Schließung des Microsoft Fernzugriffdiensts (Remotedesktop-Ports) von außerhalb der Universität zum Schutz der IT-Netzinfrastruktur der Goethe-Universität und ihrer Daten

Hintergrund

Der Microsoft Fernzugriffdienst „Remotedesktop-Verbindung (RDP)“ wird von manchen Nutzern genutzt, um beispielweise von einem Computer zu Hause aus auf ihren Bürocomputer zuzugreifen und sich einzuloggen, als würden sie an ihrem Computer am Arbeitsplatz sitzen.

Zum Schutze der Netzinfrastruktur der Goethe-Universität sowie ihrer Daten muss der externe Windows-Fernzugriff (RDP) von außerhalb der Universität auf Windowssysteme innerhalb der Universität zusätzlich gesichert erfolgen.

Anlass

In letzter Zeit diente der Microsoft-Dienst „RDP“ als Einfallstor für Hacker und Cyberkriminelle. Angriffe auf diesen Dienst sind heutzutage üblich und werden systematisch durchgeführt. Damit wird unter anderem versucht, schwache Passwörter zu erraten und Zugriff auf die Systeme zu erlangen. Weiterhin geben Windowssysteme in älteren Konfigurationen Nutzernamen und momentan angemeldete Nutzer preis.

Vor kurzem wurde eine kritische Sicherheitslücke in der Fernwartungsfunktion des Microsoft-Diensts „RDP“ entdeckt. Angreifer können diese Lücke ausnutzen und ohne Authentifizierung Schadcode ausführen. Klappt alles, kann sich dann die Malware weiterverbreiten und ganze Netzwerke infizieren. Betroffen sind alle Windowsbetriebssysteme bis einschließlich Windows 7 und Server 2008 R2. Wir empfehlen daher DRINGEND auf allen Systemen die gestern veröffentlichten Patches (Windows-Updates) umgehend zu installieren.

Zurzeit sind ältere Windowssysteme der Goethe-Universität, die weltweit aus dem Internet über Microsoft-Fernzugriff (RDP) erreichbar sind, von diesen Angriffsversuchen betroffen und gefährdet.

Maßnahmen

Aufgrund dieser akuten Situation hat das Sicherheitsmanagement-Team (SMT) der Goethe-Universität beschlossen, den RDP-Port 3389 am 15.05.2019 um 16:00 Uhr eingehend auf Netzebene am Gateway der Universität zu schließen. Eine Nutzung von außerhalb der Universität ist danach weiterhin durch Nutzung der gesicherten Netzinfrastruktur „Virtuelles Privates Netzwerk (VPN)“ des Hochschulrechenzentrums (HRZ) möglich. Windows-Fernzugriffe (RDP) von innerhalb der Universität auf Windowssysteme außerhalb der Universität bleiben wie bisher möglich.

Das HRZ-VPN bewirkt, dass der von Ihnen benutzte Rechner sich wie Rechnersysteme innerhalb der Universität verhält und externe Angreifer nicht mehr direkt zugreifen können. Die Nutzung des Windows-Fernzugriffs (RDP) ist trotzdem genauso wie bisher möglich. Die zusätzliche Nutzung des HRZ-VPN bewirkt jedoch, dass der Microsoft Fernzugriff-Dienst (RDP) nicht mehr angreifbar ist.

Auch wenn eine solche Maßnahme für eine kleine Gruppe Nutzer einen Bequemlichkeitsverlust bedeutet, ist es zur Absicherung unserer Systeme dringend notwendig diese Maßnahme zu ergreifen, da die Goethe-Universität verpflichtet ist, die Vertraulichkeit, Integrität und Verfügbarkeit unserer Daten und Systeme zu gewährleisten. Der dadurch unterbundene Angriffsvektor hat auch in

Sicherheitsvorfällen in der letzten Zeit eine Rolle gespielt, die in Zukunft durch diese Maßnahme verhindert werden können.

Eine Anleitung zur Nutzung des HRZ-VPN ist unter dem folgenden Link zu finden: www.rz.uni-frankfurt.de/vpn

Die Mitarbeiterinnen und Mitarbeiter des HRZ beraten und unterstützen Sie gerne bei der Installation der VPN-Software.