QGroup präsentiert »Best of Hacks«: Highlights Mai 2020

Frankfurt am Main, 6. Juli 2020 – Im Mai kam es zu gezielten Cyberangriffen auf europäische Hochleistungsrechenzentren. Etliche Supercomputer mussten vom Netz genommen werden. Darüber hinaus rückten auch der deutsche Medizin- und Gesundheitskonzern Fresenius, die britische Fluggesellschaft EasyJet sowie der US-amerikanische Domainregistrar und Webhoster GoDaddy ins Visier von Hackern.

Rechenzentren in ganz Europa wurden Ziele von Cyberangriffen. In Deutschland waren unter anderem das Hochleistungsrechenzentrum Stuttgart, das Leibniz-Rechenzentrum, das Forschungszentrum Jülich, das Karlsruher Institut für Technologie, das Hochleistungsrechenzentrum Archer sowie das Rechenzentrum Freiburg betroffen. Die unbekannten Angreifer hatten sich den Zugang mittels kompromittierter Account-Daten verschafft.
Die Betreiber nahmen daraufhin mehrere Supercomputer vom Netz, darunter HPE Apollo 9000 "Hawk", SuperMUC-NG, JURECA, JUDAC, JUWELS Module 1, bwUniCluster 2.0 und ForHLR II, bwForCluster NEMO. Das Incident Response Team fand auf einigen Servern Mining-Software. Zur Verschleierung nutzten die Angreifer das TOR-Netzwerk und das Kernel-Rootkit "Diamorphine". In der Folge waren in den betroffenen Hochleistungsrechenzentren die Supercomputer für die Wissenschaft nicht nutzbar. Dies hatte auch Auswirkungen auf den Kampf gegen das Coronavirus.

Ein Cyberangriff beim deutschen Medizintechnik- und Gesundheitsunternehmen Fresenius hat bei dessen Tochtergesellschaft Fresenius Kabi Produktionseinschränkungen in einer Medikamentenfabrik in Norwegen verursacht. Mehrere Rechner waren mit einer Ransomware infiziert. Der DAX-Konzern stellt nicht nur verschiedene Medizintechnikprodukte her, sondern betreibt auch Krankenhäuser.

Unbekannten war es möglich auf die Daten von 9 Millionen Kundendaten der britischen Fluggesellschaft EasyJet zuzugreifen. Neben den E-Mail-Adressen betraf dies auch die Reisedaten. In 2.208 Fällen waren sogar die Kreditkartendaten betroffen.

Mit Hilfe einer manipulierten SSH-Datei haben sich unbekannte Angreifer Zugriff auf 28.000 Hosting-Accounts des US-amerikanischen Domainregistrars und Webhoster GoDaddy verschafft. In welchem Umfang ein Datenmissbrauch stattfand, ist derzeit unbekannt.

(2.185 Zeichen)

Medienkontakt:

QGroup GmbH
Berner Straße 119
60437 Frankfurt am Main
www.qgroup.de/presse

Lars Bothe
Tel.: +49 69 17 53 63-014
E-Mail: l.bothe@qgroup.de