberangriffs auf HPC-Systeme. Auch die UDE war betroffen, so dass der Hochleistungsrechner magnitUDE in Folge offline genommen werden musste.

Nach umfangreicher Prüfung der Systeme und Verbesserung der Sicherheitsmaßnahmen wurde ein zunächst eingeschränkter Regelbetrieb im September 2020 wieder aufgenommen.

Solche Angriffe auf Computersysteme sind keine Seltenheit, sondern werden immer professioneller und routinemäßiger ausgeführt. Nur einige weitere Beispiele sind die erfolgreichen Angriffe auf die Universitäten Maastricht, Gießen und Bochum um den Jahreswechsel 2019/2020 und das Universitätsklinikum Düsseldorf im September 2020.

Einige wichtige Maßnahmen zur Abwehr zeigt Ihnen der vorliegende Flyer.

## INFORMATIONEN ZUR IT-SICHERHEIT

www.uni-due.de/zim/it-sicherheit

www.uni-due.de/ciso

ZIM
Zentrum für Informations- und Mediendienste

## HOTLINE

Mo-Fr 8-20 Uhr
Telefon (DU): 0203-379-2221
Telefon (E): 0201-183-4444

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

## E-POINT

Mo-Fr 9-19 Uhr
Telefon (DU): 0203-379-4242

Telefon (E): 0201-183-4444

## ANSCHRIFT

Campus Duisburg
Forsthausweg 2

47048 Duisburg

Campus Essen
Schützenbahn 70

45127 Essen

www.uni-due.de/zim



UNIVERSITÄT DUISBURG ESSEN

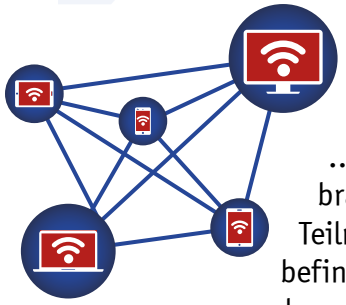
*Offen* im Denken

ZIM
Zentrum für Informations- und Mediendienste

# *IT-Sicherheit*

Informationen und Schutzmaßnahmen zum Cyberangriff 2020

# Wussten Sie schon...



... dass sich auch mitgebrachte Endgeräte anderer Teilnehmer im Campusnetz befinden, z.B. solche, die eduroam nutzen?
Viele davon sind keine Angehörigen der Universität.

... dass diese Endgeräte mit Schadsoftware infiziert sein können und eine Gefahr für Ihren Computer darstellen?

... dass Ihr Computer ist in der Regel aus dem gesamten Campusnetz erreichbar ist und so zum Ziel von Angriffen werden kann?

# Das können Sie tun...

## ... bei der Administration

Falls Sie ihr System nicht selbst administrieren, bitten Sie ihren Systemadministrator, die nachfolgenden Maßnahmen zu ergreifen.

- Halten Sie Betriebssystem und Anwendungen immer aktuell.
- Schränken Sie Serverdienste auf Ihrem Computer mit der lokalen Firewall auf die unbedingt notwendigen Ziele ein.
- Schalten Sie nicht benötigte Serverdienste ganz ab. Auf reinen Client-Systemen müssen normalerweise keine Serverdienste aus dem Netzwerk erreichbar sein.

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

**Auf Windows-Systemen**
Dienste wie Remotedesktopverbindung Datei- und Druckerfreigabe

**HÄUFIG VORINSTALLIERT ODER AKTIV**

## ... bei der Verwendung von Secure Shell

- Verwenden Sie ein starkes Passwort (mindestens 12 Zeichen) oder bevorzugt Authentifizierung per Public Key.
- Schützen Sie den privaten Schlüssel per Passphrase und speichern Sie diesen nur auf Ihrem eigenen Computer.